



Opportunities and Challenges of DLT (Blockchain) in Mobility and Logistics





FRAUNHOFER INSTITUTE FOR APPLIED INFORMATION TECHNOLOGY FIT

OPPORTUNITIES AND CHALLENGES OF DLT (BLOCKCHAIN) IN MOBILITY AND LOGISTICS

Prof. Dr. Gilbert Fridgen
Prof. Dr. Nikolas Guggenberger
Prof. Dr. Thomas Hoeren
Prof. Wolfgang Prinz (PhD)
Prof. Dr. Nils Urbach

Johannes Baur, Henning Brockmeyer, Wolfgang Gräther, Elisaweta Rabovskaja,
Vincent Schlatt, André Schweizer, Johannes Sedlmeir, Lars Wederhake

Also with the participation of:

Matthias Babel, Martin Brennecke, Patrick Camus, Benedict Drasch, Tobias Guggenberger, Luis Lämmermann, Jannik Lockl, Sven Radszuwill, Alexander Rieger, Nicolas Ruhland, Marco Schmidt, Nico Thanner, Patrick Troglauer, Malte Weißert, Felix Würmseher

Contents

1	<i>Management Summary</i>	6
1.1	Purpose of This Report	6
1.2	General Analysis	7
1.2.1	Technical aspects	7
1.2.2	Socioeconomic aspects	8
1.2.2.1	Current situation	8
1.2.2.2	Generic roles and application patterns	9
1.2.2.3	Policy on promoting the spread of DLT	10
1.2.2.4	DLT in the mobility sector	11
1.2.3	Legal considerations	11
1.2.3.1	Civil law	11
1.2.3.2	Data protection law	11
1.3	Case Studies	12
1.3.1	Shipping documents	12
1.3.2	Charging of electric vehicles	13
1.3.3	Ridesharing	14
1.3.4	Platooning	15
1.4	Conclusions	16
2	<i>Introduction</i>	18
2.1	Basic Concepts	18
2.2	Organization of the Study	19
3	<i>Technical Basics</i>	21
3.1	Basic Concepts	22
3.1.1	Blockchain networks	22
3.1.2	Transaction, distributed ledger, digital signature	23
3.1.3	How transactions flow through the blockchain	23
3.1.4	Hash values	23
3.1.5	Blocks	24
3.1.6	Consensus mechanisms	24
3.1.7	Attributes of a blockchain	25
3.2	Other Concepts	25
3.2.1	Smart contracts	26
3.2.2	Other consensus mechanisms	27
3.2.3	Sharding	28
3.2.4	Integration of external data	28
3.2.5	Oracles	28
3.3	Blockchain and DLT Infrastructures	29
3.3.1	Classification schemes	29
3.3.2	Bitcoin	30
3.3.3	Ethereum	31
3.3.4	Quorum	31
3.3.5	Hyperledger Fabric	31
3.3.6	Corda	32
3.3.7	Sovrin	32
3.3.8	IOTA	33
3.3.9	Hedera Hashgraph	34

3.3.10	Overview of DLT infrastructures.....	35
3.4	Governance of DLT Networks	35
3.4.1	Blockchain networks	35
3.4.2	Technological governance	36
3.4.3	Forks	36
3.5	Interoperability and Standardization	37
3.5.1	Blockchain-to-Blockchain Communication	37
3.5.2	ISO standards.....	39
3.5.3	Sidechains	39
3.6	Trends.....	39
3.6.1	Certification.....	39
3.6.2	Quantum computing and blockchains.....	40
3.6.3	Identification of DLT-appropriate business processes	41
4	<i>Socioeconomic Foundations.....</i>	42
4.1	Characterization of DLT Within the Scope of Digitalization	42
4.1.1	DLT and the Internet of Things.....	43
4.1.1.1	The Internet of Things is changing business and society	43
4.1.1.2	The Internet of Things requires an integrated technology architecture	44
4.1.1.3	The Internet of Things is the basis for using DLT in the physical world	44
4.1.2	DLT and Artificial Intelligence.....	45
4.1.2.1	The future-oriented technologies of DLT and AI are converging	45
4.1.2.2	DLT as the database for AI.....	46
4.1.2.3	DLT as a recording platform for AI	46
4.1.3	DLT and privacy-preserving computational methods.....	47
4.2	The Potential of DLT	49
4.2.1	Status quo	49
4.2.1.1	Startups.....	53
4.2.1.2	Consortia	53
4.2.1.3	Established companies	54
4.2.1.4	Public initiatives	55
4.2.1.5	Summary	55
4.2.2	The blockchain value proposition: trust	56
4.2.3	Generic roles of DLT	60
4.2.3.1	Improvers	61
4.2.3.2	Transformers	61
4.2.3.3	Enablers.....	61
4.2.4	Developmental stages of the Internet	62
4.2.5	Application categories	63
4.2.5.1	Neutral platforms.....	63
4.2.5.2	Forgery-proof documentation	64
4.2.5.3	Payments	64
4.2.5.4	Management of cross-organizational processes.....	64
4.2.5.5	Digital identities	65
4.2.5.6	Digital documents	66
4.2.5.7	Providerless services	69
4.2.5.8	Economically autonomous machines	70
4.2.6	Decision-making criteria for the use of blockchain	70
4.2.7	Blockchain as a digital infrastructure.....	71
4.2.8	Informational self-determination and digital sovereignty	73
4.3	Aspects of Implementation	76
4.3.1	Diffusion of DLT-based innovations	76

4.3.1.1	The economic perspective.....	76
4.3.1.2	The Business perspective	80
4.3.2	Obstacles	84
4.3.2.1	Energy consumption and transaction speed.....	84
4.3.2.2	Security, misuse and crime.....	86
4.3.2.3	Data protection and the GDPR.....	89
4.3.3	DLT and governance.....	91
4.3.3.1	Governance mechanisms for operating DLT systems	91
4.3.3.2	DLT as a governance mechanism.....	93
4.3.4	Implications for competition policy.....	95
4.4	DLT in the Mobility Sector	97
4.4.1	Fields of application.....	98
4.4.2	Preview of the special part of the study	101
5	Legal Foundations.....	103
5.1	Civil Law Considerations	103
5.1.1	Smart contracts and automated contract execution.....	103
5.1.2	Limitations on use	103
5.1.3	Conclusion of contracts	104
5.1.3.1	Smart contracts as objects of agreements.....	104
5.1.3.2	Conclusion of a contract using a smart contract.....	105
5.1.4	Contractual content and mandatory law	106
5.1.4.1	Content review, Sections 307-309 of the German Civil Code	107
5.1.4.2	Consumer contracts and special types of distribution.....	109
5.1.5	Treatment of performance problems and reversal issues	111
5.1.5.1	Performance problems.....	111
5.1.5.2	Reversal of transactions	111
5.1.5.3	Access to arbitration bodies/creation of judicial interfaces.....	113
5.1.6	Digressions	114
5.1.6.1	Supervisory issues	114
5.1.6.2	Liability for smart contracts	115
5.1.7	Summary	116
5.2	Assessment from the Standpoint of Data Protection Law	116
5.2.1	Applicability of the GDPR	116
5.2.2	Processing of personal data	117
5.2.2.1	Relevant data processing activities	117
5.2.2.2	Personal data	118
5.2.2.3	Intermediate findings	124
5.2.3	Responsibility for data processing	124
5.2.3.1	Definition of responsibility	124
5.2.3.2	Responsibility for entering data	125
5.2.3.3	Responsibility for reading data	125
5.2.3.4	Responsibility for storing data in the DLT layer.....	125
5.2.3.5	Intermediate findings	132
5.2.4	Legal basis for data processing	132
5.2.4.1	Justifications for storing and reading data.....	132
5.2.4.2	Justification of on-chain processing	134
5.2.5	Implementation of the right to rectification and erasure	135
5.2.5.1	Erasure in an “anonymization solution”	135
5.2.5.2	Erasure in “open solutions” and “centralized solutions”	136
5.2.6	Summary	138
5.2.6.1	Exclusively B2B DLT applications.....	138
5.2.6.2	Other cases	138

5.2.7	Outlook for future legal reforms.....	139
5.3	Existing Regulatory Approaches	141
5.3.1	International.....	141
5.3.1.1	USA.....	141
5.3.1.2	Switzerland	141
5.3.1.3	Malta, Liechtenstein	142
5.3.1.4	Japan	142
5.3.2	Germany and Europe	142
6	Shipping Documents	144
6.1	Economic and Technical Aspects.....	144
6.1.1	Definition and description of an example application.....	144
6.1.2	Status quo and challenges	147
6.1.3	Possible solutions and the role of DLT.....	150
6.1.4	Process description	151
6.1.5	Conclusions and recommendations for action	155
6.2	Legal Discussion	156
6.2.1	Trading documents	156
6.2.1.1	International applications of German maritime trading law	157
6.2.1.2	Credit transactions in foreign trade	157
6.2.1.3	DLT-based trading documents.....	158
6.2.1.4	Use of DLT for data protection in the context of digital trading documents.....	162
6.2.2	Conclusions and recommendations for action	164
7	Electric Vehicle Charging	166
7.1	Economic and Technical Aspects: Technical Part.....	166
7.1.1	Definition and description of the application	166
7.1.2	Status quo and challenges	176
7.1.3	Possible solutions and roles of DLT	177
7.1.4	Process description	179
7.1.5	Conclusions and recommendations for action	181
7.2	Legal Discussion	181
7.2.1	Contractual relationships.....	182
7.2.2	Blockchain-based data protection for electric vehicle charging infrastructure	183
7.2.2.1	Data protection in connection with eRoaming when no information can be obtained about natural persons behind the eMSP and CPO.....	183
7.2.2.2	Data protection with direct payment and eRoaming if information can be obtained on natural persons behind the eMSP and CPO	183
7.2.3	Conclusions and recommendations for action	185
8	Ridesharing.....	186
8.1	Economic and Technical Aspects: Technical Part.....	186
8.1.1	Definition and description of the application	186
8.1.2	Status quo and challenges	187
8.1.3	Possible solutions involving DLT	189
8.1.4	Process description	192
8.1.5	Conclusions and recommendations for action	194
8.2	Legal Discussion	195
8.2.1	Passenger transportation law	195
8.2.2	Data protection	196
8.2.3	Conclusions and recommendations for action	197

9	<i>Platooning.....</i>	198
9.1	Economic and Technical Aspects	198
9.1.1	<i>Definition and description of the application</i>	198
9.1.2	Status quo and challenges.....	201
9.1.3	Possible solutions and the role of DLT	203
9.1.4	Process description.....	205
9.1.5	Conclusions and recommendations for action.....	206
9.2	Legal Discussion.....	207
9.2.1	Road traffic law.....	207
9.2.2	Contract law.....	208
9.2.2.1	Conclusion of a contract	208
9.2.2.2	Type of contract.....	209
9.2.2.3	Malfunctions and unwinding of transactions	213
9.2.3	Data protection.....	214
9.2.3.1	Exchange of driving data	214
9.2.3.2	Exchange of data for executing the balancing payments.....	214
9.2.4	Conclusions and recommendations for action.....	215
10	<i>Final Considerations.....</i>	217
	Bibliography	220

1 Management Summary

1.1 Purpose of This Report

This report presents the economic potential, legal framework, and technical foundations required to understand distributed ledger (DL) / blockchain technology and illustrates the opportunities and challenges they present, especially in the mobility and logistics sectors. It was compiled by the blockchain laboratory at Fraunhofer FIT on behalf of the German Federal Ministry of Transport and Digital Infrastructure (BMVI). Its intended audience comprises young companies seeking, for example, a legal assessment of data protection issues related to DL and blockchain technologies, decision-makers in the private sector wishing concrete examples to help them understand how this technology can impact existing and emerging markets and which measures might be sensible from a business perspective, public policymakers and politicians wishing to familiarize themselves with this topic in order to take a position, particularly in the mobility and logistics sectors, and members of the general public interested in the technology and its potential. The report does not specifically address those with a purely academic or scientific interest in these topics, although parts of it definitely reflect the current state of academic discussion.

The fast pace of digitalization is now affecting almost all areas of society. This is the result of the ubiquitous use of computing, ever-shorter innovation cycles, and the convergence of digital technologies and innovations. One such technology with particularly great potential is distributed ledger technology (DLT). The first major application for DLT debuted in 2009 in the form of a blockchain for the Bitcoin cryptocurrency. Since then, it has evolved into a highly versatile technology; prototype DLT applications are appearing in practically every sector of the economy. Among other things, they are demonstrating the potential of so-called smart contracts for modelling business logic. It is increasingly becoming apparent that DLT, as a driver of innovation, could potentially bring about disruptive changes in many fields of business, law, society, and public administration. DLT—in the form of a transparent, electronic ledger managed by participants in a distributed computer network—provides an answer to as yet unmet expectations in connection with information and communication technology by enabling secure processing of information and transactions, resistance to manipulation, and decentralized consensus formation. As a high-level digital infrastructure, DLT is paving the way from today's "Internet of Information" to an "Internet of Trust and Value".

The mobility and logistics sectors in particular possess many characteristics that make them appear especially suitable for DLT. In the case of the mobility sector, these include networked vehicles that communicate with their environment, intermodal forms of transportation, and distributed infrastructure for charging electric vehicles. There is also potential in logistics and shipping, which are currently burdened by many inefficient cross-organizational processes (e.g. requiring a tremendous amount of paperwork) and urgently need digital support. For the first time, thanks to DLT, it may now be possible to provide it on a practical level.

DLT has potential for addressing the BMVI's responsibilities in two ways: first, for implementing promising applications in the mobility and logistics sectors and second, for designing and providing digital infrastructure. Proactively addressing DLT is essential

for ensuring that this technology will evolve in line with Germany's legal system and values and add the hoped-for value for the country's economy and society. Germany has an excellent starting position, since start-ups and research organizations there are actively pursuing the development of DLT. It is therefore logical and important for the state to become actively involved here in order to take advantage of the momentum and appropriately guide the development of DLT. This study provides a basis for formulating recommendations for further action and achieving the political goal of proactively leveraging DLT to enhance the welfare of German society and strengthen the country's economy in ways that are consistent with its laws and values.

This study identifies, analyzes and addresses economic, legal and, where relevant, technical issues both within and/or across different disciplines as appropriate. The analyses from different perspectives provided here have therefore not been prepared independently of one another, but instead with continual sharing among experts in the realms of science, business and industry, associations, and public policy.

1.2 General Analysis

1.2.1 Technical aspects

The term "distributed ledger technology" refers to a type of database system that is characterized by shared, synchronized data management in a peer-to-peer network with progressive encrypted storage of data in successive links of a chain. Blockchain is one implementation of this technology. Other examples include directed acyclic graphs. The information is stored in blocks that are strung together in chains using cryptographic methods, and redundantly stored in each of a network's nodes using peer-to-peer protocols, meaning that each participant in the network has exactly the same data. The distributed network of independent hosts (nodes) that communicate and synchronize with each other verifies and validates these blocks through a so-called consensus mechanism. The most common consensus mechanism currently used in the Bitcoin and Ethereum blockchains is called "Proof of Work". In addition, there are now several alternative consensus mechanisms that, depending on the design of the specific DLT network, confer certain advantages and/or disadvantages. In addition, second-generation DLT solutions usually offer the option of defining and using so-called smart contracts. Smart contracts are programs that can be written into a DLT platform and executed by all participants in the DLT network in a redundant and/or verifiable manner. As a result, DLTs can be used not only for securely storing data but also for modelling and executing business logic. However, because of the wide range of applications, the scalability and energy efficiency requirements of DLT systems are increasing. In order to do justice to the latest developments, research is currently being done on innovative, scalable, energy-efficient systems. This research has already had initial successes. The frequently voiced criticism that these systems are inefficient and have high energy consumption now only applies to obsolete versions.

DLT systems can also be divided into public and private as well as permissioned and permissionless systems. In principle, anyone can participate in a public system such as the Bitcoin blockchain and see which transactions are added. Such a system is self-organizing, since it lacks a central controlling entity (such as a bank), and the network participants make decisions collectively via a consensus mechanism. In this context, it is important for there to be sufficient incentives for network participants to join the consensus creation process. If this does not happen, a small number of members can wind

up dominating it, which contradicts the underlying idea of DLT and makes manipulation much more likely. Private systems, by contrast, have access restrictions, meaning that participants must register to join the network. In permissionless systems, all network participants can perform any action without restrictions. If the system is permissioned, role profiles allow certain participants to perform only certain actions. For example, it can specify that only certain participants be involved in the consensus finding process. Since a private (or even consortium-based) DLT application often already has some degree of trust among its members, more efficient consensus mechanisms than Proof of Work can be used. For example, in private DLT systems often only a small number of players actively participate in the consensus process.

Examples of well-known DLTs are Bitcoin (public, permissionless), Ethereum (public, permissionless, suitable for the development of widely usable smart contracts), Hyperledger Fabric (private, permissioned, modular design), Sovrin (public, permissioned, especially designed for digital identities), and IOTA (public, permissioned, supports micropayments). Although these are all based on the same underlying concept, so far it is not possible for different systems to directly interact or communicate beyond simply reading data. Nor are there any standardized guidelines for developing DLT infrastructures. However, different organizations are working to find ways to allow transactions between different DLTs. In addition, 11 DLT standards are currently being developed by the International Organization for Standardization (ISO). In the EU, 21 member states have joined in the European Blockchain Partnership to promote the establishment of a European DLT infrastructure.

Integrating DLT systems into existing IT systems makes it necessary to interact with the latter and integrate external data. Currently there are two basic options for the second: 1) the use of hash values as "fingerprints" on external data such as text documents, images, videos, or excerpts from multimedia databases. This method can also be used to check the integrity of external data. For this purpose, the hash value of a piece of external data is compared with the hash value stored in the DLT system. Any manipulation of external data is instantly apparent, since the hash value of the external data is identical to that stored in the DLT system. 2) Data integration performed by participants who log and verify external data and import them into the DLT system, or provide smart contracts for this process (so-called "oracles"). To ensure the correctness of oracles and their data, these are often made plausible based on input from other oracles or else certified.

1.2.2 Socioeconomic aspects

1.2.2.1 Current situation

Due to their infrastructural character, DLTs are classified as basic innovations. And as the individual components continue to evolve, such as the consensus mechanism, DLT-based IT solutions are becoming suitable for an increasing number of applications. However, it is becoming increasingly clear that many uses, both those that have already been investigated and prospective ones, require combinations of different emerging digital technologies. Particularly promising are combinations of DLT with the Internet of Things (IoT), Artificial Intelligence (AI), and privacy-preserving computing methods.

In recent years and months, companies have been investing heavily in the development of DLT solutions to unlock their potential and strengthen their innovative power. According to figures from the IDC market research firm, global investment in DLT solutions amounted to about US\$950 million in 2017 and roughly US\$1.5 billion in 2018. The forecasts of the future volume of the blockchain market diverge sharply, however. While the market research institute Tractica estimates that the global market volume for DLT will reach US\$20.3 billion by 2025, WinterGreen Research predicts that the market volume will reach US\$60 billion by 2024. By contrast, analyses by MarketsandMarkets suggest a global blockchain market worth US\$20.3 billion by 2023. The development of the number of blockchain-related patent applications also shows that there is a high level of corporate interest in the technology and a great deal of innovation. The interest in so-called initial coin offerings, which represent a means of corporate financing based on cryptocurrencies, is also increasing. ICOs are expected to raise a total of US\$14.2 billion of capital by 2019.

In Germany, an extensive ecosystem has developed around DLT, including both research and business. Most of the initiatives involve proof-of-concept or prototype development. So far not many solutions are being used productively. Given these developments, there is a considerable demand for DLT specialists. Numerous corporate and government initiatives are currently promoting and working on DLT. Startups are exploring innovative business ideas, while established companies are evaluating potential applications of the technology, either individually or as part of industry-based or interdisciplinary consortia.

DLT has potential as a digital infrastructure for propelling the Internet to a new stage of development. The first stage was the Internet in its current, well-known function as a source of information. This has in turn spawned the Internet of Things in recent years, as a result of increased networking among intelligent devices. For a long time it was only possible to copy and transmit digital information. Value transfers depended on the involvement of a trusted third party. With the introduction of DLT, however, direct value transactions have become possible. This is why the "Internet of Value and Trust" is often mentioned in this study. DLT must therefore be understood and developed as a higher-level digital infrastructure.

1.2.2.2 Generic roles and application patterns

Basically, DLT can be used for three generic roles: to optimize existing processes that are already handled without intermediaries via bilateral (peer-to-peer) interfaces, either digitally or nondigitally; to streamline operations previously carried out with the involvement of conventional intermediaries; and to enable systems that were previously technically infeasible. The possibilities for implementing various services and applications are quite varied, although certain application patterns can be identified. These include neutral platforms, forgery-proof documentation, payment transactions, management of interorganizational processes, digital identities, digital certificates, services without service providers, and economically autonomous machines.

In most cases, the use of a DLT-based IT solution is not motivated by the technology itself, but rather for economic or organizational reasons. Redundant data management and execution of applications (smart contracts) makes the performance and scalability of a DLT solution technically inferior to a centrally organized system, at least for the

time being. However, DLT opens up the possibility of digitally implementing processes that were previously only possible with the involvement of a trustworthy third party.

In platform markets, the benefits of network effects typically increase for all participants as more people participate on both the provider and the demand sides. As a result, the market usually consolidates, leaving only a few or just one platform provider ("winner takes all"). Experience has shown that monopolistic platforms can use their supremacy to create market entry barriers (in the form of data silos) to new competitors or charge inappropriately high fees. As a result, there is a fundamental skepticism about such platform solutions, especially in the B2B sector. The motivation to use DLT is clearly economic, namely to avoid a monopolistic platform operator in favor of a decentralized solution. However, it is not always necessary or sensible to completely renounce centralized structures. It is important to investigate how DLT could interact with existing mechanisms for creating trust.

1.2.2.3 Policy on promoting the spread of DLT

Looking at the general structural and economic situation, it is noticeable that German universities are not turning out enough graduates with the DLT expertise that the labor market requires. Due to the nature of the technology, it is especially important to promote programs that address the interface between at least two of the following disciplines: business, law, computer science, and possibly engineering. In addition, ministries need to start funding projects related to the development of DLT infrastructure solutions, which would not be conceivable without these technologies. A dual strategy seems advisable for encouraging the diffusion of these innovations. On the one hand, SMEs should be targeted with a variety of support programs such as research projects. On the other, existing low-threshold instruments such as the mFUND and the promotion of strategic flagship projects should also be used. Funding programs should also emphasize the interdisciplinary nature of DLT by establishing consortia. The state must also determine the extent to which incentivizing measures can be used to motivate competing market players to participate, while also monitoring compliance with regulations. A long-term, forward-looking policy that promotes DLT beyond the current hype is preferable to short-term investment. The startups, consortia, initiatives, and organizations that already exist across national boundaries depend on a consistent legal and commercial framework. Like other new technological developments, DLT can benefit from gaining valuable experience under a variety of time-related and geographical constraints and in other test environments (so-called sandboxes and real-world laboratories) constrained by other parameters. Since the technology is undergoing a nonlinear development, it is also advisable to regularly check its implementation and continued usefulness.

Since DLT is comparatively young, it still has some deficits, for example with regard to transaction speed and energy consumption. In addition, DLT has received negative press for things like money laundering and theft, particularly in the context of its most widespread cryptocurrency applications. In addition to internally developed self-governance rules, DLT systems can also potentially contribute to implementing improved governance mechanisms. To this end, the previous considerations are mainly based on two central concepts: the transparency principle for DLT systems which offers many advantages including protection from manipulation, and the inherently democratic structures of DLT, which can be implemented in decentralized autonomous organizations (DAO), for example.

1.2.2.4 DLT in the mobility sector

In the field of mobility, the applications for DLT can be divided into four application fields. The case studies on each are at different stages of development. The field of transportation and logistics includes initiatives that are using DLT to make the processes and cooperation of various transportation and logistics providers more transparent and efficient. Mobility infrastructure includes all infrastructure-related initiatives, such as chargers for electric vehicles. Mobility platform initiatives aim to integrate different mobility services (intermodal mobility) in a single platform, making them accessible to customers via a single portal or app. The field of fully autonomous mobility includes initiatives that pursue the vision of fully automated mobility, with autonomous vehicles playing a central role.

1.2.3 Legal considerations

1.2.3.1 Civil law

From a civil law perspective, the use of so-called smart contracts is particularly interesting. Smart contracts are software that automate the execution of contracts. The term "contract" suggests that this software is a contract in the legal sense. However, applying the general rules on the conclusion of contracts and interpretation of declarations of intent, it becomes clear that in most cases smart contracts will only process what has already been agreed (regardless of the DLT level). It is conceivable that declarations of intent could be expressed with software code, in which case smart contracts would resemble contract documents more closely. However, the difficulty of understanding them imposes considerable limitations.

Like all contracts, those involving the use of a smart contract are also subject to legal constraints. Their validity and legality depend on compliance with mandatory laws.

To the extent that it can be necessary to reverse a transaction that has already taken place, the immutability of DLT does not present any major challenges from a civil law perspective. It is by no means unusual for transfers of value to be subsequently undone. This is done by restoring the original economic situation, and in the case of DLT by means of a reverse transaction. It is immutable only in the sense that the record continues to show the original transaction, which is harmless.

From a contract law perspective, existing civil law thus provides an appropriate legal framework for the use of smart contracts. In practical terms, it should be noted that the current state of the technology does not permit contractual relationships to be completely automated. Software works according to predefined parameters and, so far as least, is unable to make evaluative decisions. Yet legal norms contain vague legal concepts that can only be applied by analyzing and evaluating the situation in each individual case.

1.2.3.2 Data protection law

Existing data protection law poses a legal challenge for the use of DLT. While the distributed storage of data across multiple nodes is an inherent feature of DLT, the EU General Data Protection Regulation (GDPR) follows the principle of a central responsible individual (data controller). This apparent contradiction can be partially overcome

by appropriately designing the architecture. It is becoming apparent, however, that the use of intermediaries cannot be entirely dispensed with. Central coordinating offices could be established to serve as a point of contact and responsible entity for those affected to submit claims to. Without such a central office, open exchanges of data would only comply with the GDPR if no personal data whatsoever were stored in the DLT layer. However, what may initially seem simple turns out to be very challenging to actually implement. While third-party data can often be stored outside the DLT layer (off-chain), public keys regularly contain personally identifiable information on direct users of the DLT layer. Anonymization of user identities is required; this must be not only technically possible, but also ensured in practice.

Another data protection conflict exists between the immutability of the DLT on the one hand and the rights of data subjects to have personal data on them rectified or erased on the other. In ordinary databases the data controller can make subsequent changes, but this is fundamentally neither possible nor desired on DLT platforms. Possible solutions include implementing backdoors to enable subsequent changes by an authorized party or completely avoiding the storage of any personal data on the DLT layer, which also eliminate the need to make any subsequent changes.

In general it should be noted that, in view of the rapid pace of technological developments and the potential of new technologies, future legal regulations should be as technology-neutral as possible.

1.3 Case Studies

Corresponding to the four types of DLT applications in the mobility sector mentioned above, its role is examined in detail in four case studies. For each of the four, a representative application has been selected, described in detail, and analyzed for its potential. The examples were chosen with an aim to ensuring a balanced mix of different levels of maturity and topics relevant to both the public and businesses. The principal ideas and insights on the possible role of DLT in these four case studies are outlined in the following.

1.3.1 Shipping documents

The first application is in the field of transportation and logistics: digitalizing bills of lading (BoL) and the related banking and supply chain processes in international maritime trade. A BoL is a tradable security that represents the value of shipped goods. For shipping documents in general, and especially for bills of lading as discussed in detail in the case study, DLT enables digital modelling of processes that could not previously be digitized for economic or social reasons. Since this topic was already a frequent topic of discussion in the sector even before the spread of DLT owing to its huge potential, this application is already quite mature. The report therefore describes several initiatives and quantitatively analyzes their potential. It also shows that considerable regulatory progress has already been made in Germany by incorporating digital saving clauses into the German Commercial Code.

Many of today's internationally traded goods are still documented with traditional paper documents such as BoLs. This has several disadvantages. Almost all of the steps of a largely paper-based process are slow, and it also suffers from a high error rate due to frequent manual copying of information. It is estimated that today's analog system

costs about a trillion dollars or between five and 10 percent of the total value of goods traded internationally each year. Calculated in terms of the share of German goods in international trade, this process could result in potential savings on the order of tens of billions of euros. Despite the available technical possibilities, no attempts to digitalize this process have so far been widely successful, since centralized approaches would have resulted in a monopoly for a single platform operator. DLT can address these challenges and provide a basic IT infrastructure for enabling collaboration among companies. The basis is a smart contract-enabled DLT platform. Increasing efforts in recent months to establish DLT-based solutions in the market are providing confirmation that DLT is able open up new possibilities, which the participating players regard as promising.

As already mentioned, initiatives for digitalizing shipping documents in Germany benefit from flexible, technology-neutral digital saving clauses in the German Commercial Code. These establish the equivalence of analog and digital shipping documents, since the digital versions must perform all the same functions as their paper-based counterparts.

Current initiatives should not, however, focus exclusively on bills of lading. Other documents such as insurance documents and certificates of authenticity are also important in this and similar processes and should therefore also be digitalized. Legal adjustments or clarifications may need to be made regarding the validity of electronic signatures and digital certificates, as well as the accessibility and validity of electronic transactions as evidence in court, and also the distinction between negotiable and nonnegotiable documents. Digital saving clauses are a technique that legislators could also fruitfully apply in other areas.

1.3.2 Charging of electric vehicles

Electromobility and electrified mobility have undergone rapid technical development in recent years. An indispensable prerequisite for their rapid acceptance and market penetration is the provision of publicly accessible, (rapid) charging infrastructure, especially for charging on the go. Physical, IT, and billing-related differences in charging infrastructure have led to a partitioning of (fast) charging infrastructure, i.e. a splintering of suppliers. Platform operators (special mobility service providers) are trying to counteract this barrier to electromobility with an approach that is comparable to roaming services for mobile telephones. Specifically, a mobility service provider's customers cannot easily access all theoretically available charging stations. There is considerable interest in finding a way for the customers of one supplier to purchase electricity from as many (rapid) charging stations as possible under transparent and suitable conditions, and in ensuring that the associated charging and billing process takes place smoothly and with minimal input from the driver. A DLT-based solution could contribute to this. DLTs can perform at least three potential functions that would address the challenges of electrical charging: authentication and authorization capabilities through DLT-based identity solutions; tamperproof documentation and maintenance of the charging process; billing and value transfer for the charging sessions using tokens.

In this way, a DLT solution can allow for disintermediation, i.e. the partial substitution and reduction of the participants to preclude the risks of individual actors' concentrating market power by design. In addition, new participants could be given access and allowed to participate more readily. However, it remains questionable to what extent a

DLT-based solution might achieve significant market shares, especially since in Germany the market already appears to be maturing fast and charging infrastructure operators also frequently own shares in (centralized) platform solutions. In addition, residents generally cannot be expected to understand every detail of a technology. It must be determined whether DLT, together with consumer protection portals or the TÜV inspection and certification organization, etc., could enable an understanding and acceptance of the technology among private customers. If a blockchain-based solution is established, it could be extended to include shared charging of power among several electric vehicles and proof of origin for green and local electricity. In addition, an application for charging situations with complex ownership structures (e.g. in homeowners associations) would also be attractive. This would create new opportunities for DLT solutions as a neutral platform for a new, as yet fairly undeveloped, market. Looking ahead, not only DLT-based charging but also discharging (i.e. inclusion of electric vehicles in electricity grids such as microgrids) should be promoted. However, first it is necessary to find solutions to the challenges posed by current energy laws.

1.3.3 Ridesharing

The passenger transportation sector in Germany is currently experiencing significant conflict between the traditionally heavily regulated, cooperatively organized taxi industry and public transportation, as well as novel digital mobility platforms offering opportunities for ridesharing. Ridesharing is the shared use of a vehicle by several people with similar travel requirements. But although it has great potential for improving vehicle utilization, reducing emissions, and lowering overall traffic volumes, it is facing major challenges. The most relevant one here is the risk of monopolies arising, but challenges exist also at the operational level, for example in terms of identity management and instilling trust between the parties involved, as well as issues in connection with payments. For example, there is a need to establish trust among fellow travelers, who are for the most part total strangers. In addition, there must be a way to ensure that only actually agreed and utilized services are billed in order to prevent fraud.

To prevent the formation of monopolies and associated data silos, it is necessary to create an open, shared ridesharing platform that excludes neither buyers nor providers from participating. To this end, the opportunities and implications of open and decentralized (technology-neutral) platforms should be examined. In principle, due to its decentralized nature and its ability to automate business processes through smart contracts, DLT is well-suited for rendering individual institutions obsolete as intermediaries for such bilateral transactions and for counteracting the risk of monopolies arising. For amending the German Passenger Transport Act (PBefG), it should be noted in this context that current licensing requirements not only affect the major current intermediaries, but also and especially drivers. However, in the specific context of ride-sharing, the potential of DLT for adding value is limited by technical constraints such as latency and energy consumption. In order to match those offering rides with potential passengers, large data quantities have to be continuously analyzed, updated, and processed, but their tamperproof storage is not a requirement because documentation and processing of the contracts do not take place until after a match is found. However, for regular ridesharing (for commuters) and offers with long lead times, DLT-based marketplaces could be used to coordinate supply and demand. If the case study is extended, for example by also including providers of other forms of transportation on an open, multimodal platform, DLT could potentially add value. In this scenario, existing relationships among multiple vendors must be modelled to facilitate guaranteed

billing of provided services in multimodal transportation. Exemplary approaches can be found, for example, in the initiative funded by the BMVI mFund program for the creation of an open and decentralized mobility system ("OMOS") and the call for a "Germany Ticket." Integration of multimodal services could also generally have a positive impact on the popularity of ridesharing.

In terms of identity management and trust creation, DLT can be used for selective and privacy-preserving identification and authentication of individual parties. In addition to the use of cryptocurrencies or tokens to pay for ridesharing, the use of smart contracts to implement trust agreements without the involvement of intermediary parties seems possible. DLT could therefore add value to ridesharing by facilitating various general and supporting functions.

1.3.4 Platooning

Platooning is a road traffic management system in which two or more vehicles travel at a very close distance behind each other to save fuel ("slipstreaming"). The requirements for platooning include various technologies that are typically used in (fully) automated driving, such as distance sensors and automatic control systems for the steering wheel and accelerator pedal. Platooning activities are currently limited to trucks and (still) in the pre-competitive phase of development. In addition, platooning requires digital infrastructures to coordinate technical processes. This case study shows that hardware retrofits of trucks are likely to be required to facilitate the dissemination of the platooning. In order for platooning to become reality, however, apart from technical advances it is still necessary to address economic issues. From an economic perspective, there is basically no incentive to be the lead vehicle in a platoon. The savings from lower fuel consumption are higher for the vehicles at the rear than for the lead vehicle. If, in the future, a platoon can reduce driving times, the associated savings would also not affect the lead vehicle and its operator. If an operator's vehicles take the lead more often, this would result in a competitive disadvantage compared to those in the rear, resulting in cost savings for the lead vehicle operator's competitors.

The main challenge to the broad use of platooning is how to equitably share the benefits among a platoon's participants. When a platoon consists of vehicles from different freight companies, payment transactions very different from standard payment methods are required. A system of monetary incentives that rewards the leading truck in a platoon for the cost savings achieved by the vehicles in the rear seems to be the logical consequence. In such a scenario, a central platform would act as an intermediary between the individual carriers and coordinate payment settlement. The problem with this approach is that individual platforms could eventually merge to form a monopoly.

In the form of a decentralized payment infrastructure or offsetting realized (fuel) savings, DLT could help establish a broad base for platooning. Since DLT-based payment settlement for platooning would make trips more efficient, its potential can also be quantified. Nationwide use of platooning in Germany could save up to 500 million euros for fuel and prevent 1.39 million tonnes of CO₂ emissions per year. In the future, further savings in personnel and insurance costs as well as increased road safety are also conceivable.

Thus, DLT can be useful for platooning, in particular for settling compensations among platooning participants. In addition to avoiding a monopoly, it offers the advantages of

automating real-time billing of microtransactions with a peer-to-peer approach that makes subsequent clearing unnecessary. Furthermore, documentation could provide protection against attempted fraud and ensure the traceability of driving mistakes or technical problems in any of the vehicles forming a platoon. DLT systems can thus provide the necessary confidence for the driver of the lead vehicle to be sure of fair compensation, even if the platoon contains direct rivals (i.e. other carriers). The basis for this is intelligent expansion of the Internet and its accessibility, in particular to enable realistic case studies.

From a legal perspective, a nationwide rollout of platooning requires an adjustment of the minimum spacing between vehicles (50 meters for trucks heavier than 3.5 tonnes) required by Section 4, Subsection 3 of the German Road Traffic Regulations (StVO). There needs to be a way for the police to tell whether or not two vehicles are driving very close together because they are in a platoon. It would be a good idea to access the time and location data that must be saved in accordance with Section 63a, Subsection 1 of the German Road Traffic Act (StVG). These could be used to infer the driving mode (manual vs. automatic). Although Section 63a, Subsection 2, No. 1 of StVG allows these data to be turned over to the police, this solution is a viable alternative only if the recipient and data storage location are defined more precisely. Authorization under Section 63b of StVG would be appropriate.

Interpreting platooning as break time in the sense of Articles 7(1) and 4d of Regulation (EU) No. 561/2006 does not appear to be legally completely out of the question. However, it has probably not yet been conclusively explored whether the driver's obligations under Section 1b, Subsection 1 in conjunction with Subsection of StVG to be completely alert and ready to resume driving at all times allows for it to be classified as a break. This indicates a need for further study. In addition, platooning with DLT-based payment balancing gives rise to an internal partnership as defined in the German Civil Code.

Data protection law also presents challenges. Often, the platooning platform will be used by companies, in connection with which it will be possible to use knowledge of them to deduce information on natural persons behind them (business owners, drivers, etc.). If the latter then become active on a public DLT platform a username, data processing of relevance under data protection law may occur. This would then require adjustments to the architecture. This can be accomplished by implementing a central entity to regulate data processing. Alternatively, techniques could be used to break the link between usernames and identities, e.g. anonymization. In the event that the participants are exclusively companies behind which no natural persons can be identified, it is sufficient to forego storage of personal data in the DLT layer. The information must be stored off-chain and linked to the DLT platform via hash values. However, such a solution requires prior checking of the participants to establish whether they meet the above requirements. Smaller companies in particular would probably not be able to participate in the system.

1.4 Conclusions

The present interdisciplinary study addresses current questions on the opportunities and challenges facing the use of DLT in mobility and logistics from the perspectives of economics, technology, and law.

General, but also specific application-based study of DLT, reveals that it is a comparatively young technology with great potential. Since its initial use for technically implementing the Bitcoin cryptocurrency, DLT has evolved into a broadly usable basic digital solution for economic infrastructure that is currently approaching market maturity. With regard to the four case studies presented here (shipping documents, charging of electrical vehicles, ridesharing, and platooning), the analyses show differing levels of maturity and potential. In the case of shipping documents, both technical maturity and implementation are already advanced and the financial potential is very significant. However, cross-national integration of different legal perspectives is currently an obstacle. With regard to electrical vehicle charging, the first DLT-based solutions have already been developed but appear to be more market-corrective than suitable for replacing existing centralized platforms. In the case of ridesharing, it is apparent that, due to the required real-time processing of large data volumes, the use of DLT only appears useful and advantageous for secondary functions such as identity management. Where platooning is concerned, the decentralized approach taken by DLT appears to be beneficial and superior to a centralized solution.

It is also unlikely that DLT will lead to new monopolies. However, it can be concluded that DLT solutions and systems should be actively co-shaped by the state in accordance with free democratic ideals. It appears sensible to support programs that address the interface between at least two of the disciplines of economics, law, computer science and, if applicable, engineering sciences. Funding programs should also emphasize the interdisciplinary nature of DLT by encouraging the establishment of appropriately heterogeneous consortia. Furthermore, startups, consortia, initiatives and organizations that already exist across national borders depend on having a uniform legal and commercial framework and clearly defined working conditions (e.g. including sandboxes and real-world laboratories).

2 Introduction

2.1 Basic Concepts

One way to explain how distributed-ledger technology (DLT) works is to present an analogy. Each user of a DLT network has a special notebook (called a "ledger"), and all of the notebooks are "synchronized" to ensure that they are always identical to one another. Whenever a user makes an entry in a notebook, that entry also instantly appears in all of the other notebooks. The individual pages of each notebook ("blocks") are joined by links (the "chain"). The cryptographic connections among the individual notebooks are permanent and cannot be severed. This means that, once made, entries are impossible to delete or alter, and no pages can be torn out of any of the notebooks. At any given point in time, every user of this distributed ledger has a complete history of all of the information contained in it and can be sure that it has never been manipulated.

If, for instance, transactions conducted in a digital currency are entered in such a notebook along with the initial "account balances", this attribute can be taken advantage of to create a system that is managed similarly to bank accounts. One major difference is that such a DLT-based currency system dispenses with an intermediary, which in a conventional system would be a bank. This makes it possible to digitize and store not only financial transactions, but also documents of any other kind in the form of unique, immutable blocks. A combination of transparency, restorability, and tamper-resistance ensures trust among the players. This is achieved without the need for a specially privileged party to assume the role of policeman and make sure that everyone else plays by the rules. Besides technical and legal issues, DLT also begs the question of who could implement a neutral platform of this kind. Because the platform is by definition designed to be neutral—i.e., no company "owns" it—there is no longer an operator whose business model consists of running the platform. Instead, DLT becomes an infrastructure on which other business models can be based. Because the state, and in Germany the Federal Ministry of Transport and Digital Infrastructure (BMVI) in particular, is responsible for infrastructure, it is understandable that this ministry has sought an initial substantiated assessment of the potential of DLT, especially in the realm of mobility, to better prepare itself for the future.

This study addresses political decision-makers at various levels of our federal system who seek an understanding of the possible benefits and repercussions of this technology and therefore wish to be acquainted with current challenges, also from a regulatory perspective. It also addresses established companies and associations that are looking into DLT but have not yet succeeded in assessing the implications of this technology for their industries, as well as companies active in the fields of mobility and logistics. It is also directed at startups, many of which greatly depend on the existence of a precisely defined regulatory framework. With it, the BMVI wants to make it clear that it is always open to questions on regulatory hurdles. Interested citizens are of course also warmly invited to read all or part of this study. It is not explicitly aimed at the scientific research community, because the envisioned coverage of the entire spectrum of DLT lacks sufficient depth to serve as the basis for academic or scientific studies.

This study strives to provide a simple, compact introduction to distributed-ledger technology. What is DLT? What is it already capable of today, and what could the future bring? Where is there a need for social or economic action? And also: Which legal or technical challenges are involved, e.g. with regard to data protection and for ensuring a reliable data infrastructure? Practical case studies on distributed energy systems, identity management, and self-driving vehicles are presented to provide an idea of some of the applications that are already becoming reality today, including the changes induced by them and their potential for further development. The challenges posed by digitalization are now affecting all areas of life, while the associated digital innovations are driving major changes at an ever-faster pace. In order to intelligently shape such far-reaching transformations, it is essential to investigate new digital phenomena and their potential from an early stage. These include, importantly, DLT. A comprehensive, targeted analysis of DLT is key for making sure that this technology continues to evolve in harmony with Germany's legal system and values and adds the hoped-for value for the country's economy and society. This study can also serve as the basis for formulating recommendations for further action to achieve the associated political goal: to leverage DLT in ways that proactively increase prosperity and strengthen the German economy in legally compliant ways.

This study's target group and objectives necessarily restrict its level of detail. For instance, although each of the four case studies presented (see 3.2) sheds light on the implications of DLT, it has not been possible to go into detail on specific prototypes and protocols. In addition, the case studies mainly concentrate on changes induced by the spread and use of DLT, but not on the impact of digitalization in general. While it has been possible to qualitatively assess the potential of this technology from a socio-economic perspective, it would go too far to also consider its quantitative impacts by applying transaction cost theory and forecasting its effects on public welfare, employment, and so on.

Due to the interdisciplinary nature of DLT, methods drawn from various fields have been used to prepare this study. Economic information was obtained from scientific publications, semi-structured interviews of experts, and practical projects and prototypes implemented in industry and the public administration. On the technical side, real-world implementations were studied. Legally speaking, the existing legal framework was examined and available literature on aspects of DLT, mobility, transportation and infrastructure, and data protection law was assessed. In addition, current and planned regulatory initiatives were reviewed. Parallel to this, in October 2018 an interdisciplinary workshop was held, drawing a large number of DLT experts from industry, startups, foundations, and research institutes. The attendees took part in a large number of discussion groups, the results of which were integrated into this study. This interdisciplinary debate on technical, economic, and legal topics closely related to DLT also revealed new connections and even paved the way for a few pioneering insights within the scope of this study. In addition, detailed analysis of the four case studies provided pragmatic confirmation of numerous hypotheses.

2.2 Organization of the Study

This study comprises a general part and a special part. The general analysis starts with a technical introduction to the underlying concepts of DLT, explaining concepts of cryptography and decentralized systems as well as terms such as consensus mechanisms, transactions, and smart contracts. Possible applications are also briefly reviewed.

It is shown that DLT is not a homogeneous technology with characteristic attributes, but rather a very mixed, dynamic field with a multitude of different approaches and a plethora of creative ideas. These are organized and assigned to types based on their basic features. Finally, DLT is contrasted with other technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). The possibilities for combining blockchain with these technologies are also considered.

The following section looks at the importance that DLT could have for our economic system and society. First, economic patterns that favor the use of DLT-specific attributes are identified and illustrated with examples. Special attention is paid to DLT's suitability as a tamper-resistant data storage medium, as a neutral platform, and for transferring value in the form of cryptocurrencies and tokens. Then the spread of DLT is examined to determine its prospects for becoming established in Germany and the rest of the world. Special attention is paid here to its implications for Germany and to suitable measures for promoting it. Problematic aspects are also intensively discussed, as well as the opportunities and risks associated with the technology, including ways in which it could be attacked and public key infrastructure. The implications and potential of quantum computers are also assessed.

The analysis of risks reveals that DLT possesses a number of attributes that potentially make it vulnerable to abuse if employed incorrectly or maliciously. In this context, it is also indispensable to clarify its legal situation. Particularly in connection with the civil law status of automating the execution of smart contracts and the assessment of DLT's compliance with the GDPR, a number of questions are raised and then analyzed and answered in the context of existing laws. Special attention is also paid to aspects that still need to be changed from a legal standpoint, at least to the extent that DLT-based solutions are envisaged for different uses.

The second part of the study backs up the general conclusions drawn in the general analysis by presenting several case studies, one in each of four different mobility-related fields (transportation and logistics, mobility infrastructure, intermodal mobility, and self-driving vehicles), to determine whether DLT actually adds value in each particular case. Here it emerges that, although there is a wide range of potential uses, substantial differences exist in the level of maturity of DLT. For example, the potential of blockchain for implementing ridesharing platforms must be assessed very differently from the case of a neutral platform for approving digital shipping documents. Each of the four case studies is first described from an economic and technical perspective, the role that DLT could play in it is then analyzed, and finally its suitability is evaluated and recommendations for action are provided. Finally, the legal issues and hurdles associated with each application are described.

At this point, the reader's attention should be called to the fact that chapter 3 provides a basic introduction to the complex topic of DLT. For those who are not already familiar with DLT, it is recommended reading. However, this general technical part is not necessarily essential for understanding the remaining parts of the study. Although the general socioeconomic and general legal discussions refer to one other and to the general technical part, they are designed so they can be read and understood on their own. The same statement applies to the special section of the study, in which each of the case studies can be read separately. Many statements made in connection with the case studies can be generalized, and can also be found in the general analysis.

3 Technical Basics

Contracts, transactions, and the data they contain play essential roles in our everyday lives. The ownership of factories and other assets is documented, and at least some of this documentation is in the public domain. Digitization opens up new possibilities for managing these processes, but also poses new challenges that need to be mastered. DLT technology addresses these, enabling greater data security and transparency by documenting transactions in a decentralized, secure, transparent, and immutable manner.

DLT emerged gradually across several phases. In 2008, an unknown person or group of people using the name of Satoshi Nakamoto¹ developed the idea behind Bitcoin, a cryptocurrency or form of electronic cash. The software written for it was released in 2009, thus spawning the Bitcoin network. The technical infrastructure on which Bitcoin is based is referred to as DLT 1.0. It is primarily used in the financial sector and for verifying proofs of origin. The Ethereum blockchain was then developed in 2014. The main innovation distinguishing it from Bitcoin was the addition of "smart contracts". A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Ethereum, which has also come to be known as DLT 2.0, is the best-known example of this technology. DLT 2.0 platforms are used in the Internet of Things, supply chain management, smart grids, and the mobility sector, among other things. Figure 1 shows the development over time of blockchain and DLT (distributed ledger technology).

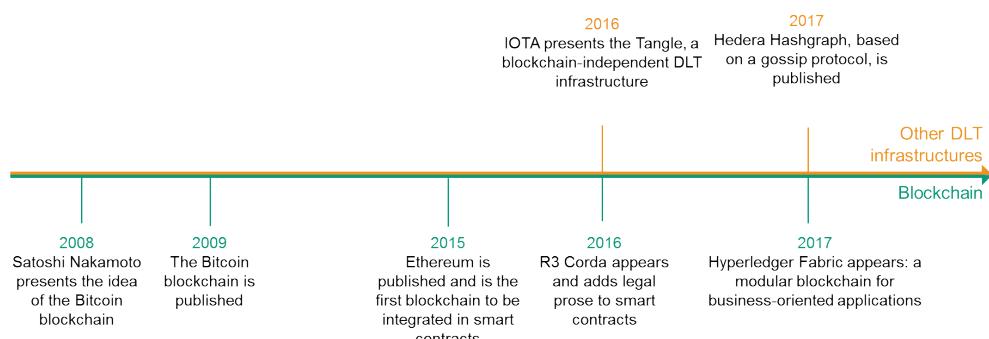


Figure 1: The development of blockchains over time

From a technical perspective, DLT technology combines methods from two fields of study: distributed systems and cryptography. DLT is organized as a network of computers administered by a distributed ledger or directory. This is in turn divided into blocks. Each block contains timestamped transaction data. The blocks are cryptographically linked in a chain known as a blockchain. The ability to trust a blockchain results from cryptographic methods that make it virtually impossible, at least with current

¹ Satoshi Nakamoto is a pseudonym. It is not yet known which person or group of people it stands for.

technology, to retroactively alter the ledger.² The basic concepts of DLT are explained in the following, mainly using the example of blockchain technology.

3.1 Basic Concepts

In order to identify, assess and discuss potential uses, it is necessary to be familiar with the basic concepts of blockchains. The following explanations mainly apply to Blockchain 1.0 and Blockchain 2.0 (currently the most commonly used platforms), on which Bitcoin and Ethereum are both based. The underlying ideas and associated characteristics of DLTs are presented here in simplified form.

3.1.1 Blockchain networks

A blockchain infrastructure is based on a network of computers that are linked in a “peer-to-peer” structure. In other words, all of the computers have the same rights. The specific way in which the computers are linked (the topology) is not fixed. In particular, it is not necessary for every computer to be connected to all of the other computers in the network. The individual computers are also referred to as nodes. The left-hand part of Figure 2 shows a blockchain network.

This simple peer-to-peer model makes it easy to change the network, with the advantage that additional computers can be very easily incorporated into it as new nodes. For example, at any time a computer can be inserted into the public Bitcoin network for executing financial transactions or even mining Bitcoins (i.e. creating new ones). However, the second of these two activities would not be very successful on an ordinary commercially available computer, since the probability of successfully mining new bitcoins increases with a computer’s power.

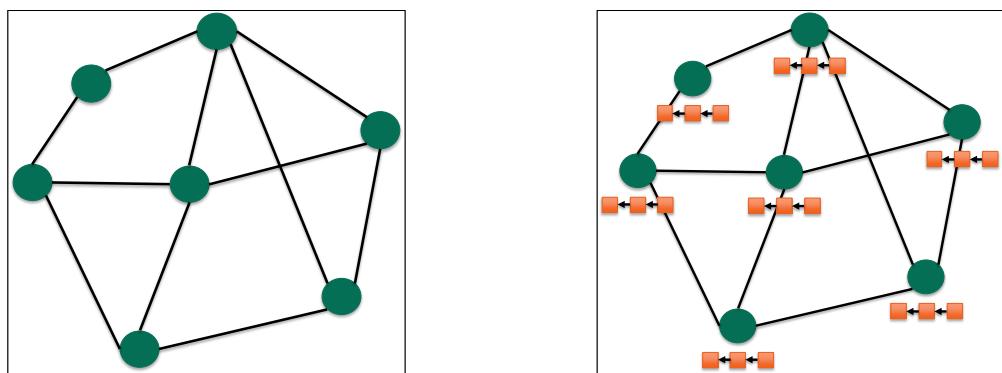


Figure 2: Blockchain network with DLT available at every blockchain node

² Under certain circumstances, however, retroactive changes are possible: namely if a majority of a blockchain’s “miners”—those who add transactions to it—team up to systematically violate the rules. See section 4.3.2.2 to learn more about these so-called 51% attacks.

3.1.2 Transaction, distributed ledger, digital signature

The second basic concept involves storing and managing data in the form of transactions. A certain number of transactions is stored in each block. The blocks are cryptographically linked to form a distributed ledger (DL) that is stored in every blockchain node (see the right-hand part of Figure 2). What constitutes a “transaction” is defined more broadly in the context of blockchains than, for example, when transferring money or goods. In particular, status information can be stored as transactions in a blockchain. Examples of transactions are: “Alice transfers 10 euros to Bob”, “Car 1518 receives 37 kWh of power at charge point L”, or “Truck 2324 travels from A to B as the third vehicle of a platoon.” The transactions are digitally signed so they can be entered in the blockchain. The digital signature can be executed by persons or by other participants in a blockchain network, such as vehicles, machines, etc.

A digital signature is based on a public key infrastructure (PKI) that supports the issuing and verification of digital certificates. Each node of a blockchain network contains pairs of public and private keys. Transactions are signed using the private key and contain the corresponding public key. This ensures that all nodes of the blockchain network can identify the node that has executed a given transaction.

3.1.3 How transactions flow through the blockchain

The way in which transactions move through the blockchain network is another basic concept. Suppose that Alice is sitting at her computer, which is a node of a blockchain network, and wants to send 10 euros to Bob. She creates, signs, and dispatches the transfer. This causes a corresponding transaction to be published and relayed to the other nodes of the blockchain network to which Alice’s computer is directly connected. They check, for example, whether Alice has enough money to transfer the sum to Bob. If this validation produces a positive result, then these nodes in turn relay the transaction to their neighbors, and so on. As a result, the transaction is propagated across the entire network. The diagram on the left of Figure 3 shows how Alice’s transaction flows through the blockchain network.

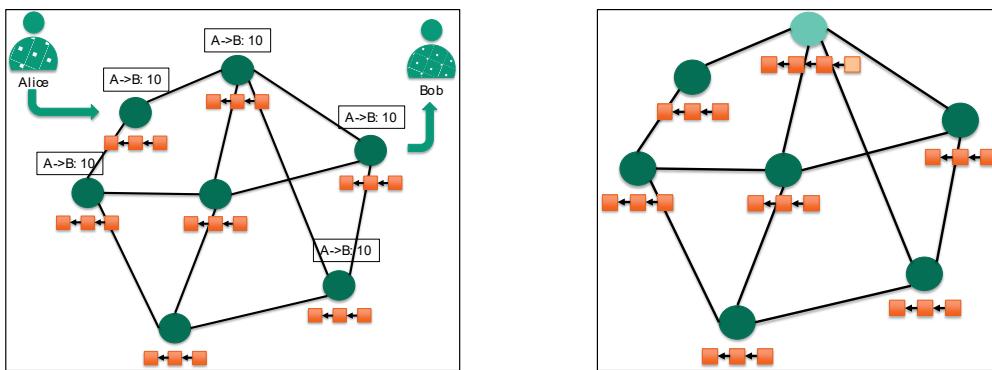


Figure 3: Transactions in a blockchain network (left); the topmost node has solved the cryptographic puzzle (right).

3.1.4 Hash values

In addition to digital signatures, so-called cryptographic hash functions play a crucial role in blockchain technology. Their purpose is to ensure that data stored in a block-

chain are very difficult to manipulate. A hash value is an unambiguous bit string of a certain length, e.g. 256 bits, that can be efficiently generated from any kind of digital information, such as text documents, images, videos or other data sets using hash functions. In the blockchain context, special cryptographic hash functions with additional properties are used.

Hash functions are one-way, meaning that it is extremely difficult to invert them and calculate the inputs that produce a given hash value. They are also collision-resistant, in other words it is virtually impossible to identify two sets of digital information that yield the same hash value.

The Bitcoin blockchain uses a cryptographic hash function known as SHA-256 (short for "secure hashing algorithm 256"). Applying it to the first sentence of this section yields the following value (in hexadecimal notation): 583939AAD746525B33D1D176A9CD3B0E87B3CA875F594910AA40411BA88C993E.

3.1.5 Blocks

A block contains a digital signature, a timestamp, a certain number of transactions, and a cryptographic hash of the preceding block in the chain, which links the two together. The serially linked blocks constitute the blockchain. This structure is illustrated in Figure 4.

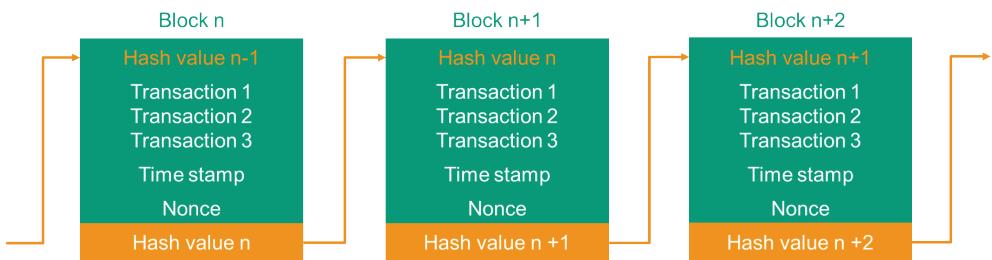


Figure 4: Structure of a blockchain linked by hash values

As soon as a certain number of transactions is reached, a new block is created and added to the blockchain. The decision as to which node of a blockchain network should generate a new block and connect it to the blockchain is part of a so-called consensus mechanism, which is discussed in the next section.

3.1.6 Consensus mechanisms

A consensus mechanism is an essential part of ensuring the blockchain's trustworthiness. The most popular algorithm for this, Proof of Work (PoW), is described in the following. The Bitcoin and Ethereum blockchains both use it.

In order to generate a new block and attach it to the blockchain, the decentralized nodes of the blockchain network have to solve a kind of cryptographic puzzle involving several input parameters. They include the list of transactions that will be stored in the new block, the hash value of the preceding block, and an unknown number called a nonce (from "number used once"). The puzzle is solved when a nonce is found that, together with the other input parameters, yields a hash value smaller than a prescribed

target. Due to the already described attributes of the hash function, the only way to solve the puzzle is by randomly picking different values for the nonce and checking to see if the result meets the criterion. The difficulty of the puzzle is usually adjusted from time to time. In the case of the Bitcoin blockchain, it is currently set so that, on average, a new block is added roughly every 10 minutes.

The first node of the blockchain network that solves the puzzle attaches the new block to its ledger; this is shown in the right half of Figure 3. The nonce and the hash value of the preceding block are entered in the header of the new block. Its predecessor receives that block's nonce and the hash value of its predecessor, and so on. This scheme ensures that the blocks are chained together in a tamperproof way. A block's integrity can be easily checked by calculating its hash value and comparing it with the hash value stored in the preceding block in the chain.

The new block is passed to the neighboring nodes, which check the correctness of the solution. Unlike the process of finding the puzzle's solution, it is very quick and easy to verify that the solution is in fact correct.³ If it is, the new block is attached to the node's chain and then passed to its neighbors and so on. The newly generated block is thus transmitted throughout the blockchain network and all of its nodes add it to their chains.

3.1.7 Attributes of a blockchain

The concepts explained above directly account for important attributes of the blockchain. The first is immutability of the distributed ledger (DL). With current technology it is impossible to tamper with a transaction after it has been added to the blockchain. Any attempt to do so would change the hash value of the corresponding block, and it would then be necessary to solve all of the cryptographic puzzles again in order to conceal the manipulation—a virtual impossibility.

The second basic attribute of the blockchain is its decentralized structure: instead of following instructions in a top-down, centralized structure, the individual nodes themselves autonomously decide which transactions to add to their distributed ledgers. They also use the consensus mechanism to determine which node should create a new block. DLT can therefore dispense with a centralized decision-making.

The third characteristic of DLT is automation of processes. This is accomplished with "smart contracts", which are presented and discussed in the next section.

3.2 Other Concepts

As the original technology of the Bitcoin blockchain evolved, it gave rise to new systems that are collectively referred to as Blockchain 2.0. New concepts also emerged that increased the possible uses of DLT and are also relevant to the case studies presented in the special part of this study. They are concisely explained below.

³ This is comparable to the fact that searching for the prime factors of very large numbers is extremely time-consuming, but once identified the prime factors can be very quickly multiplied together.

3.2.1 Smart contracts

Smart contracts are scripts (i.e. computer programming code) that the members of a blockchain network execute. In theory, they permit all deterministic calculations. A calculation is deterministic if a given input always produces the same output. Smart contracts typically contain IFTTT (= if this, then that) instructions for executing control or business logic. IFTTTs are often nested inside one another, which makes a smart contract "complex". From a purely legal perspective, however, smart contracts are neither contracts nor particularly intelligent. In the vast majority of cases, they merely control and coordinate processes or data flows. Smart contracts were not originally foreseen either for the Bitcoin network or for DLT systems based on directed acyclic graphs. Although this is now being worked on, there are already uses for these systems today, while it is also clear that DLT systems can also add value without smart contracts. The platooning case study is a case in point. Smart contracts also aggravate the storage problems of DLT. Because all data are permanently stored in a blockchain, over time the required memory resources steadily increase. These data also include the program code of smart contracts. Another important point is that smart contracts can only be used to ensure correct calculations. This does not include checking data outside the boundaries of the blockchain system. Mistakes made by users when entering data and defective, corrupted or manipulated sensors can be especially problematic. These issues are addressed in section 3.2.5.

The Bitcoin blockchain is mainly suited for financial applications. It includes a scripting language that can be used, for example, to create a trust account or make so-called micropayments. However, Bitcoin's scripting language lacks the capabilities of a full-fledged programming language such as C++ or Java, which constrains the possible uses of Bitcoin. The Ethereum blockchain, by contrast, integrates a programming language that can be used to implement smart contracts: Solidity. A smart contract is nothing more than executable program code that is immutably stored in the blockchain and then executed in response to a defined event.

In the context of mobility, for example, a smart contract could be used to automatically pay road tolls when a vehicle passes a toll booth. It would also be possible to implement auction mechanisms as smart contracts, for example for local energy trading. Charge points could automatically negotiate prices with nearby power producers and obtain electricity from them. Smart contracts also have potential for simplifying the borrowing or use of vehicles or devices by aggregating (sensor) data or managing identities.

Another example of how smart contracts can be used is for depositing data on a trust basis (also known as escrow smart contracts). In connection with online purchases, a frequent problem is that customers prefer to put off paying until they have received the product. A possible solution is for the buyer to transfer the money to a smart contract (thereby relinquishing control over it), while certain defined conditions must be met in order for the smart contract to release the money to the seller. Conditions of this kind could include, for example, digital confirmation by the customer or a previously designated third party such as a forwarder that the merchandise has been delivered.

3.2.2 Other consensus mechanisms

The Proof of Work consensus mechanism used in the current Bitcoin and Ethereum blockchains was presented in section 3.1.6. Basically anyone can join both of these so-called public blockchain networks; this means, in particular, that the trustworthiness of the individual blockchain nodes is unknown. Proof of Work ensures competition among the blockchain nodes for the privilege of creating a new block. Every change to a blockchain node generates a new block, which virtually rules out any manipulation of blocks or the transactions they contain.

In contrast to public or open blockchains, private and consortium blockchains are restricted to previously selected, trustworthy participants. Because a situation of trust has already been established, the consensus mechanisms used can be much simpler. They can range from Proof of Work with a reduced level of difficulty, across Proof of Stake and Lottery Protocol, to selected validation nodes. Figure 5 schematically shows the relationship between transaction throughput and degree of openness in blockchains based on different consensus mechanisms.

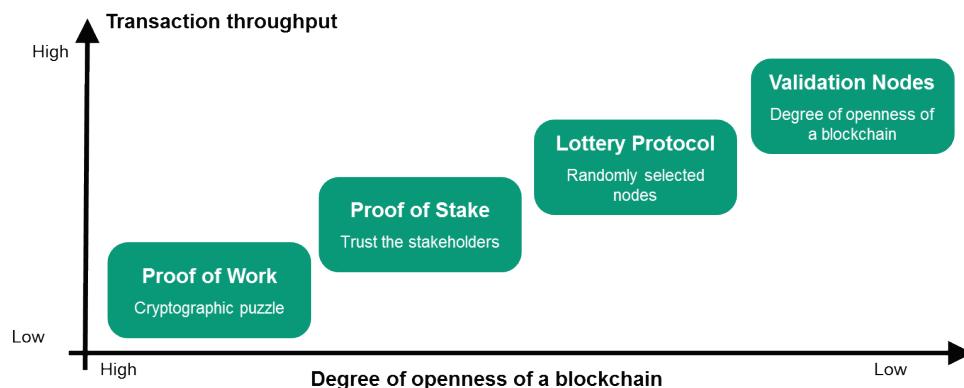


Figure 5: Performance of a blockchain as a function of the consensus mechanism

Proof of Stake

Proof of Stake designates a class of consensus mechanisms that considers the stakes that blockchain nodes (participants) hold in the network. The stakes can be, for example, monetary assets (coins), the number of added blocks, or how long they have participated in the blockchain. The corresponding stakes can be quickly calculated. The next participant to add a block is chosen by a combination of weighting their stake and applying a random factor. Security is derived from the fact that each participant has a real stake in obeying the rules of the network (analogously, in a Proof of Work approach the stake consists of energy consumed, which costs money). If anyone tries to add blocks that break a rule, they lose their stake.

Proof of Authority

This consensus mechanism is based on explicitly selected blockchain nodes: so-called validators. Only these may combine transactions in a block and add it to the blockchain. Applying a reputation-based mechanism, blockchain nodes with a good reputa-

tion can become validators. If such a node later acquires a bad reputation, it loses its validator status.

3.2.3 Sharding

The approach called sharding is now being tested to see if it can increase the transaction rate in blockchains and thus improve the scalability of blockchain infrastructures overall. It is based on a database portioning technique, with the nodes of a blockchain managing different parts of the distributed ledger. Blockchain nodes only process the transactions of the partition assigned to them, which enables parallel processing and thereby increases the transaction volume. Sharding is designed to preserve the integrity of the overall ledger. OmniLedger is an example of a prototype DLT infrastructure that uses sharding.

3.2.4 Integration of external data

On blockchain platforms, data are stored as transactions that are in turn bundled into blocks which constitute the decentralized peer-to-peer distributed ledger (see section 3.1.2). However, these transactions should not contain too many data, since the size of the DLT system increases with the number of transactions and the storage space they require. A standard method for integrating external data such as text documents, images, videos, or excerpts from multimedia databases is to add “digital fingerprints” to transactions in the form of hash values. A link to the data is stored in the blockchain along with a hash of the data. The link can then be used at any time to access the data. At the same time, it permits easy checking of the integrity of the external—and therefore changeable—data by comparing their hash with the hash value stored in the blockchain. If they fail to match, the external data have clearly been manipulated. A second class of external data is that of sensor values. Sensors capture states in the real world and are therefore indispensable for applications in the Internet of Things and supply chain processes. In a food delivery chain, for example, sensors can support the traceability of items, activating an alarm if a cooling chain is interrupted or initiating appropriate actions when products arrive at their destinations. Process automation can be supported in particular by a combination of sensor values and smart contracts. However, sensors initially provide values that are outside the blockchain. It is therefore important to verify the identity of the sensors and the correctness of the values they deliver before storing this information in the blockchain. Similar issues arise in connection with other data that are to be entered in the blockchain.

3.2.5 Oracles

These issues have led to the development of “oracles”. This is the name that has been given to externally provided services such as trustworthy sensor values and online information like weather data, sports scores and so on. Especially in the mobility sector, there is a need for blockchain infrastructures that directly implement blockchain clients on devices in the Internet of Things (IoT) to appropriately secure sensor values and communication paths. For this purpose, IoT devices have to be extended by adding the required computing power and storage capacity for securely managing keys. The relevance of the IoT to DLT is discussed in greater detail in section 4.1.1.

3.3 Blockchain and DLT Infrastructures

DLT has steadily advanced since the advent of Bitcoin. Alongside the blockchain structure consisting of linked blocks that is the basis for Bitcoin and Ethereum, other new data structures are now also delivering benefits such as better performance or scalability. The term "distributed-ledger technologies" (DLT) has become established as the generic descriptor for all of these innovations.

3.3.1 Classification schemes

Several distinct phases can be identified along the evolutionary path of DLT. Blockchain 1.0, which laid the foundation for the development of all DLT infrastructures, was first mentioned in 2008, when Satoshi Nakamoto (or the person or group of people using this pseudonym) published a paper titled "Bitcoin: A Peer to Peer Electronic Cash System". The first actual blockchain was implemented in 2009 in the form of Bitcoin.⁴ The Bitcoin blockchain is transaction-oriented; in other words, transactions for transferring Bitcoin cryptocurrency between users of this infrastructure can be stored in it. Subsequent to the publication of Bitcoin, numerous other transaction-oriented DLTs were launched, each with its own cryptocurrency. These alternative cryptocurrencies have been dubbed "Altcoins" (= alternative coins).

While the technologies of Blockchain 1.0 are used almost exclusively for transferring cryptocurrencies between users, Blockchain 2.0—as already explained in section 3.2.1—introduced smart contracts.⁵ Blockchains of this kind are also referred to as logic-oriented, since smart contracts, i.e. snippets of program code, are inserted in them and automatically executed. This has spawned a large number of further uses for blockchain infrastructures that require a certain amount of business logic. Figure 6 assigns some blockchain structures to Blockchain 1.0 and 2.0.



Figure 6: Assignment of some DLTs to the 1st and 2nd blockchain generations

In addition to classifying DLTs as belonging to the 1st or 2nd generation, they can also be divided into public (open) and private and, according to the extent that access to them is restricted, permissioned and permissionless platforms.⁶ Public platforms like Bitcoin allow unrestricted access by users, i.e. anyone can participate in the network

⁴ Lamberti/Gatteschi/Demartini/Pranteda et al., IT Professional (Early Access) 2017, 1.

⁵ Lamberti/Gatteschi/Demartini/Pranteda et al., IT Professional (Early Access) 2017, 1.

⁶ Vukolic, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, p. 3.

and see which transactions are added to the blockchain. Private platforms, by contrast, are characterized by restricted access, meaning that it is not possible for simply anyone to freely join the network; instead, it is necessary to register, which may require the consent of all current users. The most important examples of private DLTs are consortium DLT systems. This term typically designates an association of multiple users such as companies.

If a platform is permissionless, network participants can perform all actions without any restrictions; but if it is permissioned, there may be different role profiles that limit a user to performing only certain actions. On a permissioned platform, for example, a participant could be authorized to read transactions but not to add any new ones. The left-hand part of Figure 7 schematically categorizes public, private, permissioned and permissionless blockchains.

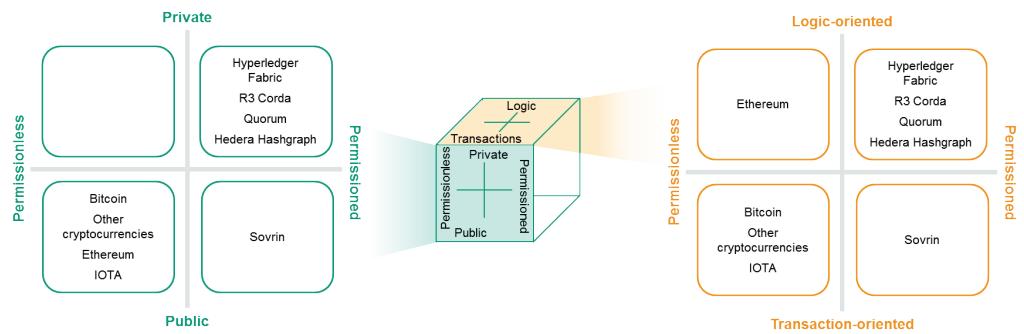


Figure 7: Classification of blockchain platforms based on public/private, degree to which access is restricted, and programmability

Another parameter for classifying blockchain platforms is programmability. Here a distinction is made between transaction-oriented and logic-oriented platforms. The Bitcoin blockchain is transaction-oriented and comes with a scripting language that can only be used to define simple relationships. Logic-oriented blockchain infrastructures feature a more powerful programming language that can be used to implement smart contracts. The right-hand part of Figure 7 shows how different blockchain platforms are classified on the basis of accessibility and programmability.

Blockchain platforms can also be distinguished on the basis of whether or not they include cryptocurrencies. The Bitcoin and Ethereum blockchains have cryptocurrencies that are used to pay for storing transactions and executing smart contracts. Miners are also rewarded for their work with a sum in the corresponding cryptocurrency. If a cryptocurrency is essential for operating a DLT system, it is also referred to as “native”.

Hyperledger Fabric is an example of a blockchain platform that performs its basic functions without the need for a cryptocurrency—there are no rewards for mining new blocks, and no transaction costs are incurred—and it therefore has no native cryptocurrency. However, suitable smart contracts (“chaincode”) can be programmed to create tokens that have all of the attributes of a cryptocurrency.

3.3.2 Bitcoin

As explained in section 3.3.1, DLT originated with the Bitcoin blockchain. This blockchain is public and permissionless, meaning that anyone can participate and there are

no restrictions on its use.⁷ As a member of the first blockchain generation, the Bitcoin blockchain has a native cryptocurrency called bitcoin and is used to generate this currency and transfer it between network users. The consensus mechanism used for it is the Proof of Work algorithm.

3.3.3 Ethereum

The Ethereum blockchain was developed in 2015 by Vitalik Buterin, Gavin Woods, and Jeffrey Wilcke, among others. The first example of Blockchain 2.0, it makes it possible not only to make digital payments via the blockchain, but also to automate entire processes with the aid of smart contracts.⁸ The cryptocurrency on which Ethereum is based is called Ether. Ether can also be converted into "gas", which is needed to pay for executing transactions and smart contracts. Like Bitcoin, the Ethereum blockchain is public and permissionless, and anyone can therefore access the blockchain and enjoy the same rights and privileges as all of the other network participants. Ethereum paved the way for the development of a large number of decentralized applications, or "DApps" for short, that are used in a wide range of fields and industries; the benefits of blockchains are no longer limited to the financial sector. Like Bitcoin, Ethereum uses a Proof of Work consensus algorithm. Because it is extremely resource-intensive (as already explained above), however, the Ethereum Foundation is planning to switch to the more resource-efficient Proof of Stake approach (see section 3.2.2).

3.3.4 Quorum

Quorum is a blockchain based on the Ethereum blockchain model. It began with a "fork", or alternative chain, of Ethereum.⁹ Unlike Ethereum, however, Quorum is a permissioned consortium-type blockchain and includes private transactions that can only be viewed by certain users. There is also no charge executing transactions, so no "gas" is needed to pay transaction fees. As a result of these modifications and the choice of an alternative consensus mechanism, Quorum is designed for greater efficiency and more privacy for transactions, which makes this blockchain particularly attractive to enterprises.

3.3.5 Hyperledger Fabric

Yet another blockchain platform is Hyperledger Fabric, which emerged from one of several Hyperledger projects hosted by the Linux Foundation.¹⁰ In contrast to Bitcoin and Ethereum, Hyperledger Fabric has no need for a native cryptocurrency. Instead, it uses container technology for creating smart contracts that are called "chaincode" because of the slightly modified blockchain architecture. When necessary, however, this functionality can also be used to generate cryptocurrencies. Hyperledger Fabric also differs from Bitcoin and Ethereum in terms of its access rights, being a private, permissioned blockchain. Like in Quorum, different rights can be implemented for users; for example, part of the transactions or the execution of smart contracts may not

⁷ Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System; Narayanan/Bonneau/Felten/Miller et al., Bitcoin and cryptocurrency technologies: a comprehensive introduction.

⁸ Buterin, Ethereum White Paper.

⁹ Baliga/Subhod/Kamat/Chatterjee, Performance evaluation of the quorum blockchain platform.

¹⁰ The Linux Foundation, Hyperledger Architecture, Volume 1.

be visible to everyone. Consequently, Hyperledger Fabric is also highly suited for cross-organization applications and therefore geared to corporate use. Depending on the application, certain components of the blockchain can be modified on a plug-and-play basis, like the consensus mechanism or membership services.

3.3.6 Corda

In contrast to Ethereum and Hyperledger Fabric, Corda was not developed to support applications across all industries and applications. Instead, its originators—an industry consortium called R3—designed it specifically for the financial sector.¹¹ Just like Hyperledger Fabric, Corda also dispenses with a native cryptocurrency, although it permits the implementation of smart contracts. In Corda, however, smart contracts can contain not only program code but also legal prose, which makes a great deal of sense for the highly regulated financial industry. Another similarity to Hyperledger Fabric is that Corda is also private and permissioned. The consensus mechanism can also be swapped on a plug-and-play basis.

3.3.7 Sovrin

The Sovrin Identity Network is a blockchain initiative that, as a result of its work on Hyperledger Indy, can be broadly grouped with the Linux Foundation's Hyperledger project. It has set itself the goal of enabling self-sovereign digital identities for everyone.¹² Sovrin is public and permissioned, so anyone can participate in its blockchain system and benefit from a digital identity, although roles with different rights are defined within the system. The idea is for everyone to have their own self-sovereign digital identity independently of a central entity or authority, so each individual has complete control over the information that comprises their identity. Relevant information can be assigned to an identity as "claims". For example, a driver's license can be issued by an authorized government office as a claim and assigned to a certain individual, thus becoming part of their digital identity. If that person wishes to share information constituting part of their digital identity, they can do so selectively. Consequently, as required only a subset of the information can be compiled and shared without revealing all parts of the digital identity. The use of a blockchain to manage identities in this way is intended to render the keeping of multiple accounts, usernames, and passwords obsolete and achieve the ideal of a single unique digital and tamperproof identity for each person. Sovrin has also eliminated the Proof of Work consensus mechanism, using a so-called RBFT (Redundant Byzantine Fault Tolerance) algorithm instead. Here it should be especially emphasized that no personal data are stored in the blockchain. Instead, the blockchain is used to manage the public keys ("addresses") of trustworthy government agencies and users, which Sovrin enables to use self-sovereign digital identities. All personal data remain the property of the individual at all times, with the blockchain ultimately being leveraged to disrupt the monopoly of "certificate authorities" (whose role is traditionally to confidentially assign public keys from a public key infrastructure (PKI) to organizations over the Internet) while also enabling private users to quickly and inexpensively obtain public addresses. Since the public keys are readily accessible in the blockchain and can be read by anyone, personal data might poten-

¹¹ Valenta/Sandner, Comparison of Ethereum, Hyperledger Fabric and Corda.

¹² Sovrin Foundation, A Protocol and Token for Self-Sovereign Identity and Decentralized Trust.

tially be deduced by comparing several interactions. Sovrin therefore also uses zero-knowledge proofs, which are described in greater detail in section 4.1.3.

i

Pseudonymization vs. Anonymization

Users are regularly pseudonymized when using DLTs, since only the public key obtained from the PKI is visible. This can make it significantly harder to establish a user's true identity. Despite this, it may be possible to deduce the user by analyzing multiple activities conducted under the same pseudonym while considering additional information. However, there are also ways to mask or change pseudonyms and achieve true anonymization. Self-sovereign digital identities are especially suited for achieving complete anonymity without losing the ability to transfer attributes under one's own pseudonyms.

3.3.8 IOTA

IOTA is an example of a DLT that does not use a blockchain as its underlying data structure. Instead, transactions are stored in the "Tangle", which is described as a directed acyclic graph (DAG).¹³ Before a new transaction can be added to the Tangle, it must first validate two preceding transactions. This ensures the network's consistency. The nodes are chosen by a complicated "random tip selection" algorithm. During validation, checks are made to ensure that the signatures of the two transactions are correct and do not add any contradictory information to the Tangle. As more new transactions validate a given transaction, either directly or indirectly—i.e. via another transaction—the user adding the transaction to the network gains greater security that the transaction in question really is valid and will remain in the final Tangle. As soon as a transaction has been directly or indirectly validated by all loose ends of the Tangle (so-called tips) that have not yet been validated themselves, it is considered completely accepted. Figure 8 shows an example Tangle with a genesis (initial) transaction, completely and partially validated transactions, and new transactions (tips) that have not yet been validated.

IOTA purports to have much greater scalability than blockchains, making it especially well-suited for applications in the Internet of Things, since the absence of transaction costs also makes micropayments feasible. This is particularly relevant for machine-to-machine transactions. Another advantage of the Tangle is that the speed with which new transactions are validated actually increases as more transactions are added. This is in stark contrast to the Bitcoin blockchain, for example, in which the transaction volume—in other words, the number of transactions completed, weighted by their data volume—remains constant, thus subjectively reducing its performance as the number of users and the network's cumulative computational overhead increase. Currently, however, the network is still in a transitional phase in which, according to the IOTA Foundation, validation of transactions is being transferred to a central moderator function.

¹³ Popov, The Tangle.

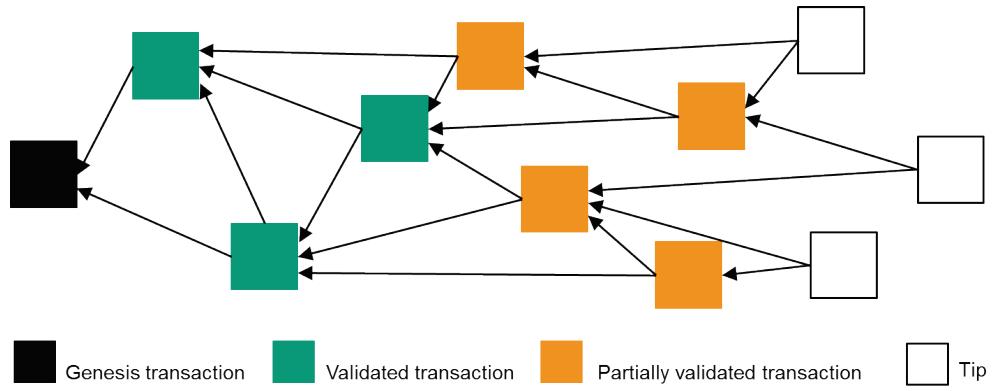


Figure 8: Schematic diagram of the IOTA Tangle

3.3.9 Hedera Hashgraph

Hedera Hashgraph is another DLT system with a nonstandard data structure. It was developed with the goal of ensuring fast distribution of information by keeping its bandwidth as small as possible.¹⁴ The underlying idea is based on the gossip principle: each of the network's users randomly chooses another user and tells them everything he or she knows about the network. Besides information on executed transactions, the entire Hashgraph is also shared, in other words information on all of the gossiping. Information distribution is therefore referred to in Hashgraph as "gossip about gossip". In other words, all of the gossiping done so far is also communicated by gossiping. In this way, the Hashgraph is propagated further and further in the network. Figure 9 illustrates how the Hashgraph works.

Another important activity is virtual voting to establish a consensus in the Hashgraph: because every user has a copy of the Hashgraph, he or she knows what the other users know and consequently how they would vote in a decision-making process. Therefore there is no need to actually vote, which significantly improves the performance of the Hashgraph network.

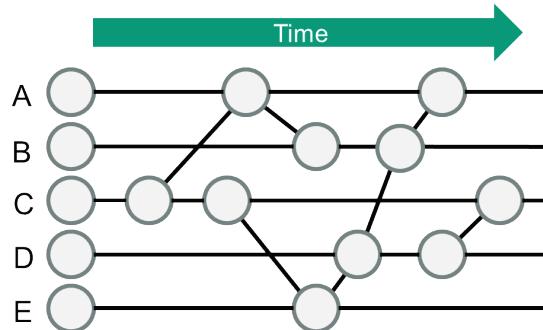


Figure 9: Schematic of Hedera Hashgraph. A, B, C, D and E are network participants. Every connection between two participants represents a gossip event in which a participant reveals everything they know to another participant.

¹⁴ Baird/Mance/Madsen, Hedera: A Governing Council & Public Hashgraph Network.

3.3.10 Overview of DLT infrastructures

Table 1 contains an overview of all of the DLT infrastructures presented in this section. They are divided into general DLT and blockchain technologies, the latter being a special case of DLT. In addition, their respective access restrictions are compared and special features listed.

	Access restrictions	Special features
Bitcoin	Public, permissionless	The first blockchain
Ethereum	Public, permissionless	Suitable for developing DApps for the masses
Hyperledger Fabric	Private, permissioned	Modular structure
R3 Corda	Private, permissioned	Smart contracts that support legal prose
Sovrin	Public, permissioned	Specially developed for digital identities
IOTA	Public, permissionless	Supports micropayments
Hedera Hashgraph	Private, permissioned	Virtual voting accelerates the validation process

Table 1: Overview of different DLT infrastructures

Besides the DLT infrastructures already discussed, there are many other variants. They include blockchains that use alternative cryptocurrencies (so-called Altcoin blockchains like Litecoin and Ripple) and some that support both a cryptocurrency and smart contracts. There are also blockchains that have arisen by diverging from another blockchain (forks): Quorum, for example, which split off from Ethereum. In addition, there are endeavors to improve the scalability of distributed systems with non-blockchain DLT infrastructures.

3.4 Governance of DLT Networks

DLT applications call for appropriate DLT networks. There are applications that can be implemented on the basis of existing publicly accessible blockchain networks such as Bitcoin or Ethereum. These applications are then subject to the rules of the system they are piggy-backed onto, like its prescribed consensus mechanism or transaction costs.

Many applications geared to industry are based on non-public DLT networks. In these cases, it matters greatly who the network partners are and which of them operate nodes. Basic considerations for defining the rules of cooperation, so-called governance principles, are discussed below. They are also relevant to the case studies in the mobility sector.

3.4.1 Blockchain networks

The network of a public blockchain is self-organizing: the blockchain is designed to eliminate the need for a central decision-making entity, administrator or function, which would normally be required for controlling and monitoring a network. Supported by a consensus mechanism, the members of the network make decisions without

additionally requiring such a function.¹⁵ In order for this to work, it is important for the network's members to have sufficient incentives to join the process of arriving at a consensus. If this is not the case, the network can be easily dominated by a few members—a situation that is contrary to the underlying idea of a blockchain and can open the door to manipulations. In a private and permissioned blockchain, the network is not completely self-organizing. Consequently, a designated body or committee is typically responsible for admitting new members to the network, expelling members if necessary, and issuing access authorizations. Alongside managing the membership, another important task of this body—which can be either a single trustworthy third party or a subset of the membership—is to choose the procedure for arriving at a consensus. Because private and consortium blockchains are usually characterized by greater mutual trust among the network's members than is the case with public blockchains, they can employ more efficient consensus mechanisms. This can mean, for example, that only a minority of players is actively involved in establishing a consensus.

3.4.2 Technological governance

In addition to managing a network's organizational structure, it is important to keep developing the underlying technology.¹⁶ Of particular relevance are regular security updates. Private and consortium blockchains in particular often have a taskforce that is responsible for advancing the technology. An alternative is open-source blockchains like Bitcoin, in which a loose community of independent programmers devotes itself to developing the infrastructure further.

3.4.3 Forks

In any given blockchain, normally each block only has one successor. But under certain circumstances a "fork" can occur, causing the blockchain to split and spawn two or more child chains. One thing that can provoke such a split is a software update.¹⁷ The outcome can be either a hard or soft fork. In a hard fork, the new version of the blockchain is no longer compatible with the old one, and consequently from that moment on there are two blockchains: one consisting of network nodes that have adopted the update and the other of nodes that have rejected it. This is illustrated by Figure 10. In the case of a soft fork, the new software is compatible with the old one and nodes that do not adopt the update continue to belong to the original blockchain. However, if nodes running on the old software subsequently add transactions that are incompatible with the new software, the soft fork can mutate into a hard one.

¹⁵ Osterland/Rose, Proceedings of 1st ERCIM Blockchain 2018, p. 1.

¹⁶ Osterland/Rose, Proceedings of 1st ERCIM Blockchain 2018, p. 1.

¹⁷ Lin/Liao, International Journal of Network Security 2017, 653.

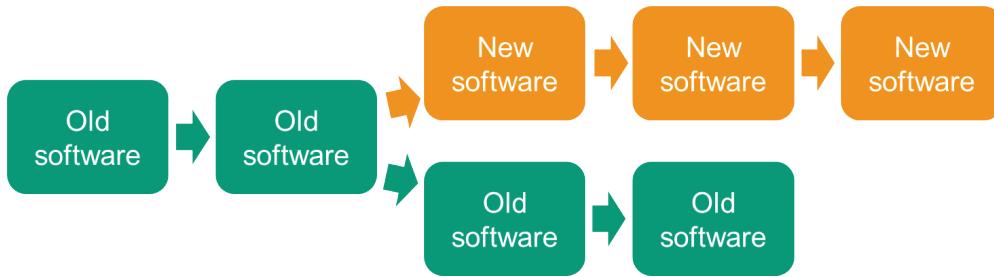


Figure 10: A "hard fork" induced by a software update

A fork can also occur, at least temporarily, if the consensus mechanism causes multiple blocks to be created at the same time, resulting in diverging versions of the blockchain.¹⁸ In this case, however, the blockchain eventually fixes itself because the longest version of the blockchain prevails while the alternatives are rejected. These temporary soft forks can occur frequently and are the main reason why it is wise to reserve judgement on whether a transaction has been irrevocably integrated in the blockchain until a sufficiently large number of additional blocks have been added. In the case of the Bitcoin blockchain, the rule of thumb is to wait until about six more blocks have been added before concluding that a transaction is secure, because by then it is safe to assume that the chain, and with it the block in question, will not be replaced by an alternative chain and a different block.

3.5 Interoperability and Standardization

As was explained in section 3.3, there are many different DLT and blockchain infrastructures. Over time, collections of similar systems arise that are based on the same technology but not necessarily able to communicate with one another. To make matters worse, no standardized guideline for developing DLT infrastructures currently exists. Various organizations are striving to alleviate this situation by enabling transactions between different blockchains. Among other things, a new ISO standard for blockchains and DLT infrastructures is now in the pipeline.

3.5.1 Blockchain-to-Blockchain Communication

Different blockchain and DLT applications for things like verifying guarantees of origin, supporting platooning (see Chapter 9), and implementing supply chain applications (see Chapter 6) also pose different requirements, both for the technology used (scalability) and for governance of the corresponding networks. Consequently, in the short term the emergence of a whole menagerie of blockchains is to be expected. But there will also be applications that are able to access information and/or execute transactions across various types of blockchains. There is also every reason to expect that smart contracts in one blockchain will acquire the ability to invoke smart contracts in other blockchains, for example as oracles, or to send them instructions. Examples of interoperable blockchain networks may also appear in machine-to-machine applications.

¹⁸ Natoli/Gramoli, 2016 IEEE 15th International Symposium 2016, 310.

Appropriate standards for data and interfaces need to be defined to prevent content from being coded specifically for only one blockchain (and unintelligibly for others), so that it can be used across multiple applications. Where guarantees of origin are concerned, the Open Badges standard for digital personal certificates already provides a workable solution. Application interfaces that abstractly implement blockchain functions enable inter-blockchain communication. Standards of this kind for data and interfaces, as well as corresponding identity management systems, are the foundation for the emergence of an Internet of Blockchains.

No simple solution is yet available for enabling the currently available blockchains to confidentially communicate with one another, but there are various approaches for enabling the interoperability of blockchain infrastructures.¹⁹ Here the goal is an “Internet of Blockchains”, in other words a way to network all blockchains analogously to how computers are now able to network over the Internet. Such blockchain-to-blockchain communication could, for example, be achieved by combining public and private blockchains to create applications for special requirements. Various initiatives striving to develop such an Internet of Blockchains have joined together in the Blockchain Interoperability Alliance (BIA). The BIA is studying ways to enable transactions and communication among various blockchains and working to develop a global industry standard and a protocol architecture for blockchain-to-blockchain networks.

One such approach to enabling communication between blockchains already exists: Blocknet, which builds so-called XBridges to enable communication, interaction, and exchanges between nodes on different blockchains. Among other things, it is working to make it possible to swap various cryptocurrencies for one another without the need for an official exchange, as well as sharing of any other data or smart contracts.

Another technology based on an alternative approach is Cosmos. The underlying idea here involves “zones” and “hubs”. Zones are individual, autonomous blockchains, and hubs are special blockchains that connect multiple zones (see also Figure 11). The blockchains can exchange information via the hub without the need for every block to establish a direct link to every other blockchain that it wants to communicate with.

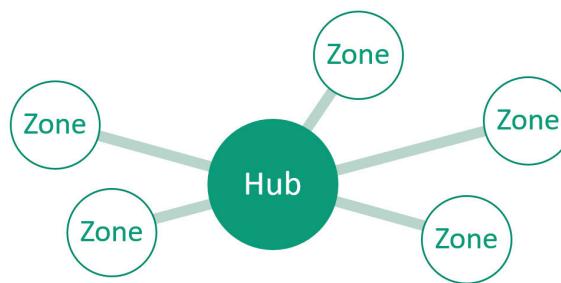


Figure 11: Schematic of Cosmos-based blockchain-to-blockchain communication via hubs and zones

The challenges for achieving blockchain interoperability range across several levels. Besides the purely technical level, which involves enabling the exchange of tokens such as cryptocurrencies and standardizing smart contract languages, it is also vital to con-

¹⁹ Underwood, Communications of the ACM 2016, 15.

sider syntactical, organizational, and legal aspects. The syntactical goals include cross-blockchain identity management and interoperability of smart contracts, the organizational level is about governance aspects and mapping of processes, and the legal level mainly addresses the validity and effectiveness of the underlying agreements and possibly whether these are correctly implemented at the technical level.

3.5.2 ISO standards

The International Organization for Standardization (ISO) is currently developing 11 standards on blockchain and distributed ledger technologies. The ISO/TC 307 technical committee has working groups devoted to the technological foundations; smart contracts and their applications; security, privacy and identity; governance; and the interoperability of blockchain and distributed ledger technology systems, among others.

3.5.3 Sidechains

A somewhat simplified way for blockchains to communicate is sidechains. A sidechain is a blockchain that is connected to and exists alongside a master chain, which can have multiple such sidechains. Tokens of a cryptocurrency can be transferred from the master chain to a sidechain and used there, then later moved back to the master chain. One major advantage of sidechains is that they can be used to achieve greater efficiency and scalability: shifting transactions to them increases the throughput of the original chain.

3.6 Trends

Despite being a relatively young enabling technology, blockchain has evolved dynamically since the advent of Bitcoin. In particular, new blockchain platforms have emerged that are universally usable or specially tailored to business applications, or make use of alternative data structures that are not based on blocks linked in a linear chain in order to manage transactions more efficiently and securely. Some other trends are discussed in the following.

3.6.1 Certification

Smart contracts are transparently and immutably stored in a blockchain and substantially boost confidence in it. They support the automation of processes and play a key role in enabling cooperation between business partners.

It is not always possible for business partners to create and check smart contracts, but they can benefit greatly from joining blockchain networks. It is therefore desirable for there to be libraries of vetted smart contracts. These libraries will contain both generic all-purpose smart contracts and application-specific smart contracts. One approach that is being discussed is that of establishing certification agencies for smart contracts. However, these are a less-than-ideal compromise because they wind up acquiring the status of central authorities.

Today's smart contracts can only be read by IT specialists. It would be a good thing if non-specialists could also read and understand them. Approaches are therefore now being developed for making smart contracts readable by ordinary people²⁰ or supporting the semiautomated translation of contractual documents into equivalent smart contracts.²¹

It appears to be technically feasible to achieve legal security with frameworks while limiting the design possibilities, with so-called Ricardian contracts providing legal security for lawmakers. When formulating legal texts, care would need to be taken from the start to ensure that the rules can be translated into and executed by software. But it is more realistic to assume that only agile (and therefore temporary) legislation, contracts, and the guidelines and rules of official inspection agencies can qualify as Ricardian contracts.

3.6.2 Quantum computing and blockchains

The security of blockchain and DLT infrastructures is based on algorithms for encrypting data and cryptographic methods such as one-way hash functions. So far at least, their security can only be broken with enormous computing power and is therefore not in any imminent danger. But the capabilities of conventional computers are steadily increasing, and new technologies like quantum computing are also on the horizon that may change this situation. It is possible that powerful quantum computers will, to some extent at least, endanger the security of the usual cryptographic methods that blockchain and distributed ledger technologies are based on, such as hash functions, asymmetrical encryption (public-key cryptography), and symmetrical encryption. This will affect nearly all digital services across the board, since digital signatures, for example, are also based on asymmetrical encryption and/or hash functions. However, quantum computers with sufficient computer power to break these codes are not expected to become available until five to 10 years from now at the earliest. And it is safe to assume that new, more secure alternatives to the currently used cryptographic methods will be found by then. If the power of conventional computers continues to increase, it is conceivable that the cryptographic puzzles used will also be made harder to solve in response or that the length of public or private keys or hash values will be scaled up. At the same time, new cryptographic methods are being developed that will also be safe from quantum computers. This area of research is referred to as post-quantum cryptography.²² Apart from this, in the unlikely case that the currently used cryptography became vulnerable to attack and no suitable new methods could be found, not only DLT itself but in fact all value transfers over the Internet would have to stop. It can therefore be concluded that DLT is not particularly threatened by quantum computers. The only difference between conventional systems and blockchain, the software of which can be continually updated to reflect the current state of technology, is that in blockchain it is not possible to retroactively alter already stored data. This important difference and its implications, especially for data protection, is discussed in greater depth in section 4.3.2.3.

²⁰ Hazard/Haapio, Proceedings of the 20th International Legal Informatics Symposium IRIS 2017, p. 425.

²¹ Frantz/Nowostawski, IEEE 1st International Workshops on Foundations and Applications on Self* Systems 2016, p. 210.

²² Bernstein/Buchmann, J. (ed.), Dahmen E. (ed.), Post-Quantum Cryptography 2009, p. 1.

3.6.3 Identification of DLT-appropriate business processes

The basic technology of DLT paves the way for a large number of possible applications (see also section 4.2.5). Yet it is often hard for organizations to tell which of their business processes could benefit from blockchain or DLT. The first comprehensive frameworks for this have already been developed. The work cited here describes and compares some of them and presents a two-stage framework.²³ This is helpful for choosing business processes, defining the parameters of the DLT implementation, and assessing the associated benefits. A technical framework that extends to cooperation by multiple parties, provides performance incentives, and supports selection of a platform is described in Osterland, 2018.

²³ Klein/Prinz/Gräther, Reports of the European Society for Socially Embedded Technologies 2018, p. 1.

4 Socioeconomic Foundations

Digital products and services change the everyday lives and activities of individuals, companies, and society in general. The impacts of digitalization are becoming increasingly clear, obliging organizations all of the world to respond to changing business rules and models. Today, more people have access to mobile telephones than to toilets,²⁴ and at least one out of five people on the planet has an actively used Facebook account.²⁵ Digitalization is changing established business rules in both the digital and the physical world and affecting all areas of life. Recent examples include Uber, the world's largest taxi company, which has no vehicles of its own; YouTube, allegedly the world's most popular media provider, although it produces none of its own; Alibaba, the world's largest retailer, which dispenses with warehouses; and Airbnb, the world's largest provider of accommodations, which owns no real estate. DLT is another type of digital technology that accelerates and strengthens, instead of curbing, the changes, opportunities, and risks for society and business that come with digitalization. These technologies therefore first need to be classified in the context of digitalization before investigating their potential and the prospects for the spread and implementation of their innovations.

4.1 Characterization of DLT Within the Scope of Digitalization

DLT is widely regarded as a groundbreaking innovation.²⁶ The (further) development of its constituent parts (e.g. consensus mechanisms) permits the use of DLT for many basic applications. However, in order for many of its envisioned and potential applications to be implemented, various emerging technologies have to come together. In the following, three key technologies are presented that have strong synergies with DLT: the Internet of Things (IoT), Artificial Intelligence (AI), and privacy-preserving computation.



Integrated View of Blockchain Technology

The Internet is a global (digital information and communication) network of networks, while the Web, formally also called the World Wide Web (www), is a collection of information. This information can be accessed with the aid of technical artifacts such as browsers. The Internet may therefore be regarded as basic infrastructure, while the Web is an application running on this infrastructure. Analogously, DLT (which is in turn also based on the Internet) is an infrastructural technology on which various other applications can be implemented. For these applications, DLT is often used in combination with other technologies, which necessitates an integrated view of this technology in the context of a larger technological landscape.

²⁴ UN News, World Book Day: New UN report spotlights potential of mobile technology to advance literacy.

²⁵ Thomas Halleck, Facebook: One out of every five people on earth has an active account.

²⁶ Klein/Kottbauer, Strategien erfolgreich entwickeln und umsetzen.

4.1.1 DLT and the Internet of Things

4.1.1.1 The Internet of Things is changing business and society

Digitalization requires companies to fundamentally reconsider their existing business and operating models against the background of digital technologies.²⁷ Digital technologies are also becoming faster and less costly. One digital technology that is considered to have enormous potential across multiple applications is the Internet of Things (IoT). In the IoT, physical objects are equipped with sensors, actuators²⁸ and computational power and linked to the Internet. The resulting smart things are becoming increasingly autonomous and helping to merge the digital and physical worlds. At the same time, smart things of this kind are enabling completely novel interactions among companies, things and individuals as well as innovative business models based on newly available data and ever-greater networking.²⁹ It is estimated that by the year 2020, over 50 billion smart things will be connected to the Internet and thus to one another, potentially adding eight trillion U.S. dollars of value.³⁰ There are already diverse examples of the Internet of Things, manifested in smart homes, smart mobility or smart factories.³¹ For instance, a smart thermostat makes it possible to adjust the indoor temperature at home while still on the road. An appropriately designed thermostat with self-learning capabilities can adapt to the daily schedules of a home's occupants in order to save energy. All of the activities of these intelligent devices, as well as all information that they capture on their surroundings, exist in the form of machine-readable data. Data of this kind are increasingly finding their way into private and business processes. Smart things and the data they generate or collect will belong to different players. The existence of these data and interest in using them as a resource for processes will thus also lead to the accumulation of increasing data volumes, and with them ownership, in the hands of certain players. It will not always be possible to assume that these players trust one another—in fact, their trust is likely to diminish as the presumed value of these data grows.

Smart things form the basis of the Internet of Things. To illustrate this, let us take the example of an agricultural machine.³² Its original function, such as plowing fields, has long since evolved further. Now the machine can also send local weather, soil, or machine data to manufacturers or farmers, who then use (semi-)automatic processes to analyze and evaluate them and base actions on them. This gives rise to new possibilities, like in the case of predictive maintenance. This makes it possible, for instance, to predict the anticipated wear to heavily used machine parts and reduce downtimes while boosting utilization and thus also productivity. Performance metrics such as daily output can be determined in the same way. In the described example, the machine is capable of more than simply transmitting data. It can also be controlled via the Internet, and this can be extended to include simultaneously controlling and coordinating a whole fleet of machines. The machine can even use data from other machines, farms

²⁷ Porter/Heppelmann, Harvard Business Review 2014, 1.

²⁸ Actuators are components that convert electric signals (which are usually output by control units) into changes in physical parameters such as mechanical movements or temperature, thus enabling active control of processes.

²⁹ Oberländer/Röglinger/Rosemann/Kees, European Journal of Information Systems 2018, 486.

³⁰ Macaulay/Buckalew/Chung, Internet of Things in Logistics.

³¹ Borgia, Computer Communications 2014, 1.

³² Porter/Heppelmann, Harvard Business Review 2014, 1.

or companies. By networking with agricultural and weather systems, it can access new external functions with potential for further development (e.g. weather forecasting) and autonomously optimize their use. At an industry's former perimeters, smart systems will be networked to forge "systems of systems".³³

4.1.1.2 The Internet of Things requires an integrated technology architecture

Even if the value added by the IoT only manifests itself at the customer interface, or when using smart things in operational processes, companies must first meet the technological prerequisites in-house. In this context, various technology architectures are being discussed, all of which share similar levels.

In all of these architectures, a physical object equipped with sensors, actuators and computational power is regarded as the foundation of the "thing level". Being connected to the Internet, smart things can also interact with various other players in their environment—such as individuals, companies, or other smart things. An important attribute of smart things is their ability to potentially integrate data from different sources and process them on the basis of Web-based and therefore interoperable standards. Captured data can be used, for example, to design innovative services. Since the innovative character of smart things manifests above all in the form of combinable (information) services, the topmost level of technological architectures is typically a service level.

4.1.1.3 The Internet of Things is the basis for using DLT in the physical world

DLT is predestined to make the interfaces between the thing, interaction, data, and service levels of the Internet of Things more secure. The previously cited example of smart homes is excellently suited for illustrating this and applying it to the industrial Internet of Things. Besides various advantages, however, the IoT also poses diverse risks that need to be dealt with. The 10 biggest security risks in the context of the IoT include, for example, identity theft, installation of malware on devices, altering of (system) information, theft or manipulation of log data, and theft of personal information.³⁴ In many cases, distributed ledger technologies—with their inherent resistance to manipulation, redundancy, and reliability—can significantly reduce these.

The risk of identity theft can, for example, be diminished with zero-knowledge proofs (see section 4.1.3). It is possible to make it more difficult to install malware by using DLT to prevent unauthorized devices from contacting the system. Alteration of system data can be made much more difficult by distributing them across different physical and virtual systems via a DLT layer. In this scenario, based on the current state of technology and research, the cost of manipulating appropriately decentralized log data is discouragingly high. These issues also exist in the industrial context and can, like the security risks present in private contexts (e.g. smart homes), also be addressed with the aid of DLT.

³³ Porter/Heppelmann, Harvard Business Review 2014, 1.

³⁴ Ali/Awad, Sensors (Basel, Switzerland) 2018, 1.

If the risks described above are reduced to the point where the Internet of Things becomes secure enough for productive use, in both private and business contexts, then the IoT can also serve as the basis for using DLT in the physical world. DLT can model the transition between human/machine and an omnipresent service level. Here the main focus is on using DLT to raise the trustworthiness of data generated in the IoT.

Whereas DLT is currently being used above all to implement cryptocurrencies and capital market transactions, it is already clear now that this technology can and will also serve as an enabler for the Internet of Things. This is the case because DLT has potential for substantially reducing the security risks (as described in the previous section) of machine-to-machine communications in the IoT. It is therefore highly probable that DLT will be widely used in this environment. In conjunction with the rapidly falling cost of IoT devices, this may also be the first "real" contact that most people have with DLT. If this technology really takes off in the market as a result, it will come to play a major role in the everyday lives of many people. The high coverage that can be achieved by combining DLT with the Internet of Things will also boost the relevance of DLT. The core task or function of DLT in this context is to instill confidence in the interactions that smart things have with individuals, other players, and other smart things that were typically unfamiliar with one another before starting to interact. It would theoretically be possible to deploy the IoT without DLT and DLT without the IoT. But the two technology packages appear on the whole to have potential for generating considerable synergies when used together.

4.1.2 DLT and Artificial Intelligence

4.1.2.1 The future-oriented technologies of DLT and AI are converging

Artificial Intelligence (AI) is increasingly developing into an important driver of digitalization. AI is an umbrella concept for machines that simulate human intelligence, embracing abilities like thinking, learning, and self-correction, among other things.³⁵ Two kinds of AI can be distinguished. The label of "strong" AI is applied to systems that possess or even surpass the intellectual capabilities of a human. For solving application-related problems, however, "weak" AI is (initially) more important. Methods borrowed from mathematics and informatics are used to design these systems while systematically striving to reproduce aspects of human intelligence. They can perform a wide variety of tasks and are already being used for many purposes. Examples include self-driving vehicles and personality detection.

Both Germany and the EU have acknowledged the importance of Artificial Intelligence for industry and society, and each of them has drawn up a corresponding AI strategy. For defining the EU's AI strategy, in April 2019 a group of experts presented "ethics guidelines for trustworthy artificial intelligence".³⁶ These require trustworthy AI to meet seven prerequisites, including "privacy and data governance", "transparency", and "accountability". They clearly reflect the goals and potential of DLT in connection with AI, suggesting that AI could take major strides forward in conjunction with DLT. In general terms, it is true that DLT is able to increase the potential uses of AI by instilling trust

³⁵ Bitkom, Künstliche Intelligenz.

³⁶ European Commission, Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran.

between players that have hitherto been unaware of each other. But AI will also directly impact the development of DLT in many areas. The complementary characteristics of DLT and AI make it likely that the overlap between these two revolutionary technologies will steadily grow in the future. In the following, this will be illustrated with examples while explaining its relevance for meeting the requirements for "trustworthy AI".

4.1.2.2 DLT as the database for AI

Data play a central role in the use of AI. The availability of data is an essential factor in all AI-related applications (e.g. for detecting patterns that permit contextual conclusions to be drawn). When data are used by AI, it often adds economic value. At the same time, however, both private individuals and companies want data sovereignty, in other words control over how their data are used or at the very least appropriate financial or other compensation. With the aid of DLT, there is now a technical means of leaving data under the sovereignty of private persons or companies and only selectively granting access to them on the basis of prior agreements, without authorizing any third parties to assign, alter or suspend the corresponding rights.

This can be illustrated with an appropriate example from the context of smart homes. A private individual generates data in their household (smart home or smart city). These data are plainly of a personal nature³⁷ (e.g. power consumption, online shopping and television watching habits) and unfiltered access to them by third parties such as companies should not be possible unless they have received permission to do so. On the other hand, the private person could, the next time they make an online purchase, allow temporary access to the television set's utilization data for the last three months in return for a discount, for example so that a company could use them for AI-based data analysis. The DLT can provide support for selectively granting permissions of this kind to different companies and documenting them. This enables the companies to use the data for improving their products. In addition, the DLT can be used to verify the source of the data and, under certain conditions, their integrity as well.³⁸

4.1.2.3 DLT as a recording platform for AI

When machines interact with people or other machines, errors will still continue to occur in records. As already discussed, a trustworthy infrastructure is a prerequisite for integrative cooperation. This is so because if any of the players suffers damage, loss or harm,³⁹ it should or must be clarified who is responsible for what. If the risk that cases of this kind will occur is assessed as too high with no possibility of clarifying them, the players will have little interest in collaborating. So it ought to be very difficult or ideally impossible for intelligent, increasingly autonomous players in particular (artificial intelligences) to re-interpret or even retroactively alter data of authorized stakeholders. At the same time, humans often have difficulty grasping how AI processes arrive at their decisions. DLT provides a way to reliably document the activities and decisions of artificial intelligences. The properties of DLT make entries transparent and safe from after-the-fact tampering, thus permitting reliable clarification of accidents, cases of fraud etc.

³⁷ For the legal definition of personal data, see also section 5.2.2.

³⁸ An example application is available from the company of Ocean Protocol (<https://oceanprotocol.com/>).

³⁹ This could initially be merely a suspicion by a player who asks whether something has proceeded in accordance with the applicable rules and laws.

by consulting the stored information. The records can be used to investigate conspicuous actions at a later point in time.

This can be illustrated with an example from the field of self-driving vehicles. Suppose that two such vehicles have a collision that causes considerable damage. To clarify the sequence of events leading to the accident and determine whether either or both was to blame, it is necessary to study the recorded data and the actions of both vehicles that were derived from them. DLT eliminates any risk that these data could have been manipulated. Say, for example, that it was reliably recorded that one of the vehicles sent a warning signal but the other never received it—and was therefore unable to process it and respond appropriately. The investigation of the accident's cause can now focus on the interruption in communication (which may have been caused by outside interference, for example), since the AI in question is cleared of any suspicion of wrongdoing. In such a case, of course, the basic prerequisite is regular recording of data or references in a suitable DLT infrastructure.

4.1.3 DLT and privacy-preserving computational methods

The most successful DLT systems to date, including Ethereum and IOTA, are public DLT solutions. So that they can unfold their full potential, data privacy should be just as important for information of a general nature that deserves protection as it is for personal data. Otherwise it is doubtful whether companies would work with a public DLT solution if data they regard as worthy of protection become public and transparent as a result. There is then a very real danger that competitors could obtain confidential information and use it for their own purposes. The transparency of data stored in DLT systems thus makes it desirable to also use a kind of complementary technology that technically enables and supports the privacy of data in DLT-based systems. There have been many calls for only "pointers" to be stored in blockchains, with all other data remaining in private "off-chain" databases. This applies especially to public blockchains. In this context, so-called privacy preserving computational methods are being discussed. In actual fact, cryptography-based approaches of this kind have been around since the late 1970s. Although they also exist independently of DLT, they have attracted a great deal of attention more recently, undergoing developmental leaps forward and being applied to other applications. In recent years, research in this field has greatly accelerated and become more focused. As a result, the technologies of DLT and privacy preserving computation are cross-pollinating one another.

Privacy preserving computational methods add value because they can be added to practically any DLT solution as an extra layer, analogously to DLT forming an additional stratum on top of the Internet. So-called "zero-knowledge proofs", a special case of secure multiparty computation, are relevant methods, or actually classes of methods. These are sketched in the following to demonstrate the relevance of their (co-)development with DLT solutions.

Secure multiparty computation (SMC) protocols are a class of algorithms that allow a group of mutually distrusting parties to evaluate functions (calculation rules) without having to disclose their private inputs. The best-known example is the "Millionaire's Problem": two parties want to know which of them is richer (i.e. to solve a "greater than function") without revealing their actual wealth (input). This problem was first solved with "Yao's Principle", which was published in the 1970s, i.e. considerably before the first DLT application debuted. Yao's Principle and other algorithms based on it are

widely used for both public and private DLT solutions to verify calculations by two or more parties without requiring them to put their private data in the DLT layer. An instructive example of an SMC protocol is secured distributed addition.⁴⁰ If three persons A, B and C possess the private numbers a , b and c and want to add the three together without any of the participants learning the private number of the others, this can be accomplished as follows: A chooses another, secret random number r and adds it to a . Since r is unknown to B, it is impossible for B to reconstruct the number a from the sum $r + a$. Now B adds his private number b to the sum and passes the result $r + a + b$ to C. Finally, C adds c to it and passes the result to A, who is the only one who knows what r is. A subtracts r and now knows the sum $a + b + c$, which he or she tells to the other two participants. Other methods exist to boost the confidence of B and C in case they doubt that A has given them the correct result. These can be cryptographic or simply involve swapping the roles of A, B and C to let them repeat the procedure in order to test whether they obtain the same result in every constellation. Most SMC protocols, of course, are far more complex. The remarkable thing about SMC is that it is DLT itself, with its inherent transparency and the issues around private data discussed above, that makes it so intriguing. Conversely, DLT provides the IT infrastructure needed to implement SMC, thus rendering it practicable. Certain special cases of SMC—so-called zero-knowledge proofs—are receiving particularly great attention in connection with DLT solutions.

Zero-knowledge proofs (ZKPs) are methods for proving attributes of data without revealing what they are. This makes it possible to store only such proofs in DLT systems without any actual input data. An intuitive negative example is a password that, without ZKPs, would have to be revealed in order to demonstrate that a party is authorized to access something. To verify that a user is authorized, it is easy to compare an entered password with one that is present in plain text. But a password of this kind is not stored in a (public) DLT system, since it could otherwise be read by every node of the network and would no longer be secret. ZKPs make it possible to check whether a user knows a certain password without the need to enter the password itself in the DLT system. A zero-knowledge proof can be imagined, for instance, as replying to a series of special yes/no questions that can only be answered correctly with knowledge of the password but cannot be used to deduce the password. In this case, the probability of guessing the correct answer to any given question correctly is 50%, but if there are enough of them then the likelihood of getting them all right by pure chance is extremely small. Due to the required repeated exchanges between a party claiming to know the password and the mechanism demanding sufficient proof, such ZKPs are also referred to as interactive. These types are not especially well-suited for DLT systems, however. So-called zk-SNARKs (= zero-knowledge succinct non-interactive argument of knowledge), by contrast, can dispense completely with interactions and are therefore a significantly better choice for use in DLT contexts. They are also mathematically more complex than interactive ZKPs.

The interesting thing about ZKPs is that this technology can provide proofs in general—i.e. not just for verifying passwords, but also, for example, for showing that data have certain attributes or that a calculation has been correctly executed. ZKPs and

⁴⁰ Schneier, *Applied Cryptography*.

especially zk-SNARKs can be used to check the correctness of calculations without the need to actually perform them. Even better, nothing is learned about what has been done, only whether it has been done correctly. Despite the fact that this technology holds great promise and could play a very important role in DLT, today it is still regarded as too compute-intensive to be practicable for many uses. That will change. While an enormous amount of research continues to be devoted to DLT itself, ZKPs also appear to be extremely important due to the potential benefits of this technology. They deserve further study to exploit their potential for ensuring the required privacy of information in public DLT solutions.

4.2 The Potential of DLT

4.2.1 Status quo

Worldwide, enormous potential is ascribed to DLT. Various quantitative assessments of the economic potential of this technology have been published in recent years. However, due to its newness, the difficulty of comparing it with other developments, and the rapid pace of technical and economic advances, it is difficult to corroborate them. One prominent study by the World Economic Forum, for example, postulates that by the year 2027 an estimated 10% of the global gross domestic product will be stored on blockchain technology. Potentially, according to this forecast, goods and assets worldwide could be linked to a DLT application and exchanged via it while deriving benefits from its properties.⁴¹ Gartner Inc., a market research company, estimates that the global introduction and use of blockchain technology could generate business value of about 3.1 trillion U.S. dollars by the year 2030 in the information technology sector alone.⁴² Overall the credibility of this estimate should be taken with a grain of salt, however, since it hinges on many assumptions regarding its future development.

In order to leverage the enormous growth potential being dangled in front of them without allowing competitors to gain an innovative edge, companies are investing huge sums in the development of DLT solutions. According to figures published by the market research company IDC, in 2017 about 950 million U.S. dollars were spent on DLT solutions and around 1.5 billion U.S. dollars in 2018. As shown in Figure 12, the annual outlay will climb to about 11.7 billion U.S. dollars by 2022. The USA will account for the lion's share of this, roughly 4.2 billion U.S. dollars.⁴³

⁴¹ Global Agenda Council on the Future of Software & Society, Deep Shift: Technology Tipping Points and Societal Impact.

⁴² Panetta, Gartner Top 10 Strategic Technology Trends for 2019.

⁴³ Statista, Blockchain.

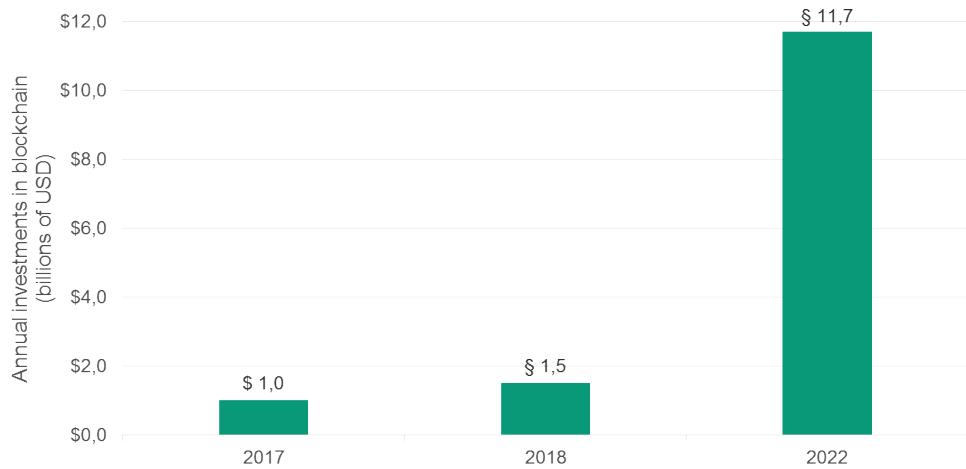


Figure 12: Expected annual expenditure for blockchain (in billions of U.S. dollar)

In this context as well, it should be noted that the estimates of different market research institutes vary considerably. While Tractica puts the worldwide market volume of DLT at 20.3 billion U.S. dollars in the year 2025,⁴⁴ WinterGreen postulates that the market volume could reach 60 billion U.S. dollars by the year 2024,⁴⁵ and the analysts of MarketsandMarkets expect the global blockchain market to be worth 23.4 billion U.S. dollars in the year 2023.⁴⁶

The number of blockchain-related patent applications confirms that companies are very interested in this technology and channeling a great deal of creativity into it. At the time of this writing, since 1999 no fewer than 3,021 patent families have been registered that are either directly related to DLT or address the technology's technical foundations. The first patent applications in the second category, dealing with aspects such as Merkle Trees or distributed and decentralized ledger systems, were submitted long before the invention of the Bitcoin blockchain in 2008. Conspicuously, the number of new patent applications submitted increased explosively in the years 2014 to 2016, rising by between 143 and 231 percent. Of the 3,021 mentioned patent families, 1,581 were from China and 951 from the United States. Europe took fifth place with only 131 patent applications.⁴⁷

The field of cryptocurrencies (see section 4.2.5.6) is also increasingly attracting attention. By the end of 2013, the market capitalization of all cryptocurrencies together amounted to about 10.3 billion U.S. dollars. Of the total of 63 cryptocurrencies on which this estimate is based, Bitcoin alone had a market capitalization of around nine billion U.S. dollars. In 2017 the Bitcoin euphoria peaked, driving the market capitalization of all then existing cryptocurrencies to approximately 614 billion U.S. dollars. The prices then crashed and continue to fall steadily. As of February 24, 2019 the market capitalization of all cryptocurrencies amounted to around 127 billion U.S. dollars.

⁴⁴ Tractica, Enterprise Blockchain Revenue to Surpass \$20 Billion by 2025.

⁴⁵ Shah, Global Blockchain Market Could Reach \$60 Billion by 2024, Shows Report.

⁴⁶ MarketsandMarkets, Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Supply Chain Management, and GRC Management), Organization Size, Industry Vertical, and Region - Global Forecast to 2023.

⁴⁷ Acs, Blockchain Innovation.

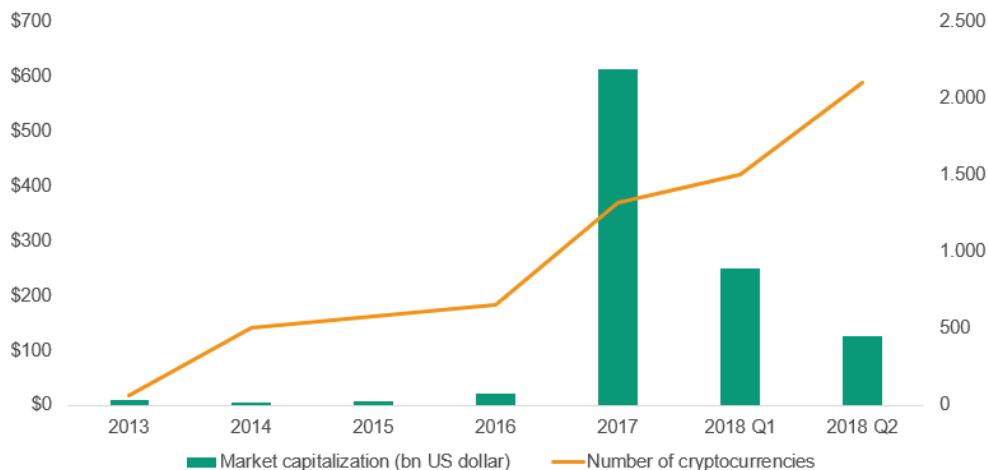


Figure 13: Market capitalization and number of all cryptocurrencies⁴⁸

Where cryptocurrencies are concerned, other trends are also increasingly impacting the financial industry. One of these, which is most pronounced in the United States, involves endeavors by financial service providers like SolidX and VanEck to launch bitcoin-based exchange-traded funds (ETFs). An exchange-traded fund tracks the value of a specified asset, in this case bitcoins, or a whole basket of underlying investments. A bitcoin ETF makes it possible to invest in a cryptocurrency without actually owning bitcoins.⁴⁹ If such an ETF is approved, it will provide not just private investors but also international investment funds with a simplified way of investing in bitcoins. Until now, investors have had to either directly purchase the currency and manage it with special software, or else acquire it via currency exchanges. Currently the U.S. Securities and Exchange Commission (SEC) is investigating the possibility of approving bitcoin ETFs. It cites considerable obstacles to approval due to the fact that the bitcoin cryptocurrency is largely unregulated and the applied-for bitcoin funds do not adequately comply with the SEC's rules for preventing fraudulent and manipulative behaviors.⁵⁰ Cryptocurrencies are a controversial topic in general. According to the Dead Coins database, a total of 934 different cryptocurrencies have failed to date. At least 680 of them were simply abandoned, but 182 were proven scams and another 60 were hoaxes or parodies. Twelve currency systems have been sabotaged by hackers.⁵¹

Interest in so-called initial coin offerings (ICOs) is also on the rise. These are a way to fund business ventures with cryptocurrencies. As of 2019, a total of about 14.2 billion U.S. dollars has been raised with ICOs. Figure 14 shows that the total capital raised each year with ICOs is increasing fast. This is mainly because the growing popularity of ICOs allows individual players to rake in significant amounts of venture capital. For example, in 2018 a startup called Block.One released a cryptocurrency called EOS and took in 200 million U.S. dollars.⁵² It is interesting to observe that about 79%, or roughly

⁴⁸ Own depiction borrowing from and based on data from *CoinMarketCap*, Historical Snapshots.

⁴⁹ Reiff, Bitcoin ETFs Explained.

⁵⁰ Marquette, Crypto-based funds crawl toward mom and pop.

⁵¹ Dead Coins, Curated List of cryptocurrencies forgotten by this world...and more.

⁵² ICOdata.io, ICO Status.

6.2 billion U.S. dollars, of the total raised with ICOs in 2018 was collected during the first half of that year. This makes it clear that this is not necessarily a stable, rising trend. The fact of the matter is that the sums gathered with ICOs are subject to substantial fluctuations, similarly to the cryptocurrencies themselves. The figures presented by different studies also vary. According to a study by Ernst & Young, for example, ICOs raised 15.5 U.S. dollars in the first half of 2018.⁵³ More information on ICOs is provided in section 4.2.5.6.3.

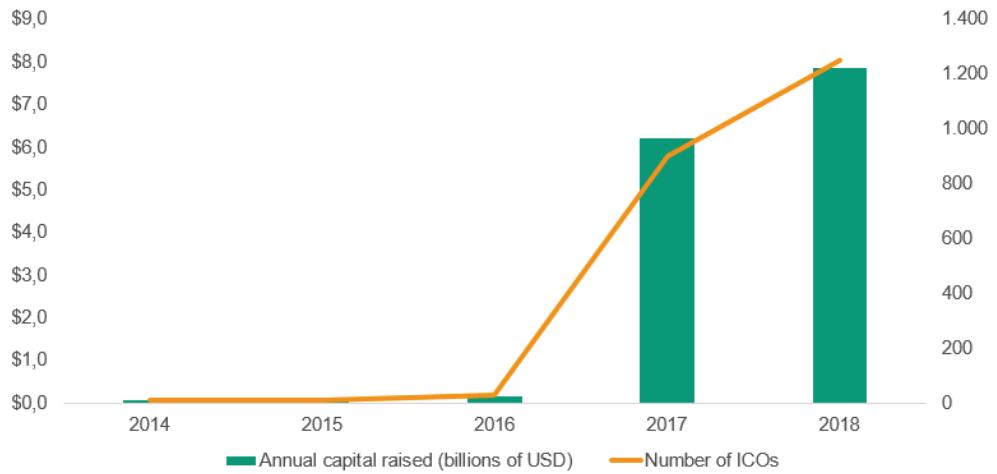


Figure 14: Number of ICOs and total capital raised per year in billions of USD⁵⁴

In Germany, an extensive DLT ecosystem spanning both research and business has emerged. However, the majority of the initiatives are still devoted to developing prototypes or conducting proofs of concept. So far only a few solutions are being used productively. As a result of these developments, however, blockchain experts are in great demand. Between August 2016 and August 2018, 737 relevant new positions were created at startups, plus another 790 at other companies. During this period, the interest in blockchain professionals quadrupled at large enterprises.⁵⁵ In an international comparison, German is a relatively attractive place for these experts to seek employment, since on average only 18 candidates compete for each job opening, a relatively low figure. By comparison, in the USA about 57 individuals looking for blockchain-related employment vie for each DLT job vacancy.⁵⁶ These positions typically require excellent technical skills. To meet the growing demand for developers and other specialists, efforts are being made to disseminate relevant knowledge (training, research, and companies). The first dedicated programs are appearing, including one for a master's degree in blockchain and DLT at the Mittweida University of Applied Sciences in Germany. The blockchain laboratory of the Fraunhofer Institute for Applied Information Technology (FIT) is also facilitating the release of research findings to the economy.

In addition, both companies and governments worldwide are launching numerous initiatives to promote and study DLT. Startups are experimenting with innovative busi-

⁵³ Ernst & Young, Initial Coin Offerings (ICOs): The Class of 2017 – one year later.

⁵⁴ Based on ICOdata.io, ICO Status.

⁵⁵ Joblift, Nach Startups entdecken auch Konzerne die Blockchain: über 1.500 Stellen rund um die innovative Technologie in Deutschland.

⁵⁶ Müller, study on the international job market.

ness ideas, and established companies are evaluating—both internally and in consortia—possible uses for this technology within specific industries and across multiple sectors. Government initiatives are supporting these activities with promotional programs or studying the potential of this technology for use in public administrations.

4.2.1.1 Startups

A large and lively ecosystem of young startups with business models around DLT has emerged, as a 2018 study documents: about 179 new firms have so far been established across various sectors in Germany. It is also plain that innovation hubs like Berlin, which accounts for 89 of the startups in question, is an extremely attractive environment for these ventures.⁵⁷ In fact, it boasts one of the world's largest and most important DLT scenes. With such a high concentration of startups, Berlin also accounts for a large share of the German professionals working in this field.⁵⁸ Munich is Germany's second-largest blockchain hub, with 23 startups as of this writing.

4.2.1.2 Consortia

In the corporate context, distributed ledger technologies have potential for use as a tool for supporting collaboration between enterprises (see section 4.2.5.4). Consequently, the creation of DLT solutions also encourages inter-company cooperation as well as initiatives to develop standards and infrastructures for solutions of this kind.⁵⁹ It therefore makes sense that consortia embracing both established companies and startups are appearing in the DLT ecosystem with increasing frequency. These include consortia that primarily pursue technological goals as well as business-focused consortia formed to investigate possibilities for leveraging DLT in a specific industry.⁶⁰ There are also consortia that, like R3, straddle both categories.

The goal of technology-focused consortia is to make DLT usable by different companies for a widening range of applications. To accomplish this, they apply technical standards, e.g. for architecture and performance and scaling specifications. Examples of consortia of this type include Hyperledger, Ethereum, and IOTA. The International Organization for Standardization (ISO) should also be mentioned in this context. Although it is an independent international association and not a consortium of companies, it belongs in this category on account of its technology-focused goals. Currently 11 different standards are being developed for aspects of blockchain and DLT, including terminology, architecture, and the legal validity of smart contracts.⁶¹

Business-focused consortia are now predominantly arising in the financial sector and in the fields of mobility and energy. An example of a consortium in the financial industry is Bankchain in India. Among other things, it is studying DLT applications in a special software environment with the goals of minimizing fraud in the financial sector while also increasing the efficiency, security, and transparency of financial services.⁶² Along-

⁵⁷ BTC-Echo, *Der deutsche Blockchain Index*.

⁵⁸ Müller, *Studie über internationalen Arbeitsmarkt*.

⁵⁹ Gratzke/Schatsky/Piscini, *Banding together for blockchain*.

⁶⁰ Virmani, *18 blockchain consortia you should know about*.

⁶¹ International Organization for Standardization, *Standards Catalogue ISO/TC 307*.

⁶² For more information, see <http://www.bankchaintech.com/index.php>.

side consortia that are focused on a certain industry, there are also cross-industry consortia, with the Climate Chain Coalition being a case in point. It takes its orientation from the long-term goals of the Paris Agreement and systematically supports the development of DLT solutions that will help combat climate change.⁶³

4.2.1.3 Established companies

More and more established players are exploring the possibilities of DLT. Prototypical implementation of blockchain solutions and development of Proofs of Concept for specific applications are therefore steadily increasing. Because most companies possess relatively little in-house DLT expertise, however, they investigate applications with the help of consultants or work with other initiatives within the scope of a consortium. In 2018, for example, IBM teamed up with 45 customers from various industries to develop DLT solutions. Cooperation with Maersk, a logistics group, for example, led in August 2018 to the go-live of the DLT-powered TradeLens platform, which enables more efficient management of shipping processes.⁶⁴ In addition, a trend is becoming noticeable for companies to take advantage of the blockchain-as-a-service (BaaS) offerings of large cloud providers like Microsoft, Amazon, IBM, and SAP. This enables them to leverage technologies for automating, protecting, or optimizing their processes without having to build their own DLT infrastructure.⁶⁵

The breakdown of the blockchain market shown in Figure 15 reveals that in 2018 the financial sector accounted for the largest share of the total market value of blockchain solutions, at 60.5%.

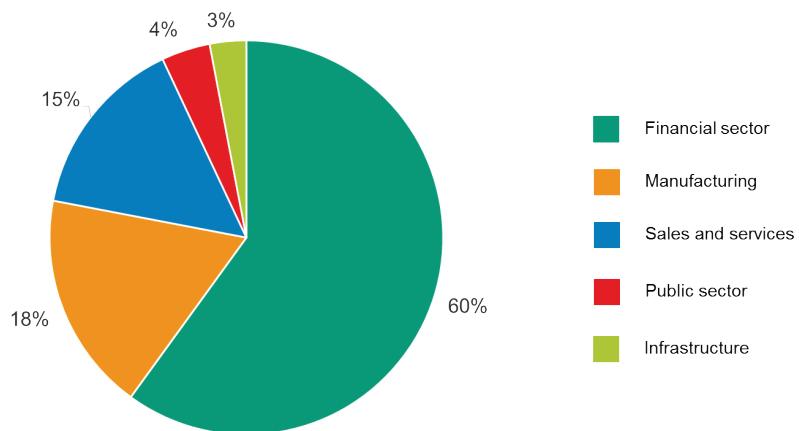


Figure 15: Blockchain market value breakdown by economic sectors in 2018⁶⁶

The Tractica market research agency predicts that the five most important markets for DLT applications will be the financial sector, manufacturing, the public sector, health,

⁶³ For more information, see <https://www.climatechaincoalition.io/>.

⁶⁴ Bajpai, IBM and Blockchain: What It Did In 2018, and Where It's Going In 2019.

⁶⁵ Joos/Karlstetter, Blockchain-as-a-Service im Unternehmen nutzen.

⁶⁶ Statista, Blockchain.

and insurance.⁶⁷ Here too, of course, it should be noted that forecasts of future potential are difficult to get right.

So far the potential of DLT has mainly been recognized by startups and large corporations, so it is hard to assess the extent to which small and medium-sized businesses will also benefit from this technology. Tellingly, in a survey carried out by YouGov 43% of questioned decision-makers at medium-sized enterprises stated that they were not familiar with any of the common uses of distributed ledger technology.⁶⁸

4.2.1.4 Public initiatives

More and more government initiatives are being launched to address DLT. This could be due to two factors. For one, countries have an understandable interest in identifying the potential of DLT for their government institutions. Studies conducted on this have revealed that governments would like to use DLT solutions to store critical information of residents on digital identity cards or similar instruments. These could then be used to identify them unambiguously, reliably and verifiably to facilitate access to digital services.⁶⁹ The other is that public initiatives are gaining momentum because they have an interest in making sure that technologies develop there and not elsewhere, along with the associated expertise and jobs.

Also at the EU level, public initiatives are being organized to promote DLT. The "European Blockchain Partnership", for example, is a framework that makes it easy for the 28 member states to share information on the international uses of the technology at the governmental level.⁷⁰ Within an even larger framework, the EU Blockchain Observatory and Forum is monitoring current activities and trends in the European DLT ecosystem.⁷¹

4.2.1.5 Summary

In Germany, efforts to promote and regulate DLT are only just getting started. The regulation of cryptocurrencies in particular is increasingly coming into focus (also in other countries). A positive aspect here is that in most cases, these regulatory measures do not yet go as far as restraining the innovative potential inherent in blockchain technology. Right now, Berlin is the most attractive location for DLT startups. This needs to be encouraged by closely networking this budding industry with companies, scientific institutions, and government. However, Germany is also competing with aspiring new venues such as Malta that have intentionally created favorable conditions including a regulatory framework and a DLT strategy, with the goal of attracting young startups. For example, a regulatory framework for DLT and cryptocurrencies is now being worked on there with the goal of creating transparency and legal security. The Malta Digital Innovation Authority, which was set up in February 2018 to address DLT and AI, among other things, has placed digital innovations high on its agenda. The blockchain-related topics addressed by this institution include creating regulatory con-

⁶⁷ Tractica, Enterprise Blockchain Revenue to Surpass \$20 Billion by 2025.

⁶⁸ YouGov, Umfrage zur Bekanntheit von Einsatzmöglichkeiten einer Blockchain im Mittelstand 2017.

⁶⁹ Lyons/Courcelas/Timsit, Blockchain for Government and Public Services.

⁷⁰ European Commission, European countries join Blockchain Partnership.

⁷¹ EU Blockchain Observatory and Forum, About the European Union Blockchain Observatory and Forum.

ditions that are conducive to certifying DLT platforms and legalizing the use of smart contracts.

Here it is vital for Germany to keep up and not lose the lead that it now enjoys in this field. Regrettably, the country's universities are not releasing enough graduates with appropriate DLT expertise into the job market. Due to the nature of this technology, it is especially important to promote programs that address the interface between at least two of the following disciplines: business, law, informatics, and possibly engineering as well. In addition, there is a need for Germany's ministries to launch project-based programs to encourage the development of DLT infrastructure solutions, which would be inconceivable without these technologies. Programs of this kind should be modeled after consortia to underscore the interdisciplinary character of DLT.

Cooperation within the scope of the European Blockchain Partnership, the establishment of the EU Blockchain Observatory and Forum, and the European Blockchain Services Infrastructure (EBSI) initiative are important steps in the right direction. This collaboration and these initiatives constitute a favorable framework for establishing common foundations and conditions not just for promoting, but also for actively shaping the future evolution of DLT in the EU. It is imperative for the establishment of this partnership to be followed by energetic action in the legal, economic and political realms. Collaboration on all of these levels must be intensified further to ensure that the required contributions can be made.

In this sense, it is essential to additionally intensify this cooperation at all levels, which will also favor the developments in the field of DLT. The cross-border startups, consortia, initiatives and organizations that already exist depend on having a consistent legal and commercial environment in which to operate and clearly defined parameters to guide them.

4.2.2 The blockchain value proposition: trust

Following the so-called Internet of Information, the Internet of Services, and the Internet of Things, DLT is being hailed as the enabler of the fourth generation of the Internet: the Internet of Trust.⁷² In other words, DLT has come on the scene with the value proposition of instilling trust.

Trust is a desirable state that can be described as a valuable asset,⁷³ because trust must be acquired and upheld. After all, trust is not necessarily permanent, because there is always a risk of losing it again. Trust can arise in the context of an interaction between at least two parties, e.g. persons, institutions or organizations, and is typically required in situations in which one party relies on "the other party to not take advantage of what the first initially provides."⁷⁴ In other words, a giver trusts a taker to reciprocate. With stronger mutual trust, general insecurity diminishes. In this way, trust helps reduce complexity, because it is impossible for anyone to absorb and process all potentially available data, thus reducing imbalances and overcoming information deficits.⁷⁵

⁷² Prinz, Blockchain and CSCW – Shall we care?

⁷³ Beck, Die Finanzkrise ist auch eine Vertrauenskrise.

⁷⁴ Beck, Die Finanzkrise ist auch eine Vertrauenskrise.

⁷⁵ Römer/Tscheulin, Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 2008, 434.

Trust opens the way for cooperation, which can in turn increase the effectiveness of economic activities.⁷⁶

Especially as a result of digitalization and the growing importance that platform economies have for our society, there is an increasing need to create digital trust characterized by security, identifiability and traceability. After all, for example, purchased software can turn out to be harmful, an involved party can pretend to be someone other than they really are, or contractual agreements can be difficult to understand and implement. The opportunities that platforms like Uber or Airbnb provide for offering and using services are creating an ever-greater need for trust, since the parties that conclude contracts are now increasingly private individuals instead of companies.⁷⁷ Platforms usually only act as mediators and brokers. Here DLT can provide the required identifiability and traceability for creating digital trust, thus extending or supplementing the feasible limits of trust.

In these times, different kinds of trust can arise in different ways. Systemic trust, for example, is often instilled by way of institutions⁷⁸ and "... accounts for the phenomenon of individuals placing trust in social systems, organizations and institutions."⁷⁹ These institutions are normally active in a certain sector of the economy, like the European Central Bank in the financial services sector, or across multiple industries, like TÜV certification facilities. When a product is certified by such an institution, buyers trust the certificate and thus also the product's quality. Certification thus engenders trust. Another way that trust can arise is in response to someone's reputation.⁸⁰ The more trustworthy someone has been in previous interactions, the more trustworthy they are assumed to be in future interactions. Reputational systems based on this principle can now be encountered in many online situations:⁸¹ when purchasing merchandise in online shops, when selecting a hotel at a holiday destination, or when choosing a nearby physician.

The major trust-building institutions of our society include banks. After all, their clients entrust a great deal of information to them and also trust them to manage (at least part of) their wealth. Nearly all of a bank's clients trust it to perform the task of transferring a sum of money to another party on their behalf and assume that the money they keep there is exposed to only minimal risks, if any.

This trust in the global banking system took a beating during the financial crisis of 2007/2008. Several banks also collapsed in Germany, prompting Chancellor Angela Merkel and Peer Steinbrück, who was then the finance minister, to publicly reassure the population that their savings were in no danger.⁸²

⁷⁶ Beck, Die Finanzkrise ist auch eine Vertrauenskrise.

⁷⁷ Mattila/Seppälä, Digital trust, platforms, and policy.

⁷⁸ Public institutions responsible for certain tasks to benefit or increase the wellbeing of individuals or society in general.

⁷⁹ Bruckner, Organisationales Vertrauen initiieren.

⁸⁰ Beck, Die Finanzkrise ist auch eine Vertrauenskrise.

⁸¹ Here it should be noted that especially this kind of trust tends to be abused, as shown by the increasing talk about fake evaluations posted by paid service providers instead of actual customers.

⁸² Spiegel Online, Merkel und Steinbrück im Wortlaut.

Bitcoin, a DLT-based currency, was developed at least partly in response to the events before and during the financial crisis, when confidence in the world's financial markets and banks was badly shaken.⁸³ ⁸⁴ In DLT systems, trust is no longer created via institutions, but instead by the DLT system itself, whose architecture enables transparent access to information, thus making it possible to reduce asymmetrical information and directly perform peer-to-peer interactions while dispensing with a mediator. Trust thus acquires a different basis: confidence in the protocol, algorithm or code.

Peer-to-peer interactions are also already possible on other, non-DLT-based platforms. For example, it is possible for private individuals to rent accommodations or purchase used objects from other private individuals. However, in these cases their interactions are technically executed by a mediator, namely a platform operator. The associated trust therefore involves confidence that the operator will execute the transactions as wished and is able to resolve conflicts, and this trust is supported by reputation systems in which all of the participants can be evaluated. But the operator can also change the rules, reduce transparency, and control competition on the platform to suit his own interests.

DLT enables direct peer-to-peer interactions without the need to place trust in an institution (i.e. a mediator). Instead, trust in the DLT system itself is the basis. This trust is greatly strengthened by the fact that the system is distributed, immutable, and transparent. Due to the unchangeable nature of entries, which are stored in the nodes of a distributed network, all participants (or possibly only certain authorized participants) know that information, once stored in this way, can no longer be altered. The (desired) degree of transparency of a particular system can be increased by stored information. Moreover, the "rules" are predefined for all system participants, in other words all processes obey the rules of the DLT protocol and are not influenced by the vested interests of a platform provider. Ultimately, the trust in such a network is derived from confidence in the underlying (technical) system, its rules, and how it is implemented. In addition, smart contracts provide a way to implement a wide range of interactions and modes of cooperation to maintain this trust, in a relatively dynamic manner, in previously unforeseen situations. This trust in the program code is expressed by the maxim that "the code is law": the program code defines the rules of cooperation, after-the-fact changes are impossible, and execution is automated.⁸⁵

The case of a money transfer can serve to show the difference. Normally, when someone wants to send money to another person, the transaction is handled by one or more institutions, which are typically banks. The parties at both ends of the transaction—the sender and the receiver—trust that the institutions in the middle will correctly execute it as follows: sender -> bank -> bank -> receiver. In a DLT system, however, there is no mediator, i.e. no institution that handles the transaction. Instead, it is carried out directly "peer-to-peer" (sender -> receiver). The two parties trust the system to carry out the transaction correctly. The rules for doing so are clearly defined in advance and cannot be altered by individuals.

⁸³ Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

⁸⁴ Otte, Die Finanzmärkte und die ökonomische Selbstbehauptung Europas.

⁸⁵ Filippi/Hassan, First Monday 2016, 1.

Nevertheless, this principle also carries inherent risks. For one thing, program code is often very context-specific and therefore less flexible than legal contracts (or laws, for that matter). There is no or only very limited room for interpretation. In particular, there is a risk that implementations may contain errors or bugs. Probably the best-known example of a defective implementation is the infamous "DAO hack": thieves took advantage of a loophole in the programming of a "decentralized autonomous organization" (DAO) to steal about 50 million U.S. dollars' worth of the Ether cryptocurrency. This incident also unleashed a debate within the Ethereum community about whether "the code is law" principle also applies to programming mistakes.

Cases like this can shake confidence in a system. In many cases it is virtually impossible for ordinary users to tell whether or not such a system has weaknesses. However, this statement also applies analogously to mainstream systems: users have an equally hard time judging whether today's institutions really deserve their trust or if their platforms are compromised by competition or reputational mechanisms.

DLT provides a novel way to build trust, namely on the basis of confidence in the technology, its underlying concept, and how it is implemented. Here it should be noted that a certain degree of blind faith is also required in the case of DLT. However, it is shifted from the involved persons, institutions and organizations to the DLT protocol and its consensus mechanism.

DLT can thus either displace or complement other trust-building mechanisms. It would be conceivable, for example, for the use of blockchain to prompt established institutions, like banks or TÜV certification facilities, to become more transparent and comprehensible.

It is also imaginable that utterly new ecosystems will emerge or that existing ones will be replaced further down the road. It is even possible that different trust-building mechanisms will meaningfully complement one another in shared ecosystems in the future. For instance, it would appear to make sense for DLT systems to be supplemented by reputation systems to generate as much trust as possible.



The DLT Value Proposition

Further study is required to illuminate the interplay of established, trust-instilling mechanisms with DLT. The questions here include whether DLT exists alongside and complements existing mechanisms or could potentially replace them. If so, in which circumstances would this happen? And to what extent does DLT change how trust is acquired? What trust-related risks are inherent in DLT? An illustrative example is Sovrin, which enables self-sovereign digital identities. DLT can also increase “trust” between institutions such as ministries, educational institutions and so on with which citizens have a classic relationship of trust. Smart contracts can both increase and endanger trust: on the one hand they document processes, which helps make sure that inputs are deterministically and verifiably converted into outputs (“white box”). On the other, they can be marred by programming mistakes; for example, the concurrency of these scripts (= the ability to execute different parts of them in any order without changing the final result) is often overestimated. Hackers have exploited weaknesses in the recent past, and it is likely that there will be more cases of this kind. Thought should be devoted to whether certification agencies for smart contracts would increase confidence in these or instead aggravate the community’s mistrust of “centralistic” mechanisms and institutions.

4.2.3 Generic roles of DLT

In contrast to software for performing specific tasks, like a wage accounting system, DLT should be understood as software with an inherently infrastructural character. The corresponding systems do not constitute business models in their own right; instead, they provide a basis for implementing applications and possibly business models.

In most cases, a decision to use a DLT-based IT solution is made for economic or organizational reasons, not technical ones. Because DLT uses redundant data storage and program execution (smart contracts), it is technically inferior to a centrally organized system in terms of performance and scalability, at least so far. Its advantage is the ability to digitally implement processes that, in the past, required the involvement of a trustworthy central authority. Nevertheless, its use does not necessarily make sense in all scenarios. On so-called platforms, beneficial network effects typically increase for all parties as the number of participants grows on both the supply and the demand side. As a result, a small number of platform providers wind up dominating the entire market. Experience has shown that these monopolistic platforms take advantage of their dominance to erect barriers to the market entrance of new competitors (“data silos”) or charge inappropriately high utilization fees. The B2B economy in particular is permeated by a fundamental skepticism of or aversion to platform operators, who could potentially dominate the market. In the long term, centralized solutions generally pose threats to free competition, with the associated disadvantages for final customers. Consequently, in most cases the reason for using DLT is economic in nature: namely to prevent monopolies. It is not always necessary or sensible to dispense entirely with centralized structures, however. In this context, it is important to ask whether a combination of existing trust-inspiring mechanisms and DLT would work. Generally speaking, DLT can directly create trust between parties while effectively replacing intermediaries and raising integrity in connection with data and processes. DLT

can assume various roles for implementing processes. In a possible generic classification, for instance, it can play the role of improver, transformer, or enabler.⁸⁶

4.2.3.1 Improvers

First of all, DLT can improve existing processes that are already being executed without any intermediaries via bilateral (peer-to-peer) interfaces (which can be digital or non-digital). Here the emphasis is mainly on attributes that previously could not be implemented as well or were implemented using conventional paper-based processes. They include, for example, retroactive protection of stored data in centralized systems from manipulation and digital modeling of paper-based processes with smart contracts.

4.2.3.2 Transformers

Second, DLT is able to transform and streamline existing processes that were previously executed with the involvement of classic intermediaries. In these cases, the focus is on its trust-instilling character as a system for distributed coordinated and integral modeling of direct interactions. A hypothetical example of how this technology can serve as a transformer is the execution of escrow agreements via smart contracts.⁸⁷ Whereas in the past third parties have served as escrow agents and provided corresponding guarantees, the details of certain agreements can now be implemented in the program code of a smart contracts with autonomous distributed execution of functions like disbursing certain sums of money.⁸⁸

4.2.3.3 Enablers

Third, DLT can pave the way for implementing innovative systems that were not technically feasible in the past. Frequently, these systems enable or improve direct interactions between different parties. These services, which are often generic in nature, can be integrated in a wide range of applications. An example of DLT in the role of enabler is the implementation of new kinds of (digital) identification systems (digital identities) that can be used as modules across applications for selectively releasing information without violating the privacy of individuals (the keyword here is informational self-determination).

At an interorganizational level, DLT can enable the execution of tamper-resistant transactions between mutually mistrustful network participants. It can thus provide a basis for controlled cooperation among competitors to benefit customers. Until now, this has only been possible by means of trustworthy intermediaries or strict regulation. Even in the absence of trust, DLT can, at the technical level, enable fair, transparent behavior by multiple participants, thus potentially rendering intermediaries and strict regulation obsolete.

⁸⁶ Shen/Pena-Mora, IEEE Access 2018, 76787.

⁸⁷ See also the general technical discussion and the special section on shipping documents.

⁸⁸ However, here it is important to note that the logic of the escrow agreement must be modelled in software.

Another general scheme for classifying the uses of DLT is based on the attributes of this technology as used in different cases.⁸⁹ Tamper-resistant recording of data and coordination of cross-application processes take priority here. Of importance are DLT's abilities for dealing with data or commands in connection with access management, modelling direct interactions between different parties, and implementing collective decision-making mechanisms.

4.2.4 Developmental stages of the Internet

DLT provides a digital infrastructure for implementing a variety of services and applications. In this context, it may be regarded as the next stage in the evolutionary development of technological infrastructures. The nature of digital content (software, media, and data of all kinds) is such that it can be easily and freely reproduced almost without marginal costs. Until now, it has therefore been out of the question to execute digital value transactions without the involvement of a central controlling function. This has not affected the sharing of information, however, which is why the Internet as originally conceived may also be referred to as the "Internet of Information". Once information-driven services had been enabled, the next step was to implement cyber-physical systems that integrate physical objects with the digital world to extend their abilities. The Internet gained a large number of new applications in this way. This trend has culminated in the "Internet of Things" (see section 4.1.1). In the context of the invention of Bitcoin, solving the double-spending problem provided the foundation for a broader ecosystem: DLT now also enables, on the basis of the Internet of Information, direct transactions without the need to rely on or trust another party. In this context, the terms "Internet of Trust" and "Internet of Values" are often used. It is notable here that DLT can also enable interactions between nonhuman parties, thus also broadening the Internet of Things.

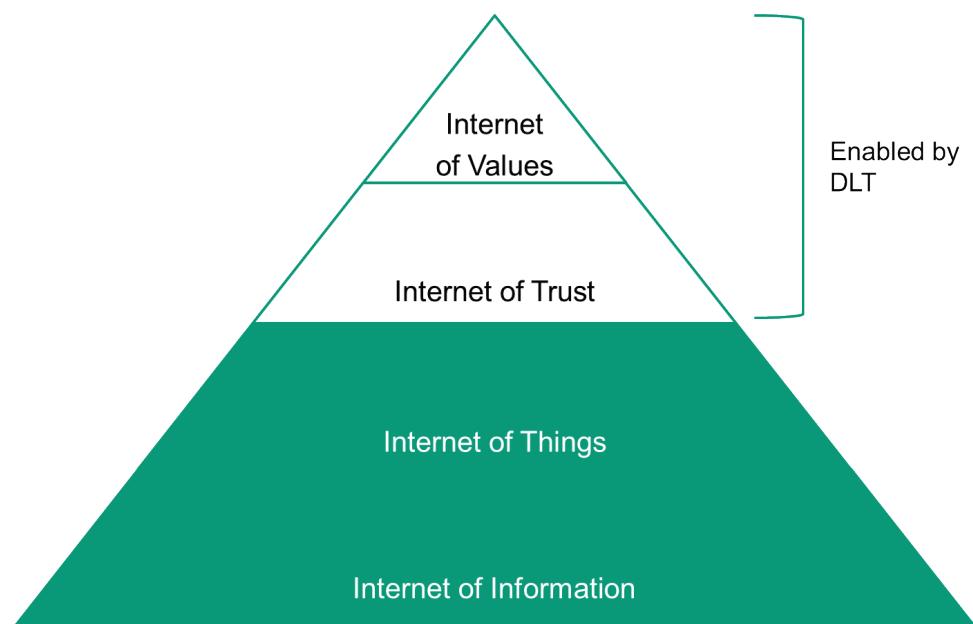


Figure 16: Developmental stages of the Internet (own depiction)

⁸⁹ Shen/Pena-Mora, IEEE Access 2018, 76787.

4.2.5 Application categories

It does not make sense to use DLT for purely technical reasons, since it is less efficient than centralized systems due to the cryptographic methods used (especially for mining in DLT systems with the Proof of Work consensus mechanism), redundant execution of smart contracts, and redundant data storage.^{90,91} But the fact of the matter is that, in most cases, the use of a distributed solution is not motivated by economic or organizational considerations. For example, processes can be made more efficient by directly creating trust without the involvement of central operators.⁹²

The potential applications of DLT are diverse. Correspondingly, this technology is being discussed and tested across nearly all industries and areas of society. The applications are all specific, yet certain patterns can be discerned that we will refer to in the following as *application patterns*. These application patterns generalize specific applications by bringing together recurring attributes that can be encountered across industries or sectors. Application patterns are not averse to being split; a given application can belong to multiple application patterns. Application patterns constitute an intermediate level between specific applications on the one hand and abstract concepts, such as "instilling trust", on the other. This will help us understand the wide range of possibilities for using this technology. As already mentioned, in this connection it can be observed that each individual application pattern could also be implemented by centralized systems. The question as to whether DLT is an apt solution to a given problem that is described as an application pattern can only be answered on a case-to-case basis and is—as explained in the foregoing—more of an organizational issue than a technical one.

4.2.5.1 Neutral platforms

Alongside emerging informational asymmetries and data silos, monopolistic platforms based on centralized infrastructures pose additional challenges. The associated issues around governance and the use of data increase in complexity as more companies join the platform. Moreover, mistrust and fear of dependency on a central operator often lead companies to shun platforms that actually make sense in terms of their processes. Currently existing quasi-monopolistic platforms, especially in the B2C market (e.g. Facebook), impressively demonstrate this "winner takes all" principle. As a rule, companies try to avoid falling into a dependent situation like this, striving instead to prevent the rise of monopolistic platforms in their industries.

Neutral platforms that use DLT as an infrastructure make it possible to implement business processes between different organizations via a neutral technological platform that is designed to prevent improper behavior on the part of individual participants. DLT, by virtue of its distributed nature and (in some implementations) transparency, makes it feasible for the platform to be jointly coordinated and administered by

⁹⁰ This could even be formulated as a theorem: supposing there were a distributed system that is "better" than a centralized system, this distributed system could be integrated in ("built into") a centralized system to create a centralized system that is similarly efficient and able to perform its tasks.

⁹¹ See also section 4.3.2.1.

⁹² See also section 4.3.

its participants. The defining paradigm is that the platform is not available to an individual company, being based instead on a distributed approach. Of course, for such a platform to work it is necessary, for example, to define responsibilities for development and maintenance. However, no operator of a centralized platform of this kind profits from running it and strives to turn it into a monopoly. A platform of this kind can, for instance, be used to automate (interorganizational) processes with smart contracts. The advantages of a platform economy can thus be enjoyed without having to tolerate the disadvantages of sharing it with a potential monopolist. Such neutral platforms can also host digital applications in the form of marketplaces, games or other applications or provide an environment for digital ecosystems.

4.2.5.2 Forgery-proof documentation

One of the fundamental properties of DLT systems is their immutability, which prevents or at least documents any retroactive manipulation of data stored in them (e.g. documents, contracts, machine protocols etc.). The use of a DLT system thus permits the establishment of a credible log for various kinds of information that all participating parties can view. This can also make it possible to access stored data for auditing or other purposes. For example, it is conceivable to trace access by certain individuals to sensitive data in a DLT application and prevent unauthorized access. For this purpose, however, as a rule actual data are not stored in DLT systems but only their hash values,⁹³ which can be used to confirm that a document available outside the system already existed in exactly the same form at an earlier point in time.

4.2.5.3 Payments

Payments are probably the use of DLTs that the public is most familiar with. The most prominent examples are cryptocurrencies like Bitcoin. DLT creates a way to make digital payments without having to resort to intermediaries such as the banking system. Two parties can then directly make payments to one another without the need for a detour via their banks or a service provider such as PayPal. The entire transaction is conducted “peer-to-peer” via the DLT infrastructure, and even very small sums can be transferred.⁹⁴ The use of such direct value transfers can make sense in many scenarios, often supplementing other functions provided by a DLT system.

4.2.5.4 Management of cross-organizational processes

Processes between companies, or business-to-business (B2B) processes spanning multiple enterprises or organizations belonging to a value creation network, are—often in order to protect business secrets, but also due to a lack of standardization—typically afflicted by system and media fragmentation and consequently a marked lack of trans-

⁹³ A kind of “digital fingerprint” of data, see 3.1.4.

⁹⁴ With Bitcoin and Ethereum, due to the (currently) high market value of these cryptocurrencies the transaction costs are also quite high (amounting to several euros per transaction), thus making micro-transactions too expensive. Public systems, which are intended to be virtually free of transaction costs, are now being studied; a prominent example is IOTA. For non-public systems (e.g. Ripple), there are already solutions that minimize energy consumption and therefore also do not have any transaction fees worth mentioning. A priori, the costs incurred when executing digital transactions via conventional banks are negligible compared to the overhead consisting of administrative costs etc.

parency. In some interorganizational situations like this, a centralized solution emerges (e.g. operated by a process participant with considerable market power) and integrates the data and businesses processes of all of the other participants. In practice, however, this only occasionally succeeds, while giving already-strong market players even greater opportunities to exert influence. In many cases, the background is not necessarily technical challenges, but rather political and economic issues. In the case of a centralized solution, a single company or organization must take responsibility for establishing and running the system, thus also gaining an advantage over its rivals within the value creation network in terms of access to information. Data silos frequently also result. An alternative to monopolistic platforms like this can be neutral platforms implemented with DLT. They are described in depth in connection with the next application pattern.

Rapid distribution of information to all of a DLT network's members makes it possible to coordinate processes across organizations. Once process information has been written into the DLT system, it can be utilized for triggering subsequent processes. This can thus potentially slash the duration of gaps between processes. The well-considered use of smart contracts on DLT systems can also enable automatic monitoring of processes and eventually also (partial) automation of selected process steps.

To cite an example, the logistics industry is typically characterized by a large number of different process participants who are involved in the successive stages that stretch from the start to the finish of a supply chain. Frequently, the data generated in connection with production, packaging, inventory, transportation, customs, storage and security management can only be rendered transparent after a considerable delay, if they are communicated at all.⁹⁵ These information deficits and asymmetries result in inefficiencies and waits. Private DLT systems, for example, would be a way to improve the flow of information between process players. Information on progress made while traversing the process can, for instance, be tamper-resistantly modelled in a chronological register. Job tickets, invoices, certificates of origin, and customs documents can all be documented more easily while ensuring their integrity and security. At the same time, processes spanning multiple organizations can facilitate cooperation by all of the companies involved in the flow of goods.⁹⁶ This shows that DLT-based IT, serving as a distributed, transparent and tamper-resistant infrastructure, can be a valid alternative for improving intercompany collaboration within the scope of shared processes, thus increasing the transparency of information and reducing inefficiencies in how the participating companies work together.

4.2.5.5 Digital identities

Many applications require digital versions of physical things (so-called digital identities or digital twins⁹⁷) for representing persons or objects in the digital world. These digitally model attributes and actions of a person or object to subsequently permit digital

⁹⁵ Christopher/Lee, Mitigating supply chain risk through improved confidence.

⁹⁶ Gilbert Fridgen/Sven Radzuwill et al., 51st Annual Hawaii International Conference on System Sciences (HICSS) 2018, 1.

⁹⁷ The term "digital twin" is used in this study, but "digital shadow" would actually be more precise because an object's digital image is not a full simulation but only metadata of the real object in the digital world.

interactions with that person or object.⁹⁸ DLT provides a way to define identities of this kind. Unambiguous, validated and sovereign identities can make it considerably more difficult to commit identity theft and manipulate data in other ways.

The German Federal Office for Migration and Refugees has already taken the initiative in this regard. It is currently investigating the possibility of creating unique digital identities for refugees that would facilitate administrative processes.⁹⁹ The common ground with cross-company processes is also evident here: it would be relevant to have unambiguous digital identities that could be used for processes across multiple government institutions. It would also be technically possible to accomplish this with today's centralized systems. But considering that several thousand facilities are involved, it would be difficult to implement in actual practice. The use of a DLT application has potential for establishing digital identities of this kind in a single, all-embracing infrastructure.

4.2.5.6 Digital documents

Analogously to the idea of digital identities, other objects or assets in the real world can also be represented by tokens, thus mirroring—like today's legal documents—ownership of property, for example. Such a digital document (the keyword is tokenization) digitally models attributes of an object. The digital document then makes it possible to denominate and trade objects, such as assets, in (almost) any way. The digital document thus constitutes an alternative to paper-based documents, which are typically difficult to manage in terms of preventing forgeries—by ensuring that they can be validated anywhere and anytime—and document logistics. This can open up new applications that would involve too much effort to implement today, while also making existing applications more efficient or less prone to fraud (e.g. possibly also for American depositary receipts, which have been attracting criticism for tax fraud since late 2018).

Thanks to DLT and tokens implemented on it, for the first time digital value and digital property can thus be divided up without the need for an intermediary. No exact definition of DLT tokens exists yet. The concept of digital tokens originated in informatics, where tokens were used as a means of identification and authentication. Basically, a DLT token is linked to value or authorizations. These can include voting rights, assets, or services, among others. The use of DLT tokens as a general cryptocurrency is a prominent application, e.g. for bitcoins. In addition to functionally differentiating tokens, they can also be distinguished on the basis of their tradability. Tradable tokens are also referred to as fungible, and non-tradable tokens as nonfungible. Precisely these nonfungible tokens cannot be transferred. This is important in connection with digital identity documents, among other things, since these are usually tied to a certain person or object. In recent years a large number of new digital token systems have appeared, since such tokens can enable new forms of corporate, startup and project funding. This is accomplished by issuing them via various paths to investors. The most common approach is a so-called ICO (also often called a "token generating event"). It involves the use of smart contracts to issue tokens that are paid for using a fiat currency (e.g. EUR or USD) or cryptocurrency. Tokens, which have primarily originated in

⁹⁸ See also section 4.2.4.

⁹⁹ Florian Guggenmos/Jannik Lockl et al., Informatik-Spektrum 2019, 1.

connection with such ICOs, open up a host of technological and economic possibilities due to the fact that they can be very flexibly configured. For example, they can be issued in the form of utility, security or equity tokens, which are discussed in the following in greater detail.

4.2.5.6.1 Classification of tokens

Over the course of the last few years, many different kinds of tokens have appeared, and as a result this phenomenon has also become a focus of scientific research.¹⁰⁰ Several different schemes now exist for classifying tokens. However, the goals achievable with tokens and the corresponding possibilities for their use have not yet been conclusively identified. Three basic types of tokens can be distinguished: cryptocurrencies, utility tokens, and security tokens. The oldest kind of token is cryptocurrencies, which are used as digital money—among other things, for purchasing goods or services. By contrast, a utility token can have a variety of functions. For example, it can confer authorization for someone—e.g. its owner—to access something (similarly to an admission ticket) or serve as a “value container” for paying or rewarding a user for behaving in a certain way. Security tokens, finally, are corporate shares that include the right to receive dividends or a share of profits. This last type of token in particular is now in the sights of regulatory institutions because tokens that are equivalent to securities fall (in Germany) under the Securities Trading Act and as such are monitored by the Federal Agency for Financial Services Supervision.¹⁰¹ So far, however, no uniform legal framework for tokens exists for the EU or Germany. Overall, there is still a considerable need for study and political action in this area.

4.2.5.6.2 Cryptocurrencies

Cryptocurrencies are an example of digital tokens. Common to digital currencies (regarded here as a superordinate category) is that they are used as a medium of exchange, value depository, or accounting unit.¹⁰² For example, they can be exchanged for physical goods or services, among other things. Their use may be limited to an online location such as a casino or an airline website. In this context, they are also designated as virtual currencies. Bitcoin initiated the spread of a new type of digital currency, namely so-called cryptocurrencies. It was inspired by the financial crisis of 2007. At that time, the world's central banks flooded the markets with fresh money, causing the value of physical currencies to plummet. In that situation, a person or group of people known by the pseudonym of Satoshi Nakamoto developed a new currency that was independent of banks and countries and therefore could not be centrally controlled, dubbing it Bitcoin. Cryptocurrencies thus differ from other digital currencies in that they are based on a distributed network. By March 2019, there were more than 2,000 different cryptocurrencies¹⁰³ broadly based on DLT. One advantage that cryptocurrencies have over conventional means of payment is that they permit fast execution

¹⁰⁰ Oliveira/Zavolokina/Bauer/Schwabe, *To Token or not to Token: Tools for Understanding Blockchain Tokens*.

¹⁰¹ Blockchain Bundesverband Finance Working Group, *Statement on Token Regulation with a Focus on Token Sales*.

¹⁰² Monetary Authority of Singapore. 2018. Crowd Genie Financial Services pte. ltd.: Incorporated in Singapore. <https://eservices.mas.gov.sg/fid/institution/detail/201066-CROWD-GENIE-FINANCIAL-SERVICES-PTELTD>.

¹⁰³ <https://coinmarketcap.com>.

of transactions across countries. While the banking system can take up to several days to complete an international transaction, cryptocurrencies provide a unified system in which transactions can be handled worldwide within seconds or minutes. Sweden and China are taking very innovative approaches by having their central banks develop their own cryptocurrencies. The director of the International Monetary Fund, Christine Lagarde, also underscored their potential and future importance by proposing a digital currency in October 2017.¹⁰⁴ On the other hand, one characteristic of current cryptocurrencies that has often been criticized is the fact that their value often fluctuates greatly. This topic is illuminated further in section 4.2.5.6.4.



Legal Status of Tokens

The legal status of tokens should be clarified in the near future to eliminate the insecurity surrounding this issue. Once this is done, the obligations of token owners and companies that issue them will come into focus. This should probably begin in the realm of securities and tax law. Schemes for classifying tokens should be expanded and developed further to create a basis for identifying their legal status. Unless and until this is done, there is a risk that Germany will lose talented individuals, experts and entrepreneurial potential to other countries able to offer appropriate legal security.

4.2.5.6.3 Initial coin offerings (ICOs)

An ICO is a way to raise capital, and from the perspective of the financial markets can be directly compared with a traditional initial public offering or crowdfunding. ICOs are also referred to as a kind of fund raising that uses blockchain to implement the underlying idea of crowdfunding¹⁰⁵ without relying on intermediaries such as banks. In contrast to classic crowdfunding, no third parties are involved in concluding contracts or handling monetary transfers. ICOs are therefore also described as "truly peer-to-peer"—i.e. they do not rely on any intermediaries. In an ICO, an investor receives tokens in return for a deposited investment. The investment takes place as an exchange of cryptocurrencies. An investor sends, for example, a number of bitcoins to a project's network address and receives in return a corresponding number of the tokens associated with the project, based on a defined exchange rate. New tokens are often created on a DLT system with the aid of smart contracts. The equivalent value and functionality behind an invested token can vary depending on the ICO's design. The generic functions of tokens have already been described in detail. The revenues obtained via the ICO are available in full to fund the development project. ICOs thus strive to provide incentives for private individuals to invest in the technology. Because the "blockchain community" is self-organized and unregulated, black sheep often take advantage of the situation. With fake initiatives that often involve blockchain in name only, they attempt to fraudulently obtain money from unsuspecting investors. In 2018, for example,

¹⁰⁴ Schulze, 'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency.

¹⁰⁵ Crowdfunding is a type of funding in which a group of individuals or organizations fund projects by pooling their resources.

a Vietnamese company calling itself Modern Tech scammed some 32,000 investors for 660 million U.S. dollars with an ICO for "Pincoin".¹⁰⁶ The open, global nature of blockchain and ICOs make it difficult to regulate and even harder to "prohibit" schemes like this at the national level. Overall it is imperative to study more exhaustively the conditions under which ICOs can be a sensible way for startups and established companies to raise money, as well as how investors can be more effectively safeguarded from fraudsters.

4.2.5.6.4 Value fluctuations

As a rule, the value of tradable tokens depends on supply and demand in the market. Their value (and especially that of cryptocurrencies) therefore fluctuates often—not least because of the large numbers of speculative investors interested in this sector. Since tokens are often used as an incentive to actively participate in operating DLT systems, these value fluctuations are problematic. As described in section 3.3.1, calculations performed by smart contracts often cost something in the applicable currency. Due to pronounced fluctuations in their value, the costs for executing applications implemented on their basis are difficult to forecast, which is problematic in economic terms. This can provide negative incentives, especially in the case of utility tokens, which are inherently based on the idea of usefulness and can, for example, be used to pay for services within the network. This idea is often at odds with the idea of participation in the ecosystem, which in many cases is also inherent in the same tokens. For example, in some ecosystems a token can be used to buy goods or services, but its value fluctuates. Using tokens increases their value, but this value is lost at the same time. In addition to tradable tokens, whose value is directly determined by the market, there are also models in which tokens are pegged to the value of other objects such as fiat currencies.

4.2.5.7 Providerless services

Forward-looking concepts are often discussed in connection with DLT, and they should at least be mentioned here. One frequently encountered idea is that of a decentralized autonomous organization (DAO). This is understood as a form of organization that is based exclusively on DLT and whose rules (and business processes) are entirely implemented as smart contracts. For example, a DAO has no management in the conventional sense; instead, all decisions are made by shareholders.

 **Decentralized Autonomous Organizations (DAOs)**

Decentralized autonomous organizations use smart contracts to coordinate a group of individuals who share the same interests and goals. They function in accordance with defined governance rules using tokens, and after being implemented do not necessarily require any more human involvement.

Shermin, Strategic Change 2017, p. 499.

¹⁰⁶ Bambrough, A Gold Standard of ICOs Is Needed -- But It Won't Be Easy.

In this context, “providerless services” are also conceivable. Digital services implemented as smart contracts can—once they are made public—remain available without any additional maintenance by the original developer, as long as the underlying DLT system keeps running, i.e. continues to be used by the community (or, for example, a DAO). This results in services without providers: a state of affairs that was not foreseen by conventional economic theory.

4.2.5.8 Economically autonomous machines

Autonomous machines (like self-driving vehicles) are currently being developed and enhanced on a large scale. It is therefore only a matter of time until machines begin interacting autonomously in an economic sense as well. Without central monitoring, such interactions require a trust-inducing technology like DLT. As a consequence of parallel development trends in the fields of artificial intelligence and the Internet of Things, in the years ahead there is every reason to expect the advent of autonomously acting machines for a wide range of applications. The examples include mobility (self-driving vehicles), transportation and logistics (drones), and manufacturing (industrial robots). A blockchain could serve as the infrastructure for these machines to also interact economically (e.g. charging for mutually provided services on a “pay-per-use” basis). Apart from this, it is also conceivable that any taxes due on work done by robots could be automatically transferred to the responsible taxation authority in an easily audited form.

4.2.6 Decision-making criteria for the use of blockchain

Decisions on whether or not to use DLT must take various aspects into account. In terms of design, a distributed system is inferior in many respects to conventional data storage technologies (e.g. central databases). It is therefore important to individually check every application to see if the use of DLT adds significant value. To facilitate these decisions, researchers and practitioners have developed various approaches, some of which have different focuses or priorities. The World Economic Forum, for example, has presented a decision tree based on relevant criteria.¹⁰⁷ It includes three initial criteria for immediately ruling out the use of blockchain. The first question is “Are you trying to remove intermediaries or brokers?” Owing to the distributed nature of DLT, in most cases it provides few additional benefits if a central unit is already adequately administering and controlling the system. The next question is “Are you working with digital assets (versus physical assets)?” If this is not the case, then these assets cannot be processed by a blockchain either. This criterion can also be regarded as a fundamental design principle of DLT systems. Since one of the core attributes of DLT is long-term, immutable storage of data, it must also be possible to create a permanent, authoritative record of the digital asset in question. Accordingly, implementing DLT should be avoided until all three criteria are met. It should be noted that the study by the World Economic Forum does not consider business factors, combinations of technical attributes of different distributed ledger technologies, or different generations.

Scanning the entire trajectory of DLT up to the present, four technological attributes can be repeatedly spotted that have been used to derive the decision-making criteria

¹⁰⁷ Mulligan/Scott/Warren/Rangaswami, *Blockchain Beyond the Hype*.

of various tests. The Bitcoin protocol, for example, succeeded in eliminating intermediaries (in this specific case, banks). The two principal technological bases for this are a high degree of protection from tampering and a single shared store of information. The high degree of protection from tampering, which is often incorrectly described as immutability, is achieved with Proof of Work. A single shared store of information is achieved—leaving aside the occasional temporary existence of two parallel chains, or “forks”—by everyone agreeing on a timestamp. Ethereum became the next significant stage in the evolution of the blockchain idea by making it possible to store so-called smart contracts (later also referred to as “chaincode”, among other things) at the protocol level, thus enabling all participants to store executable code in the blockchain. As a result, the added value that blockchain could generate for organizations gained a new dimension: the implementation and execution of logic by any number of participants. This made it possible, for example, to manage processes across organizations. In this case it is not only about eliminating a central process manager (and thus an intermediary), but also about linking together participants independently of existing systems and implementing distributed logic. Since then, there have been numerous other attempts to overcome certain technological constraints and, for example, enable the sustainability of Proof of Work and the interoperability of different distributed ledger technologies, with theoretically unlimited scalability being the one with the greatest potential impact. IOTA, a new distributed ledger technology, is attempting to achieve it by, for instance, departing from the basic idea of the blockchain and implementing a database structure based on directed acyclic graphs. However, this technology falls short of achieving that goal without dispensing with a common store of information.

The last example in particular shows that decision-making criteria need to be both comprehensive and flexible. Blockchain cannot be limited to a single application, although this is the case with the decision tree of the World Economic Forum. Rather, it is necessary to consider the current and steadily evolving capabilities of distributed ledger technology as they apply to a particular application. Combinations of tamper resistance, concurrent information, distributed logic, and high scalability are what various derivative technologies are striving for and can only be individually compared with conventional technologies.

4.2.7 Blockchain as a digital infrastructure

Although DLT was originally conceived for the purpose of technically implementing a digital currency,¹⁰⁸ it is more recent versions of it in particular that may be regarded as generic digital infrastructures.¹⁰⁹ Infrastructures of this kind make it possible to take their attributes (such as protection from tampering), render them usable, and disseminate them via interfaces for different kinds of applications. On the technical level, as a rule such a DLT interacts with conventional IT systems instead of being used as a standalone infrastructure.

An analogy borrowed from a very classical field is well-suited for illustrating the infrastructural character of distributed ledger technology, against the background of still-

¹⁰⁸ Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

¹⁰⁹ Olnes in Scholl/Glassey et al., Electronic Government, 253; Schlatt/Schweizer et al., White paper / Fraunhofer Institute for Applied Information Technology FIT 2016.

new, barely studied effects on business and society: cities are undoubtedly responsible for municipal infrastructure such as streets and central facilities. In order to improve their quality of life, attract businesses, and thus generate revenues, cities leverage the basic infrastructure of "streets and roads" in order to offer higher-order infrastructure like "weekly markets". This higher-order infrastructure can then serve as a platform for bringing together and rendering accessible the products or services of providers. In this analogy, the streets and roads correspond to the data lines that, in the context of expanding broadband services, paved the way for the "Internet of Information" (see also section 4.2.4). The analogy of a weekly market would be DLT-based infrastructures of the "Internet of Value and Trust". Commerce is also conducted by private businesses on the basis of a DLT-based infrastructure. Here the key questions include how to establish such infrastructures in Germany, and in particular how to ensure that they are compatible with the German system of laws and values and add value for Germany's economy and society. Unless these questions are asked at an early stage and strategies developed for national policies based on the answers, in the long term DLT infrastructural solutions imported from other countries could prevail.

Smart contracts and tokens in particular lend themselves very well to modelling relationships and interactions among different entities. These interactions take place on various levels, generally while using the most relevant kinds of DLT systems in each case. In an economic context, relationships among equivalent private individuals can be subsumed under the heading of consumer-to-consumer (C2C). Relationships among companies are referred to as business-to-business (B2B). And relationships involving government organizations are grouped, for example, under the label of government-to-business (G2B).

In this context, it is frequently postulated that C2C relationships could be accurately modeled by means of public DLT systems (cf. the technical section), since the parties involved in these relationships do not necessarily trust one another and therefore require a generally accessible infrastructure with objectively verifiable protection from tampering. These DLT systems in particular may be regarded as public digital infrastructure. Any individual or organization can join an appropriate network by operating a node with the corresponding protocol. In the same way, each of these entities can develop applications on the basis of the infrastructure in order to, for example, implement business models or completely self-serving applications. Public systems thus exhibit potential for generating new kinds of ecosystems based on the generic attributes of DLT. In technical terms, DLT is in turn based on the Internet as a digital infrastructure. However, DLT still lacks a clear, generally acknowledged, and comparable layered model. Users are also occasionally challenged by the large number of public DLT systems, the paucity of standards, and the frequently lacking interoperability of individual systems. This is problematic, since it limits the economies of scale that public DLT systems require. Besides generic DLT systems that are suited for general applications, there are also domain-specific systems offering, for example, optimized protocols for financial uses.



DLT as a Value-Adding Digital Infrastructure

DLT deserves further study as a digital infrastructure technology for generic services of various kinds. It can be used to implement a range of applications that can deliver benefits to private individuals and businesses across sectors, like for identity management. This also calls for research on the underlying technologies and cross-application value creation models of DLT. Overall, DLT needs to be understood and managed as a digital infrastructure technology.

4.2.8 Informational self-determination and digital sovereignty

In recent years, large digital enterprises—which are sometimes bundled under acronyms like FAANG (Facebook, Amazon, Apple, Netflix and Google)—have made a steady stream of headlines in connection with the excessive storage, use and/or abuse of data. When, shortly after the 2016 U.S. presidential election, it emerged that the British company of Cambridge Analytica had used millions of Facebook profiles in an attempt to influence the outcome, the resulting debate reshaped public perception of these issues in an unprecedented way. The data were used without the users' consent or knowledge. These and similar incidents clearly show that users themselves often know little about and can do even less to influence how their personal (utilization) data are disseminated after they use popular online services. Many smartphone apps automatically pass utilization data to Facebook or Google, for example, even when they are not directly related to the services in question. Researchers at Oxford University, for example, found that over 90% of all apps include tracking functions belonging to a U.S. company.¹¹⁰ In terms of tracking volumes, Alphabet—Google's parent company—takes first place by a large margin at 88%, even beating Facebook (44%).¹¹¹ Limiting the scope of this comprehensive tracking, when apps allow it, is often very difficult or impossible to do, even for tech-savvy users.

Yet the right of informational self-determination dictates that individuals are entitled to decide themselves how their personal data are used. The term "digital sovereignty" is often used in this context.¹¹² Although no consistent definition of digital sovereignty exists yet, in general it means that the individual is enabled to "move in the digital world in a self-determined way [...] and actively exercise [their] rights to informational self-determination."¹¹³ The use of the term digital sovereignty implicitly strengthens the connection to today's digitalized world and its conditions and challenges.

The GDPR already addresses some of the challenges that are arising in this context. For example, it regulates data protection and the security of personal data. Now data on users may only be captured if this is necessary in order for them to use a system or application.¹¹⁴ In addition, steps must be taken to ensure that the ways in which these data are stored and used are transparent to users. Apparently, however, these and

¹¹⁰ Binns/Lyngs/Kleek/Zhao et al., Proceedings of the 10th ACM Conference on Web Science 2018, 23.

¹¹¹ Binns/Lyngs/Kleek/Zhao et al., Proceedings of the 10th ACM Conference on Web Science 2018, 23.

¹¹² Beyerer/Müller-Quade/Reussner, DuD 2018, 277.

¹¹³ Beyerer/Müller-Quade/Reussner, DuD 2018, 277.

¹¹⁴ Beyerer/Müller-Quade/Reussner, DuD 2018, 277.

similar regulations are frequently ignored, as evidenced by a record-breaking fine that was recently imposed on Google by the French data protection regulator, the Commission Nationale de l'Informatique et des Libertés (CNIL). Google has been ordered to pay a penalty of 50 million euros for violating "transparency and informational obligations".¹¹⁵ CNIL said that Google provided insufficient information to users on how their data are used and also failed to specifically obtain their consent for using their data for various services including the Google search function, Google Maps and YouTube.¹¹⁶

This case touches on some fundamental issues. For one, some software is difficult or impossible to use without the implemented tracking functions, since it is simply not available or it is extremely difficult to find a version that does not have them. For another, users must overcome considerable hurdles in order to disable these functions. The situation is additionally aggravated by the platform or network effect that has already been mentioned here a number of times: for many users there is no alternative to widespread services like chat platforms, because only these services have a sufficiently large user base for generating real value. In order to take advantage of these services, users therefore often knowingly or unknowingly take associated data protection issues or a lack of privacy in stride.

A transition from this status quo toward greater digital sovereignty of individuals, and also of governments and companies, requires more approaches that actively place decision-making powers in the hands of users instead of those of software providers and platform operators. In the digital world, approaches of this kind must be appropriately software-based and/or it must be possible to integrate them in existing solutions. In order to comply with the stipulations of the GDPR, for example, all applicable legal requirements need to be technically implemented, including, for example, interoperable data formats and the ability to delete data.¹¹⁷ Relevant economic and social aspects—such as platform or lock-in effects—must also be considered when developing them.

In the real world, the sovereignty of one's personal identity is relatively simple to manage. A commonly cited example is verification of an individual's age. If, for example, it is necessary to check someone's age to determine whether they may purchase alcoholic beverages or play certain computer games, they can show their identity card or passport. In this simple example no other data are relevant and there is therefore also no need to divulge them, and by and large they are not captured either. As already explained, however, the situation "online" is quite different. In that world, a wide variety of information on individuals is constantly collected, disseminated and evaluated.

DLT can help mitigate excessive data use, for example by preventing data from being used for purposes other than the one at hand, thus contributing to greater digital sovereignty. Going forward, it can serve as an enabling technology for digital, self-sovereign identities. DLT-based platforms are already being developed for managing digital identities (see section 4.2.5.5). Such a platform provides the required infrastructure for each participant to actively manage their digital identity. It is relevant that

¹¹⁵ Böhm, Spiegel Online, Jan. 21, 2019.

¹¹⁶ Böhm, Spiegel Online, Jan. 21, 2019.

¹¹⁷ Diepenbrock/Sachweh, DuD 2018, 281.

none of the data are directly stored in the DLT-based infrastructure; the blockchain only serves as a verification layer. In this context, the key aspects are the security, controllability, and portability of identities.¹¹⁸ As the term suggests, it should be completely up to the user to manage their personal identity, thus enabling genuine digital sovereignty. The user alone decides which attributes of their identity they want to share and with whom. For example, individual aspects such as age, height, gender, contact data or payment information may be relevant in different situations and used independently of one another.

In the following, the use of a self-sovereign identity is briefly and simply explained, taking the example of digital age verification. A user signs on to the identity platform. It is of course necessary to verify his or her age before he or she is allowed to purchase age-restricted products such as alcoholic beverages. He or she therefore needs a way to confirm and verify his or her age, such as a new ID card. Once his or her age has been verified, he or she alone is entitled to decide who he or she shares this information with. The key aspect is that the information—for instance, his or her exact date of birth—is not stored on the platform in a publicly accessible form. Instead, there are only encrypted pointers to the data, and the platform is only used to confirm attributes (such as age) toward other users (such as an online shop). When making an online purchase, the user can now answer the question “are you over 18?” with “yes” by directly sharing the verified attribute of “age” with the shop. He or she does not even have to share information on his or her actual age, only on whether or not he or she is at least 18 years old (yes/no). Processes of this kind are closely related to other digital technologies and concepts such as secure multiparty computation.^{119,120}

Initial verification of certain attributes is a frequent sticking point in discussions of whether DLT is the best technical foundation for a system of this kind. A verifying function needs to be accessed in this process, but the jury is still out on whether other technological solutions might be equally well-suited. Various startups have already set themselves the goal of developing DLT-based digital identities and providing corresponding platforms that will give users complete privacy and control.

DLT-based approaches are a first step in this direction. Looking ahead, they will technically enable the achievement of greater digital sovereignty. However, this purely technical capability will hardly be sufficient. Appropriate general economic and legal conditions will also have to be met to truly bring about a change in how the topic of informational self-determination is addressed. In practice, the crux of the matter will probably be how to successfully traverse the path from the status quo of “complete dependence on platform operators and software vendors” to “complete digital sovereignty of the individual”. Various aspects of this conundrum are already being debated. One is the need for an appropriate legal framework, for instance to justify changes to existing laws, also against the opposition of large digital enterprises.¹²¹ Moreover, from a purely market economy perspective it is already hard to restrict the storage and processing of

¹¹⁸ Mühle/Grüner/Gayvoronskaya/Meinel, Computer Science Review 2018, 80; Tobin/Reed, *The Inevitable Rise of Self-Sovereign Identity*.

¹¹⁹ Zare-Garizy/Fridgen/Wederhake, *Security and Communication Networks* 2018, 1.

¹²⁰ See also section 4.1.3.

¹²¹ Beyerer/Müller-Quade/Reussner, *DuD* 2018, 277.

data, activities that are dominated by U.S. companies, to European or German jurisdictions. These market-dominating services are typically not provided by European companies,¹²² since European or German alternatives to the mainly U.S.-based software are rare. It is also necessary to clarify these issues in DLT-based IT infrastructures, since—at least in public blockchains—no territorial restrictions can be enforced. In the future as well, it will be essential to enable the use of new digital services (such as intelligent household assistance systems) while safeguarding privacy and security.¹²³ Further technological advances must not be allowed to endanger digital sovereignty. DLT can make a contribution here.

4.3 Aspects of Implementation

4.3.1 Diffusion of DLT-based innovations

4.3.1.1 The economic perspective

DLT can provide a high-value digital infrastructure for supporting economic viability. But it is not a business model in itself. Despite all the media hype around innovative technologies, and especially blockchain, there is still insecurity in government, business and society regarding the potential of blockchain and whether this potential can be leveraged to achieve their goals. In the context of digitalization and ever-shorter innovation cycles, companies are constantly on the lookout for ideas and approaches that will let them unlock new fields of business or optimize existing processes (see section 4.2.7).

However, there is no reason to think that DLT is already replacing firmly established intermediaries. It may also be assumed that in the future, both centralized platforms and distributed, democratically organized DLT platforms will be present, even coexisting in many cases. In the case of the platform-based business models that are so widespread today (Amazon and Uber being cases in point), their value for customers is mostly due to the many interactions and business partners available there. But this also comes at a price, because market power is usually concentrated in the hands of semi-monopolistic providers (along the lines of the “winner takes all” principle). A conventional centralized platform operator can therefore do business virtually unrestrained; in particular, it can respond faster and more dynamically to both positive and negative external developments. What is more, it pursues its own interests with the platform, thus making it easier to convince investors of the profitability of its business model. As a consequence, major platform operators achieve an initial efficiency advantage compared to decentralized platforms, which do not constitute business models in their own right and in which decisions have to be made jointly by all (or at least a majority) of their participants, who also take responsibility for them. In the long term, however, if central platform operators abuse their market dominance or fail to adequately meet customers’ needs (for example, by ignoring data protection requirements), a sustained, coordinated migration away from them to a DLT-based, neutral, and distributed alternative is within the realm of possibility. In the final analysis, whether a platform succeeds or fails depends on users, and because they have different preferences with

¹²² Markl, Informatik Spektrum 2018, 433.

¹²³ Beyerer/Müller-Quade/Reussner, DuD 2018, 277.

regard to the above-mentioned advantages and disadvantages, it is probable that centralized and distributed DLT-based platforms will continue to coexist in the future. It may be assumed that, in markets where a centralized platform has prevailed, the mere possibility of a DLT-based distributed alternative arising can be enough to persuade the platform operator to abandon its monopolistic tendencies. In other words, the potential existence of DLT alone can have a market-correcting effect.

The use of DLT can also be very promising in situations where an intermediary could benefit but the market or political environment has prevented one from emerging. For example, in the foreseeable future it would not make sense to replace the German land registry with a DLT. But in countries where such registries do not exist or do not function reliably (for example, because of corruption), it could make a great deal of sense to introduce a corresponding DLT-based system.

A fundamental prerequisite for the successful use of DLT is digitization of the processes to be supported.¹²⁴ Provided that this is done, various e-government solutions can be enriched by the attributes of DLT.

 **E-Government**

eGovernment is the use of (typically web-based) technologies to provide public services and information to stakeholders.

Layne/Lee, Government information quarterly 2001, 122.

DLT opens up the possibility of an infrastructural IT solution for federal business and administrative processes where it is important to respect the data sovereignty of the stakeholders involved while applying the once-only principle.

 **Once-Only Principle**

The once-only principle is the idea that citizens only have to share information with government agencies once. It is one of the pillars of the European Union's digitalization strategy.

TOOP Project, Once-Only.

Generally speaking, these approaches have potential whenever processes call for communication and cooperation across organizations. The current practice, in which many organizations separately store their data, definitely also has many advantages but tends to interfere with collaboration due to a lack of mutual data-related and technical integration. From an economic standpoint, integrating the data of all government organizations (in a "federal database") would also increase the efficiency of administrative processes and government work.

¹²⁴ Nærland/Müller-Bloch/Beck/Palmund, 38th International Conference on Information Systems (ICIS), 1.

In Germany, however, being a country with a federalist system of government and political culture, centralized data storage is frowned upon. Here DLT could help achieve cross-agency processes without requiring central data storage. This would facilitate communication, support cooperation, and at the same time strengthen the data sovereignty of individual citizens.

In order to efficiently deploy DLT, public administrations require knowledge of processes within and across agencies, appropriate skills for reorganizing processes against the background of the possibilities of DLT, legal expertise (for example, on implications of data storage), and technical capabilities for implementing these approaches. Projects of this kind can be supervised and monitored by facilities that possess appropriate expertise.

In a global survey by the World Economic Forum, 73% of 816 questioned information and communication technology experts said that they expected the first government to begin using DLT to collect taxes by the year 2023.¹²⁵ In the following, three other promising eGovernment applications for DLT are discussed. One involves designing digital proof of identity that does not reveal any personal information that is not relevant to the case at hand. Its core element is a secure DLT-ID that is verified a single time by a trustworthy authority (e.g. a local community) and can then be used by citizens. In addition, there are interesting uses for DLT applications that document a circumstance or change of status only once. Rapid, secure distribution of new information to all of a blockchain network's members also permits cross-organizational coordination of business processes and administrative processes. A change of status can, for example, trigger subsequent processes at other government agencies. Besides the applications that have already been described here, DLT also has potential for use within the scope of democratic processes. Specifically, this technology can be leveraged to support the democratization of elections and administrations while strengthening citizens' sovereignty.

The digitization of elections typically poses strict security requirements. But ensuring secrecy and anonymity is not the only challenge. Election systems are also an attractive target for manipulation attempts. DLT, being inherently impervious to falsification, unchangeable and transparent, has potential for mitigating problems that have hitherto plagued attempts to digitize elections and even for creating a more reliable standard than paper-based elections. This is due to the fact that votes submitted on paper have to be digitized in order to count them, a process that is prone to errors and vulnerable to manipulation. The credibility of results can therefore only be ensured by a disproportionate effort. In elections held with the aid of DLT, by contrast, the entire process is digital from the start—and at the same time transparent and safe from manipulation. Voter identification could take place outside this system, for example using biometric verification techniques like retina, fingerprint or dorsal hand vein scanning. Identification is not the core of DLT, however, but only the interface to users. Here it is essential to pay close attention to make sure that no unwanted monitoring possibilities arise from the use of DLT. Although experimental approaches and pilot projects provide an idea of the form that such a system could take, before actually implementing it

¹²⁵ Global Agenda Council on the Future of Software & Society, Deep Shift.

there is a need for additional intensive research and testing.¹²⁶ Also where interagency processes and communication are concerned, DLT can help pool information without the need for a central database for all citizens. The German Federal Office for Migration and Refugees, for example, has tested a DLT solution with promising results and is already implementing it on a pilot basis for the purpose of improving interagency co-operation.¹²⁷

In order for DLT to prevail in an application, a critical mass of relevant parties has to be convinced of the advantages. For the most part, the principal challenges associated with implementing a DLT application are not technical or legal, but political and organizational. Even if the initial effort required to launch it is minor, its productive use can be very costly. A certain minimum number of organizations need to use a DLT application in order to achieve economies of scale. Even if DLT can increase efficiency within a consortium, all of its stakeholders first have to be convinced that such a solution makes sense. In large, dynamic consortia this process introduces inefficiency. Alternatives that do not involve DLT are also available; one possibility is joint ventures with a centralized system managed according to legal rules instead of technical ones. Yet this type of cooperation is often also dogged by problems, which improves the prospects of DLT. Joint ventures often fail due to a lack of mutual trust or self-serving members, leading to corruption. These problems are addressed in the context of shipping documents in Chapter 6. Appropriate policies can encourage competitors to join forces, also without the use of DLT. To establish the right priorities, however, it would appear to be necessary to provide legal security by applying antitrust laws.

Another challenge in connection with DLT is that market players have little knowledge or understanding of this technology. As a result, companies commonly ignore it when making decisions. The role of coordinator of a consortium in particular leads to misunderstandings and two possible problems. First, confidence in a distributed solution can be hindered by a lack of technical understanding. For example, it is doubtful that the members of a small network of public transportation providers will possess the expertise required to implement and actively participate in running a distributed mobility platform like OMOS (a collaboration of TÜV Rheinland, Fraunhofer FIT and Motion-Werk). Second, it can happen that a consortium's supposedly distributed design is only faked by its coordinator. It is very important to foster technical understanding (and thus confidence) in DLT, especially at small and medium-sized German companies, even if this alone is insufficient to enable productive use of the technology. At large DAX-listed corporate groups, it is now common for managers to use DLT to make investment decisions, despite being clueless as to how it actually works and despite the fact that these companies could easily afford an R&D department devoted to this technology. The situation is different at small and medium-sized German firms. These are usually too small to actively study such a technology themselves. Especially in a country like Germany, where small and medium-sized companies constitute the backbone of the economy, it would therefore make political sense to help them acquire relevant knowledge. A consortium of small and medium-sized firms would contribute to achieving a critical mass and thus accelerate diffusion of the technology. Even if no appropriate solutions are yet available for these companies in the marketplace, the

¹²⁶ Kshetri/Voas, Blockchain-Enabled E-Voting.

¹²⁷ Fridgen/Guggenmos/Lockl/Rieger et al., Bundesamt für Migration und Flüchtlinge 2018, 1

technology itself is already mature enough to seize early-stage opportunities and gain a competitive edge. In other countries where small and medium-sized firms do not play such an important role, there is no risk of a technology drain.

4.3.1.2 The Business perspective

DLT is regarded as a disruptive technology. Digital disruption is caused by innovations that largely or completely displace established technologies, products or services. This faces companies with issues that also arose in the past in a similar form but were far less frequent and above all not as broadly relevant. How do I deal with the new possibilities and challenges that digitalization offers me as a company?

4.3.1.2.1 DLT as a disruptive technology

The use of DLT was initially debated in the financial services industry, but in recent months (the time of this writing is April 2019) diverse companies have taken the initiative in the field of DLT and are addressing corresponding applications and problem solutions, in many cases within the scope of industry-specific consortia. This trend reveals a fundamental difference between disruptive and conventional technologies. Existing or emerging applications are being sought in which disruptive technologies can be meaningfully deployed (see Figure 17). In this context, more and more companies are attempting to counter disruptive innovations with conventional practices and approaches—and are running the risk of failing in this endeavor. Miscalculations by major enterprises in connection with disruptive technologies are public knowledge (the examples include Nokia and Kodak), and so are the negative consequences and failures they have suffered as a result. When trends are misinterpreted, even current technology leaders can be forced out of their markets in just a few years.

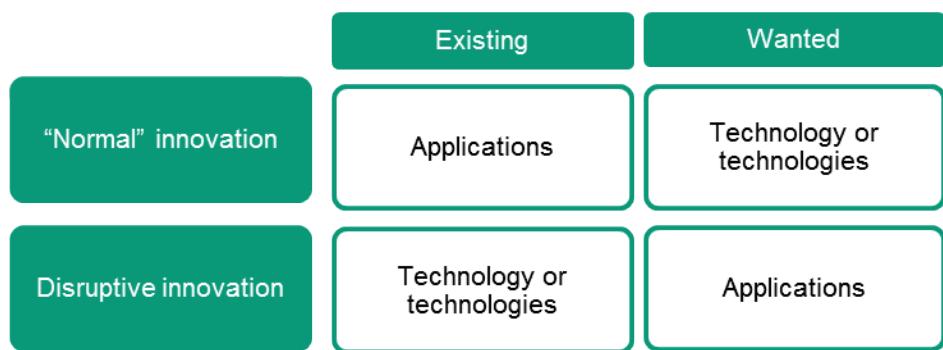


Figure 17: The consequences of disruptive technologies are different from those of normal technologies.

In the case of “normal” innovations, there are plenty of applications for which appropriate technologies are being sought. Where disruptive innovations are concerned, the opposite is generally true: the technology is already known, but sensible uses for it are still being debated.

4.3.1.2.2 DLT calls for a different approach to innovation management

Past developments associated with DLT exhibit clear analogies with earlier disruptions. It is therefore conceivable that the fate of today’s established market players can take a similar course if they incorrectly assess the potential and effects of DLT. When evaluating disruptive technologies, it is important to take a broad perspective while simulta-

neously keeping technological developments, the market, and the competitive situation in view (for example, in neighboring industries and general technological trends). It is not a good idea to focus exclusively on a single source of information. If a company concentrates too exclusively on customers' wishes and expectations—although precisely this is a frequently recommended approach in the age of digitalization—it runs the risk of no longer looking "out of the box" and developing tunnel vision. A simple analogy makes this clear. In the early 20th century, if merchants or entrepreneurs had been asked how the Atlantic might be crossed more quickly, they very probably would have answered that a new generation of even faster ships would accomplish this. Then, in 1919, the disruption arrived: the first nonstop transatlantic flight, piloted by Britons John Alcock and Arthur Brown. But it was Charles Lindbergh, an American, who attracted the most attention by accomplishing the same feat by himself several years later in 1927. A few years also passed between the creation of the first bitcoins in 2009, which attracted relatively little attention, and when this cryptocurrency began making headlines. It will presumably also take a while until DLT is widely and productively used. But it would be a mistake not to take this technology into account in today's strategic considerations. There is currently no way to know how important DLT will ultimately be in various fields and industries. According to the "hype cycle" of the firm of Gartner, blockchain, in other words DLT, is now just past the "peak of inflated expectations".¹²⁸ While in the case of some DLT applications this assessment has been apparent in the negative reports published since mid-2018, especially for the cryptocurrency markets, it is unclear whether it is also accurate for DLT in general.

Assuming that the bundle of technologies collectively referred to in this study as DLT is in fact now in the vicinity of the "peak of inflated expectations", going forward from here three different scenarios are imaginable (see Figure 18). One is that DLT will become a standard technology in the near future and deeply transform a wide range of markets and industries. Another is that the current hype will be followed by a consolidation phase. Over time, the fields of application in which DLT can be productively used while conferring real benefits will become clear. In the third, it will turn out that DLT's disruptive potential is being wildly overestimated and it will not succeed in surmounting existing obstacles, thus relegating it to the status of a niche technology. The most likely outcome is that DLT, like many other technologies, will take the middle road. Innovative companies should therefore get ready for a "plateau of productivity" and not fear the "trough of disillusionment".

¹²⁸ Panetta, Gartner Top 10 Strategic Technology Trends for 2019.

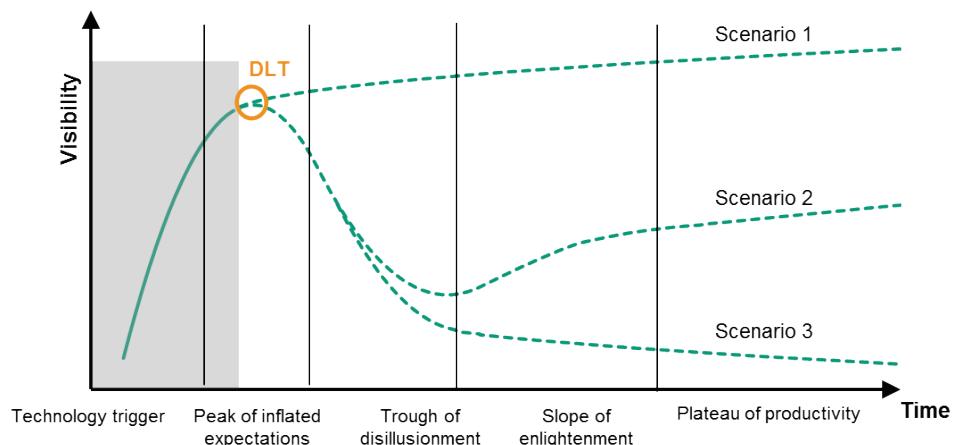


Figure 18: DLT at the peak of inflated expectations: after this point, there are three conceivable scenarios.

In the best-case scenario, companies take a multistage approach (see Figure 18). Across all industries, it is important to involve both business and technically competent staff in the innovation process. This is the only way to ensure that the technology's disruptive nature is considered at all of an enterprise's levels. The perspective of employees with expertise on infrastructure or applications often differs from that of those who are responsible for a company's business model. And it is essential to look at things from all of these standpoints in order to capture the full breadth of possible applications and their implications. An example of the successful application of this procedural model is presented in Fridgen et al. (2017).

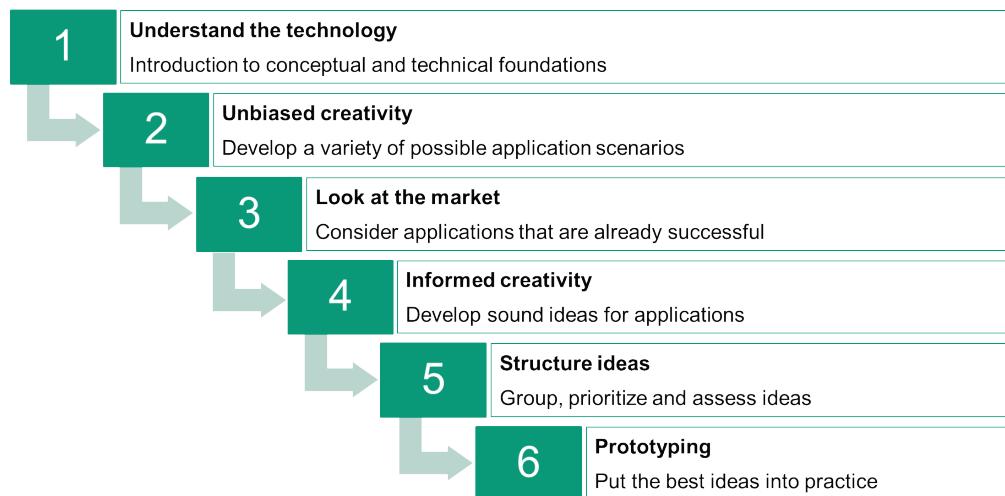


Figure 19: Procedural model for dealing with disruptive (digital) technologies

1. Understand the technology: Introduction to conceptual and technical foundations

In most cases, companies and their employees have only rudimentary experience of DLT. Either they completely lack relevant expertise, or it is limited to particular applications such as cryptocurrencies. But in order for all involved employees to be able to recognize the potential of DLT, avoid unrealistic expectations, and assess as precisely as possible its impact on their own company and industry, they need to thoroughly

familiarize themselves with its conceptual and technical foundations. Sufficient time should be allotted for this phase of the procedural model, since it constitutes the basis for all further efforts and is indispensable for developing and discussing possible DLT applications.

2. Unbiased creativity: Develop a variety of possible application scenarios

After digesting the basics and attributes of DLT, it makes sense to creatively approach potential applications with an open mind. In this phase, it can be a good idea to involve employees who have had no prior contact with this technology; this will encourage unbiased creativity. A creative workshop should be held, focusing on the following questions: How could your company use this technology? Which intermediary currently hinders your company the most? Are your company's data in great danger of manipulation in the context of some processes? Which processes take too long? Which processes have (too) many participants? For which processes and services does your company pay too much?

3. Look at the market: Consider applications that are already successful

In a further step, existing projects within the same industry are considered and analyzed. Looking farther afield to find and consider other perspectives on and uses for the technology is advisable. This step facilitates a much better understanding of the possible situations that can arise and how mature the technology is.

4. Informed creativity: Develop sound ideas for applications

After becoming familiar in this way with existing applications and possibilities, it is a good idea to hold another workshop to build on all the impressions that have been gathered and ask once again: How could your company use this technology? Experience has shown that this step can already yield detailed intermediate results against the background of market observations.

5. Structure ideas: Cluster, prioritize and assess ideas

A certain number of possible DLT applications have already been identified by this point. Now the most promising of them should be chosen for further study. By applying selected criteria to these and asking the right questions, a good and detailed overview of suitable candidates can be obtained relatively quickly. An example of a question for consolidating the list is: How does this process with DLT compare to the status quo, and what benefits or drawbacks would it bring? If, after working through the list in this manner, too many promising DLT applications are still left, further consolidation should be considered. For example, it can be useful to eliminate the most complex applications and choose those that express the technology's attributes best. In addition, the development processes and what has been learned from them should be straightforward to apply to other cases.

6. Prototyping: Implementation of the best ideas

The goal of prototyping is not necessarily to develop a market-ready solution. Rather, it is about accumulating expertise in the company to enable swift responses to future developments. For implementing selected applications, it is advisable to take an agile approach and move from the initial example to a productive application in a series of

iterative steps. This iterative approach rapidly yields initial results that can then be used to communicate the technology within the company and educate staff about it. This approach also makes it possible to quickly respond to changes or new insights in the ongoing evolution of DLT.

Digitalization, and especially disruptive technologies, are exerting a profound influence on nearly all parts of society, industries and companies. The associated changes often completely permeate all of a company, from its infrastructure all the way to its business model. A host of different development scenarios are conceivable, from the development of new products and services to the displacement of "big players" to the creation of new markets. Companies are asking themselves how, in this complex environment, they can keep up with developments. In many cases there is a lack of a tailored concept for dealing with situation and managing disruptive innovations. The example of blockchain shows that these technologies are evolving at a rapid pace. Although no one can accurately assess their true potential, companies should nevertheless address them. They are well-advised to keep their sights on the future and actively acquire relevant knowledge about blockchain.



Two-Pronged Strategy for Disseminating Innovations

A two-pronged strategy for disseminating innovations appears to be a good idea. One is a "push" approach for systematically addressing small and medium-sized companies in a variety of ways. This can be done via industry associations with a multiplier effect or by organizing dialog events. The other is a "pull" approach: using existing low-threshold instruments like the mFUND program or promoting strategic lighthouse projects. Ideally, the corresponding projects should generate synergies with other national and international goals, such as more widespread use of electromobility, and evoke considerable interest.

In order to adequately understand the possibilities of DLT and identify applications for it, an approach is needed that combines analytical and creative methods. Companies should observe the market and engage in a dialog with other firms, definitely including rivals that only compete with them in some areas. It is often worthwhile to track current technological developments in one's own industry and beyond.

4.3.2 Obstacles

4.3.2.1 Energy consumption and transaction speed

One frequently cited criticism of DLT is that it suffers from a low transaction speed in combination with high energy consumption. In the following, both of these aspects are addressed and put in relation to DLT.

4.3.2.1.1 Transaction speed

The transaction speed and power consumption of a DLT system mainly depend on the consensus mechanism used. More than 30 different consensus mechanisms meanwhile exist, of which Proof of Work is the best-known. This is because of its long history and close association with the Bitcoin system. It is therefore often taken as a basis for comparison and regarded as the standard or as representative of all other DLT systems.

However, in many cases this fails to take the current state of the technology into account. Other consensus mechanisms are more efficient in various ways; section 3.2.2 provides an overview.

Generally speaking, the transaction speed of a DLT-based system is slower than that of a central database. There are two reasons for this. One is that the consensus mechanism typically requires verifications and iterative communication with other network participants, which quickly adds up with global communication. The other is that, because the system is distributed, all transactions have to be redundantly stored in all or at least a subset of all network nodes. In particular, this means that every transaction must be communicated to every network node and processed by it.

The transaction speed of a DLT system largely depends on its design. Public and permissionless DLT systems are typically characterized by slower transaction speeds than private permissioned systems. This has to do with the varying security requirements of DLT systems. Whereas in public, permissionless DLT systems like the Bitcoin blockchain everyone can participate in creating new blocks, in a private permissioned DLT system—such as Hyperledger Fabric—this right is restricted to certain nodes. As a rule of thumb, more open DLT networks have greater security requirements and slower consensus mechanisms. This is due to the fact that there is always greater mistrust toward other network participants in public, permissionless DLT systems. Moreover, every participant hides behind a pseudonym and their real identity is unknown. In private, permissioned systems, by comparison, there is always a certain minimum level of trust. This minimum trust is based on the fact that the identities of the network participants entitled to create new blocks are known. Whenever a network node behaves in a harmful manner, this strengthens the system under which individual users can be easily identified and prosecuted if necessary. Ultimately, the underlying basic trust reduces the security requirements that the consensus mechanism must meet, thus letting it be designed for greater speed and efficiency.

Transaction speed is still a bottleneck in public DLT systems. But as consensus algorithms continue to evolve, such as Proof of Stake,¹²⁹ their performance is also improving. New data structures, such as directed acyclic graphs (DAGs),¹³⁰ could enable significantly faster transaction speeds. Although DLT systems typically fall short of centralized systems in terms of performance and efficiency, there are definitely applications in which slow transaction speeds are sufficient. To determine the economic impact of transaction speeds, the associated efficiency losses need to be separately calculated for each application. Introducing DLT-based solutions to an existing system can result in significant changes, making it advisable to consider the implications in each case.

4.3.2.1.2 Energy consumption

Besides low transaction speeds, another issue that has attracted attention in the media is the notoriously high energy consumption of Bitcoin. Here it is important to keep in mind that its Proof of Work consensus algorithm was intentionally designed to be compute- and therefore energy-intensive. The costs of mining are an essential ingredi-

¹²⁹ See also section 3.2.2.

¹³⁰ As used in the case of IOTA, see also section 3.3.8.

ent in order for the incentive system to work. The level of difficulty of the compute-intensive puzzles, and with it the energy-intensiveness of mining, is regularly adjusted. But the energy consumption of Bitcoin does not increase in proportion to the number of transactions per second—this rate is artificially constrained in order to limit the volume of data that each network node must process and store. Instead, energy consumption grows with the effort that miners have to expend in order to generate new blocks and be rewarded with a certain sum of bitcoins. Other consensus mechanisms, like Proof of Stake¹³¹ for example, could reduce the energy consumption of DLT systems that use them to negligible levels compared to Bitcoin.

Data storage is substantially less energy-intensive than calculations, and recent developments (memristors are an example) may additionally defuse this aspect. There are also technical approaches that, like Sharding,¹³² seek to reduce processed and stored data volumes, especially in public DLT systems. Table 2 below provides an overview of the energy consumption and average transaction speeds of various DLT systems compared to conventional value transfer systems.

Table 2: Duration of 100,000 transactions at maximum capacity

VISA	ripple	NANO	Ethereum	Bitcoin
1.8 seconds	2 seconds	10 seconds	2 hours	4 hours

Power consumed for one transaction, expressed as the time during which it would illuminate a standard 60W lightbulb¹³³

1 48 minutes	hour	11 seconds	3 11 hours	days	1 118 days	years	9 187 days	years
-----------------	------	------------	---------------	------	---------------	-------	---------------	-------

4.3.2.2 Security, misuse and crime

DLT is not a technology that exclusively encourages or discourages criminal acts. It depends on the application. The possibility of executing transactions under a pseudonym or completely anonymously can of course aggravate the described problems. This makes it important to address payment-related challenges right from the development stage of new DLT applications and to come up with technical and/or organizational solutions.

One approach could be to introduce an official European digital currency (which might be called the e-Euro or Crypto-Euro) as the legally compliant basis for DLT applications. This was also proposed by Christine Lagarde, Managing Director of the International Monetary Fund, in a speech he or she gave at the Singapore Fintech Festival in

¹³¹ See also section 4.2.2.

¹³² See also section 4.2.3.

¹³³ Brandt, Neue Kryptoprojekte bald so effizient wie Visa.

November 2018.¹³⁴ By enabling unambiguous identification of (legal) persons and documenting transactions, cryptocurrencies could also pave the way for applications that make it easier to fight crime while also meeting our expectations with regard to security, consumer protection, and data privacy.

4.3.2.2.1 Loss or theft of passwords or private keys

The biggest security challenge in connection with DLT implementations currently involves the private keys that asymmetrical cryptosystems require. If a private key is lost due to a technical glitch, stolen, or simply forgotten, it is no longer possible to log in. Unlike systems operated by an intermediary such as a bank, in the case of DLT it is usually impossible to restore a lost key. In the case of cryptocurrencies, this means that the money is irretrievably lost.

A recent example concerns QuadrigaCX, a Canadian cryptocurrency exchange. Its founder suddenly died in December 2018, taking keys required to access the exchange's wallets with him to the grave. Deposits worth about 190 million euros were thus effectively lost.¹³⁵ And according to Chainanalysis, a blockade analysis company, 23% of all bitcoins have been lost forever as a result of missing personal keys.¹³⁶

Large-scale theft of cryptocurrency has become a common occurrence. The most spectacular cases have all involved hacking cryptocurrency exchanges to steal bitcoins (a prominent victim was Mt. Gox, a Japanese exchange that has since declared bankruptcy).¹³⁷ However, these attacks have not targeted the underlying DLT but instead the exchanges' IT security systems, making them comparable to classic bank robberies.

To get around the problem of lost or stolen keys, these could be kept by intermediaries or software vendors, e.g. in so-called wallets, thus presumably reducing the risk of their complete loss. But this solution is not ideal, since the wallet providers then also become a very attractive target for criminals—and in fact have already frequently been preyed on by hackers. Once keys fall into the hands of criminals, these can freely dispose of the money. Billions of euros' worth of cryptocurrencies have been stolen in this way in recent years.¹³⁸

Many other applications are vulnerable to similar problems. If criminals get hold of private keys, they can use them to execute transactions or, for example, illegitimately sign off process steps. The actual consequences depend on the specific application, but in many cases this is directly comparable to identity theft.

It should be stressed that DLT systems themselves are regarded as relatively secure. The described problems affect other IT systems in similar ways. And like with other IT systems, what matters is the sum total of all implemented security measures. Plus, due to the rapid evolution of cryptocurrencies, these have not or could not have always

¹³⁴ Christine Lagarde, November 11, 2018: "Winds of Change: the Case for New Digital Currency", <https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency>

¹³⁵ Martin-Jung, Süddeutsche Zeitung, Feb. 4, 2019.

¹³⁶ Dittmer, n-tv, Nov. 29, 2017.

¹³⁷ See <https://www.mtgox.com/>.

¹³⁸ Martin-Jung, Süddeutsche Zeitung, Feb. 4, 2019.

been carried out with the requisite care and thoroughness, thus leading to the described situations.

4.3.2.2 The DAO hack

In 2015 a German DLT startup calling itself "Slock.it" began developing a framework for centralized autonomous organizations (DAOs) using Ethereum's Solidity smart contract programming language.¹³⁹ The idea was to create an open source standard for future decentralized organizations. In March 2016, Christoph Jentzsch, an employee of Slock.it, published a whitepaper describing the DAO code that had been developed for automating organizational governance and decision-making.¹⁴⁰ A sizeable community grew up around the project and launched the DAOhub forum to become independent of Slock.it. The DAOhub community then elected a group of 12 curators who were responsible for supporting the project, which was dubbed "The DAO" and hailed as the "mother of all DAOs".¹⁴¹ The DAO was launched on April 30, 2016 and held a four-week DLT-based crowdsale, collecting US\$150 million in crowdfunding.¹⁴² About six weeks later, an unknown person took advantage of a vulnerability in the smart contract code of The DAO to steal more than 3.6 million Ether worth US\$70 million at the time.¹⁴³ Slock.it, numerous cryptocurrency exchanges, and other informal technical decision leaders immediately took action to contain the damage, prevent the stolen Ether from being traded on exchanges, and launch counterattacks. In the end, however, the entire project was terminated and a hard fork of the Ethereum blockchain intentionally induced to restore the original state of the "immutable" ledger.¹⁴⁴

In the described case, flawed smart contracts were systematically exploited by hackers. Consequently, the actual protocol of the DLT, specifically of the Ethereum blockchain, was not itself affected. Instead, the hackers targeted the vulnerable source code of a program that a user had uploaded. To prevent more incidents of this kind in the future, templates and modules for frequently used smart contract applications can be expected to appear. In order to develop dependable standard modules, there is a need for certification and technical inspection agencies for testing the process and application integrity of smart contracts, and also for smart contract libraries and marketplaces. Warning systems should also be developed so weaknesses can be detected and fixed at an early stage.¹⁴⁵

Especially small organizations using blockchain and DLT stand to benefit from developments of this kind, since in contrast to large companies they are not in a position to

¹³⁹ DuPont, Bitcoin and Beyond 2017, 157.

¹⁴⁰ Jentzsch, Decentralized autonomous organization to automate governance. Whitepaper, November 2016.

¹⁴¹ Tual, Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir announced amongst exceptional DAO Curators.

¹⁴² DuPont, Bitcoin and Beyond 2017, 157, Etherscan, www.etherscan.io.

¹⁴³ Falkon, The Story of the DAO — Its History and Consequences.

¹⁴⁴ Securities Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO.

¹⁴⁵ Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, University of Passau, Blockchain und Smart Contracts.

establish their own departments for forging blockchain/DLT applications and smart contracts and must therefore rely on externally purchased expertise and services.¹⁴⁶

4.3.2.2.3 Other kinds of attacks

DLT networks that use the Proof of Work consensus mechanism are vulnerable to so-called 51% attacks, among other things. In order for such an attack to succeed, the attacker or attackers must control more than half of the network's computing power, allowing them to feign transactions, for example. This is highly improbable, however, given the large size of today's major cryptocurrency networks and the huge amount of computing power that would therefore be required.

"Double spending" is when an attacker succeeds in spending the same money twice by taking advantage of the latency period until a transaction is definitively confirmed to make a copy of the digital tokens and send it to another party as well. The risk of this scenario has been significantly reduced by the faster speeds at which transactions are now executed in today's DLT systems; in addition, watchful users can prevent it from happening, especially in the case of large transactions.

Finally, the interface to the real world is still a weak point in DLT security. For instance, even if sensor data are documented in a forgery-proof format, the sensor itself could be manipulated. But this attack scenario can only materialize if users are unaware of the risks and blindly trust information that has been stored in a DLT. In other words, although DLT reduces the danger of fraud, it cannot completely eliminate it.

4.3.2.2.4 Anonymity, tax evasion and money laundering

DLT implementations that ensure users' anonymity can permit criminal behavior such as tax evasion or money laundering. Bitcoin in particular was long suspected of being used mainly for black market transactions and money laundering. Since Bitcoin users hide behind pseudonyms, transactions conducted with bitcoins cannot be attributed to natural persons or legal entities, at least not directly. In the past, criminals have taken advantage of this fact to launder money.

Where other applications for DLT are concerned, whether to use an anonymity-preserving or non-anonymity-preserving implementation must be determined on a case to case basis. For B2B transactions in particular, it is generally out of the question and/or makes no sense to choose an anonymity-preserving system, because as a rule the parties involved are known to one another. It may therefore be presumed that the major problems affecting cryptocurrencies are rare or nonexistent in other applications.

4.3.2.3 Data protection and the GDPR

It should be kept in mind that data stored in a DLT system can be read by every other entitled participant. In order to nevertheless protect data from prying eyes, the idea of storing personal data or business secrets in encrypted form might be tried. But it

¹⁴⁶ Schütte/Fridgen/Prinz/Rose et al., Blockchain und Smart Contracts.

should be taken account that data stored in a DLT system may remain there forever without any possibility of changing them.

For the reasons described in section 3.6.2, it is to be expected that it will eventually be possible to decrypt with relatively little effort stored data that has been encrypted using today's technology, thus allowing it to be read by anyone. However, here it is important to distinguish between conventional encryption methods and hashing. In conventional encryption (with symmetric keys), there is a one-to-one correlation between the encrypted and unencrypted texts: if you know the key, you also know the plaintext text. Hash functions, which are "one-way", usually compress the data. In other words, each data packet is mapped onto another data packet of a smaller (fixed) length. A very large number of data packets yield exactly the same hash value, so no "key" is unique. Increasing the available computing power only produces more candidates for the original data packets.

This results in a set of "notes on use".¹⁴⁷ Only data that are absolutely essential for an application and can be revealed without violating data protection laws (i.e. "immediately become worthless") should be stored as plaintext in a DLT system, and only data that will become "worthless" in the foreseeable future should be conventionally encrypted. As far as is known today, hashed data can be securely stored provided that the original data are sufficiently long and "unstructured" (this can be achieved by, for example, conventionally encrypting them before hashing or by inserting long sequences of random digits). The result does not, strictly speaking, correspond exactly to the original information, which is lost as a result of hashing. However, it can be used to prove that information has not been altered since storing its hash value in the blockchain. If the old hash value on a DLT system corresponds to the hash value of data whose integrity needs to be demonstrated, then it may be assumed that they are identical to the original data. This approach is referred to as "combined on-chain and off-chain storage", since the actual data themselves are not present in the DLT system (and consequently cannot be deleted either), and the DLT system only provides proof of their integrity by storing hash values.

The supposed incompatibility of DLT with the GDPR is a frequently discussed issue. This topic will be taken up again in greater detail in section 5.2; here only the main nonlegal aspects are briefly presented.

Since DLT enables pseudonymization but not anonymization, any node operator can, now or in the future, use (encrypted or unencrypted) data on DLT systems, either by themselves or in combination with other data, to obtain information on individuals or corporate processes. The clever use of hash values (on-chain/off-chain combinations as discussed above) can dramatically reduce the risk of their deriving personal or confidential information from them and identifying the individuals concerned. However, the impossibility of retroactively deleting data rules out data sovereignty in the event of incorrect design or use or intentional misuse. Moreover, it may be possible to analyze metadata stored in a DLT system (activity of addresses (public keys)) to derive personal information. Especially in the case of public DLT systems, in which the individ-

¹⁴⁷ See the section on (in-)efficiency for a discussion of the technical limitations.

ual participants are basically responsible for data protection, this makes it difficult to comply with the data erasure requirements of GDPR. Despite this, DLT is compatible with the spirit of GDPR: it helps to promote sensible use of data and mainly hurts large data processors, which are threatened and could even be rendered obsolete by it. GDPR-compatible DLT solutions could definitely be designed, although in many cases this is only possible with workarounds and makes applications unnecessarily complex. The following three points illustrate this:

- (1) In blockchains that do more than simply document transactions, there are approaches (e.g. Zerocoin) that use cryptographic methods (zero-knowledge proofs) to uncouple owned assets and addresses from one another.
- (2) Complete anonymization, for instance by using new addresses (public keys) for every interaction that takes place on a blockchain, is basically feasible. This might be accomplished, for example, by advances in the field of self-sovereign identities (e.g. Sovrin¹⁴⁸).
- (3) On the other hand, complete anonymity is not wished by regulatory authorities, especially in connection with financial transactions. But attempts are being made to integrate "backdoors" in anonymization solutions that would permit access by authorized agencies (while preventing them from doing so secretly).

It would therefore be a good idea to see whether GDPR could be adjusted in a direction that, without opening the door for abuse, would pave the way for achieving more of the regulation's goals.

4.3.3 DLT and governance

4.3.3.1 Governance mechanisms for operating DLT systems

In connection with the governance of DLT systems, one issue is determining who is responsible for developing, implementing, operating, and maintaining them. Another important aspect is continual further development of DLT systems. It is also essential to anticipate future technical and societal requirements and ensure that systems appropriately respond to them.

Due to the fundamental decentralized character of DLT, newly arising DLT systems are calling for fresh governance approaches that differ from existing solutions. Unlike a centrally managed system, in a DLT-based solution a large number of stakeholders are directly involved in development and maintenance. The existence of a network of parties representing different interests adds complexity to tasks that until now have tended to be relegated to internal governance. This makes it necessary to create an appropriate set of rules for implementing responsibilities, decision-making powers, and incentives to maximize the benefits for all participants. New kinds of players that had never previously been part of regular techno-economic systems are also posing new kinds of questions.¹⁴⁹ The associated field of study is still relatively young, and many of these issues are now being actively addressed by researchers.¹⁵⁰

¹⁴⁸ See the general technical section.

¹⁴⁹ Mattila/Seppälä, Collaborative Value Co-Creation in the Platform Economy 2018, 183.

¹⁵⁰ Beck/Müller-Bloch et al., Journal of the Association for Information Systems, 2018, 1020-1034.



In order to be competitive in the digital economy, besides making investments in information technology (IT) it is also important to acquire knowledge of IT governance. IT governance involves mechanisms for properly organizing and effectively deriving benefits from IT.

Grembergen/Haes in Bui, Proceedings of the 51st Hawaii International Conference on System Sciences, 4877.

As DLT becomes increasingly well-established, different approaches to DLT governance are emerging. Owing to the decentralized structure of all DLT solutions, entrusting their operation and maintenance to a single central party should be avoided as far as possible. However, mostly for the sake of efficiency, a centralized structure is needed for developing a DLT system and performing the associated research activities. To mitigate this centralized character, DLT systems tend to be open-source projects. Three main governance models have crystallized for development, implementation, further development, and marketing. They include projects carried out by communities, foundations and companies.

Many DLT systems, a case in point being the Bitcoin network, completely lack a central administrative entity. Instead, both organizational and productive tasks are assumed by the user community. Here attention should be called once more to the fact that Bitcoin is backed by a core team of developers who manage the blockchain repository. Any significant changes to the program code require the community's consent and may not be implemented by the team of developers in an uncontrolled manner. In systems of this type, governance primarily arises via the team of developers and acceptance of the protocol by the community.¹⁵¹ Development, implementation, further development, marketing, operation, and maintenance of the infrastructure are largely performed by the community. In other words, anyone can participate in executing the protocol and developing it further. Whether or not a given change is ultimately adopted for the entire system depends primarily on the network participants who use the DLT protocol. The more support a change receives from members of the community, the more likely it is that it will be adopted. Special challenges arise when there is disagreement in the community about the system's future. This phenomenon occurred a few years ago in connection with the Bitcoin and Ethereum blockchains, both of which wound up forking into two separate networks. These schisms were prompted by opposing views within the communities: in Bitcoin regarding how to increase block capacity, and in Ethereum on how to eliminate a security vulnerability. While part of the communities supported the original protocol, another part backed changes that led to a split.

In addition to this completely community-driven brand of governance, in recent years foundations and companies in particular have been entrusted with governance functions. These approaches make it possible to fund projects while increasing the efficiency of a system's overall development process. The greater efficiency results mainly

¹⁵¹ Beck/Müller-Bloch/King, Journal of the Association for Information Systems 2018, 1020.

from the ability to make changes to the protocol without having to achieve a consensus within the community.

Both have been observed especially often in connection with ICOs, which have special needs: tokens are sold to raise funds for developing and marketing the DLT system.

However, this funding approach is often subject to the rules of the financial market in which an ICO is made. Investments of this kind are allowed in some parts of the world but forbidden in others. In Germany, this is regulated by the Federal Financial Supervisory Authority (BaFin).¹⁵² Another approach to governance that has appeared in connection with ICOs involves companies such as limited-liability or joint-stock corporations. Here the approach to governance resembles that of foundations, but often places much greater emphasis on operational business activities. In contrast to foundations, protocol development is usually a relatively centralized process.

Alongside these foundations and companies that have emerged from ICOs, established enterprises can also join in a consortium to develop and operate a DLT system. A well-known example is the R3 consortium¹⁵³, which now comprises more than 200 companies. In this case as well, the protocol is open-source, meaning that it can be freely viewed and used. The Corda network developed by R3 is managed not by the community, but instead by the Corda Network Foundation.¹⁵⁴ The foundation's directorship is elected by the members of the Corda network and is supposed to act independently of the R3 member companies. The intention is to achieve more transparent, credible management of the network. Another example of a DLT initiative involving a group of companies is Hyperledger.¹⁵⁵ Its protocols are also open-source software. The Linux Foundation¹⁵⁶ launched the Hyperledger umbrella project and is responsible for technically managing it. This means that all technical decisions, such as which new functions to implement, are made by developers who have in turn been selected by the community. Operation and maintenance of this network differ from those of Bitcoin, Ethereum and IOA, since it is private and permissioned instead of public and permissionless. So each collaborating company, or group of companies, operates the DLT system. Changes can also be made by them individually after they have consulted the others.

4.3.3.2 DLT as a governance mechanism

DLT systems, and projects to develop them, require appropriately implemented governance rules. In turn, their attributes and possibilities can potentially also contribute to implementing better governance mechanisms. As already mentioned, "governance" refers to a set of organizational rules for a system. So far, discussions of this topic have generally been purely theoretical, often referring to constructs that have not yet been actually implemented in practice. They revolve mainly around two central precepts. One is the principle of transparency, which most DLT systems share and (it is hoped)

¹⁵² Hahn/Wons, Initial Coin Offering (ICO).

¹⁵³ <https://www.r3.com>.

¹⁵⁴ <https://corda.network>.

¹⁵⁵ <https://www.hyperledger.org>.

¹⁵⁶ <https://www.linuxfoundation.org>.

has potential for generating a host of benefits, and the other is so-called decentralized autonomous organizations (DAOs).¹⁵⁷

One possible approach for improving corporate governance involves mapping the ownership structure of a company onto a DLT system by issuing digital share certificates.¹⁵⁸ This could yield various desirable benefits. One is greater transparency of ownership situations, which can be expected to affect different interest groups in different ways. While owners of only a small number of shares and investment fund managers are likely to have an interest in greater transparency, the situation with larger shareholders and employees would diverge. According to the author, large shareholders could purchase more shares in enterprises that are not mapped onto a DLT solution and therefore characterized by less transparency. It would also be potentially easier to detect insider trading. But the extent to which it is desirable or feasible to deanonymize companies' shareholders is unclear. DLT systems could also be used to distribute tokens to listed shareholders that entitle them to vote in elections. The hope is that this would improve the precision and verifiability of election results while curbing attempts to influence them by secretly lending shares to others. It could also facilitate audits, assuming that companies execute their financial transactions via a DLT system, due to its transparency and safety from retroactive tampering.¹⁵⁹

From an economic standpoint, smart contracts could potentially affect principal-agent relationships.



Principal and Agent Theory

This theory addresses problems that arise in relationships involving a person or entity (the agent) who is in a position to make decisions or act on behalf of another person or entity (the principal). Such a relationship is always problematic when there are conflicts of interest and one of the two is better informed than the other. The deviation of the actual costs incurred from the costs of an ideal solution is called the agency cost. The goal is to minimize this cost, for example by concluding agreements that provide an incentive.

Hochhold/Rudolph, Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende 2011, 131.

For example, companies can reduce the moral risk by agreeing to a smart contract (which can no longer be revoked once it has been activated in a DLT system), thus sending a message to refrain from opportunistic behaviors in the future. This has potential for lowering the agency cost.¹⁶⁰ In this context, smart contracts can harmonize the interests of different groups, e.g. with incentive systems that involve distributing tokens (see 4.2.5.6) to interest groups via a DLT system.¹⁶¹ Here the basic idea is to give participants in a network, and possibly also in business models implemented on the basis of it, a direct interest in the success of a given application. The transaction costs

¹⁵⁷ Shermin, Strategic Change 2017, 499.

¹⁵⁸ Yermack, Corporate Governance and Blockchains.

¹⁵⁹ Yermack, Corporate Governance and Blockchains.

¹⁶⁰ Yermack, Corporate Governance and Blockchains.

¹⁶¹ Shermin, Strategic Change 2017, 499.

can be reduced by standardizing the rules for smart-contract-based transactions. This works because the rules of interaction are formalized in smart contracts and, after the parties have consented to a smart contract (e.g. using digital signatures), automatically executed in the DLT system under certain defined conditions.^{162, 163, 164}

A case study¹⁶⁵ on a decentralized (autonomous) organization assesses the potential of DLT for governance. It reveals that criteria diametrically opposed to the ideal of decentralization are often still applied, especially when developing DLT-based applications. When these applications are then used, however, it turns out that the decision-making rights are more decentralized than in centralized applications: for example, pricing is directly left to providers whereas in other cases it is directly influenced by the owners of technical infrastructure. Concerning the assumption of responsibility in connection with DLT applications, according to the authors a central intermediary is still required to resolve disputes. Reputation systems are therefore often implemented in DLT systems to encourage the assumption of responsibility. Another interesting aspect of incentivization is that when interest groups use DLT systems as a digital infrastructure for providing services, this also gives them an incentive to maintain the infrastructure themselves, for example.¹⁶⁶ In particular, this could include operating network nodes, active involvement in open-source protocol development, and publication of relevant tools.

4.3.4 Implications for competition policy

Assuming that the use of DLT will become widespread, it may also have implications for competition policy. The use of DLT to create a neutral information layer can potentially offset information asymmetries. In addition, the opportunity to participate in an open system can facilitate market entry by lowering barriers and thus encouraging competition, thanks to the basic possibility of implementing applications on (public) DLT systems and in smart contracts.¹⁶⁷ Another idea concerns the use of smart contracts: patent application processes, for example, could be standardized and DLT systems used to store patent information in a way that makes it generally accessible.¹⁶⁸

Due to the greater transparency of DLT systems, it is to be expected that irregularities in financial and other transactions will become easier to spot. For example, unlawful collusion could be revealed, although this begs the question as to how much access to DLT systems must be ensured.¹⁶⁹ It is especially urgent to answer this question in connection with permissioned DLT systems (see section 3.3.1). The opposing view maintains, however, that DLT is more likely to encourage collusion, since it can be used to make market information more readily accessible, thus also setting the stage for illegal price fixing etc.¹⁷⁰ Assessments of this position suggest, however, that these objections

¹⁶² Glatz, What are Smart Contracts? In search of a consensus.

¹⁶³ Shermin, Strategic Change 2017, 499.

¹⁶⁴ Pike/Capobianco/Gomes, Blockchain Technology and Competition Policy - Issues paper by the Secretariat.

¹⁶⁵ Beck/Müller-Bloch et al., Journal of the Association for Information Systems, 2018, 1020-1034.

¹⁶⁶ Beck/Müller-Bloch et al., Journal of the Association for Information Systems, 2018, 1020-1034.

¹⁶⁷ Cong/He, Blockchain disruption and Smart Contracts.

¹⁶⁸ Tulpule, CPI Antitrust Chronicle 2017, 45.

¹⁶⁹ Pike/Capobianco/Gomes, Blockchain Technology and Competition Policy - Issues paper by the Secretariat.

¹⁷⁰ Cong/He, Blockchain disruption and Smart Contracts.

are to some extent exaggerated, and that public antitrust bodies will improve their monitoring processes and methods in response to new technological developments.¹⁷¹ Overall, DLT could make it easier to provide evidence of restrictive practices when prosecuting presumed cartels, owing to its built-in protection from retroactive tampering.¹⁷²

How DLT is assessed in legal terms and its implications for subsequent action within the scope of competition policy law may have enormous repercussions for companies. Based on a preliminary assessment, competitive restrictions may be imposed mainly on domain-specific DLT systems (or their developers) for their role as operators of a dominant infrastructure. They could, for example, be prevented from arbitrarily setting prices in their respective DLT systems or taking other steps that might potentially exclude competitors.¹⁷³ Overall, this aspect favors the implementation of appropriate governance mechanisms and corresponding systems by suitable neutral organizations.

Technical standards, which representatives of various industries have often called for as being essential for the broad dissemination of DLT,¹⁷⁴ are also relevant to competition policy. For one thing, technical standards are generally believed to foster competition. However, it is vital to ensure that standards are not established by groups with vested interests while excluding other groups or making it difficult for them to enter the market.¹⁷⁵ In this context there is also discussion of the extent to which access to permissioned DLT systems must be granted if this is required in order to enter a market and/or gives competitors a significant extra advantage. To judge this, however, various aspects must be considered, for example whether or not and if so under which circumstances it can be justified to exclude players.¹⁷⁶



Promoting Cooperation

It is important to clarify the extent to which incentives can be provided, especially for the purpose of motivating competing market players to participate. The nature and structure of DLT systems make them dependent on cooperation by various organizations, since otherwise it would be impossible to establish decentralized networks. It is known that DLT solutions are subject to Metcalfe's Law, according to which the impact of a telecommunications network is proportional to the square of the number of connected users. In the age of digitalization, the importance of cooperation is increasing as a consequence of smaller-scale value creation. It is therefore essential for many DLT networks to make initial investments to enable cooperation and collaboration. After achieving a critical mass, they can then become self-sustaining. To define the focuses of promotional policies, it appears necessary to achieve legal security by analyzing the situation in the context of antitrust law.

Metcalfe, Computer 2013, p. 26.

¹⁷¹ Simpson/Cooke, Blockchain: competition issues in nascent markets.

¹⁷² Tulpule, CPI Antitrust Chronicle 2017, 45.

¹⁷³ Simpson/Cooke, Blockchain: competition issues in nascent markets.

¹⁷⁴ Hyland-Wood/Khatchadourian, The JBBA 2018, 3724; Michael Ortmeier 13.02.2019.

¹⁷⁵ Simpson/Cooke, Blockchain: competition issues in nascent markets.

¹⁷⁶ Simpson/Cooke, Blockchain: competition issues in nascent markets.



Sandboxes and Living Labs

Analogously to other technological experiments, DLT can also benefit from experience gained in experimental environments that are delimited in terms of time and space (and possibly other parameters as well) and in which certain legal requirements are suspended. This would help drive greater innovation (e.g. charging infrastructure in communities of housing owners). Such an approach is necessary because regulation typically lags behind technical progress. It is being successfully practiced on a large scale in other countries and to some extent has also been implemented in Germany, like with the SINTEG smart energy showcases set up in connection with the Energy Revolution.



Design According to Liberal Democratic Principles

The state should be actively involved in designing DLT solutions and systems in keeping with liberal democratic principles. Among other things, this means that the state itself applies this technology in pilot projects, thus serving as a role model. Prohibiting the use of the technology (like other nations have done in connection with cryptocurrencies) should be avoided. It would be difficult in any case to prevent it from being used owing to its inherent attributes (such a decentralization). Since DLT systems by nature allow disintermediation, this could also be taken advantage of for functions performed by the state. The state should consider this in good time. If DLT is used to carry out state tasks and functions, the state can also share responsibility for setting up and/or operating the corresponding systems and networks. An appropriate division of responsibilities (among ministries, organizations, and the federal and state governments) should be discussed at an early stage.



Technological Strategy

Since the technologies around DLT are not evolving in a linear fashion, it is important to regularly monitor their benefits and implementation. Neutral and objective assessments are necessary for sensibly evaluating opportunities and risks. Biased assessments can potentially have a detrimental effect on opportunities for deriving socioeconomic benefits. Misperceptions, myths, and "fake news" (like in connection with energy consumption and crime) hinder this. A stakeholder dialog with (interested) citizens, large, small and medium-sized companies, and blockchain start-ups would help in presenting a realistic picture of the technology and the associated opportunities and risks. Moreover, the German state recognized at a relatively early stage that DLT was worth investigating, and has already demonstrated its willingness to shoulder the associated responsibilities.

4.4 DLT in the Mobility Sector

In the mobility sector, which is being shaped more and more by automation and digitization, the use of DLT is growing. It is inherently suited for addressing many re-

quirements associated with current developments; examples include increasingly networked vehicles, intermodal transportation schemes, and greater future decentralization of this sector with autonomous traffic participants. This section surveys existing DLT initiatives in the mobility sector. Going further, it then derives and describes the basic areas of application in this sector. Finally, it introduces the four applications that are analyzed in detail in the special part of this study.

4.4.1 Fields of application

The first step was to identify a large number of existing DLT initiatives and assess their impact on the mobility sector by reviewing the relevant literature, searching the Internet, and interviewing a large number of experts. The findings are shown in Figure 20 below.

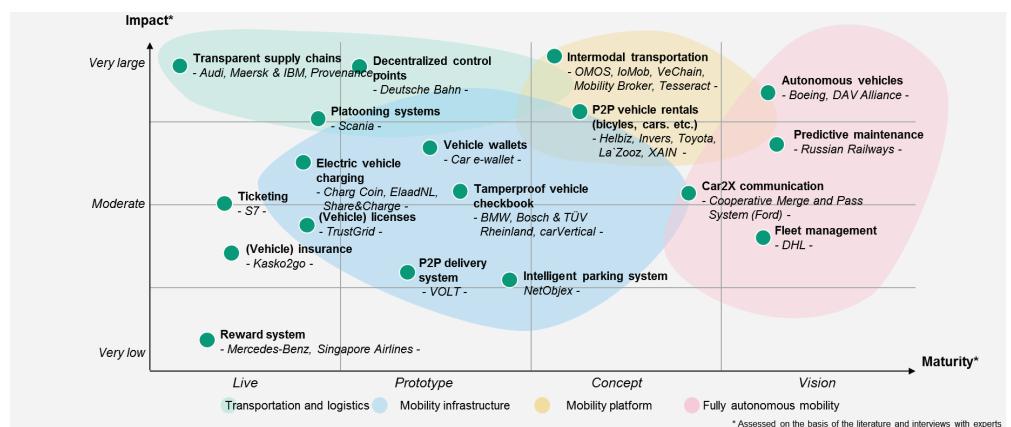


Figure 20: Overview of existing initiatives and identified applications

Depending on initiatives' level of maturity, they are classified as live, prototype, concept, and vision. In terms of their impact, they differentiated on a scale ranging from very low to very high. Mapping them in these two dimensions—maturity and (potential) impact on the mobility sector—clusters of similarly oriented and advanced initiatives appear. The four identified clusters have been labeled *transportation and logistics*, *mobility infrastructure*, *mobility platform*, and *fully autonomous mobility*. It is also obvious that numerous initiatives exist where these overlap as well as across different application areas.

To establish a consistent understanding and clear definitions of important concepts, the four identified clusters are briefly described in the following.

The application area of **transportation and logistics** spans initiatives that aim to leverage DLT solutions above all in order to increase the transparency and efficiency of processes and collaboration involving multiple transportation and logistics providers. Owing to the stiff competition in this domain, there is considerable pressure to innovative. Consequently, currently many different applications are being experimented with, which also demonstrates that this area has already attained a relatively high level of

maturity. For example, Maersk and IBM have developed and introduced a decentralized DLT register called TradeLens in which globally operating trading partners can model the supply chains for the goods they transport in order to speed up and improve cooperation between government agencies and freight forwarders.¹⁷⁷ In a project with Nord/LB, moreover, a DLT-based prototype was developed for optimizing the processes involved in creating and handling letters of credit. Letters of credit play a particularly important role in the logistics sector, where importers use them to assure exporters that they will pay their bills provided that certain conditions are met. Since the currently used paper-based approach is very slow due to the large number of parties involved, this initiative has great potential for replacing it with a digital DLT-based process. In addition, the we.trade consortium is working on a DLT platform for facilitating the conclusion and administration of contractual agreements between banks and their clients such as logistics service providers. Due to the pioneering character of the individual initiatives, the use of DLT in the field of transportation and logistics can be expected to have a major impact on the mobility industry. However, the cited initiatives must first gain additional experience and put the developed DLT solutions to the test.

The initiatives belonging to the cluster of **mobility infrastructure** include solutions that make it possible to intelligently and inexpensively launch charge points for electric vehicles and enable reliable and, for consumers, straightforward and transparent charging. Many of them have already reached the prototyping stage and will presumably have between moderate and great impacts on future mobility while fostering the widespread availability of charging opportunities. In particular, this could address the challenges posed by the limited range of today's e-vehicles and the considerable amount of time required to charge them. It also has potential for advancing the achievement of the German government's target, anchored in its Energy Concept 2010, of increasing the number of electric vehicles in Germany to six million by the year 2030.¹⁷⁸ Other examples of initiatives focusing on charging infrastructure are Share&Charge, ElaadNL, and Charg Coin, all of which are already being tested with prototypes. Here the focus is on establishing a consistent, DLT-based charging protocol that brings together various providers and simplifies or even automates payments between them. But the initiatives also include digital (vehicle) registration and driver's licenses, vehicle wallets, tamperproof vehicle checkbooks, and intelligent parking systems, among others. The applications in the field of mobility infrastructure are also characterized by the fact that nearly all of the initiatives will play a role in the field of fully autonomous mobility but can also already be taken advantage of today (with the exception of fully autonomous vehicles). They may thus also be regarded as accelerators or enablers of an infrastructure of the kind required for fully autonomous driving, along with the relevant standardization. Going further, one challenge is to create additional incentives to stimulate initiatives and investments in the field of mobility infrastructure and establish standards. For example, here there is an opportunity to enable, with the help of DLT and crowdfunding approaches based on it, private companies and individuals to help fund public infrastructure and profit from it later.

¹⁷⁷ In the context of the application of "freight papers", this initiative is addressed in greater detail in the special section (Chapter 6).

¹⁷⁸ BMWi, Energiekonzept für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung.

The application area of **mobility platforms** is inspired by the vision of implementing the idea of intermodal mobility. Initiatives of this cluster pursue the goal of integrating a variety of mobility services on a single platform and then making it available to customer via a unified platform or a single app (MaaS Alliance 2017).¹⁷⁹ Such a mobility platform opens up the possibility of fundamentally improving intermodal transportation and greatly boosting the mobility of individuals. They could then, for example, utilize such a solution to book a taxi to the train station, a train from there to the airport, and a flight to a holiday destination as a package requiring only a single confirmation and payment, instead of having to purchase a separate ticket for each leg of the journey. The high user-friendliness and low complexity of such a booking could also contribute to overcoming barriers to the use of public transportation and achieve greater utilization of its capacities. This would also reduce the number of vehicles using roads and thus contribute to improving the overall environmental balance sheet of mobility. In principle, it would also be conceivable to technically implement such a mobility platform without DLT in the form of an infrastructural system established, operated and controlled by a single enterprise. However, past attempts to accomplish this have failed mainly because established mobility providers refuse to collaborate for fear of dependencies.

Only on a smaller scale has it been possible, with initiatives like moovel, to create intermodal mobility platforms in individual cities such as Stuttgart. In order to create a scalable solution that would work for entire countries or regions, in the long term the large number of involved mobility providers and the required extensive collaboration make it sensible to choose a DLT-based platform. The initiatives of this kind—such as IoMob, Mobility Broker, OMOS, Tesseract and VeChain—are all currently in the inception phase. Agreeing on shared standards is a long and arduous process and confronts mobility providers with the challenge of entering into strategic partnerships. Implementation is therefore presumably only feasible in the medium to long term.

The area of **fully autonomous mobility** includes initiatives that pursue the vision of fully automated mobility. The case of autonomous vehicles assumes central importance here. Several companies in the automotive industry are already working on ideas for making self-driving cars and trucks a reality. It will probably also eventually become possible for public road vehicles, waterborne vessels, and aircraft to operate autonomously. Aircraft manufacturer Boeing is already designing and testing self-flying planes, and aims to have them ready for use by 2030. The key function for autonomous vehicles is reliable communication with their surroundings. A very promising approach for this is a DLT-based communication protocol. In the case of cars, it would enable wireless car-to-X communication, in other words between an automobile and elements of the road infrastructure.¹⁸⁰ The decentralized nature of DLT in particular is regarded as vital for providing protection from aggression and system failures. Apart from that, the development of self-driving vehicles will greatly benefit from the initiatives of in the fields of infrastructure and mobility platforms. Autonomous vehicles have enormous potential for influencing various other aspects of the mobility sector. Among

¹⁷⁹ MaaS Alliance, Guidelines & recommendations to create the foundations for a thriving MaaS Ecosystem.

¹⁸⁰ Rowan/Clear et al., Securing Vehicle to Vehicle Communications Using Blockchain Through Visible Light and Acoustic Side-Channels.

other things, intelligently controlled driving can reduce fuel consumption and increase passenger safety. Decreasing the number of required cars in metropolitan areas can also slash the need for parking spaces, and personalized services can improve passengers' mobility. The maturity of the presented initiatives is currently very low, since for the time being fully autonomous driving must be regarded as a vision for the future. And in any case, the associated ethical issues need to be clarified before self-driving vehicles are introduced on a large scale. The 20 theses advanced by the ethics commission formed by the German Federal Ministry of Transport and Digital Infrastructure (BMVI 2017)¹⁸¹ are an initial effort in this direction.

Figure 21 provides a summarizing overview of the identified application areas.

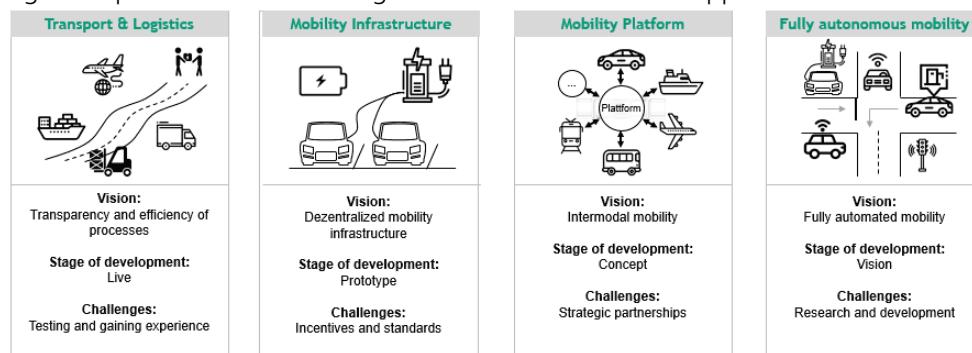


Figure 1: DLT application areas in the mobility sector

4.4.2 Preview of the special part of the study

The special part of this study takes a closer look at the just-described four application areas in the mobility sector that, based on public or academic discussions, seem pre-destined for the use of DLT. To keep the analysis in a suitable framework, one example has been chosen from each of the four application areas, described in detail, and analyzed to identify its potential. Each of the four descriptions is divided into an economic-technical part and a legal part. In the economic-technical part, first the current scenario, i.e. the status quo, is described along with the problems and constraints that characterize the present situation. Then the areas in which DLT may possibly prove to be advantageous for increasing efficiency in the affected industry are identified. Taking this analysis to its next logical step, after calling attention to the potential uses of DLT, a possible architecture of a DLT solution is sketched. The economic-technical part then concludes with a summary of the insights gained and—as far as appropriate—provides recommendations for action. The legal section on each application investigates, while referring back to the findings of the economic-technical part, the compatibility of the presented DLT solution with current laws. If any problems are identified here—particularly with respect to the challenges associated with data protection and privacy—thought is devoted to possible solutions, once again culminating in recommendations for action.

The first application falls under the heading of transportation and logistics and involves digitizing bills of lading and associated bank and supply chain processes in interna-

¹⁸¹ BMVI, Ethik-Kommission: Automatisiertes und Vernetztes Fahren.

tional maritime shipping. DLT can serve as an enabler for these, since it can model on an IT platform processes that have until now resisted digitalization for economic and/or cultural reasons. Due to the enormous potential benefits of this approach, it was often debated prior to the spread of DLT. Now it is possible to describe several initiatives and quantitatively assess their potential. It can also be shown that considerable progress has already been made in adding digital saving clauses to the existing laws and regulations.

The situation in the case of charging electric vehicles (which has been chosen to represent the category of mobility infrastructure) is different. Here the extent to which DLT can improve processes between charge point operators and eRoaming service providers (B2B¹⁸²) is analyzed. In contrast to the paper-based processes in international maritime shipping, here nearly all processes have already been digitized. But the market is still relatively small, young, and highly fragmented. It is therefore only possible to describe in qualitative terms how a DLT-based solution might differ from a prospective monopolistic provider and positively impact the acceptance of electromobility.

The third application is peer-to-peer ridesharing, in other words the organized provision of noncommercial opportunities to ride in others' vehicles. Its level of maturity is comparable with that of e-vehicle charging, but because it falls in the category of C2C¹⁸³ its structure and needs differ. Here too, it is difficult to quantify the potential of a DLT solution, since established platform operators such as Uber already exist and additional study is required to determine how much better a neutral platform is for a national economy than an established commercial ridesharing platform. Moreover, in the case of ridesharing currently these tend to focus more on supplementary functions such as payment processing than on exclusively brokering ride services.

The special section concludes by addressing the application of platooning: a technoeconomic system of road transportation in which two or more vehicles drive very close together to save costs. This is definitely the most visionary application, since in contrast to the other three the widespread use of platooning requires extensive retrofitting of trucks. Nevertheless, DLT could, in the form of a decentralized administered payment infrastructure for sharing achieved (fuel) savings, contribute to establishing platooning in the logistics sector. Since DLT-based payment processing for platooning would yield efficiency gains for trips already being made, in this case the potential can be quantitatively analyzed.

There is an opportunity for the Federal Republic of Germany, as a large national economy with highly regarded regulatory standards, to be the first to occupy what is currently still a vacuum in Europe.

¹⁸² Business-to-Business.

¹⁸³ Customer-to-Customer.

5 Legal Foundations

5.1 Civil Law Considerations

5.1.1 Smart contracts and automated contract execution

A smart contract can be understood as software that processes digitally verifiable events and executes legally relevant actions based on this, resulting in automated contract implementation.¹⁸⁴ If programmed accordingly, a smart contract can also perform functions similar to those of a trustee or escrow agent.¹⁸⁵ For example, the solvency of a contracting party can be ensured by providing the owed sum to the smart contract beforehand. However, the payment is not released to the recipient unless and until an agreed event is reported to the smart contract. In this case, the smart contract assumes the role of a trustworthy third party that keeps the amount to be disbursed, checks whether the agreed event has taken place and, if it has, issues the payment. On the other hand, a smart contract can be used in the way that another service or action will only be provided or carried out if the amount due has been paid. For example, the engine of a rented vehicle could be prevented from starting until the smart contract receives notification that payment has been made. This provides a strong incentive for a party to meet its part of the bargain, which becomes an objective precondition for receiving the reward. Overall, the use of smart contracts is supposed to reduce the risk of advanced performance for both sides.

Since smart contracts are nothing but software, they can also be used independently of DLT. However, implementing them in the context of a DLT system enables direct transactions and has the advantage of high tamper-resistance, thus ensuring the integrity of the program code. The execution of an agreed action is guaranteed (providing that the programming has been done correctly). The need to trust contractual partners and intermediaries is at least partly replaced by trust in the underlying technology, i.e. confidence that the transaction concerned will be executed without any errors.

5.1.2 Limitations on use

The use of smart contracts is subject to certain objective constraints. Not every exchange of goods or services can be completely modeled by software.¹⁸⁶ The reason is that the exchange must take the form of "if x, then y". The triggers are limited to those that can be digitally captured—e.g. charging of a battery with a certain amount of electricity, or traveling a certain number of kilometers. Information of this kind can be conveyed to a smart contract via interfaces called oracles. In addition, it must also be possible for software to execute, or at least initiate, the corresponding response, such as releasing a payment.

¹⁸⁴ See the definition proposed by Kaulartz/Heckmann, CR, 2016, pp. 618-624.; see also section 0 above.

¹⁸⁵ Heckelmann, NJW 2018, 504.

¹⁸⁶ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (620).

Vague legal terms (e.g. "after an appropriate time has passed") cannot be processed by smart contracts,¹⁸⁷ since software only works on the basis of predefined parameters and (at least so far) is unable to make value judgements.

These constraints are not rigid, however, since they can change with technical advances. As AI technologies continue to evolve, the possible uses of smart contracts can also be expected to expand.

5.1.3 Conclusion of contracts

The basis for mutual performance between two or more parties exchange is a contract. The conclusion of a contract presupposes at least two corresponding declarations of intent (an offer and its acceptance).¹⁸⁸ A declaration of intent is defined as any statement that expresses the will to induce legal consequences.¹⁸⁹ Within the process of concluding a contract, a smart contract can assume varying degrees of legal relevance.

5.1.3.1 Smart contracts as objects of agreements

Currently, the greatest practical relevance seems to lie in the cases where the conclusion of a contract is legally independent from the use of a smart contract. Whether or not certain conduct is equivalent to a declaration of intent, in other words whether it expresses a person's legal will, must be interpreted (acc. to Sections 133 and 157 of the German Civil Code) from the recipient's objective standpoint while considering all of the circumstances of the case in question.¹⁹⁰ This general rule does not change in the context of DLT applications. Executing DLT transactions can thus imply declarations of intent (in the context of both contractual and material obligations).¹⁹¹ More often, however, contracts are concluded independently of them, i.e. as a result of external circumstances.¹⁹² For example, providing an operational fueling station is regarded as an offer, and the use of it by a vehicle operator as acceptance of the offer.¹⁹³ These principles can also be applied analogously to the installation of charge points and the initiation of charging. When the parties agree that payment is to be made with the aid of a smart contract, this merely constitutes an ancillary agreement about the payment method.¹⁹⁴

In this context, the following should be considered: should smart contracts be used in practice for transactions with a broad public (as would be the case in the mobility sector), it is doubtful that the participating individuals will be able to directly interact with the DLT level and deduce how a smart contract works by looking at the program code.¹⁹⁵ As a rule, therefore, it will be necessary to design an interface that anyone can

¹⁸⁷ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (620).

¹⁸⁸ Jauernig/Mansel, Vorbemerkungen zu §§ 145 ff. Rn. 2.

¹⁸⁹ Staudinger/Singer, Vorbem. zu §§ 116-144 Rn. 1.

¹⁹⁰ Staudinger/Singer, § 133 Rn. 18.

¹⁹¹ Kaulartz/Heckmann, CR, 2016, pp. 618-624. (621); Paulus/Matzke, ZfPW, 2018, pp. 431-466. (448).

¹⁹² Compare Bertram, MDR, 2018, pp. 1416-1421. (1419); Djazayeri, jurisPR-BKR 12/2016 Anm. 1; Froitzheim, Rechtsfragen digitaler Transformationen, pp. 311-325. (314); cf. Heckelmann, NJW 2018, 504 (507); Kaulartz/Heckmann, CR, 2016, pp. 618-624. (621); Paulus/Matzke, ZfPW, 2018, pp. 431-466. (447).

¹⁹³ Jauernig/Mansel, § 145 Rn. 7.

¹⁹⁴ See also Paulus/Matzke, ZfPW, 2018, pp. 431-466. (438).

¹⁹⁵ See Kaulartz/Heckmann, CR, 2016, pp. 618-624. (621).

read and understand, for example in the form of an app.¹⁹⁶ Depending on the design of a given application, use of the corresponding functions will be interpreted as a declaration of intent.¹⁹⁷ The conclusion of a contract thus often precedes the use of the smart contract.¹⁹⁸ The smart contract is therefore comparable with the mechanical workings of a vending machine, which merely perform a contractual obligation under defined conditions.¹⁹⁹

Consequently, it is always necessary to distinguish between the legal (semantic) and technical (syntactical) levels,²⁰⁰ and only the former is relevant to the legal assessment. Despite its name, a smart "contract" must therefore not be regarded as a contract in the legal sense.²⁰¹

5.1.3.2 Conclusion of a contract using a smart contract²⁰²

However, it is also possible to use program code to express a declaration of intent,²⁰³ resulting in a smart contract that resembles a written contractual document. Using a programming language to formulate a contract is acceptable, at least for individual agreements. In keeping with the principles of free choice of language²⁰⁴ and freedom of design and form set forth in Section 311, Subsection 1 of the German Civil Code, the parties to a contract are at liberty to select any living or dead language²⁰⁵ for expressing their declarations of intent. In a legal system that is open to the use of technology, no distinction ought to be made between statements made in a natural language on the one hand and in program code on the other.²⁰⁶ The sending of a transaction may be regarded as the issuance of a declaration of intent, and the ability to call it up in the target wallet as its receipt.²⁰⁷ Moreover, a smart contract can not only express the content of one or more declarations of intent, but also (automatically) generate and communicate them, thereby concluding a contract.²⁰⁸

It is doubtful, however, whether program code may be used vis-à-vis consumers if it contains standard business terms, in other words if a programming language is used to express general terms and conditions.

First of all, one might argue that there is no acceptable way of consulting such standard business terms (in the sense of Section 305, Subsection 2, No. 2 of the German

¹⁹⁶ Also to meet the information obligations of sections 312 ff. of the German Civil Code, cf. section 5.1.4.2.

¹⁹⁷ Cf. Hoeren/Sieber/Holznagel/Kitz, Part 13.1 Rn. 11.

¹⁹⁸ Cf. Kaulartz, Taeger (ed.) – Smart World, 2016, pp. 1023-1037. (1031).

¹⁹⁹ Kaulartz/Heckmann, CR, 2016, pp. 618-624. (621).

²⁰⁰ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (624).

²⁰¹ Djazayeri, jurisPR-BKR 12/2016 Anm. 1; Kaulartz/Heckmann, CR, 2016, pp. 618-624 (619); Paulus/Matzke, ZfPW, 2018, pp. 431-466 (433 f.).

²⁰² This can increase in relevance, particularly with a future increase in M2M communications, cf. Kaulartz/Heckmann, CR, 2016, pp. 618-624. (621); on issues related to automatic declarations Heckermann, NJW 2018, 504 (506); Kaulartz, Taeger (ed.) – Smart world, 2016, pp. 1023-1037 (1032); Paulus/Matzke, ZfPW, 2018, pp. 431-466 (439 ff.).

²⁰³ Heckermann, NJW 2018, 504 (505); a.A. Djazayeri, jurisPR-BKR 12/2016, Note 1.

²⁰⁴ Kling, Sprachrisiken im Privatrechtsverkehr, 2008, pp. 305.

²⁰⁵ Staudinger/Singer, § 119 Rn. 18.

²⁰⁶ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (621 f.).

²⁰⁷ Paulus/Matzke, ZfPW, 2018, pp. 431-466 (447); on access when attaching a new block to a blockchain cf. Heckermann, NJW 2018, 504 (506).

²⁰⁸ Paulus/Matzke, ZfPW, 2018, pp. 431-466 (439).

Civil Code). In cases like this, the clauses concerned do not become part of the contract. An acceptable way of taking note of the contents exists if the clauses in question can at least be understood without additional effort. This has already been rejected for standards business terms written in English, despite the relatively large number of persons who know English.²⁰⁹ Therefore, it would be unreasonably difficult for an average consumer to understand the contents of program code.²¹⁰ If the applicability of Section 305, Subsection 2, No. 2 of the German Civil Code is denied due to a similarity between smart contracts and standard form contracts,²¹¹ contract passages formulated in software code could turn out to be "surprising clauses" in the sense of Section 305c, Subsection 1 of the German Civil Code. However, the use of a foreign language alone is not typically sufficient to render the content of clauses unusual or surprising.²¹²

Finally, the use of software code as a contract language can constitute an unreasonable disadvantage in the sense of Section 307, Subsection 1, Sentence 2 of the German Civil Code, which would render the clauses void according to Section 307, Subsection 1, Sentence 1 of the German Civil Code. In order to comply with the requirement of transparency, the party setting the terms and conditions must clearly and understandably describe the rights and obligations of the contractual parties so that the reader, while exercising due care and diligence, is able to sufficiently understand the meaning of a clause.²¹³ The use of clauses in foreign languages does not typically meet the transparency requirement due to their incomprehensibility.²¹⁴ This statement must therefore apply especially to the use of a programming language, since most people will lack even the most rudimentary knowledge of it. Consumers would have to rely on an expensive or time-consuming translation to learn about the content of a contract. Consequently, using a programming language to formulate standard business terms would inappropriately disadvantage consumers in accordance with Section 307, Subsection 1, Sentences 1 and 2 of the German Civil Code. This may change eventually if generally understandable programming languages are developed.

5.1.4 Contractual content and mandatory law

Regarding the content of contracts, the legal level takes precedence over the technical level.²¹⁵ The content of a contract²¹⁶ must be determined by interpreting the declarations of intent as per Sections 133 and 157 of the German Civil Code. This agreement between parties must then be technically implemented. If contradictions or gaps arise

²⁰⁹ Ulmer/Brandner/Hensen/Ernst, Part 2 (44) Rn. 32.

²¹⁰ Paulus/Matzke, ZfPW, 2018, pp. 431-466. (459 f.); cf. BeckOGK/Lehmann-Richter, June 1, 2018 on the German Civil Code, Section 305, Rn. 220, 256.3; in German: Ulmer/Brandner/Hensen/Ulmer/Habersack, § 305 Bürgerlichen Gesetzbuchs Rn. 151, Teil 2 (44) Rn. 32; in English LG Berlin, Judgement of May 9, 2013 – 15 O 44/13, CR 2014, 676; Jauernig/Stadler, § 305 Rn. 14.

²¹¹ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (622).

²¹² Cf. on German-language terms and conditions of business for foreigners who don't speak German, BAG, Urteil vom 19.3.2014 – 5 AZR 252/12 (B), JuS 2015, 65 (66); Ulmer/Brandner/Hensen/Ulmer/Schäfer, § 305c BGB Rn. 18.

²¹³ Schulze/Schulte-Nölke, § 307 Rn. 21.

²¹⁴ Ulmer/Brandner/Hensen/Ernst, Teil 2 (14) Rn. 15, (44) Rn. 23, (51) Rn. 5.

²¹⁵ Cf. Heckelmann, NJW 2018, 504 (507).

²¹⁶ On the influence of virtual currencies on contractual typology, see Ammann, CR, 2018, pp. 379-386. (380 f.); Beck/König, JZ, 2015, pp. 130-138.; Heckelmann, NJW 2018, 504 (508); Kaulartz, CR, 2016, pp. 474-480. (477 f.); Paulus/Matzke, ZfPW, 2018, pp. 431-466. (450 f.); Reiter/Methner in Taeger, Rechtsfragen digitaler Transformationen, 359 (365 f.); Shmatenko/Möllenkamp, MMR, 2018, pp. 495-501. (498 ff.); Spindler/Bille, WM, 2014, pp. 1357-1361 (1362).

between what is agreed and what is implemented, steps must be taken to achieve the agreed conditions.²¹⁷

The effects of a smart contract must of course be compatible with applicable laws.²¹⁸ These are always the measure of a contract's validity and legality.²¹⁹ The content captured in a DLT system, on the other hand, makes no statement about the legal correctness of individual entries.²²⁰ This means that the act of programming may, on purpose or inadvertently, yield results that violate existing laws and must therefore be corrected.

Occasionally the question is raised whether automatic execution by a smart contract can constitute unlawful interference with possession in the sense of Section 858, Subsection 1 of the German Civil Code.²²¹ This question must be asked in particular if access to or use of something can be blocked by a smart contract (e.g. a leased car that can no longer be started if a payment is missed, or a smart lock that prevents occupants from entering a dwelling until they have paid the rent). In cases of this kind, it must be ascertained whether possession has been compromised in a way that qualifies as unlawful interference. In addition, specific questions need to be asked in connection with the type of contractual relationship in each case—for example, in connection with the protection granted to residential tenants. In the cases that this study investigates in the mobility sector, this issue is less relevant, since smart contracts are only used there to facilitate payments. The tokens used are not things in the sense of Section 90 of the German Civil Code, so the provisions of Section 858, Subsection 1 of the German Civil Code may at most be applicable by analogy. In addition, smart contract-based transactions are often set up so that the party owing payment must pay up front (see 5.1.4.1.1). He or she relinquishes control over a certain sum of money in advance by authorizing the smart contract to execute a corresponding transaction. The smart contract therefore does not access property that is under the payer's control, and consequently it is unlikely that the recipient unlawfully interferes with possession.

5.1.4.1 Content review, Sections 307-309 of the German Civil Code

If a smart contract is intended to express declarations of intent (see section 0) and contains conditions that are pre-formulated for a large number of contracts and have been unilaterally inserted by one party (Section 305, Subsection 1 of the German Civil Code), then these are subject to the legal restrictions on standard business terms and thus also to the tests of Sections 307 to 309 of the German Civil Code.²²² There are no differences from the content review of other contracts, since in this case contractual terms are merely expressed using a programming language. This is only relevant to business transactions with entrepreneurs (Section 310, Subsection 1, Sentence 1 of the German Civil Code), since the use of program code as the contract language is not permissible vis-à-vis consumers (see section 0).

²¹⁷ Djazayeri, jurisPR-BKR 12/2016 Anm. 1.

²¹⁸ Djazayeri, jurisPR-BKR 12/2016 Anm. 1; Froitzheim, Rechtsfragen digitaler Transformationen, pp. 311-325. (314); Heckelmann, NJW 2018, 504 (509); Kaulartz/Heckmann, CR, 2016, pp. 618-624. (623).

²¹⁹ Heckelmann, NJW 2018, 504 (507); Paulus/Matzke, ZfPW, 2018, pp. 431-466. (448).

²²⁰ Paulus/Matzke, ZfPW, 2018, pp. 431-466. (437).

²²¹ Djazayeri, jurisPR-BKR 12/2016 Anm. 1; cf. also C. Paulus/Matzke, CR, 2017, pp. 769-778.

²²² Kaulartz/Heckmann, CR, 2016, pp. 618-624 (622).

When the use of a smart contract is agreed as a method of performance (see 5.1.3.1), this is typically accomplished with standard terms of business. It is therefore important to investigate the extent to which stipulating automated performance of standard business terms in connection with a contract passes the content review.²²³

5.1.4.1.1 Breach of Section 309, No. 2 of the German Civil Code

First of all, automated execution could constitute a violation of Section 309, No. 2 of the German Civil Code. Section 309, No. 2a) of the German Civil Code forbids the exclusion or restriction of an existing right to refuse performance (from Section 320 of the German Civil Code), while Section 309, No. 2b) of the German Civil Code bans any exclusion or restriction of the right of retention set forth in Section 273 of the German Civil Code (provided that it is based on the same contractual relationship) via standard business terms. . Since as a rule the execution of a smart contract cannot be halted once it has begun, the user is in effect prevented from exercising any applicable right to refuse performance or right of retention. Unlike, for example, a debit authorization, DLT transactions provide no means of instructing a bank to cancel a payment or recovering sums once they have been transferred.²²⁴

However, automated execution bears a certain resemblance to an agreement of an obligation of advance performance. This means that one party's contractual obligations are due before the other party's.²²⁵ The use of a smart contract per se does not oblige one party to perform completely in advance, i.e. before receiving the contracted product or service in return. Still, the user relinquishes control over the funds beforehand and as a rule is no longer able to unilaterally prevent them from passing to the other party. The intention of Section 309, No. 2 of the German Civil Code is not to generally forbid parties to agree on obligations of advance performance. Tests of such agreements are therefore based not on Section 309, No. 2 but on Section 307 of the German Civil Code.²²⁶

5.1.4.1.2 Unreasonable disadvantages as per Section 307, Subsection 1, Sentence 1 of the German Civil Code

An agreement to automate the performance of a contract could impose unreasonable disadvantages in the sense of Section 307, Subsection 1, Sentence 1 of the German Civil Code. An unreasonable disadvantage occurs when the user of standard business terms unilaterally pursues interests and fails from the outset to adequately consider the other party's legitimate interests.²²⁷

A starting point for assessing a clause of a consumer agreement (Section 310, Subsection 3 of the German Civil Code) that calls for the use of a smart contract can be found in the legal assessment of the aforementioned obligations of advance performance. .

²²³ Cf. Bertram, MDR, 2018, pp. 1416-1421 (1420); cf. Schrey/Thalhofer, NJW, 2017, pp. 1431-1436 (1436).

²²⁴ Cf. BeckOGK/Weiler, Jan. 1, 2019, BGB § 309 No. 2 Rn. 74.

²²⁵ Jauernig/Stadler, § 320 Rn. 21.

²²⁶ BeckOGK/Weiler, Jan. 1, 2019, on the German Civil Code Section 309 No. 2 Rn. 28 ff.; cf. BeckOK on the German Civil Code/Becker, Nov. 1, 2018, Section 309 No. 2 Rn. 8; Jauernig/Stadler, Section 309 Rn. 3; MüKo BGB/Wurmnest, § 309 No. 2 Rn. 13; Palandt, Grüneberg, § 309 Rn. 13; Schulze/Schulte-Nölke, § 309 Rn. 13; Staudinger/Coester-Waltjen, § 309 No. 2 Rn. 7.

²²⁷ Ulmer/Brandner/Hensen/Fuchs, § 307 BGB Rn. 96.

Such agreements require an objective reason to justify the disadvantages imposed on the customer.²²⁸ Section 320 of the German Civil Code in particular provides a means of pressuring the contractual partner to perform their part of the agreement while providing a safeguard against the risk of their insolvency.²²⁹ However, this protection is not always required. For example, the use of advance performance clauses is regarded as permissible in mass market operations involving large daily volumes when the individual transactions involve a low business value and negligible warranty concerns and/or when advance performance coincides with the technical requirements of contract execution.²³⁰

It must also be taken into account that the use of smart contracts actually reduces the burden on users in comparison with a true obligation of advance performance. Without them, users would be required to completely fulfill their part of the bargain before receiving anything in return. In particular, smart contracts reduce the advance performance risks of both sides and ensure that only actually received products or services are charged for. Finally, automated performance also gives the user a guarantee that the provider will reciprocate. A situation in which a party has an interest in withholding their performance is most likely to arise in the event of technical malfunctions. These, as well as intentional manipulations of the accounting infrastructure, can be guarded against by certifying smart contracts and oracles. Automated contract execution does not unilaterally help the provider gain an advantage; it also grants the user adequate prospects of an appropriate counter performance in return,²³¹ so that the associated loss of leverage does not appear to constitute an unreasonable disadvantage.²³²

The preceding discussion is also relevant if one were to demand an objective reason for stipulating advance performance obligations in B2B transactions as well.²³³

5.1.4.2 Consumer contracts and special types of distribution

In the context of mobility, standards dealing with special approaches to distribution also deserve attention. Which specific standards these are will depend on the details of each individual case. In the following, attention is nevertheless called to several regulations that will probably assume relevance in connection with DLT-based mobility solutions.

In the presented scenarios, contracts are concluded electronically: via websites or apps or at self-service points (the latter mainly have importance in connection with vehicle charging infrastructure). Consequently, it is necessary for e-commerce transactions to

²²⁸ BeckOGK/Zschieschack, Dec. 1, 2018, BGB § 307 Vorauszahlungsklauseln Rn. 22; cf. BeckOK BGB/Becker, Stand: 01.11.2018, § 309 No. 2 Rn. 9; MüKo BGB/Wurmnest, § 309 No. 2 Rn. 13; Schulte/Schulte-Nölke, § 309 Rn. 13; Staudinger/Coester-Waltjen, § 309 No. 2 Rn. 7.

²²⁹ BeckOGK/Zschieschack, Dec. 1, 2018, on the German Civil Code § 307 Vorauszahlungsklauseln Rn. 23.

²³⁰ BeckOGK/Zschieschack, Dec. 1, 2018, on the German Civil Code § 307 Vorauszahlungsklauseln Rn. 26; BeckOK on the German Civil Code/Becker, Nov. 1, 2018, § 309 No. 2 Rn. 10.

²³¹ Cf. MüKo on the German Civil Code/Wurmnest, § 309 Rn. 13.

²³² Cf. BeckOGK/Zschieschack, Dec. 1, 2018, BGB § 307 Vorauszahlungsklauseln Rn. 27.

²³³ Graf von Westphalen/Thüsing, Vertragsrecht, Vorleistungsklauseln Rn. 15; BeckOGK/Weiler, Jan. 1, 2019, BGB § 309 No. 2 Rn. 98; Palandt/Grüneberg, § 309 Rn. 16.

meet the obligations of Sections 312i and 312j of the German Civil Code. The general obligations set forth in Section 312i of the German Civil Code apply to all of a trader's customers, in other words also B2B customers. Section 312j of the German Civil Code lists special obligations vis-à-vis consumers. The provider must use telemedia (electronic information and communication services) in the sense of Section 1, Subsection 1 of the German Telemedia Act. In other words, services must be used that convey the trader's and customer's declarations of intent of or at least allow the customer to submit an order by electronic means.²³⁴ In particular, this includes concluding contracts within the scope of mobile commerce (i.e. the use of mobile telephones as mobile terminals, for example with mobile browsers or apps, to electronically conduct commercial transactions).²³⁵ Here the definition of "service" must be broadly interpreted; it extends beyond that given in Section 611 of the German Civil Code and refers to anything performed by a trader that does not consist of supplying merchandise.²³⁶ Furthermore, a contracted service does not itself need to be provided electronically.²³⁷ Services in the mobility sector may therefore fall under the provisions of Sections 312i and 312j of the German Civil Code. These obligations are not subject to the restrictions of Section 312, Subsections 2 to 6 of the German Civil Code and always apply whenever a contract is electronically concluded.

A distance contract in the sense of Section 312c of the German Civil Code may be simultaneously concluded, thus invoking Sections 312d et seq. of the German Civil Code. In order for this to be the case, a contract must be concluded exclusively via telecommunications media, i.e. without requiring the physical presence of the parties to the contract.²³⁸ The trader must furthermore have at his or her disposal a system that is organized for remotely selling or providing services, i.e. he or she must have met the material and personnel-related prerequisites within his or her operation for regularly conducting off-premises or remote business activities.²³⁹ Here too, the concept of services is defined broadly so that anything provided for remuneration may be the object of a distance contract.²⁴⁰ Section 312c of the German Civil Code (as well as Section 312a, which contains general obligations for doing business with consumers) is, according to Section 312, Subsection 1, only relevant to consumer contracts in the sense of Section 310, Subsection 3. Moreover, none of the exceptions listed in Section 312, Subsection 2 must be applicable, since in that case, only Subsections 1, 3, 4 and 6 of Section 312a would apply.

The exception made in Section 312, Subsection 2, No. 5 for contracts relating to the carriage of passengers may be relevant. This applies to taxi and similar services such as chauffeur services, as well as to trips made using other forms of transportation.²⁴¹ Not

²³⁴ BeckOK BGB/Maume, Nov. 1, 2018, § 312i Rn. 15; Hoeren/Sieber/Holznagel/Föhlisch, Part 13.4 Rn. 56; MüKo BGB/Wendehorst, § 312i Rn. 31.

²³⁵ Spindler/Schuster, Schirmbacher, BGB § 312i Rn. 12.

²³⁶ BeckOK BGB/Maume, Nov. 1, 2018, § 312i Rn. 8; Spindler/Schuster, Schirmbacher, BGB § 312i Rn. 7.

²³⁷ BeckOK BGB/Maume, Nov. 1, 2018, § 312i Rn. 17; MüKo BGB/Wendehorst, § 312i Rn. 38; Spindler/Schuster, Schirmbacher, BGB § 312i Rn. 7.

²³⁸ Tamm/Tonner/Schirmbacher, § 9 Rn. 31.

²³⁹ Hoeren/Sieber/Holznagel/Föhlisch, Part 13.4 Rn. 39.

²⁴⁰ Hoeren/Sieber/Holznagel/Föhlisch, Part 13.4 Rn. 33; Tamm/Tonner/Schirmbacher, § 9 Rn. 18.

²⁴¹ Spindler/Schuster, Schirmbacher, BGB § 312 Rn. 40.

exempted, however, are brokers and booking platforms.²⁴² Section 312, Subsection 2, No. 9 may also be relevant, since automated business premises include all self-service facilities in which a trader's services are exclusively provided by way of an automated system.²⁴³

5.1.5 Treatment of performance problems and reversal issues

5.1.5.1 Performance problems

In the event of performance problems, automated processing can encounter certain limits. To begin with, not every failure to comply with obligations can be adequately captured or modelled by software. Whereas it is relatively easy to digitally establish whether a party has not complied with an obligation or has done so late or inadequately, poor performance is more difficult to assess. For example, deciding whether or not merchandise is defective probably exceeds the abilities even of the best oracles now in existence. In addition, the possible constellations involving violations of obligations to take due care and consideration and protect others from harm are so complex and numerous that it would be practically inconceivable to model them in a flow chart with if-then junctions. Other prerequisites for secondary judicial remedies, e.g. culpable behaviors, likewise cannot be easily digitally represented, or else depend on valuations in individual cases and therefore cannot be processed by smart contracts, at least not yet.²⁴⁴ Even in a constellation that could allow software-assisted handling, this eventuality would have had to be thought of beforehand and incorporated into the programming. Otherwise the parties' only recourse for asserting their rights is a court of law. In practical terms, the use of smart contracts makes most sense when the risk of performance problems is very slight or when these can be identified and assessed without value judgements.

5.1.5.2 Reversal of transactions

In every exchange, a situation can arise in which the transaction must be reversed. One party may rescind the contract, which creates an obligation to reverse transactions (Section 346, Subsection 1 of the German Civil Code).²⁴⁵ A transaction can also be invalid or declared null and void ex tunc as a result of being challenged²⁴⁶ (Section 142, Subsection 1 of the German Civil Code). In these cases, whatever has changed hands must be returned in accordance with Section 812, Subsection 1, Sentence 1, Alternative 1 of the German Civil Code.

The objection that the irreversibility of entries in DLT systems conflicts with reversal constellations does not hold up in a civil law context.²⁴⁷ While it is true that entries on already-made transactions can no longer be erased from the blockchain, the invalidity

²⁴² Hoeren/Sieber/Holznagel/Föhlisch, Part 13.4 Rn. 49; Spindler/Schuster, Schirmbacher, BGB § 312 Rn. 41.

²⁴³ BeckOGK/Busch, Dec. 1, 2018, BGB § 312 Rn. 52.1; Tamm/Tonner/Schirmbacher § 9 Rn. 43.

²⁴⁴ Paulus/Matzke, ZfPW, 2018, pp. 431-466. (463).

²⁴⁵ Also in the case of revocation in acc. with Sections 355 and 357 of the German Civil Code (unless this is excluded), MüKo BGB/Fritsche, § 355 Rn. 59.

²⁴⁶ On challengingg in case of use of smart contracts: Kaulartz/Heckmann, CR, 2016, pp. 618-624. (622); Paulus/Matzke, ZfPW, 2018, pp. 431-466 (454 ff.).

²⁴⁷ Also acc. to Paulus/Matzke, ZfPW, 2018, pp. 431-466. (460); a.A. Schrey/Thalhofer, NJW, 2017, pp. 1431-1436. (1435 f.).

of a contract does not imply that transfers of rights or acts carried out to perform the contact may not exist. This applies especially to cases of rescission, in which the original exchange reflects the legal situation and is not reversed until later. Furthermore, it is not transactions *per se* that are void, but the underlying legal acts.

Finally, there is also no legal requirement to destroy all documentation pertaining to a retroactively reversed transaction. If, for example, a payment is made by interbank transfer and must later be returned, the original transfer continues to appear in the account statements of the parties to the transaction. A comparison can also be drawn with land registry law: Section 46, Subsection 1 of the German Land Register Code mandates that incorrect entries must be deleted not by completely removing them from the register, but only by inserting a deletion note.²⁴⁸

The possibility that value transfers may occur that do not reflect the substantive legal situation, or that registers may document a formal legal situation that is substantively inaccurate, is not unique to DLT.²⁴⁹ When reversing a transaction, it is therefore sufficient to restore the legal economic situation by means of suitable reverse transactions.²⁵⁰

The details of rights to a refund under the law of restitution largely depend on the type of token transferred. Tokens essentially consist of nothing more than exclusive, unique, and non-reproducible database entries. In a token transaction, therefore, instead of actually moving a set of data only the entitlement to the database entry is changed.²⁵¹ The value of tokens arises either as a result of supply and demand or because they represent rights or claims.²⁵² After they have been assigned to a user's wallet, he or she can transfer the represented quantity of tokens by entering their private key.²⁵³

From this it follows that the factual possibility of accessing tokens, in the form of the right to change their database entries, is already an asset in the sense of Section 812, Subsection 1, Sentence 1 of the German Civil Code. So in any case, the previous assignments in the database must be restored when reversing a transaction. With so-called currency tokens or virtual currencies that can be used as means of payment,²⁵⁴ this is also sufficient. Their transfer is simply a real act.²⁵⁵ Since tokens are not physical things, they also cannot be acquired in good faith.²⁵⁶ If a token represents a claim or right (like in the case of "utility tokens", which can be exchanged for a good or service,²⁵⁷ and some so-called asset-backed tokens, namely those that reflect a right to a certain asset²⁵⁸), authorizing a token transaction may be interpreted as an implied dec-

²⁴⁸ Saive, DuD, 2018, pp. 764-767 (767).

²⁴⁹ Paulus/Matzke, ZfPW, 2018, pp. 431-466 (461).

²⁵⁰ Cf. Beck/König, AcP, 2015, pp. 655-682 (662); cf. Bertram, MDR, 2018, pp. 1416-1421 (1420); cf. MüKo BGB/Grundmann, § 245 Rn. 34; Paulus/Matzke, ZfPW, 2018, pp. 431-466 (460); cf. Saive, DuD, 2018, pp. 764-767. (766).

²⁵¹ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283; Paulus/Matzke, ZfPW, 2018, pp. 431-466. (437).

²⁵² Kaulartz/Matzke, NJW, 2018, pp. 3278-3283.

²⁵³ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3279).

²⁵⁴ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3279).

²⁵⁵ Heckelmann, NJW 2018, 504 (508); Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3280); Paulus/Matzke, ZfPW, 2018, pp. 431-466. (451).

²⁵⁶ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3283).

²⁵⁷ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3279).

²⁵⁸ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3280).

laration of assignment in accordance with Sections 398 and 413 of the German Civil Code.²⁵⁹ In the case of an invalid causal contract, in addition to restoring the original register entry it would also be necessary to reassign the claim.

If an asset-backed token represents ownership of a thing,²⁶⁰ in the event of a reversal every acquired position (property and/or possession) would have to be returned. However, it is questionable whether a token-based transaction can be sufficient for transferring property.²⁶¹ When authorizing a transaction, an implied declaration of intent can definitely exist within the scope of the in rem agreement. But if the original owner fails to allow the acquirer to at least indirectly take possession of the thing in question, there can at most be a surrogate in the sense of Section 931 of the German Civil Code. An acquisition in good faith would only be possible if the prerequisites of Section 934 are met. Since the acquisition (in good faith) of ownership to tokens is out of the question (see above), categorizing tokens as bearer instruments would not facilitate the acquisition of ownership.²⁶²

5.1.5.3 Access to arbitration bodies/creation of judicial interfaces

To assert their claims, the parties are obliged to resort to courts of law, which is also the normal procedure. The special feature of DLT transactions is that the claimant requires the participation of the adversary, since only the latter is able to execute the transaction by signing with their private key. So if it is about asserting a claim to a return transfer of tokens, the claimant has no choice but to petition for the other party to be sentenced to execute the reverse transaction.²⁶³ There are typically no third parties, such as a bank, that are able to do this for them.²⁶⁴ The execution of a DLT transaction is an example of an act that cannot be performed by a proxy in the sense of Section 888, Subsection 1, Sentence 1 of the German Code of Civil Procedure and can only be enforced under threat of a fine or imprisonment.²⁶⁵ It is impossible to seize²⁶⁶ tokens, however.

To simplify the process of asserting a claim, and possibly also to prevent faulty smart contracts from running, a kind of backdoor could be created for use by a trustworthy third party. This could conceivably be an interface to a judicial authority²⁶⁷ or a pro-

²⁵⁹ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3280).

²⁶⁰ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3280).

²⁶¹ Also in the case of trading documents, which according to the view presented here can be replaced by tokens, transfer of ownership does not automatically result from handing over papers, cf. Baumbach/Hopt/Merkel, § 448 Rn. 2, 3.

²⁶² Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3281 ff.).

²⁶³ Saive, DuD, 2018, pp. 764-767 (766). Doing this for all nodes etc. does not appear practicable. Cf. however a suit for executing a rescue fork at <https://www.silvermillerlaw.com/wp-content/uploads/2018/04/2018-4-6-DE-1-CLASS-ACTION-COMPLAINT-1.pdf> (last accessed on Feb. 5, 2019).

²⁶⁴ Paulus/Matzke, ZfPW, 2018, pp. 431-466 (463).

²⁶⁵ Cf. Kütük/Sorge, MMR, 2014, pp. 643-646 (645); Kaulartz, CR, 2016, pp. 474-480 (479) while noting that in cases of this kind it is also possible to divulge the file in which the private key is stored or to transfer the right to receive it from the wallet provider; Paulus/Matzke, ZfPW, 2018, pp. 431-466 (464); Saive, DuD, 2018, pp. 764-767 (767).

²⁶⁶ Cf. on the applicability of Section 244 of the German Civil Code to virtual currencies: Beck/König, AcP, 2015, pp. 655-682 (662 ff.); cf. also BeckOGK/Freitag August 1, 2018, BGB § 244 Rn. 28. However, this regulation standardizes a right to replacement on the part of the debtor, Jauernig/Berger, § 244 Rn. 16. Using it to benefit the creditor is therefore out of the question.

²⁶⁷ Bertram, MDR, 2018, pp. 1416-1421 (1420); Kaulartz/Heckmann, CR, 2016, pp. 618-624 (624); Simmchen, MMR, 2017, pp. 162-165 (164).

grammed extrajudicial arbiter.²⁶⁸ However, allowing subsequent manipulations in this way²⁶⁹ would cause DLT-based smart contracts to sacrifice some of their technically ensured credibility, among other things because of the risk that these possibilities might be abused by unauthorized parties. A kind of three-person solution could make sense: two out of three of their keys would be needed to halt the execution of a smart contract or roll back a transaction. The keys would be distributed to the parties concerned plus a trustworthy third party (e.g. an arbitration body). If the two parties to the transaction fail to agree, the third could be called upon to tip the scale.²⁷⁰

5.1.6 Digressions

5.1.6.1 Supervisory issues

Supervisory implications must be taken into account when designing DLT-based payment systems. Under certain circumstances, obligations to obtain permits may apply, especially under Section 32, Subsection 1 of the German Banking Act (KWG) or Section 10, Subsection 1 of the German Payment Services Supervision Act (ZAG).²⁷¹ According to the German Federal financial Supervisory Authority (BaFin), owing to the many different ways in which tokens can work it is necessary to examine each individual case on its own merits.²⁷² As a guide, however, certain general principles can be applied. For so-called utility tokens that may only be used within the issuer's own network, exchanging them for merchandise or services, there is a tendency to assume that there is no need to obtain a permit. But the case can be different if tokens also serve as means of payment, since they are then more likely to qualify as a unit of account and thus as a financial instrument as defined by the German Banking Act.²⁷³

Bitcoins have been classified by the BaFin as financial instruments in the sense of Section 1, Subsection 11, Sentence 1 of the German Banking Act, which also applies to other virtual currencies (and currency tokens). As a general rule, the BaFin does not regard the use of virtual currencies as a means of payment (as substitutes for cash or book money) as an activity subject to licensing. However, additional circumstances may trigger an obligation to obtain permission. In particular, these include activities such as

²⁶⁸ Kaulartz/Heckmann, CR, 2016, pp. 618-624 (624).

²⁶⁹ On the technical feasibility of so-called chameleon hashes, cf. Saive, DuD, 2018, pp. 764-767 (766 m.w.N.).

²⁷⁰ On the three-person solution, cf. Werbach, Berkeley Tech. L.J., 2018, pp. 491-552 (548); see also section 3.2.1 above.

²⁷¹ Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), letter of Feb. 20, 2018, GZ: WA 11-QB 4100-2017/0010; cf. also Keding, WM, 2018, pp. 64-72..

²⁷² Fußwinkel/Kreiterling, Blockchain-Technologie – Gedanken zur Regulierung, available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html?nn=11056122#U33 (last accessed on Feb. 5, 2019); see also European Securities and Markets Authority (ESMA), Advice Initial Coin Offerings and Crypto-Assets, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf, Rn. 76 f. (last accessed on Feb. 5, 2019) and European Securities and Markets Authority (ESMA), Own Initiative Report on Initial Coin Offerings and Crypto-Assets, available at https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_report_on_icos_and_crypto-assets.pdf, Rn. 46 ff. (last accessed on Feb. 5, 2019); similarly to European Securities and Markets Authority (ESMA), ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf, pp. 1 f. (last accessed on 05.02.2019); Parhofer/Klöhn et al., ZBB, 2018, pp. 89-106. (102 f.).

²⁷³ Fußwinkel/Kreiterling, Blockchain-Technologie – Gedanken zur Regulierung; cf. also European Securities and Markets Authority (ESMA), Advice Initial Coin Offerings and Crypto-Assets, Rn. 86.

operating platforms or exchanges, as well as exchanging sums between legal tender and virtual currencies.²⁷⁴

5.1.6.2 Liability for smart contracts

Another issue has to do with liability for providing faulty smart contracts. Here it is necessary to make a distinction based on who does the actual programming. If this is done by the service provider itself, and if a user suffers damages as a result of programming errors—provided that the general prerequisites are met—the provider is contractually liable to the user, having failed to meet his due care obligations under Section 241, Subsection 2 of the German Civil Code. However, if the provider obtains the software from a third party, then the latter is liable to the provider within the scope of their contractual relationship.²⁷⁵ In the context of the provider's relationship with the user, contractual liability may be given; this depends mainly on whether the provider has culpably used a faulty smart contract, in other words if the problem was recognizable.

Smart contracts may also be available free of charge in the public domain. In this case, the laws on gifts²⁷⁶ may be applicable, along with the corresponding liability privileges (acc. to Sections 521 et seq. of the German Civil Code). In such cases the existence of an intention to be legally bound may be questionable, since the software may have been made available merely as a favor. However, the likelihood of this is diminished by the economic importance that software usually has, the risk of damages, and the interest of the party providing software in imposing his licensing conditions.²⁷⁷

As the connection to the real world grows stronger, so does the probability of infringing on a right protected by Section 823, Subsection 1 of the German Civil Code with a faulty smart contract.²⁷⁸ If tokens as such are affected (e.g. in the case of a faulty transaction), the problem arises that neither assets as such nor claims are protected under Section 823, Subsection 1 of the German Civil Code.²⁷⁹ An exhaustive discussion of the tort liability of tokens would exceed the scope of this study, however, so the reader is referred to relevant literature on this aspect.²⁸⁰

²⁷⁴ Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Virtuelle Währungen/Virtual Currency (VC), available at https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel.html (last accessed on Feb. 5, 2019).

²⁷⁵ On the issue as to whether the creation of smart contracts constitutes a legal service or legal advice, cf. Heckelmann, NJW 2018, 504 (509); Kaulartz, Taeger (ed.) – Smart world, 2016, pp. 1023-1037 (1033 f.).

²⁷⁶ Auer-Reinsdorff/Conrad/Kast, § 12 Rn. 143, 150; Leupold/Glossner/von dem Bussche/Schelinski, Part 1 Rn. 261; Redeker, IT-Recht, 2017, Rn. 595a.

²⁷⁷ Redeker, IT-Recht, 2017, Rn. 595a.

²⁷⁸ On the issue of the applicability of the German Product Liability Act to software, cf. BeckOGK/[Rebin, May 1, 2018, ProdHaftG § 2 Rn. 49 ff.](#); BeckOK BGB/[Fürster, Stand: 01.11.2018, ProdHaftG § 2 Rn. 22 ff.](#); Dauner-Lieb/Langen/Katzenmeier, ProdHaftG § 2 Rn. 3; MüKo BGB/Wagner, ProdHaftG § 2 Rn. 17 ff.

²⁷⁹ MüKo BGB/Wagner, § 823 Rn. 291, 370.

²⁸⁰ Engelhardt/Klein, MMR, 2014, pp. 355-360. (358); Kaulartz, CR, 2016, pp. 474-480 (479); Pau-lus/Matzke, ZfPW, 2018, pp. 431-466. (453 f.); Reiter/Methner in Taeger, Rechtsfragen digitaler Transformationen, 359 (365); Seitz in Taeger, Recht 4.0, 777 (786 f.); Shmatenko/Möllenkamp, MMR, 2018, pp. 495-501 (498); Spindler/Bille, WM, 2014, pp. 1357-1369 (1363).

5.1.7 Summary

Overall it may be concluded that the existing civil law provisions are adequate for regulating the use of smart contracts. The unique technological attributes of DLT do not pose any insoluble legal issues.

Despite their unique attributes, the general rules must also be applied to contracts involving the use of a smart contract for a certain purpose (in connection with concluding a contract or merely as a means of execution). Whether or not a declaration of intent exists, in which behavior it may be surmised, and its content must be determined in the light of Sections 133 and 157 of the German Civil Code. In many cases, the actual contract will be concluded outside the DLT application. Moreover, contracts concluded or executed while using DLT are subject to the same constraints as all other contracts. The parties must therefore respect the applicable laws, including those on standard business terms and consumer protection. Despite the immutability of DLT systems, questions posed by the reversal of transactions can be satisfactorily answered, since it is sufficient to restore the original economic situation. Overall, the achievable degree of automation is constrained by the limits of what is technically feasible. In many cases, legal decisions call for value-based assessments that software is not yet capable of. This applies both to exchanges of performance and remuneration that can be implemented by a smart contract and to issues related to problems in meeting contractual obligations.

5.2 Assessment from the Standpoint of Data Protection Law

This section looks at the extent to which DLT solutions in the mobility sector process personal data in the sense of the GDPR. Its aims include identifying the controllers under data protection law, ascertaining the legal basis of their authority, and determining how they can comply with their obligations to erase and correct data. This discussion is limited to data that are processed by the involved parties via a DLT platform. The same data protection requirements also apply to personal data that are processed in other ways for operating mobility solutions, but these are excluded in the following due to the lack of specific issues.

The following passages apply independently of the specific application in each individual case. The intention in this section is to identify generally applicable solutions that are consistent with data protection law across all implementations of DLT technology in the mobility sector. Further below, the findings are applied to individual applications.

5.2.1 Applicability of the GDPR

The GDPR applies when a data processing controller is based in the European Union. It does not matter where the data are actually processed. The GDPR also applies whenever data are processed in connection with offering products or services to individuals residing in the EU, even if the responsible controller is located outside the European Union.

To the extent that the DLT solutions studied here are also or exclusively offered to natural persons residing within the European Union, it may be assumed that the GDPR applies to processing of their data. Charging infrastructure for electric vehicles and ridesharing services also target natural persons residing within the European Union.

Consequently, the GDPR applies to all processing of their data in connection with these services. If DLT is used to create a platform for a platooning application or to enable processing of electronic title documents, this does not typically involve offering products or services to natural persons. However, the GDPR is also applicable in these cases if the controller is based in the EU. One of the aims of the following investigation is to ascertain who is the responsible controller under data protection law.

5.2.2 Processing of personal data

According to Art. 1 (2) GDPR, the objective is to protect fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. The processing of data is therefore not generally relevant in the context of data protection law, but only when "personal data" are involved.²⁸¹

In the following, it is investigated where personal data may be processed in connection with implementing mobility concepts with DLT applications. First it is established which types of data processing are relevant. Then it is checked whether the processed data are of a personal nature and who is the responsible controller.

5.2.2.1 Relevant data processing activities

The GDPR broadly defines the concept of data processing. Art. 4, No. 2 provides a legal definition, according to which data processing is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

When transmitting data via a DLT architecture, a basic distinction must be made among entry of data, decentralized storage processes, and readout of the data. In the following, the extent to which these activities fall under the definition of data processes is briefly explained. The question as to who is responsible for data processing is answered in a later step.²⁸²

5.2.2.1.1 Data entry in DLT platforms

Any information intended for decentralized storage on a DLT platform must first be entered somewhere. It is possible for only parts of a data set to be placed in the DLT layer, while other parts remain local. It is nevertheless possible to create links to data sets that are stored off-chain. As a result of being entered, data are made available to all persons who may read them. In a public DLT application, anyone may do so; in the case of a private DLT application, only its direct participants. This approach to making data accessible may also be regarded as disclosure by transmission or dissemination; as a minimum, however, it qualifies as "another form of delivery" to all participants who

²⁸¹ See also Ehmann/Selmayr/Klabunde, Art. 4 Rn. 7; Sydow,Ziebarth, Art. 4 Rn. 9; Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p. 4.

²⁸² Cf. 5.2.3 for a detailed discussion of the controller's role under data protection law.

are entitled to read them, and it may therefore be assumed that data processing takes place.²⁸³

5.2.2.1.2 Processing of data on DLT platforms

Data to be stored in a decentralized database are received by participants of a peer-to-peer network and distributed within the network to all participants. This processing may be categorized as "dissemination" of data. Depending on the consensus mechanism used, the newly obtained data are added to the central database, possibly by miners. These actions, which may be categorized as "organizing", "ordering" and "storing" of data, also constitute data processing.

5.2.2.1.3 Reading data from DLT platforms

Data are read when needed by authorized system users with reading access. This applies to both on-chain and linked off-chain data. These reading activities also constitute data processing.

5.2.2.2 Personal data

The processed data would have to be "personal data". This concept is defined in Art. 4, No. 1, Sentence 1 of the GDPR as follows: "'Personal data' means any information relating to an identified or identifiable natural person ('data subject')." The concept of personal data had already been the subject of EU Directive 95/46/EC (Data Protection Directive) and was investigated further by the Article 29 Data Protection Working Party.²⁸⁴ Accordingly, personal data is defined by four elements: "any information" "relating to" "an identified or identifiable" "natural person".²⁸⁵ Here it must always be kept in mind that these elements must be evident to the observer; whether or not a relationship to an identifiable person exists is therefore always relative.

5.2.2.2.1 Natural persons

Only data of natural persons are protected by the GDPR. All human beings count as natural persons, regardless of their nationality, but only living persons are included, not the data of deceased persons.²⁸⁶ The member states may, however, enact their own rules on the protection of these data. It must be noted that data related to a deceased individual can simultaneously include data on still-living persons.²⁸⁷ The processing of information on legal entities is irrelevant under data protection laws, provided that it cannot be used to deduce information on natural persons.

Natural persons affected by data processing can be among the users of DLT applications, which can in turn also capture data of third parties.

²⁸³ The same statement applies to public blockchains: cf. Marnau in Eibl/Gaedke, INFORMATIK 2017, 1025 (1033).

²⁸⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data.

²⁸⁵ Also Ehmann/Selmayr/Klabunde, Art. 4 Rn. 8.

²⁸⁶ GDPR, Recital 27.

²⁸⁷ BeckOK DatenschutzR/Schild, Art. 4 Rn. 11; Kühling/Buchner,Klar/Kühling, Art. 4 Rn. 5; Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p. 26.

5.2.2.2.1.1 Users of DLT applications

The affected persons can primarily be the users of a DLT application. For determining whether data protection laws apply to processing of data on the application's users, different groups can be distinguished.

5.2.2.2.1.1.1 B2B DLT applications

DLT applications can be designed in such a way that they are not available for use by private individuals. If a DLT application is used exclusively by businesses, then data protection laws are not relevant to the processing of data related to these businesses. The only exception is when a business is so tightly linked to a natural person that information on the business also constitutes information on the natural person behind it. Among other things, it is conceivable that revealing information on the assets of a business could be equivalent to revealing information on the assets of the natural person linked to the business. This may be assumed to be true in the case of "one-person companies" in particular, although other cases are also conceivable. For example, a company's name could include the name of its proprietor. The probability of receiving information on the natural persons behind a business diminishes as the size of the business increases. Especially with smaller companies, however, this possibility definitely deserves to be considered.

If only companies directly use a DLT application, and transactions performed by one of the companies using a key do not permit any conclusions to be drawn about any natural persons, then the associated data processing is not relevant under data protection law. If a mobility application permits an approach in which only such companies are able to execute transactions, it is preferable from the standpoint of data protection law (without taking any other factors into account). An exclusively B2B DLT application of this kind will typically require a closed DLT platform in order to prevent any companies from participating that do not meet the mentioned prerequisites. This is theoretically also possible with the participation of natural persons, e.g. as final customers, in a mobility solution. In such a case, however, these persons may not be directly involved at the DLT level with their own user keys. It will typically be necessary to prevent payments from being made directly by natural persons to those providing the service in question. Instead, the natural persons must have a contractual relationship with an intermediary. Only the latter then executes transactions with the service providers via the DLT platform, while payments between natural persons and the intermediary take place off-chain.

5.2.2.2.1.1.2 B2C and C2C DLT applications

If, however, a DLT application is designed to let private individuals directly participate as users at the DLT level, all processing of data related to them is relevant under data protection law.

5.2.2.2.1.2 Third-party data on a DLT platform

A DLT application is inherently designed to bring about a consensus among the participating parties regarding every piece of information. The possibility cannot be excluded that, depending on the application, the information may also include data on natural persons who are not users of the system.

If a mobility application can be designed in such a way that only enterprises are active at the DLT level, then final customers (i.e. natural persons) do not directly use the system. However, data processing by the enterprises on the DLT platform can also be relevant under data protection law, namely if processed on-chain data contain information on the application's final customers.

5.2.2.2.2 Information

The term "information" is broadly defined and can refer either to objective information (such as name and place of residence) or to subjective information (such as opinions and statements made). Whether or not the information is true is irrelevant. It can be present in any conceivable format.²⁸⁸

Nearly all data processed in a DLT context are characterized by more or less large informational content. Although users do not typically operate under their actual names, information relating to them can be present in the form of usernames, account balances or time stamps. Even the fact that an interaction has taken place on a DLT platform qualifies as information.

However, information can only be extracted from data when the latter can also be read and understood by the observer. Encrypted data, although they can be viewed by anyone, can only be read by those persons who are in possession of the corresponding key. From the perspective of persons that lack the key, encrypted data are therefore not personal data.²⁸⁹

5.2.2.2.3 Relationship to a person

In the view of the Article 29 Data Protection Working Party, a relationship to a person exists if there is a "content," "purpose," or "result" element. A "content" element is present when information is given about a particular person, a "purpose" element if "data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behavior of an individual."²⁹⁰ A "result" element is present if the information could impact a certain person's rights and interests. It is enough if the individual might be treated differently than other persons as a result of processing the information.²⁹¹ When investigating these elements, all of the circumstances surrounding a precise case must always be taken into account.

²⁸⁸ Ehmann/Selmayr/Klabunde, Art. 4 Rn. 9; Sydow,Ziebarth, Art. 4 Rn. 41.

²⁸⁹ Also according to the Article 29 Data Protection Working Party, Position Paper 4/2007, on the concept of personal data, WP 136, 01248/07/EN, p. 23, which asserts that no personal data are involved if a piece of information cannot be created by technical means. The German Federal Blockchain Association does not make this distinction, instead taking the basic position that all encrypted data are pseudonymized data. Blockchain Bundesverband, Blockchain, data protection and the GDPR, S.4, available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf (last accessed on Jan. 7, 2019).

²⁹⁰ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, pp. 11 f.

²⁹¹ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, p. 13.

5.2.2.3.1 Data on users of an application

Users regularly interact using their keys. The fact that a username is assigned to a natural person already constitutes information on that individual (in the form of a content element). The same statement applies to other information that may be linked to the username, such as account balances, time stamps, or records of interactions that have taken place while using that username. These kinds of information are relevant to those network participants who have an interest in recording them. The information enables them to tell whether a user has had a required interaction. It therefore serves the purpose of letting users assess one another (purpose element). This in turn affects the rights and interests of the users concerned (result element). User names and information associated with them thus contain information on the corresponding users.

5.2.2.3.2 Data on third parties

Stored data can also contain information on third parties. The extent to which this is true must be decided in each individual case.

5.2.2.4 Identification or identifiability

An individual can be identified if he or she differs from all other persons in a group.²⁹² According to Art. 4, No. 1, Sentence 2 of the GDPR, a person is identifiable if they "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Whether or not a person is identifiable always depends on the specific circumstances of each individual case. According to Recital 26 of the GDPR, account should be taken of all of the means that are reasonably likely to be used to directly or indirectly identify a person, such as singling them out. The Court of Justice of the European Union has elaborated on this in its judgment on whether dynamic IP addresses constitute personal data, concluding that this is the case if a data processor possesses all information required to identify a person or at least has legal instruments for obtaining this information from third parties.²⁹³

5.2.2.4.1 Direct identification of a person by knowing their identity

As a rule, knowing someone's name is considered to be equivalent to directly identifying them.²⁹⁴ However, since names are not unique, additional information is required to unambiguously identify them, such as a date of birth, photograph, or address.²⁹⁵

Users do not use their actual names in the DLT layer. Consequently, they cannot be identified by means of their names. The situation can be different for affected third parties whose data are stored in the DLT layer. If actual names are stored here, direct identification is possible.

²⁹² Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, p. 14.

²⁹³ EuGH, Judgment from 19 October 2016 - C-582/14, Rec. 49.

²⁹⁴ BeckOK DatenschutzR/Schild, Art. 4 Rn. 16; Sydow,Ziebarth, Art. 4 Rn. 14.

²⁹⁵ BeckOK DatenschutzR/Schild, Art. 4 Rn. 16; Kühling/Buchner,Klar/Kühling, Art. 4 Rn. 18

5.2.2.2.4.2 Indirect identification of a person by correlating their username and identity

Personal data also include those that can be assigned to a natural person by taking additional information into account (pseudonymized data).²⁹⁶ It could therefore also be possible to identify a person on the basis of the username that they use in a system.

Each of a DLT network's participants has a unique username called a public key. For each public key, there is also a private key that the user keeps secret. The private key can be used to create a digital signature that lets others verify that the signer actually possesses the private key corresponding to the public key, without the need for the signer to reveal it. Nor is it possible with current technology to calculate the private key from the digital signature and public key.

If a participant wishes to transfer a data set to the decentralized database, he or she uses his or her public key to send a message to this effect to all of the system's participants. He or she signs this message with his or her private key. The rest of the participants can then check whether the message has actually come from someone who knows the private key corresponding to that public key.

The public keys are linked to information on the DLT platform. If an observer knows which natural person is behind a public key, he or she has information on that natural person. This continues to be the case for as long as the observer either directly possesses this additional information or has a way of obtaining it from third parties.

Initially, only the individual concerned knows the identity of the natural person behind a public key. This has no relevance to data protection requirements as long as no other persons acquire knowledge of this key or are enabled to receive it from the user. Participants in the DLT application use their keys to demonstrate to other participants the existence of circumstances that are important to the relationship between them. In order to use the DLT application to execute a contract between two participants, the provider of a service needs to show the recipient that the agreed service has been provided. This typically makes it necessary to communicate his or her public key to the other party. If the recipient knows the identity of his or her contractual partner, he or she can correlate all information that is (for his or her) visibly linked with his public key on the DLT platform with his or her identity. Natural persons thus become identifiable when they reveal the link between their identity and a public key to third parties.

5.2.2.2.4.3 Indirect identification by a user's IP address

The users of a peer-to-peer network interact by means of IP addresses that have been assigned to them by their respective Internet service providers. As already discussed, the Court of Justice of the European Union has ruled that an IP address alone constitutes personal data, owing to the possibility that a processor may exercise a right to obtain additional information from the corresponding Internet service provider.²⁹⁷ Knowledge of the IP address could, in combination with other data, be used to correlate the content of an associated message with the sender.

²⁹⁶

GDPR, Recital 26.

²⁹⁷

EuGH, Judgment from 19 October 2016 - C-582/14, Rec. 49.

When sending a transaction in the network, the sender's IP address is revealed to the message's recipient. The transaction is conveyed by the sender to the nearest node, which checks the message and passes it on. In this way, the message propagates across the system until every node has received the transaction. Not every node sees the IP address of the original sender, but only the address of the node from which it has received the transaction. It can therefore not be sure that the IP address actually belongs to the message's sender. However, in a peer-to-peer network it is possible to draw conclusions about the sender of a transaction by analyzing the messages. If the participants succeed in carrying out such an analysis, and if it may reasonably be assumed that they will also use the results, then the transactions linked to the IP address constitute personal data.

5.2.2.4.4 Indirect identification by looking at all available information

In order for a user to be identifiable, it is not absolutely necessary for the observer to know the key in order to establish a connection between it and a natural person. Indirect identification is also possible if a "unique constellation"²⁹⁸ of information is available that, in its entirety, can only fit to a certain natural person, even when the individual pieces of information do not allow any conclusions to be drawn. This includes the special attributes cited in Art. 4, No. 1, Sentence 2 of the GDPR that express a natural person's physical, physiological, genetic, mental, economic, cultural or social identity. As the density of the set of available information on a person increases, the probability that they can be identified also grows.²⁹⁹

The sender dispatches the message for the purpose of storing certain information in a decentralized database in a tamperproof manner. Depending on the details of a given case, this information may be sufficient to deduce the sender's identity. This can also be true if the observer lacks knowledge of the key linking the user's identity and username. This appears to be possible in cases in which the content of the message, based on logical analysis, can only come from a specific natural person. It does not need to be possible for anyone whatsoever to make the deduction. In some cases, only individuals with certain special knowledge will be able to do so. For example, the recipient of a service may not know the key for linking the username to a natural person but does know that the interaction, owing to the time and circumstances of its execution, can only come from his or her contractual partner, whom he or she knows.

Even if the observer cannot view the content of a signed message, cases are conceivable in which he can deduce the natural person behind it by considering all of the messages sent under the same username. This can be the case, for example, if information is added to the database at certain times while repeatedly using the same username. Whether or not this permits conclusions to be drawn about the natural person behind these actions depends on the circumstances of each individual case, especially the total number of participants and the normal frequency of data storage operations.

²⁹⁸ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, p. 16.

²⁹⁹ BeckOK DatenschutzR/Schild, Art. 4 Rn. 16; Sydow, Ziebarth, Art. 4 Rn. 17, 21.

5.2.2.3 Intermediate findings

In DLT applications (in the mobility sector), data are processed whenever data are stored, read or used in the DLT layer. The processed data are personal data if, from a given observer's perspective, they contain information on a natural person. This can be the case if a dataset being stored contains information on a natural person. This can be a user of the system or an (uninvolved) third party. Transaction data associated with a signed message may also contain information on system users. This is the case if an observer is able to correlate the username with a user and the user is a natural person, or if the user is not a natural person but the observer is able to identify the natural persons active behind the user. The observer can make this correlation by knowing the key linking the username and the identity of the user or deducing it on the basis of other available information. This information can include the user's IP address or an overall view of all information linked to a username that the observer is able to access.

Since the existence of usernames, as a bare minimum, is indispensable for a DLT platform, as a rule processed data reveal links to specific persons, at least from the perspective of a certain group of observers. The only exception is when a system's users are not natural persons, the natural persons behind the users cannot be deduced, and no data of third parties are processed in the system. In all other cases, it must be possible to identify the agent responsible for these data processing activities.

5.2.3 Responsibility for data processing

Responsibility for meeting the requirements of the GDPR rests with the "controller".³⁰⁰ Only this officer is legally authorized to process data. Vis-à-vis data subjects, the controller is the party responsible for complying with data protection obligations. Pursuant to Arts. 12-14 of the GDPR, the controller must transparently inform data subjects on how their data are processed and used. Furthermore, Art. 14 grants subjects the right to receive information on how their personal data are processed. According to Arts. 16-19, the controller must rectify or erase any data that are incorrect or no longer required. For these reasons, the definition of the role of controller has special significance. It is also possible for there to be two or more joint controllers who share responsibility (Art. 26). The controller can also make use of processors (Art. 28) who follow his instructions.

5.2.3.1 Definition of responsibility

According to Art. 4, No. 7 of the GDPR, the controller is the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes of processing personal data and the means used to do so. The question as to who "decides" is answered by determining who actually influences decisions. The formal legal appointment of a decisionmaker is only indirectly relevant.³⁰¹

³⁰⁰ *Sydow, Raschauer*, Art. 4 Rn. 114.

³⁰¹ Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 00264/10/EN, p. 15.

"Determining the purposes" refers to the expected or planned outcome of processing, while "means used" refers to how this outcome is achieved.³⁰² The term "means" includes technical methods and the scope of processing, authorization to access data, when data are erased and so on.³⁰³

5.2.3.2 Responsibility for entering data

Initially, all data are passed by participants to other participants for further processing. The participant who enters data has the sole right to decide on the purposes and means of this transfer. To the extent that the entering individual is himself the subject of entered personal data, his actions are irrelevant from the standpoint of data protection law. However, if the datasets contain personal data of other participants or third parties, there must be a justification for this. Justification is only required when conveying data that are also personal data of the recipients. The recipients are, to begin with, all system participants with reading access.

5.2.3.3 Responsibility for reading data

When data are read, only the party reading them decides whether and which data are read. Consequently, only it decides on the purpose and means of data processing. Like in the case of data entry, the reading party is only responsible for the processing of data concerning other participants or third parties. In order for this responsibility to exist, the reading party must be able to determine whether information is of a personal nature. He or she is thus exclusively responsible for processing the act of reading.

5.2.3.4 Responsibility for storing data in the DLT layer

One challenge can be to determine who is responsible for data processing activities that participants of a decentralized network carry out for the purposes of creating and maintaining the decentralized database. To determine who actually influences data processing activities, it is first necessary to distinguish between "permissioned DLT applications" and "permissionless DLT applications".

5.2.3.4.1 Permissioned DLT application ("centralized solution")

In a permissioned DLT application, access by and the reading and writing rights of participants are assigned by a central entity. This central entity can consist of a group of individuals who join forces to operate the system. It defines rights and role systems for determining which persons should have access to which data. Access to the database is only possible via the higher-level system of the central entity. The central entity sets the rules for processing of data after these have been entered by network participants. The nodes, and possibly miners, of the underlying DLT platform either belong to the same group as the central entity, or act in accordance with its instructions by managing it according to rules defined by the central entity.

³⁰² Ibid., p. 16.
³⁰³ Ibid., p. 17.

In this type of scenario, the central entity exerts direct control over all data processing. It decides on the purpose and means of data processing, and may therefore be regarded as a controller in the sense of the GDPR.³⁰⁴ Nodes and miners, unless they belong to the group of individuals who constitute the central entity, are subject to its instructions and can therefore be contracted processors as defined in Art. 28 of the GDPR.³⁰⁵ The prerequisite is the conclusion of a data processing contract between the central entity and the nodes and miners. This contract defines how data processing must take place. For example, it can dictate that processing may only be done according to the rules of the provided software.

The use of a permissioned DLT application can simplify the search for a controller as defined by data protection law. The disadvantage of this approach, however, is that it is necessary to form a central entity that in turn heavily influences all data processing that takes place. This rules out the creation of a decentralizing sharing platform that dispenses with intermediaries, at least in its pure form. There is therefore a need to study whether or not and if so to what extent the role of controller can also be assigned in a permissionless DLT application.

5.2.3.4.2 Permissionless DLT applications

The search for a controller in the sense of data protection law is more challenging in the case of permissionless DLT systems, since there no central entity can be directly identified as being responsible for controlling data processing operations. To some extent, therefore, the position is taken that every node must be regarded as individually responsible, since it relays data and records them in the database copy that it keeps.³⁰⁶ Others regard all of the participants of an open DLT system as being collectively responsible.³⁰⁷ However, the latter view apparently treats the concepts of participant and node as equivalent. The fact of relaying transactions within the network and recording data in a local database copy is cited as evidence of responsibility. In this view, nodes decide to process data according to the rules of the software they use. But each node could also opt to refrain from processing data or process them according to different rules. Consequently, each node individually decides on the purpose and means of its data processing activity.

Since the nodes collectively constitute the DLT platform's infrastructure, it might be supposed that they process data as joint controllers in the sense of Art. 26 of the GDPR. But such joint responsibility would require decisions on the purposes and means of data processing to be made collectively by all of the nodes. In actual fact, however, the nodes of a permissionless DLT application do not typically agree on anything. Each of them makes autonomous data processing decisions. It must therefore be concluded that each node is an independent controller.

³⁰⁴ Bitkom, Blockchain und Datenschutz – Faktenpapier, p. 30; Blockchain Bundesverband, Blockchain, data protection and the GDPR, p. 7.

³⁰⁵ Martini/Weinzierl, NVwZ, 2017, pp. 1251-1259 (1254).

³⁰⁶ Martini/Weinzierl, NVwZ, 2017, pp. 1251-1259 (1253 f.); Bitkom, Blockchain und Datenschutz – Faktenpapier, pp. 28 f.

³⁰⁷ Schrey/Thalhofer, NJW, 2017, pp. 1431-1436 (1433 f.); Bechtolf/Vogt, ZD, 2018, pp. 66-71. (69).

Such a conclusion is not necessarily in the interests of those participating in a DLT application. Under some circumstances, therefore, it will be necessary to make adjustments to the platform's architecture. In the following, a distinction is made based on whether all of the participants share an interest in all on-chain data or only selected participants have an interest in certain on-chain data. The aim is to present a solution for the role of controller in each case that is in harmony with existing laws.

5.2.3.4.2.1 All participants have an interest in all on-chain data ("open solutions")

All participants of a DLT network may have an interest in all data that are processed on-chain. This concerns cases in which a decentralized database is openly kept by all participants in the interests of all. In other words, they are not supposed to keep information secret from one another. Virtually all cases of this kind will require a closed DLT application that can only be viewed by the participants themselves. However, not every closed DLT application will meet the cited prerequisites, since there could definitely also be an interest in not sharing information with all other participants. Regarding cases of this type, the reader is referred to the discussion further below.

If all of the participants have a legitimate interest in processed data, this opens up the possibility of distributing responsibility across all nodes. In such a case, the type of responsibility discussed above will be virtually impossible to put into practice. But the nodes can develop a way of cooperating that also leaves room for an agreement to jointly share responsibility in the sense of Art. 26 of the GDPR.

5.2.3.4.2.2 Only selected participants have an interest in on-chain data ("anonymization solution")

The case of a database that is openly kept by all participants will tend to be the exception rather than the rule. Participants will often have an interest in only sharing information with certain other participants. Complying with such an interest on a permissionless DLT platform will pose the greatest data protection challenges. In particular, a problem arises when data processed on-chain are of a personal nature from the perspective of all of the participants. Unless all of the affected participants have a legitimate interest in knowing these data, the participant storing them will be unable to comply with data protection requirements by sending personal data of third parties to all of the network's participants, since he or she will lack a legal basis for doing so.³⁰⁸ Furthermore, as already explained above, all of the network's nodes would then have to be categorized as controllers in the sense of data protection law. In an open network, however, it would be difficult for these persons to collaborate, and it is not likely that they would be able to meet their data protection obligations.³⁰⁹

Spreading the responsibility among all of the network's nodes would not do justice to their interests here. Instead, a solution must be found in which responsibility is limited to those persons who have an actual interest in the transaction concerned. Such a result could be achieved by adapting the DLT platform's architecture. Here the principle can be applied that whether or not data are personal is relative and depends on

³⁰⁸ See 5.2.4 on the legal foundations for data processing.

³⁰⁹ Especially problematic is the obligation to rectify and erase data. For further discussion of this, see 5.2.5 below.

who views them. The role of controller also requires processed data to be personal from the controller's perspective. If only data are processed that are personal from the perspective of third parties, but the processor has no way of identifying the affected person, then the processor cannot be the controller. The architecture must therefore be designed in a way that prevents on-chain data from being ascribed to any natural person without additional information. Once this is achieved, no personal data will be processed by the nodes in the DLT layer. The consequence of this is that they cannot be controllers in the sense of data protection law for the data processing that is taking place. They are thus absolved of any responsibility for on-chain data processing, which instead rests solely with those who possess the additional information required in order to correlate the on-chain data with a person.

5.2.3.4.2.2.1 Eliminating the personal nature of information about third parties

When storing on-chain information on third parties, steps must be taken to ensure that it can only be read by persons who have a legitimate interest in the information.

5.2.3.4.2.2.1.1 Encryption of information

After personal information has been securely encrypted, it only constitutes personal information for those who possess the key for decrypting it. The key may only be known to those who genuinely require access to the encrypted information. Encryption can reduce the group of individuals for whom the stored data are personal in nature to those who have a legitimate interest in learning them. For everyone else, information stored on-chain in encrypted form constitutes data without informational content. The key is required in order to turn them into personal data. This provides a way to shift responsibility for data processing from the participants of a public DLT application to the keeper of the key. Then it is not the nodes that are responsible for data processing, but those who have the key. When an obligation to erase data exists, the key must also be deleted. This renders the on-chain data anonymous and irrelevant from the stand-point of data protection law.

According to Arts. 25 and 32 of the GDPR, the controller has the obligation to adequately safeguard the rights of data subjects by implementing appropriate technical measures. Sending personal data for processing on a DLT platform could not satisfy these requirements, not even in encrypted form. Data are potentially stored forever by the nodes of a DLT platform, and a form of encryption that is regarded as secure today could eventually be broken by future computing technology. If this becomes possible, the personal data concerned will be visible to everyone in the public DLT application. The selected encryption method must therefore be so secure that it is highly improbable that it will be broken during the lifetime of the DLT platform, or else an exclusively encryption-based solution should not be relied on.

5.2.3.4.2.2.1.2 Off-chain storage with hash value links

To counter this problem, it can be sensible to store data off-chain as far as possible. This means storing personal data off-chain in encrypted form under the control of the storing party. A hash value is generated on the basis of the data. The corresponding hash value is then stored on-chain along with a link to the on-chain data. The network's participants cannot tell that personal data are involved without further information. This can only be done by parties with rights to access the off-chain data. The hash value ensures that the data have not been tampered with since being stored on

the DLT platform. The data stored off-chain are always under the control of the storing party and can be erased by it at any time.

5.2.3.4.2.2.2 Eliminating the personal nature of information about users of the system

Off-chain storage and links to hash values cannot be a viable solution for all data. Certain information must be known to all nodes of the system. Usernames, time stamps and account balances, for example, cannot be stored in this way. If they were stored in this way, all of the nodes would need access to the information in order to monitor it, and subsequent erasure would render it impossible to check the validity of new transactions—and the actual goal of off-chain storage, namely to allow only selected individuals to access information, could no longer be achieved.

Unless all data can be stored off-chain or at least encrypted, information stored on-chain should only be identifiable as relating to certain users if the viewer has a legitimate interest. Although it is impossible to monitor who views on-chain data in a public DLT application, the DLT architecture can be adjusted to ensure that participants cannot associate on-chain data with persons unless they are in possession of additional information.

Even when usernames, account balances, and executed transactions are visible on-chain, these can only be linked to persons unless it is possible to assign the username to a natural person. Initially, only the owner of a username knows the key linking them. He or she can share this information with selected third parties while hiding it from everyone else. By controlling knowledge of this key, it is possible to prevent anyone who is not privy to it from extracting information on specific users from the on-chain data. For this to work, the on-chain data may not reveal any personal data to anyone who does not know the key. Preparation is required in order to establish such a system. It must be ensured that only those familiar with the key are able to associate the data with specific persons.

5.2.3.4.2.2.2.1 Single-time user of usernames

First of all, it must be ensured that none of a transaction's content could be used to deduce the natural person behind a username. In extreme cases, this can be done solely by knowing that the username was employed at a certain point in time. Depending on the number of users and the circumstances of an individual case, conclusions may be drawn that reveal the identity of the natural person behind the username. If the potential group of users is sufficiently large, however, as a rule it is safe to assume that the mere fact of a username interacting with another cannot reveal anything about the parties concerned.

It appears to be essentially possible for users to generate a different username for every transaction executed on the DLT platform. Each transaction is then linked to a unique ID. Only the person in question knows the key linking the ID and their identity. He or she can share it with those who have an interest in the transaction. It can typically be assumed the identity of the user cannot be deduced from a single use of a user ID. The only exceptions are scenarios in which, owing to the circumstances of an individual case, it may be possible to identify individual natural persons by considering the

entirety of the circumstances surrounding a single interaction involving the use of a particular username at a certain time. However, as soon as the application grows past a certain size, this should no longer be possible.

Nevertheless, generating a new username for every single interaction runs up against technical limits when values (e.g. tokens) are linked to a username and need to be transferred between users. If a user wants to merge, pass on, or cash out such values, he or she will have to use the same ID again, and several interactions with the same username could give rise to patterns that others can detect and use to draw conclusions about the participating persons. It is difficult to generally characterize the circumstances under which such knowledge could be derived by analyzing data. A solution is therefore preferable that prevents multiple uses of the same username. This in turn calls for additional adjustments to rule out any possibility of deducing the user's identity. Various solutions enter into consideration for this, and in some cases it may be possible to combine them for added security. In the following, the approaches of off-chain transaction balancing, zero-knowledge proofs, and stealth addresses in conjunction with ring signatures are briefly presented by way of example.

5.2.3.4.2.2.2.2 Off-chain balancing of transactions

One approach that appears feasible, especially for B2B DLT solutions that do not inherently rule out any possibility of drawing conclusions about the natural persons behind a company, is off-chain balancing of transactions by the network's participants. Instead of directly entering every transaction in the DLT platform, each party has a separate account for balancing transactions. At regular intervals, all of the parties make balancing payments on the platform. This approach synchronizes the frequency and spacing of the participants' activities, thus making it more difficult to draw conclusions about processes within the company and the associated individuals. It also becomes harder to detect patterns by analyzing the data.

One serious drawback of this balancing approach is a loss of transparency. The participants are individually responsible for forming balances. Since there are regular periods during which no entries are made in the decentralized database, it is impossible for participants to check balances in advance. But in situations in which this risk is acceptable and could possibly be managed with appropriate precautions such as random checks, balancing can be a feasible way to anonymize data records.

5.2.3.4.2.2.2.3 Use of zero-knowledge proofs

The use of zero-knowledge proofs appears to be a way to send a transaction to the network without having to reveal one's own username, that of the recipient, or the sum being sent.³¹⁰ Nodes can check the transaction's validity without receiving any information on the sender, recipient, or transferred amount. From the perspective of the network's participants, therefore, the data do not refer to specific persons. Under these circumstances, the nodes are thus not responsible for the data processing that takes place. Assuming that zero-knowledge proofs are securely implemented, their use can

³¹⁰ Presented by Sasson/Chiesa et al. in The Institute of Electrical and Electronics Engineers, IEEE Symposium on Security and Privacy, 459-474.

be a highly promising approach for creating an open DLT solution that complies with data protection regulations.

5.2.3.4.2.2.4 Use of stealth addresses in combination with ring signatures³¹¹

In order to prevent transactions sent to a user from being linked to his or her public username, a “stealth address” can be generated for receiving each one. The sender and receiver generate it by exchanging keys. Transactions can be sent to a stealth address without the network’s participants being able to see the corresponding public address. Only the recipient, by using a secret key, can find out which stealth addresses are assigned to his username. Another secret key lets him access the value stored at them.

The use of stealth addresses conceals a transaction’s recipient while the senders remain visible. Transactions that make use of stealth addresses can therefore also be observed and conclusions drawn about them. Ring signatures are a way to also disguise the addresses from which transactions are executed.

Ring signatures have multiple inputs and outputs, which makes it impossible to tell which of a group of users have sent which transactions to which recipient. On a second level, transactions can be combined in a way that only lets a given transaction’s sender and recipient see the amount transferred. Combining stealth addresses and ring signatures could thus be a way of eliminating links between usernames and identities for a system’s participants. The stored transactions are then anonymized for participants who do not possess the keys required to associate them.

However, it is important to not lose sight of the consequences of technical anonymization, whether this involves zero-knowledge proof, ring signatures in combination with stealth addresses, or another approach. If the aim is to create a DLT-based payment system, criminals can also benefit from the associated anonymization. As a comparison with cash transactions shows, at first sight nothing seems to be wrong with a way of making payments largely anonymously. But digital cash equivalents harbor far greater risks, since they can be exchanged by anyone from anywhere at any time. The goal of data protection is partly at odds with the need for (state) supervision of payment transactions. If all participants in a digital payment system are anonymous, it can become more difficult to fight crime. When governments promote the use of a DLT platform incorporating a technical anonymization solution, these consequences must be taken into account.

5.2.3.4.2.2.3 The risk that platform participants may break the rules

The aim of an anonymization solution is to completely eliminate personal data from the DLT layer. No one except those directly involved in a transaction should be able to connect it to individuals on the basis of on-chain data. The approaches described for achieving this state of affairs pose considerable challenges. If data unintentionally make their way into the DLT layer that can then be used by the network’s nodes to extract information on natural persons, then these—as already explained—are respon-

³¹¹ As implemented in the Cryptonote Protocol, Saberhagen, CryptoNote v 2.0.

sible for processing this information. This poses the difficult task of asserting the affected individuals' rights. No central entity exists that could intervene and rectify the situation. If the wish is to do without such a central entity, then the software used by the nodes of the DLT platform must not allow a situation in which nodes become controllers. It must therefore be designed so that all on-chain information processed by the nodes is in a format that prevents it from being associated with natural persons.

5.2.3.5 Intermediate findings

Each participant is responsible for the data he or she stores and reads out. Unless the architecture is additionally modified, responsibility for on-chain processing is shared by all of a network's nodes. In case all of the network's nodes have a legitimate interest in all processed data, this can definitely be a workable solution (open solution).

As a rule, however, not all of a DLT platform's participants will have a legitimate interest in all processed information. In such a case, assigning legal responsibility to all of them will lead to undesirable results. Owing to the obligations associated with such responsibility, the role of node will become unattractive. It will be difficult for nodes to meet their responsibilities, or even impossible if they are required to rectify and erase data. Moreover, every time that personal data are entered in the DLT platform they would be relayed to an undefined group of persons, for which the party entering them would have no legal justification.

Alternative solutions therefore need to be created for distributing the responsibility. This in turn requires adjustments to the DLT platform's architecture. If not all of the participants have a legitimate interest in all processed data, then either a responsible central entity must be created by implementing a permissioned DLT application (a centralized solution) or, in the case of an open DLT application, a way to eliminate the personal nature of all data processed on-chain (an anonymization solution) must be found.

5.2.4 Legal basis for data processing

According to the GDPR, the controller is fundamentally prohibited from processing data without permission. Data may only be processed by the controller if there is a legal basis for doing so. The legal bases for processing personal data are mainly given in Art. 6 of the GDPR. The following sections seek to identify suitable legal bases for storing, reading and on-chain processing of data.

5.2.4.1 Justifications for storing and reading data

To begin with, participants who store and read data must be able to cite a legal basis for doing so. A distinction can be made depending on whether all of the data in question are personal data of the other parties involved in a specific transaction, or data of third parties are also processed.

5.2.4.1.1 Processing of personal data of other parties involved in a transaction

Independently of a specific case, it can be generally ascertained that the storage or reading of data to meet a contractual obligation takes place with the other party involved in a transaction. According to Art. 6 (1) Subparagraph 1 (b) of the GDPR, pro-

cessing of data is lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The term "contract" covers all legal transactions and similar contractual relationships.³¹² It covers all of the performance, ancillary and other obligations associated with a contract.³¹³ Processing of data is necessary if a contract could not otherwise be fulfilled as the parties to it have agreed.³¹⁴ In each specific case, the parties to the transaction are in a contractual relationship (the details of which can vary). The participants use a DLT architecture to enable tamper-resistant exchange of information that they need in order to meet their respective contractual obligations. To the extent that the processed data are limited to what is required to fulfill the contract, Art. 6 (1) Subparagraph 1 (b) of the GDPR serves as the legal basis for processing them.

5.2.4.1.2 Processing of the personal data of third parties

The situation is only different when a transaction, in addition to the data of the parties involved in it, also contains data on uninvolved third parties. This cannot be justified with the legal basis for fulfilling a contract, since in that case persons whose data are processed must themselves be parties to the contract. Instead, other legal justifications must be found for this. The main possibilities are processing of data to meet legal obligations, processing of data to protect legitimate interests of the controller or a third party, and processing of data after obtaining the consent of the affected person.

5.2.4.1.2.1 Meeting of legal obligations, Art. 6, Paragraph 1, Point c of the GDPR

It appears possible that the data of third parties may be entered and read in order to comply with a legal obligation. According to Art. 6 (1) Subparagraph 1 (c) of the GDPR, data may be processed if this is necessary to comply with a legal obligation to which the controller is subject. According to Art. 6 (3) Subparagraph 1 of the GDPR, this obligation can derive from European Union law or the law of a member state. It must be a legal provision stipulating a standardized obligation that directly applies to data processing. It is not sufficient for the controller to cite a random legal obligation and process data for the purpose of meeting it.³¹⁵

5.2.4.1.2.2 Protection of legitimate interests of the controller or a third party, Art. 6, Paragraph 1, Point f of the GDPR

According to Art. 6 (1) Subparagraph 1 (f) of the GDPR, data processing is also lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by interests or fundamental rights and freedoms of an affected person that require protection of their personal data. Legitimate interests include not only legally justified ones, but also actual, economic, value-based, emotional and idealistic interests.³¹⁶ It may be generally assumed

³¹² BeckOK DatenschutzR/Albers/Veit, Art. 6 Rn. 30.

³¹³ BeckOK DatenschutzR/Albers/Veit, Art. 6 Rn. 31.

³¹⁴ Kühling/Buchner,Buchner/Petri, Art. 6 Rn. 40; Paal/Pauly,Frenzel, Art. 6 Rn. 14.

³¹⁵ Kühling/Buchner,Buchner/Petri, Art. 6 Rn. 76.

³¹⁶ Kühling/Buchner,Buchner/Petri, Art. 6 Rn. 146

that affected persons deserve protection. For deciding whether or not this applies in a given case, it is necessary to consider its details. The tasks and purposes pursued by the controller by processing data must be taken into account, as well as the sensitivity of the data with regard to the affected individual's personal rights.

5.2.4.1.2.3 Consent of the data subject, Art. 6, Paragraph 1, Point a of the GDPR

Finally, according to Art. 6 (1) Subparagraph 1 (a) of the GDPR, the consent of the affected person may justify processing of personal data for one or more specific purposes. This consent must be explicitly given and refer to the specific purpose of the data processing. It must be provided voluntarily, in an informed manner, and unmisunderstandably. According to Art. 7 (1) of the GDPR, the controller must be able to demonstrate that the consent of the person concerned has been obtained. According to Art. 7 (3) of the GDPR, the affected person has the right to withdraw his or her consent at any time. This does not affect the lawfulness of data processing that has already taken place, but no further processing may be carried out. Not least due to the possibility that a data subject may withdraw consent at any time, as well as the associated documentation requirements, this should only be resorted to when no other possible legal basis for processing is applicable.

5.2.4.2 Justification of on-chain processing

The legal basis for on-chain processing depends on the solution chosen for assigning responsibility. In the "anonymization solution" described above, there is no need to justify on-chain processing. If only selected participants have an interest in on-chain data, an architecture is required in which the network participants cannot detect any connections between them and natural persons. If this is the case, then they have no obligations under data protection law and consequently also no need to legally justify processing of the data.

The situation is different in "open solutions" and "centralized solutions". A justification for processing data in these is discussed in the following.

5.2.4.2.1 Legal basis for data processing in "open solutions"

If all participants have an interest in all on-chain data, and if the DLT application is designed to be open, then all participants are equally responsible, and possibly jointly responsible under Art. 26 of the GDPR, for processing of data. In this case, they may conclude a contract for jointly managing the database and storing data. Then data processing takes place in fulfillment of this contract. If no contract is concluded, then data processing may take place in the legitimate interests of the jointly responsible participants. Since all participants have an interest in processing data, reciprocal processing of their own personal data will most probably pass the test of a balancing of their interests. The parties would also need to have a legal basis for processing the personal data of third parties. For this purpose, the third party and processor could conclude an agreement that can only be fulfilled by processing the data in the distributed database. Alternatively, the participants could have a justified interest. Finally, it appears possible to obtain each individual third party's consent for processing their data.

5.2.4.2.2 Legal basis for data processing in “centralized solutions”

In a permissioned DLT application, a central entity is responsible for data processing. The nodes regularly process data at the request of the central entity. The central entity must also demonstrate a legal basis for on-chain processing. To begin with, here it is also evident that that central entity concludes a contract with the participants. The subject of the contract is operation of the decentralized network by the central entity. The data processing that takes place is thus required to fulfil the contract. If data of third parties are processed in the database, the possible legal basis for this could be an obligation arising from the contract between the central entity and third parties, a justified interest of the central entity, or the consent of the third party. However, in this context it is always necessary to check whether the data of third party actually need to be processed on-chain or off-chain storage of the data, linked by hash values, would also be possible.³¹⁷

5.2.5 Implementation of the right to rectification and erasure

One challenge posed by data processing on a DLT platform is protecting the rights of affected persons that are codified in the GDPR. While Articles 13 to 15 of the GDPR contain relatively few special provisions that are directly relevant to obligations to provide information, the right to rectification (Art. 16) and the right to erasure (Art. 17) in particular can be problematic. These are therefore examined more closely in the following.

According to Art. 16, Sentence 1 of the GDPR, a data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. He or she also has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay if one of several reasons listed in Art. 17, Paragraph 1 applies. It follows that in the procedure being considered here, erasure can be mandatory if the data are no longer required for the purposes for which they were captured, if the data subject withdraws consent given to process data and there are no other overriding legitimate grounds for the processing, if the person concerned exercises his or her right to object to the processing, if the personal data have been unlawfully processed, or the personal data must be erased in order to comply with a legal obligation under laws of the European Union or a member state to which the controller is subject.

How the erasure obligations are met once again depends on whether an “anonymization solution”, an “open solution” or a “centralized solution” is involved.

5.2.5.1 Erasure in an “anonymization solution”

In an “anonymization solution”, the erasure obligations are relatively simple to meet. Not all of the system’s participants are responsible, but only those who hold the key linking a person’s username and identity for a given transaction or control the personal data stored off-chain. If data are stored off-chain and linked at the DLT level by a hash value, then the data stored off-chain can be erased by the controller at any time. Then

³¹⁷ For more on erasure obligations in centralized solutions, see section 5.2.5.2.

the remaining on-chain pointer to the off-chain data goes nowhere. The remaining data have no connection to a natural person. Only those data are still personal that can be attributed to a natural person provided that the key linking their username and identity is known. The key is in the possession of the controller responsible for data processing. If the controller has the obligation to erase the personal data concerned, it is not the on-chain data but the key linking the username and identity that is deleted. Then not even the controller is able to identify the natural personal solely on the basis of the remaining on-chain data. Consequently, the data have then been permanently anonymized. This is equivalent to erasing them.³¹⁸

5.2.5.2 Erasure in “open solutions” and “centralized solutions”

If an open solution is chosen, all participants are collectively responsible and jointly obliged to erase data if one of the applicable grounds exists. In a centralized solution, however, responsibility rests with a previously denominated central entity. This highlights another challenge that both solutions face. While the role of controller can be assigned to all participants as a group or to a central entity, in both cases it must be possible to meet erasure obligations: in the first this falls to all participants as a group, and in the second to the central entity. In these models as well, it must not be possible for the contents of a block to be retroactively manipulated by the participants. Possible solutions must therefore also be provided for this.

As a general rule, data should not be erased as long as they continue to be required for meeting the purpose of their processing. If a contract is concluded between the central entity and the participants or among the participants of an open solution concerning data processing on the DLT platform, then data processing based on this contract is lawful as long as it is required for performing the contract (as per Art. 6, Paragraph 1, Point b of the GDPR). If the contract calls for tamperproof storage of data of the participants on a DLT platform, it could be argued that, due to the architecture of DLT, the data must remain stored forever. Any subsequent manipulation of the data would interrupt the chain and endanger the purpose of the contract. In centralized and open solutions, the erasure of participants’ personal data could therefore be dispensed with as long as all of the participants have entered into a contractual relationship with one another or with the central entity before joining the DLT project. This contract would prescribe the running of a fundamentally unchangeable DLT platform by the central entity or all of the system’s participants, while clearly designating processed data as such and limiting them as far as possible. However, this approach also leaves third-party data out of account. If data of third parties are also processed in addition to data of the system’s direct participants, who use usernames to perform actions on the DLT platform, it is therefore also necessary to conclude a contract with each such third party on permanent storage of their data.

Even if such a contractual agreement exists among the participants, it is additionally necessary to prevent unlawful data processing. According to Art. 17 (1) (d) of the GDPR, unlawfully collected data must also be erased if they have been processed on the basis of a contractual agreement. However, it is impossible to rule out the possibility of unlawful processing in advance. This could, for example, have the effect of rendering the

³¹⁸ For example, *Martini/Weinzierl*, NVwZ, 2017, 1251-1259 (1256).

contract between the parties void due to defects. The controller can then no longer cite the contractual agreement as the basis for processing data. In order to comply with existing laws, therefore, a centralized or open solution must be equipped from the start with ways to retroactively manipulate the chain. These are briefly discussed in the following.

5.2.5.2.1 Redactable blockchains

At least for blockchain solutions, one way to comply with obligations to erase and rectify on-chain data can be the use of advanced "chameleon hashes" in a "redactable blockchain".³¹⁹ Chameleon hashes are used instead of ordinary hash functions to link individual blocks, the difference being that they include a "trapdoor". A secret key makes it possible to generate the same hash value with an altered input, thus making it possible to retroactively manipulate the content of a block while keeping the chain intact. The special feature is that when this hash function is used in a "redactable blockchain", after a changed block has been published any collisions of the hash function can only be found with knowledge of the key. This keeps the blockchain unassailable by outsiders despite the changes. Changes can be reconstructed by the network's participants, however. This prevents those in possession of the key from making any unnoticed changes. The key can be kept locked away by a central entity and only used when required. Alternatively, a multipart key can be spread among multiple participants so the blockchain can only be altered by all of them working together.³²⁰ In a centralized solution, the key can be administered by the central entity. In an open solution, it is conceivable to divide the key among all of the system's participants or designate a group of "administrators" within the system who are responsible for performing this task.

5.2.5.2.2 Forks

When all participants work together in an open solution, to comply with an erasure obligation all of the nodes effectively agree on a fork. A central entity could order the nodes, acting as processors, to implement a fork. This changes the rules of the DLT platform. All datasets with content to be erased could be removed from the DLT platform, ignored by the nodes from that point on, and deleted. Since all nodes are either jointly responsible or act as processors engaged by a central entity, such an approach basically appears to be conceivable.

5.2.5.2.3 Off-chain storage and one-time issuing of usernames

If the solutions presented are not feasible, an approach comparable to an anonymization solution can definitely be taken in open and centralized solutions. Usernames are issued once, and data that permit association with a person are stored off-chain and linked to the chain with hash values. Then the erasure obligations can be met like in an anonymization solution. The keys linking usernames and identities are administered by

³¹⁹ The concept of redactable blockchains was presented by Ateniese/Magri et al., 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 111-126. It was also proposed by Martini/Weinzierl, NVwZ, 2017, pp. 1251-1259 (1256 f.); Marnau in Eibl/Gaedke, INFORMATIK 2017, 1025 (1030); Bechtolf/Vogt, ZD, 2018, pp. 66-71 (70); Finck, EDPL, 2018, pp. 17-35 (31).

³²⁰ Ateniese/Magri et al., 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 111 (117).

the central entity in the case of a centralized solution, and by all of the system's participants in the case of an open solution. If required, they can be erased by the controller in each case to ensure permanent anonymization of the data.

5.2.6 Summary

In connection with a DLT solution, data processing is performed either in connection with providing merchandise or services to a person residing in the European Union or by a controller based in the European Union. In both cases, the GDPR applies.

In terms of whether personal data are processed at the DLT level, it is possible to differentiate between exclusively B2B solutions that exclude any possibility of identifying natural persons using the system, and all other cases.

5.2.6.1 Exclusively B2B DLT applications

Individuals affected by data processing can be users of a system or third parties. If a DLT application is directly used only by companies whose activities do not allow anything to be deduced about the natural persons behind them, processing of data on the system's users is not relevant under data protection law. If an application requires the participating companies to exchange data via third parties, e.g. final customers, then these data must be stored off-chain. No personal data are therefore processed at the DLT level, and none of the processing is relevant under data protection law. If a mobility solution allows such an approach, it deserves preference under existing data protection laws. The associated challenge is how to prevent natural persons behind the participating company from being identified. Larger companies are not exempt from this. Each individual case must therefore be carefully examined.

5.2.6.2 Other cases

If an exclusively B2B solution as described above neither possible nor wished, the application will typically require the processing of personal data. The users of B2C and C2C applications are mostly natural persons. Natural persons can also be affected in the case of B2B applications if the persons behind the company are known.

These persons rarely appear under their actual names in stored datasets, but they can be identified if the key linking their identities and usernames is known. Nor is it possible to rule out the possibility that they may be identified even without knowledge of the key, namely by analyzing all available information stored on-chain.

The controller responsible for storing and reading data is the active agent in each case. If data on a transaction partner are involved, Art. 6 (1) Subparagraph 1 (b) of the GDPR will typically constitute a viable legal basis for data processing. In the case of third-party data, these can be stored and read in order to comply with a legal obligation or protect legitimate interests or with the consent of the affected third party.

Responsibility for on-chain processing is shared—unless the architecture is additionally modified—by all of the network's nodes. In the event that all of the network's nodes also have a legitimate interest in all processed data, this can definitely be a viable (open) solution. If not all of the participants have a legitimate interest in all processed data, then in the case of a permissioned DLT application it is necessary to either create a responsible central entity (centralized solution) or, in the case of an open DLT appli-

cation, eliminate the personal nature of all data processed on-chain (anonymization solution). In the event of an anonymization solution, no legal basis for on-chain data processing is required because the data concerned are not personal. However, anonymization solutions do pose one major challenge: namely ensuring that the software used by the nodes will not allow on-chain storage of any personal data. In an open or centralized solution, the personal data of users can be processed on the basis of a contract, to protect legitimate interests, or with the consent of the affected individuals.

The hardest part in all of these models is enforcing the right to rectification and erasure. While in anonymization solutions this is fairly easy to accomplish simply by deleting the key and using off-chain data, open and centralized solutions require additional tweaks. If the use of a redactable blockchain, forks, or comparable instruments for retroactively manipulating the DLT layer fails to deliver a viable solution, then under existing laws erasure obligations can only be countered by choosing an anonymization solution, in other words refraining from storing any personal data in the DLT layer.

5.2.7 Outlook for future legal reforms

The investigation shows that the use of DLT applications for mobility projects is basically compatible with the GDPR. Depending on the specific application, however, extensive adjustments to the architecture will be needed to meet the erasure obligations. In some cases, this may require considerable programming work.

In terms of data protection law, the main obstacles to the use of DLT applications are, for one, unsatisfactory assignment of the controller function to all of the nodes of a DLT platform and, for another, the lack or impracticability of possibilities for retroactively deleting stored information. The best arrangement would be one in which responsibility for on-chain process of data is clearly allocated, making it superfluous to erase stored information.

Future laws could achieve this goal by assigning a controller role to each participant in a specific transaction. The nodes of the network act on their own as data mediators and have no interest in the processed information. While it is true that they determine the purpose and means of data processing in their copies of the database, from a larger perspective they are actually tools that the DLT application's users employ for exchanging and storing data.³²¹ A law could therefore stipulate that the controller responsible for processing information linked to usernames in a DLT application is identical with the participants behind the usernames who, after receiving detailed information, have freely opted to use the application. If a transaction also contains usernames of other participants (in addition to the storing party's own username), then these will subsequently be responsible for the personal data contained in the stored information in the form of their usernames.

This approach would give rise to a situation in which the affected individuals themselves become (joint) controllers of relevant data processing. Commingling the roles of controller and data subject in one and the same person would cancel out their respec-

³²¹ This is how the German Federal Blockchain Association (Blockchain Bundesverband) argues in *Blockchain, data protection and the GDPR*, p. 6.

tive data protection obligations. Erasure of data is not explicitly called for, but the participants know this in advance. By participating, they agree to this state of affairs. The shared goal of those using a DLT platform to exchange information depends on long-term storage of information on the platform. This fact could be taken advantage of to find a way to securely implement DLT applications in compliance with data protection law.

However, no matter which approach is taken it is always essential to keep in mind that data protection law, as an extension of general personality rights, is extremely important. Suggestions to roll back data protection laws to allow technologies that are able to execute value transactions more efficiently must therefore be treated with caution. In any case, it is out of the question for such a change to justify processing the data of third parties who are not themselves participants in a network. There is no alternative to storing their personal data off-chain. Also after amending existing laws, on-chain data must be kept to a bare minimum to prevent any data besides a username and an associated value transaction from being stored in the DLT layer. Participants in a DLT application would have to be thoroughly informed in advance about the consequences of concluding a contract, and especially those of permanently storing information linked to their usernames.

Any such amendment would face considerable hurdles. First of all, the concept of controller is anchored in European Union law. Individual member states do not have the right to independently interpret or standardize it. Consequently, any adjustment to the concept of the controller would require a change to the GDPR at the EU level. In addition, the risks involved in shifting responsibility to the participants in a given transaction must be considered. Joining a DLT platform would require users to partially waive their data protections. But no situation may arise in which citizens relinquish control over their own personal data as a result of careless or (de facto) obligatory participation in a DLT project. Candidates would also have to be thoroughly informed about how data are processed on a given DLT platform before joining it, which begs the question as to who or what is obliged to provide this information. It is conceivable that future laws will require the information to be embedded in the DLT platform's software. If any DLT application then fails to comply with this requirement and nevertheless processes data, all of its participants would be guilty of violating data protection law.

Another problematic situation can arise if individual participants, either intentionally, negligently, or as a result of technical defects, enter personal data in the DLT network that do not comply with the system's requirements. This can result in the constant publication of personal data of third parties or participants that exceed the required minimum. A participant who does this could be held accountable, but he or she would be unable to comply with the associated erasure obligations. At the very least, possibilities for claiming compensation would have to be provided. But it is highly doubtful whether a system that can be intentionally or unintentionally misused in this way could do justice to the data protection principles of Art. 5 of the GDPR and the privacy by design and privacy by default requirements of Art. 25. One possible solution is DLT platforms that are technically configured to prevent such misuse, for example by designing the software to only accept datasets that cannot possibly contain personal data that should not be published.

5.3 Existing Regulatory Approaches

5.3.1 International³²²

5.3.1.1 USA

In the USA, the U.S. Securities and Exchange Commission (SEC) oversees ICOs and trading in cryptocurrencies and tokens.³²³ No nationwide federal legislation exists on this,³²⁴ although various states have passed their own laws. The best-known regulatory system is probably that of the BitLicense issued by the New York State Department of Financial Services (NYDFS)³²⁵ to companies that engage in virtual currency activities.³²⁶

As of early 2019, several laws related to DLT technology have been proposed.³²⁷ Most of them aim to regulate virtual currencies, but some also call for the use of DLT technologies by the government and the introduction of rules to facilitate the enforceability of smart contracts.

5.3.1.2 Switzerland

In Switzerland, virtual currencies and other DLT applications (including smart contracts) are being monitored by the Swiss Financial Market Supervisory Authority (FINMA), which assumes certain kinds of activities to be subject to regulatory licensing requirements.³²⁸ The FINMA has also published guidelines for handling enquiries from ICO organisers.³²⁹

In early 2018, the State Secretariat for International Financial Matters launched a working group on blockchain and ICO to review the Swiss regulatory framework and identify possible need for action. The declared goals were, among others, to increase legal security and ensure a technologically neutral regulatory system.³³⁰ A recent report by the Swiss Federal Council refers to a certain need for legislative action. Among other things, it recommends adjusting the laws on securities to achieve greater security and enable technology-neutral transmission of value rights via entries in distributed regis-

³²² A selection of laws and initiatives is presented here. For an overview of international regulation of virtual currencies (regularly updated), see: <https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html> (last visited on February 7, 2019)

³²³ Cf. for example: Securities and Exchange Commission, Statement on Digital Asset Securities Issuance and Trading, available at <https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading> (last visited on February 7, 2019).

³²⁴ Cf. also Hofert, Regulierung der Blockchains, 2018, pp. 208 f.

³²⁵ Available at <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf> (last visited on February 7, 2019).

³²⁶ For more information, cf. Hofert, Regulierung der Blockchains, 2018, pp. 205, 216 ff.

³²⁷ An overview is available at <https://www.virtualcurrencyreport.com/2019/01/blockchain-week-in-review-week-of-january-14-18-2019/#more-3837> (last visited on February 7, 2019).

³²⁸ FINMA, Faktenblatt Virtuelle Währungen, updated on August 30, 2018, available at <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaett-virtuelle-waehrungen.pdf?la=de> (last visited on February 7, 2019).

³²⁹ FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16.02.2018, available at <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de&hash=6518A4B3067554A0E22600E167601EF59AA20542> (last visited on Feb. 7, 2019).

³³⁰ Schweizer Bundesrat, Medienmitteilung vom 18.01.2018, available at <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69539.html> (last visited on February 7, 2019).

ters.³³¹ It also sees a need to update bankruptcy law by, for example, conclusively regulating the separation of cryptocurrency-based assets from an estate in liquidation.³³² The financial market law is regarded as being adequately technology-neutral with no need for any substantial adjustments at this time.³³³

5.3.1.3 Malta, Liechtenstein

In 2018 the Maltese parliament passed three laws containing specific provisions on DLT applications. The Malta Digital Innovation Authority Act (MDIA Act)³³⁴ created the Malta Digital Innovation Authority, whose tasks are to include supervising and regulating innovative technologies. The law explicitly refers to DLT technology and smart contracts. The Innovative Technology Arrangement and Services Act (ITAS Act)³³⁵ deals with the certification of DLT applications. Finally, the Virtual Financial Assets Act (VFA Act)³³⁶ contains provisions on virtual currencies, ICOs etc.

Liechtenstein³³⁷ has drafted a law for establishing a secure legal framework for DLT.

5.3.1.4 Japan³³⁸

In Japan, reforms of several laws entered into force in 2017. They contain special provisions on virtual currencies. Art. 2 (5) of the Payment Services Act contains a legal definition of the concept of "virtual currency". Now there is also a registration requirement for providers wishing to operate exchanges for virtual currencies. To help combat money laundering and funding of terrorism, operators of exchanges must now establish the identities of their clients. New consumer protection rules were also established.

5.3.2 Germany and Europe

No DLT-specific legal provisions exist yet at the federal level in Germany. The current discussion is revolving around issues related to legislation on financial and capital markets, especially whether to treat tokens as securities and the associated supervisory implications. The German Federal Financial Supervisory Authority (BaFin) has taken a stand several times on issues related to virtual currencies, tokens, and ICOs.³³⁹ In par-

³³¹ Schweizer Bundesrat, Bericht Rechtliche Grundlagen für Distributed Ledger-Technologie und Block-chain in der Schweiz, available at https://www.mme.ch/fileadmin/files/documents/Publikationen/2018/181207_Bericht_Bundesrat_Blockchain.pdf, pp. 67 f. (last visited on February 7, 2019).

³³² Bericht des Bundesrates, pp. 72.

³³³ Bericht des Bundesrates, pp. 9 f.

³³⁴ Available at <http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1> (last visited on Feb. 7, 2019).

³³⁵ Available at <http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1> (last visited on Feb. 7, 2019).

³³⁶ Available at <http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1> (last visited on Feb. 7, 2019).

³³⁷ Communication of August 29, 2018, available at <https://www.liechtenstein.li/en/news-detail/article/liechtenstein-preparing-blockchain-act/> (last visited on Feb. 7, 2019).

³³⁸ Cf. Danwerth, ZVglRWiss, 2018, pp. 117-155..

³³⁹ Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Hinweisschreiben vom 20.02.2018, GZ: WA 11-QB 4100-2017/0010; Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs), available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html?nn=11056122 (last visited on Feb. 7, 2019); Fußwinkel/Kreiterling, Blockchain-Technologie – Gedanken zur Regulierung.

ticular, it has acknowledged virtual currencies as units of account in the sense of Section 1, Paragraph 11, Sentence 1, No. 7 of the German Banking Act (KWG).³⁴⁰ All of its assessments have been made on the basis of existing laws.

At the European Union level, the first directive mentioning virtual currencies was finalized in December 2017: the term "virtual currency" now appears in Art. 1 (2) (d) of the 5th Money Laundering Directive. In August 2018 a petition to extend the provisions on crowdfunding of ICOs was integrated.³⁴¹ The European Union is also considering additional measures for creating a competitive, innovative financial market, including blockchain technology.³⁴² Overall, the emphasis here is on legal issues around financial and capital markets, especially as regards protections for investors.³⁴³

³⁴⁰ Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Merkblatt Finanzinstrumente vom 20.12.2011, geändert am 26.07.2018, available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.htm (last visited on Feb. 7, 2019); a.A. KG Berlin, Urteil vom 25.9.2018 – (4) 161 Ss 28/18 (35/18), NJW 2018, 3734.

³⁴¹ Cf. Europäisches Parlament, 2018/0048(COD), available at <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-626.662&format=PDF&language=DE&secondRef=02> (last accessed on Feb. 7, 2019).

³⁴² Cf. Europäische Kommission, COM(2018) 109 final, available at <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-109-F1-DE-MAIN-PART-1.PDF> (last accessed on Feb. 7, 2019); Europäische Kommission, Blockchain Technologies, available at <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> (last accessed on Feb. 7, 2019).

³⁴³ European Securities and Markets Authority (ESMA), Advice Initial Coin Offerings and Crypto-Assets, Rn. 14 ff.

6 Shipping Documents

6.1 Economic and Technical Aspects

6.1.1 Definition and description of an example application

A bill of lading (BoL)³⁴⁴ is a key document in the context of international shipping and logistics. It is a special transferable shipping document that simultaneously confers title to the goods in question. It is typically issued by a carrier (a shipping company or forwarder) or its agent, initially to serve as a receipt by documenting acceptance of the freight by the exporter (loader) for shipping. It contains important information on the type of goods involved and the details of their carriage. Normally it is given to the importer (unloader) after it has been signed by the exporter and carrier and the cargo has been paid for. In international trade, the BoL derives its importance primarily from the "International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading and Protocol of Signature" of 1924.³⁴⁵

A BoL serves three main functions:³⁴⁶ it is a receipt acknowledging that goods have been loaded, it contains or evidences the terms of the contract of carriage concluded between the exporter and the carrier, and it documents title to the goods. This last function means that the designated consignee or lawful holder of the BoL owns the goods and is therefore legally entitled to receive them, and can also use the BoL to transfer ownership of the goods to another participant in the delivery chain.³⁴⁷

Bills of lading play an important, internationally acknowledged role in global shipping. In the context of international trade, the importer and exporter require additional security whenever there is a lack of mutual trust, for example due to differing legal systems in their respective countries. Ideally, the exporter does not want to give up possession of goods until he or she has received payment for them from the importer. Conversely, the importer has a legitimate interest in receiving confirmation that he or she will receive the goods in the agreed condition before paying for them. The BoL is used as an instrument for resolving this conflict of interests. When the cargo is loaded, the exporter receives the BoL from the carrier as a receipt. It guarantees ownership of the goods, even if they are no longer physically in his possession. A copy of the BoL is often sent to the importer to serve as evidence that the goods have been dispatched. After the importer has made payment for the goods, the exporter sends the BoL, in other words he or she physically sends it to the importer or an agent designated by him or her, who then takes delivery of the goods while physically handing the BoL to the carrier. Figure 22 illustrates how this works.

³⁴⁴ See the legal section.

³⁴⁵ Also known as the Hague Rules.

³⁴⁶ Beecher, *The International Lawyer*, 2006, pp. 627-647.

³⁴⁷ The so-called trading effect; see the legal section.

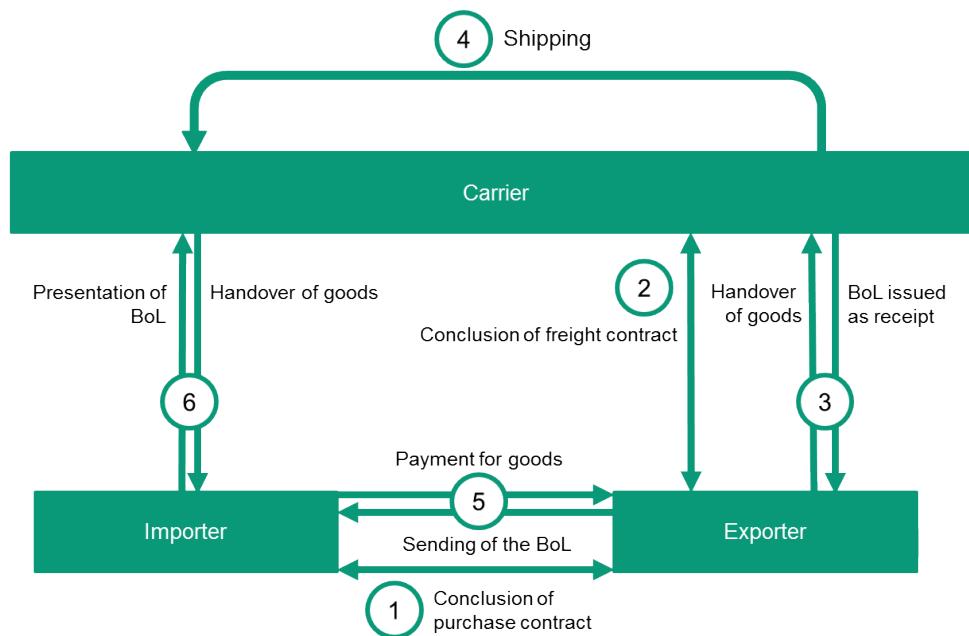


Figure 2: Simplified depiction of the role of a BoL in international shipping

A BoL typically contains the following information³⁴⁸:

- Data on the exporter and importer (name/company, contact information)
- Possibly contact information of third parties that need to be informed of the current status of shipping
- Data on the carrier (company, logo, address, contact information and terms of carriage)
- BoL number (a unique number assigned by the carrier or shipping company)
- Name of the ship/vehicle and number of the trip
- Place of receipt, loading port, unloading port, place of transfer, final destination
- Container number, seal number, registration number
- Description of goods (total weight, volume etc.)
- Applicable Incoterms³⁴⁹ (international contract terms)
- Place and date of dispatch and signatures of the exporter, carrier and importer
- Terms of carriage and possibly shipping specification such as "port-to-port" or "combined transportation".

The BoL can also contain special agreements between the exporter and carrier that deviate from those of the shipper.³⁵⁰

Owing to the comprehensive documentation of the carriage terms included in the BoL, its legal station and its long tradition, it is the preferred instrument for letters of credit

³⁴⁸ Section 515 of the German Commercial Code.

³⁴⁹ The International Commercial Terms are a series of voluntary rules for interpreting standard contractual formulations used in international shipping.

³⁵⁰ Beecher, *The International Lawyer*, 2006, pp. 627-647.

(LC) in international shipping.³⁵¹ The standards for using letters of credit are defined in the UCP 600 (UCP = Uniform Customs and Practice for Documentary Credits) of the International Chamber of Commerce (ICC).³⁵² A letter of credit is defined there as follows:

A (documentary) letter of credit is a payment mechanism used in international trade. The importer's bank (issuing bank) undertakes to pay to the exporter of goods the corresponding value after certain previously defined documents have been completely and correctly presented. The process is illustrated in simplified form in Figure 23.³⁵³

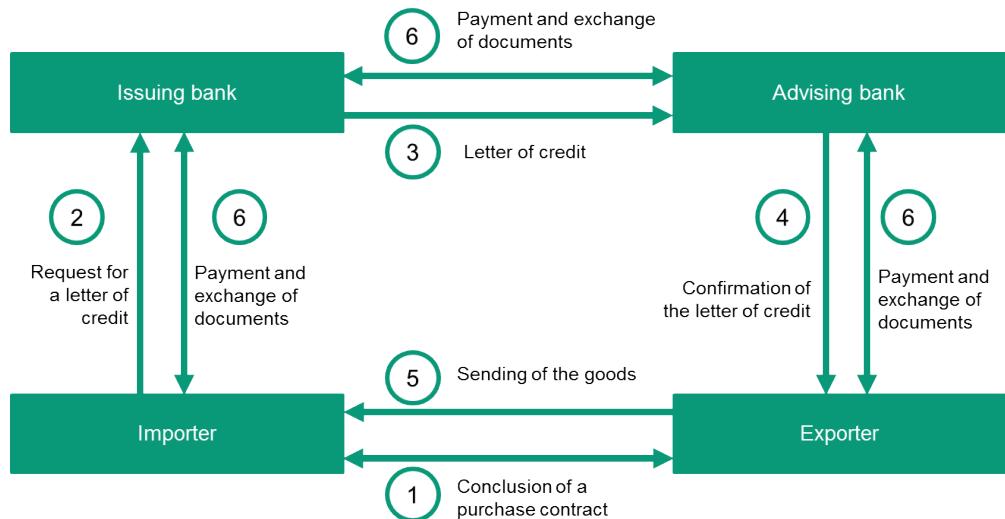


Figure 3: Simplified diagram of a letter of credit process

Consequently, as a rule four parties are involved: an importer (applicant or buyer), an exporter (beneficiary or seller), an issuing bank and an advising bank. The letter of credit is always based on a contract for buying certain goods (1), in which a letter of credit is specified as the instrument of payment. The letter of credit itself, however, is separated from this purchase contract. Only the terms that the letter of credit contract specifies for the documents to be submitted are relevant for implementing the process.

After the purchase contract (1) has been finalized, first the importer requests his bank (issuing bank) to issue a letter of credit (2) and ask the advising bank (3) to inform the exporter that the letter of credit (4) has been issued. Then the exporter sends the goods to the importer (5) and submits all previously stipulated documents (e.g. the bill of lading) to his bank (6). The advising bank checks to make sure that these documents are complete and correct. This check is often carried out manually using paper-based documents. If the right documents have been received, they are passed on to the issuing bank, which performs the same checks on them. As soon as this bank has also verified that the documents are correct, payment is made to the exporter.

³⁵¹ There are many different versions of letters of credit; here only documentary letters of credit are meant.

³⁵² UCP 600 (Uniform Customs and Practice for Documentary Credits).

³⁵³ For a detailed description of the LoC process, cf. e.g. Grassi, 7 Pace Int'l Rev., 1995, 81-128.

In this case study, the BoL—representing all kinds of documents used in international trading—is examined more closely and the (document) letters of credit that are frequently associated with them analyzed in greater depth to identify possibilities for employing DLT. In addition, the closely related implications for supply chain processes will be analyzed.

6.1.2 Status quo and challenges

In 2017 goods worth a total of nearly 18 trillion U.S. dollars were traded in the world's markets,³⁵⁴ 90% of which were transported between countries by sea.³⁵⁵ This trading and the associated logistical processes are increasingly dependent on highly complex and specialized supply chain processes that, in many cases, have in turn only become feasible as a result of introducing and/or using advanced communication and information technologies. However, documentation of these processes is still largely paper-based, similarly to the case of bills of lading.

The use of paper-based documents has various drawbacks. The single biggest disadvantage is probably that they have to be physically transported. An importer must present the original paper BoL in order for the carrier to release the goods to him. In the best of cases, the exporter is able to obtain the BoL from the carrier very quickly (e.g. a day after the ship leaves port). On average, however, exporters wait three days for this to happen, and sometimes a week or more can elapse. The BoL must then be sent to the recipient of the goods (or an agent authorized to accept them on his or her behalf). Even if the documents are sent by express mail (i.e. airmail), they take an average of another four to seven days to arrive. Then the recipient has to turn them over to the local freight forwarder, which can take up to two days because the customer service offices of most shipping companies are far from the port.³⁵⁶ The situation is additionally complicated by the fact that many different parties are involved in even the most straightforward international shipping processes.³⁵⁷

The problems are compounded when banks are also involved in the process, for example in connection with letters of credit. The exporter has to provide them with the BoL and other documents for crosschecking the credit terms. These documents must also be physically relayed to the next party in line, for example by a courier or airmail. In a letter of credit process the documents also have to be checked to make sure that the conditions are met. This is often painstakingly done by hand by bank employees.

The bottom line is that it frequently takes longer to send the documents than the merchandise, which prevents timely pickup of the shipment at the port of destination—everyone has to wait for the original BoL to arrive. A study carried out by the import manager of a large shipping company found that penalty fees were levied on about 25% of all shipments involving a letter of credit transaction because they were not collected on time. The problem is aggravated by the fact that the average available time window for delivering the BoL has been shrinking in recent years as cargo ships

³⁵⁴ Statista, Trends in global export volume of trade in goods from 1950 to 2017.

³⁵⁵ International Chamber of Shipping, Shipping and World Trade Shipping and World Trade.

³⁵⁶ Beecher, The International Lawyer, 2006, pp. 627-647. Beecher, The International Lawyer, 2006, pp. 627-647.

³⁵⁷ The figures vary according to the source, typically the figure of at least 10-30 participants is given.

have been getting faster. For example, it now takes only nine days for a freighter to get from Bremen to New York. Overcrowding of ports has become a serious problem as shipping volumes steadily increase, putting pressure on carriers to clear merchandise off piers as quickly as possible.

The upshot is that the heavily paper-based process slows down almost all of the steps involved, while manual copying of information is a major source of errors.³⁵⁸ Insufficiently digitized processes and the associated low level of automation frequently result in a lack of information, like for tracking merchandise, thus generally making supply chain processes quite inflexible. This in turn requires companies to keep larger quantities of raw materials on hand, which incurs additional costs. Overall, today's analog system is estimated to generate costs on the order of between five and 10 percent of the total value of all internationally traded goods³⁵⁹ each year, totaling around one trillion U.S. dollars. In recent decades, intensive study has been devoted to identifying ways of digitalizing international trade and replacing bills of lading, which still play a central role, by a suitable electronic process with the same functionality. Such an electronic alternative, referred to in the following as an "e-BoL", could significantly reduce the time required to process documents and also greatly improve security with encryption and digital signatures. Efficiency could also be improved by eliminating error-prone manual copying of information. IBM has estimated that faster provision of information and associated efficiency gains in logistical processes could save so much time between processes steps that total maritime shipping costs could be slashed by as much as 40% for a saving of up to several thousand dollars per container.

The current situation and its challenges have sparked an intensive search for alternatives. In recent decades, the Sea Waybill has emerged as one practicable option.³⁶⁰ In contrast to conventional bills of lading, this solution eliminates the need to physically hand over goods in order to transfer ownership of them. It is sufficient for the receiver to present a copy of the Sea Waybill as proof that he or she is authorized to pick up the merchandise. This at least permits digitization of the information flow, although not of the ownership transfer processes associated with handing over a BoL. The use of bills of lading, since they are legally comprehensive and universally usable instruments, continues to be very widespread.

The technical requirements for creating a digital BoL could definitely be met with conventional digital technologies. A public/private key infrastructure could enable authorization, encryption and integrity (SSL/TLS), and a central register could be set up to ensure that each valid e-BoL corresponds to only one transaction.

The first attempt to create an electronic BoL based on these principles that deserved to be taken seriously was BOLERO,³⁶¹ a centralized private registration and communication system supported by a consortium comprising several shipping companies, banks, insurers, and telecommunication providers. It enabled the participants in a given ship-

³⁵⁸ It is estimated that every other document contains at least one error as a result of incorrect copying of information.

³⁵⁹ Todd, Journal of International Banking Law, 2000, pp. 410-418.

³⁶⁰ Boom, European Transport Law (ETL), 1997, pp. 9-24. Boom, European Transport Law (ETL), 1997, pp. 9-24.

³⁶¹ Bill of Lading Electronic Registry Organization, since 1998.

ping process—and only them—to join and read or edit transactions. Cryptographic methods were used. The platform also provided a means for members to communicate with one another.

One problematic aspect was the internationally unrecognized electronic format of the BoL (as well as the lack of a legal basis for its use). An attempt was made to get around this by appropriately defining the platform's terms of business. But it remained unclear whether the owner's right to take receipt of the goods was actually transferred under national law in every case. Independently of the issue as to whether or not the rules should allow this, it is questionable whether an electronic BoL can enable it. This is because the associated freedom to conclude contracts could very well collide with the legitimate interests of third parties, such as creditors of players involved in the transfer. Most authors assume that, under current laws, an electronic BoL cannot transfer ownership of goods and thus also rights and obligations.³⁶² BOLERO was unable to achieve a breakthrough in the marketplace, nor did any other centralized platform succeed in doing so either.

In recent years, however, events have accelerated. In late 2017 IBM and Maersk undertook a fresh attempt by developing TradeLens, a blockchain based on Hyperledger Fabric, for managing the container shipping supply chain. They succeeded in digitizing all of the documents involved in the process and allowing containers to be tracked. According to IBM, 92 enterprises including both shipping companies (e.g. Maersk and Pacific International) and port operators (e.g. Rotterdam and Singapore) with over 200 docks are now participating, representing about 20% of all international shipping, plus roughly the same number of other docks (around 235). So far more than 250 million "shipping events" have reportedly been handled via TradeLens.³⁶³ It should be mentioned that no way to transfer ownership of eBoLs has yet been implemented, so it has thus far only been possible to use TradeLens for reliably documenting supply chain processes for all of the players involved in moving a shipment of goods. A few national authorities, among them the Saudi Arabian customs authority, are also planning to adopt TradeLens.³⁶⁴ However, IBM and Maersk charge fees, about which very little information is currently available, for access to the TradeLens system. They are also claiming intellectual property rights arising from the project. In effect, this cancels out the solution's decentralized nature. Although it has been growing fast, its long-term ability to successfully compete against a completely open solution therefore remains questionable.

Presumably in response to this, in late 2018 some of the world's largest shipping companies and terminal operators founded another consortium for the purpose of developing a DLT-based platform for a global trading ecosystem called the Global Shipping Business Network (GSBN). Currently it is striving to digitalize and automate the documentation and processes for hazardous goods, which are typically hampered by a number of regulations. Ultimately, the aim is to enable seamless end-to-end sharing of documents and data throughout the maritime shipping process.

³⁶² Beecher, *The International Lawyer*, 2006, pp. 627-647.

³⁶³ Tradelens, *The Power of the Ecosystem*.

³⁶⁴ Customs, *Saudi Customs Pilot Sees the Integration of Customs Tracking Feature with IBM and Maersk TradeLens Blockchain Solution*.

Wave, an Israeli startup, and Barclays said that they executed the world's first shipping transaction with blockchain technology in 2016.³⁶⁵ Wave is already working on a commercial solution involving bills of lading digitized with DLT; currently it is testing various pilot implementations together with several shipping companies.³⁶⁶ Another startup, Slovenia-based CargoX, announced in late 2018 that it was making a DLT-based electronic BoL solution commercially available. The system makes it possible to issue and transfer electronic BoLs on a public blockchain. In January 2018, CargoX raised over seven million USD with an ICO for the purpose of conducting pilot projects in the second half of the year with several logistics service providers that are now also using the platform. They include Schweizer Fracht AG, Sprint International Express, Globalink, Global Value Network and Freightalia. According to CargoX, users can issue and transfer a BoL in minutes for only 15 U.S. dollars.

BlockLab, an entity established by the Port of Rotterdam Authority and the Municipality of Rotterdam, is currently implementing another pilot project in which Samsung SDS and ABN AMRO, among others, are also involved.³⁶⁷ The goal is complete, paperless integration of all physical, administrative and financial streams of international distribution chains.

6.1.3 Possible solutions and the role of DLT

An e-BoL must perform the three basic functions of a BoL that were described at the start of this chapter. In particular, it must stipulate the terms of carriage, provide confirmation that the carrier has received the goods, and enable transfer of ownership to them. In addition, an e-BoL should be inexpensive and extremely difficult to counterfeit. For such an e-BoL to prevail in practice, the cost of introducing and using it must also be relatively low. At the same time, there naturally also has to be a way of ensuring that only persons with a legitimate interest in the transactions concerned receive access to the data contained in an e-BoL.

As far back as the mid-1990s, the legal prerequisites for digitizing bills of lading were addressed by the United Nations Commission on International Trade Law (UNCITRAL). It identified the already-discussed "guarantee of uniqueness", which any electronic implementation of a BoL must provide, as the biggest challenge.³⁶⁸

Centralized platforms operated by an intermediary such as BOLERO, which until recently were the only available possibility for technically implementing an electronic BoL (e-BoL), are saddled by disadvantages and risks for the involved players. For example, centralized platforms all suffer from a vulnerability known as a "single point of failure"

³⁶⁵ Reuters, Barclays says conducts first blockchain-based trade-finance deal.

³⁶⁶ Gtreviaw, New blockchain shipping consortium to rival Maersk and IBM's TradeLens [gtreviaw](#), New blockchain shipping consortium to rival Maersk and IBM's TradeLens.

³⁶⁷ Port of Rotterdam, ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a Container logistics blockchain pilot.

³⁶⁸ Article 17(3) of the Model Law of UNCITRA states: "If a right is to be granted to, or an obligation is to be acquired by, one person and no other person and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique."

that becomes a potential target. There is thus always a danger of intentional manipulation by hackers or intermediaries. The main problem, however, like in many other B2B situations in which multiple organizations must cooperate in order to digitalize a process, is that as a rule a competitive situation exists with other enterprises in the same value chain, leading to a lack of mutual trust. The market dominance that the operator of a centralized platform can potentially derive from a monopolistic situation based on control of the platform also poses considerable economic risks for competitors. It is also very possible that, due to the enormous economic and therefore also strategic role of international maritime trade, some countries may have reservations about a platform controlled by monopolists in another country. This typically leads to a situation in which it is practically impossible to recruit collaborators for a centralized platform.

As already explained in the general section, DLT can address these issues and, particularly in situations of this kind, enable cooperation by enterprises by serving as basic IT infrastructure. When implementing such a solution, there are several challenges that have to be mastered in order for an e-BoL to be recognized and adopted. Alongside the use of digital signatures instead of manual signatures, it is essential to make sure that it cannot be copied in a distributed system. The use of digital signatures is already quite widespread in Germany and other countries, so no new technological innovations are needed to accomplish this. Although it is not possible to technically stop an electronic document from being copied in a DLT system, consensus mechanisms can prevent both the existence of multiple valid copies of the same e-BoL and multiple valid uses of the same e-BoL. The basic idea behind digitalizing bills of lading is thus to model them as "asset-backed tokens"³⁶⁹ and ensure, by means of governance rules in the DLT, that they can only be used once by design. Thanks to the PKI³⁷⁰ that is usually inherent in a DLT solution, the digital signatures required for the e-BoL have already been implemented. In addition, DLT-enabled tamperproof process documentation ensures auditability³⁷¹ and legal security in the event of disputes.

An e-BoL could also be enhanced to enable greater automation of credit transactions. For example, an escrow smart contract³⁷² could be used to freeze the fee that an importer must pay when creating the e-BoL. When unloading the goods, the token for the e-BoL can then be transferred from the exporter to the importer, thus triggering the dissolution of the smart contract and releasing the frozen sum of money. It will later be important to analyze other downstream effects in such a system, such as associated lockups of capital.

6.1.4 Process description

The following technical architecture, which executes a digital twin of each analog step now performed, could be used to digitalize bills of lading while meeting the requirements described above.

³⁶⁹ See also section 0.

³⁷⁰ See also section 0.

³⁷¹ An audit is a procedure for checking whether processes, e.g. in a company comply with legal or corporate standards. They include e.g. business audits and quality management audits.

³⁷² See also section 0.

- Like in the conventional system, before goods are dispatched the importer and exporter conclude a purchase contract and the exporter/importer and carrier conclude a shipping contract, for instance by reciprocally signing corresponding electronic contract documents.
- The moment that the goods are loaded, an e-BoL containing the data required of a BoL³⁷³ is created by the carrier and digitally signed by him and the exporter. All of the participants in the logistical process then receive information on the content of this BoL. The ownership situation can be unambiguously represented by implementing the e-BoL as an asset-backed token³⁷⁴ that is initially assigned to the exporter.
- This token is essentially no different from a smart contract, in other words a DLT address to which messages can be sent and the content of which can be changed in accordance with certain rules on which a consensus exists in the network.
- The token's ownership situation can be represented by defining an "owner" entry for the corresponding smart contract containing the owner's public key. The owner's private key is then an essential prerequisite for changing this field.

One possible version of a digitalized e-BoL process is schematically shown in Figure 24.

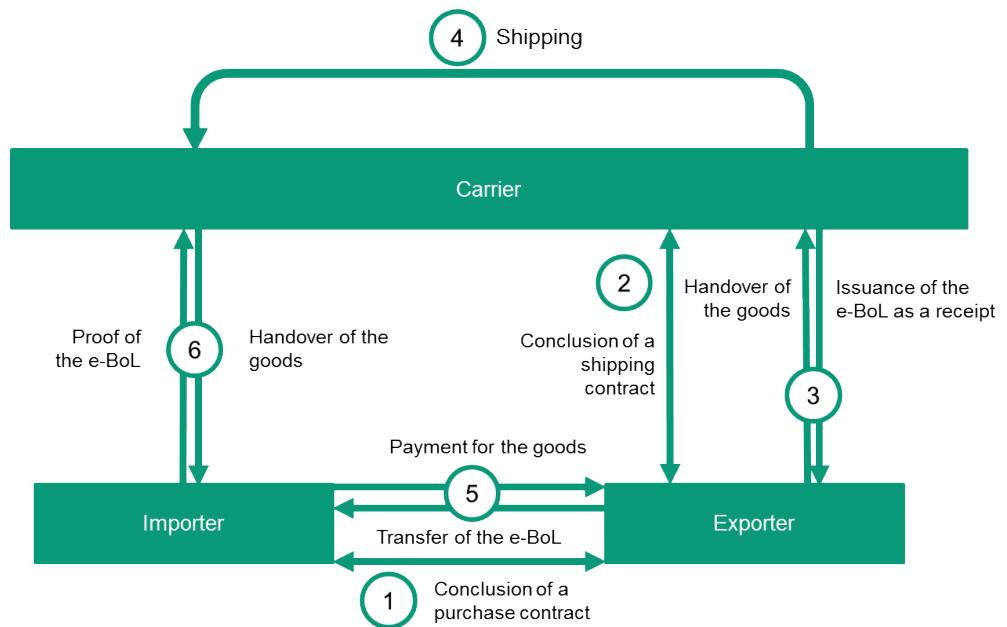


Figure 4: Schematic depiction of e-BoL-based international trading

It should be noted that smart-contract-capable DLT is a prerequisite for such a system to work. One possibility, which is used by TradesLens and others, is to implement it in Hyperledger Fabric. Solutions of this type also involve architectures that are especially well-suited for representing the process associated with the BoL. In the case of

³⁷³ See also section 6.1.1.

³⁷⁴ See also section 0.

TradeLens, there are several REST-APIs³⁷⁵, for example an API for adding or removing players involved in the process (e.g. ports, forwarders etc.) and an API for entering events in the TradeLens platform, such as expected arrival times, which are then automatically passed on to the involved nodes and process participants. The TradeLens platform thus already integrates a large number of comprehensive APIs that participating companies or authorities can use to submit documents for defining events related to shipping containers or goods. Although this platform apparently does not yet include a way to transmit e-BoLs, it is possible to generate an e-BoL for documentation purposes, as well as general documents such as scans of papers. It should be stressed that an appropriate implementation, for example in Hyperledger Fabric,³⁷⁶ would provide a comprehensive range of possibilities for safeguarding companies' secrets:

- The use of a private blockchain automatically keeps the number of nodes that are able to access data very small. These can include, in addition to shipping companies, upstream forwarders or large customers, as well as ports or national authorities such as customs agencies.
- In addition, Hyperledger Fabric integrates comprehensive data security functionality. For example, it is possible to administer multiple private blockchains with a subset of the nodes participating in each one. The architecture behind TradeLens can therefore be described as a collection of blockchains, with only those nodes having reading and writing rights for a given shipping event—for example, moving a container from A to B—that are actively integrated in the process, for instance by the creator of the e-BoL.
- It is also possible to keep data completely private within one of these blockchains. For example, if it is wished to keep the contents of a container or a company's identity secret, then these data are only revealed to authorized nodes. The same possibility also exists for input or output values flowing into or out of a smart contract (chaincode).

Where letters of credit are concerned, an e-BoL could also conceivably be used to completely automate the analog process described above by means of DLT, e.g. as shown in Figure 25.

³⁷⁵ An API (application programming interface) is a programming interface of an IT system, i.e. a part of a program that is used to link it to other programs. REST-API is a standard for APIs that are considered to be especially reliable. An API for inserting process steps or events in international shipping ("shipping events") can be found e.g. at <https://platform-sandbox.tradelens.com/documentation/swagger/?urls.primaryName>.

³⁷⁶ See the general technical section 1.2.1.

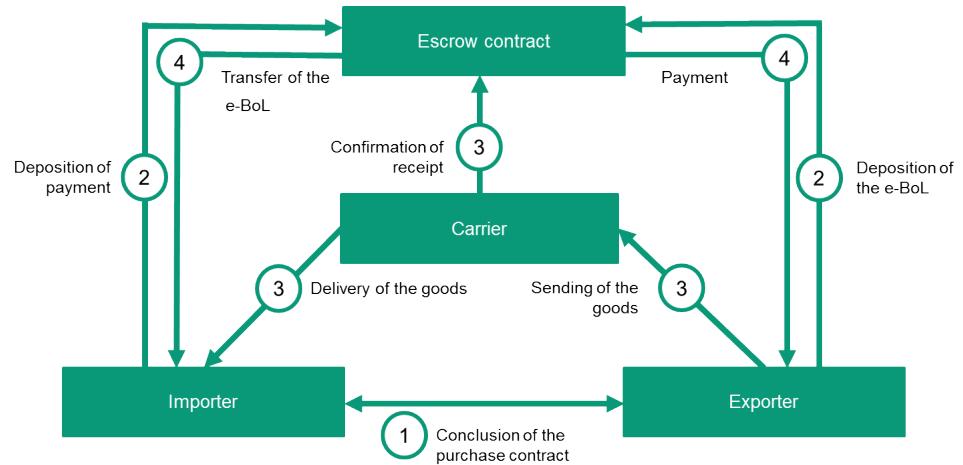


Figure 5: Letter of credit process based on an escrow smart contract

This process could in principle be executed without the involvement of any banks. First, any additional documents required for the letter of credit besides the e-BoL are defined. Before the goods ship, the sum owed by the importer is coded in a so-called escrow smart contract.³⁷⁷ As soon as a previously defined trustworthy party³⁷⁸ (such as a courier) digitally has confirmed the dispatch or arrival of the goods³⁷⁹ and verified that the stipulated conditions are met, the money can be released to the exporter. The escrow smart contract thus not only checks³⁸⁰ whether conditions are complied with, such as whether certain deadlines are met, but also secures the payment, a function that would normally be performed by one or more banks. Here the question arises whether payment can be directly executed via DLT (e.g. using tokens) or if the smart contract can only perform a triggering function while actual payment is made via established channels.

Moreover, a letter of credit—in addition to its transaction function—can, in particular, also assume a financing function for the exporter via so-called reverse factoring, which is significantly reduced in processes based on escrow smart contracts. Due to the fact that in this approach (i.e. bypassing banks) liquidity is bound up in the smart contract, it will later be necessary to discuss the legal implications of using smart contracts to manage funds on an escrow basis.

Overall the discussed processes make it very clear that a flow of information is a prerequisite for digitalizing bills of lading and letters of credit. Functions for real-time tracking and tamperproof storage of data should be an integral part of any DLT-based ecosystem for documents such as bills of lading. This is confirmed by the fact that TradeLens is actually, first and foremost, a platform for the exchange and tamperproof storage of information contained in shipping documents. It is safe to assume that both here and in other approaches that are now appearing in the market, over time addi-

³⁷⁷ See the corresponding part of the general technical section 1.2.1.

³⁷⁸ Not a platform operator, so no problems arise concerning the formation of monopolies etc., which is what ultimately provides the arguments for dispensing with intermediaries.

³⁷⁹ See also 3.2.5 in the general technical section.

³⁸⁰ Here too the general question arises as to how automated checks by a smart contract should be treated in the event of disputes; see the general legal section 1.2.3.

tional possibilities such as the use of e-BoLs or completely digitalized letters of credit will also appear.

6.1.5 Conclusions and recommendations for action

There are many reasons why the digitalization of international shipping has not yet progressed very far, especially concerning bills of lading. The enormous complexity and diversity of international shipping activities, conflicting legal systems, and a lack of suitable cross-country infrastructure, among other factors, have conspired to prevent the establishment of a consistent, standardized digital solution. One frequently cited explanation for the relatively low digitalization of the logistics sector (as opposed to, for example, the financial sector) is collisions between the laws of different countries.³⁸¹ Skepticism toward the idea of a central institution as a trust-inspiring intermediary also tends to be great in an industry that has traditionally been relatively unfettered. Add to this the fact that central platforms tend to be driven by a single operator and lead to monopolistic conditions. This prevents the adoption of centralized solutions in B2B contexts. Competitors have no incentive to participate in the platform of a direct rival.

Mistrust of digital solutions is also widespread, among other reasons due to growing insecurity around who might be able to view confidential information and concerns that information could be lost as a result of programming mistakes or malicious attacks. Also cited as barriers are high insurance premiums for unknown programs and risks, as well as initially low potential benefits in return for substantial investments (with a platform effect only becoming noticeable relatively late in the game). Smaller companies in particular are usually challenged because they have to join the same ecosystem as large corporations in order to derive benefits from a digital solution and must also make comparable investments, for example to integrate appropriate application programming interfaces (APIs) into their systems. In a survey published in 2008, the reason most frequently given for not joining a platform was that the infrastructure, market and/or trading partners were not yet ready for such a solution (51%), followed by concerns about its legality (44%). Other reasons such as inadequate security (25%), excessively high costs (12%) and confidentiality issues (10%) played only a minor role.³⁸² In the case of BOLERO, logistics companies apparently lacked a sufficiently strong incentive to switch from time-proven processes to digital solutions.

As described above, a digital equivalent to a bill of lading can be implemented either by a central authority or on the basis of a DLT solution. Solutions involving a centrally coordinated platform have been technically possible for a long time but have nevertheless failed to take off. However, increasing efforts in recent months to establish DLT-based solutions in the market suggest that DLT is in fact able to give rise to solutions that the participating players regard as highly promising.

A prerequisite for any electronic system to get off the ground, regardless of whether it is DLT-based or not, is international harmonization of the relevant legislation³⁸³. Once this is done, widespread acceptance and use of e-BoLs are a genuine possibility.

³⁸² Goldby, Electronic bills of lading and central registries: what is holding back progress?

³⁸³ Details can be found in the legal section.

In all initiatives, however, it is essential to avoid focusing attention exclusively on bills of lading. Instead, these should be regarded as just one among various important types of documents. Other documents that play important roles in these and similar processes, like insurance papers or certificates of authenticity, should also be addressed. In addition, it may be necessary to adjust or clarify existing laws to ensure the validity of electronic signatures and digital certificates, as well as the accessibility and probative strength of electronic transactions in courts of law and the distinction between negotiable documents (especially bills of lading) and nonnegotiable ones. In the long term, it will also be necessary to shed light on liability issues in connection with programming and system errors and the resulting lack of clarity with respect to the ownership of electronic bills of lading.

Unfortunately, efforts by regulators and legislators to encourage a shift to electronic documents have so far evoked little interest in the commercial sector, as various examples show. It therefore makes sense that lawmakers are mostly taking a wait-and-see stance, especially since legislation in general tends to be reactive rather than proactive. But politicians are well-advised to consistently monitor new developments, since otherwise they run the risk of endangering Germany's foreign trade interests by failing to keep up with the latest technological trends.

6.2 Legal Discussion

Going further from the preceding economic and technical analysis of the potential of digitalizing bills of lading and analysis of possibilities for implementing this with DLT, it is now important to investigate the status of this internationally important document in German maritime shipping law. Attention will then turn to the issue of data protection in connection with digital shipping documents.

6.2.1 Trading documents

Bills of lading are covered by Sections 515 ff. of the German Commercial Code (HGB). In maritime shipping, the bill of lading securitizes a claim for surrender of the shipped movable goods. It also represents the goods themselves, so that they can be disposed of only by handing over the paper (the "trading effect"³⁸⁴). Besides the bill of lading, the German Commercial Code also defines the consignment bill (Section 443, mainly applicable to domestic shipping³⁸⁵) and the warehouse warrant (Section 475c), both of which also represent goods and can be traded in lieu of them, which is always why all three are also referred to as trading documents. What is common to the traditional securities is that the legislator often gives the same normative structure. This is illustrated by the almost identical digital saving clauses of Section 443 (Subsection 3), 475c (Subsection 4) and 516 (Subsections 2 and 3) of the German Commercial Code, which give equal status to conventional paper-based trading documents and their functional

³⁸⁴ Section 448 of the German Commercial Code on bills of lading, Section 475g on warehouse warrants and Section 524 on consignment bills; their treatment under property law is disputed, on this see Baumbach/Hopt/Merk, § 448 Rn 2.

³⁸⁵ Rabe/Bahnsen/Vor 481 Rn. 121.

digital equivalents and are therefore relevant to DLT applications.³⁸⁶ Consequently, today it is already permissible to use DLT-based digital trading documents provided that they perform all of the same functions as their paper-based equivalents. On balance this is also positively assessed in the literature, constrained only by the challenges described below.³⁸⁷

6.2.1.1 International applications of German maritime trading law

Germany has ratified the Hague Rules (formally the "International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading and Protocol of Signature") but not later updates of them such as the Hague-Visby Rules and the Hamburg Rules.³⁸⁸ Nor has Germany so far signed the later Rotterdam Rules (formally the "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea"), the first to include rules on electronic documentation.³⁸⁹ An insufficient share of the other signatory states has also so far failed to ratify them, and they are consequently not yet in force.³⁹⁰ Despite this, they have served as a model for updating German maritime trading law.³⁹¹ The Hague Rules, to the extent that they are applied, take precedence over national law, including Sections 476 ff. of the German Commercial Code.³⁹² Maritime trading agreements primarily specify the applicable law and/or legal venue.³⁹³ If there is a conflict, i.e. in the event of a neglected or invalid agreement, German maritime trading law may be applicable under Article 5, Subsection 1 of EU Regulation no. 593/2008 (Rome I).

6.2.1.2 Credit transactions in foreign trade

Credit transactions in foreign trade illustrate the advantages of DLT-based trading documents, as already discussed above in section 6.1.4 in an international context³⁹⁴. On that basis of that, here credit transactions are also briefly covered before explaining how trading papers can be represented on the basis of DLT.

If a German importer (buyer) purchases goods from an exporter (seller) in Asia, it is in the exporter's interests to wait for proof of payment before releasing them to the carrier, and it is in the importer's interests to withhold payment until proof is provided that the goods have been turned over to the carrier. This conflict of interests can be resolved, as already described in 6.1.1, by a credit agreement between the trading partners. Accordingly, the buyer undertakes to pay for the goods by arranging a letter of credit at a bank.³⁹⁵ For this purpose, the buyer (or applicant) requests the bank to issue

³⁸⁶ Additional digital saving clauses are found on waybills in Section 408 Subection 2 of the German Commercial Code and on sea waybills in Section 516 Subsection 4. In contrast to trading documents, they are not instruments but rather (if signed by both parties) simply evidence of the conclusion and content of (sea) waybills and acceptance of the goods by the carrier, Baumbach/Hopt/Merk, § 409 Rn 1.

³⁸⁷ Saive, TranspR, 2018, pp. 234-238.; Saive, RdTW, 2018, pp. 85-89..

³⁸⁸ MüKo BGB/Martiny, Rom I-VO Art. 5 Rn. 97.

³⁸⁹ Cf. Arts. 1 and 8 of the Rotterdam Rules.

³⁹⁰ On the current status of signing and ratifications, cf. http://www.uncitral.org/uncitral/en/uncitral_texts/transport_goods/rotterdam_status.html.

³⁹¹ BT-Drs. 17/10309 pp. 41f.

³⁹² Wieske, Transportrecht, 2012. pp. 313.

³⁹³ Rabe/Bahnse, Vor § 481 Rn. 125, 131.

³⁹⁴ Saive, TranspR, 2018, S. 234-238.; Saive, RdTW, 2018, S. 85-89.

³⁹⁵ Baumbach/Hopt, BankGesch K/1.

the letter of credit (via an agreement on non-gratuitous management of his affairs as per Section 675 of the German Civil Code), whereupon the bank undertakes to make the seller an abstract promise to fulfill an obligation as per Section 780 of the German Civil Code (a so-called letter of credit, which is defined in greater detail in the "Uniform Customs and Practice for Documentary Credits" (UCP) of the International Chamber of Commerce (ICC), the latest version of which is UCP600.^{396,397} The seller thus acquires a direct and independent claim against the so-called issuing bank for payment in return for the documents on the goods. The latter are checked for correctness by the bank within the scope of the agreement with the buyer before instructing a nominated bank in another country or the seller's bank, mainly with respect to the type and quantity of the goods, packaging, shipping deadlines and quality certifications. If and when all of the documents pertaining to the goods precisely meet the conditions of the letter of credit, and only then, the payment is made. This arrangement grants the seller a separate claim to payment from the bank that is independent of the buyer's interests. The buyer, for his part, receives all of the documents from the exporter that are required to demand concurrent release of the goods by the carrier in accordance with Section 521, Subsection 1 of the German Civil Code as their legitimized owner while returning the bill of lading in accordance with Section 521, Subsection 2 of the German Civil Code. In practice, it can take longer to check and send the documents than it does to ship the goods (this aspect has already been covered in detail in 6.1.2).³⁹⁸ DLT-based trading documents hold promise for solving this problem by automating data management and evaluation.

6.2.1.3 DLT-based trading documents

According to Section 443 Subsection 2, Section 475c Subsection 4, and Section 516 Subsection 2 of the German Commercial Code, DLT-based trading documents are only equivalent to the paper-based originals if they digitally duplicate all functions of the paper-based trading documents, thus ensuring that the analog and digital versions are equivalent. Besides issuing trading documents, it is therefore particularly important to duplicate the documentation, blocking, trading and legitimization functions of the paper-based versions.³⁹⁹ The following discussion looks at bills of lading by way of example, but the same requirements also apply to consignment bills and warehouse warrants.

6.2.1.3.1 Issuance

In the analog world, trading documents require an issuance agreement⁴⁰⁰ for transferring a documented right to receive payment to the owner of a document, which must also be turned over to him. These documents must contain the information stipulated in Section 443 Subsection 1 in conjunction with Section 408 Subsections 1 to 3 and Section 515 of the German Civil Code. The same statement also applies to the corresponding digital equivalents in accordance with Section 443 Subsection 3, Section

³⁹⁶ Baumbach/Hopt, ERA vor Art. 1 Rn. 4.

³⁹⁷ Baumbach/Hopt, BankGesch K/1.

³⁹⁸ Saive, TranspR, 2018, pp. 234-238 (236).

³⁹⁹ BT-Drs. 17/10309, p. 93.

⁴⁰⁰ Contract between the carrier and unloader to the benefit of the legitimized bearer of the bill of lading (Art. 328 of the German Commercial Code), von Bernstorff, RIW, 2001, pp. 504-512 (508).

475c Subsection 4 and Section 516 Subsection 2 of the German Civil Code. In the context of DLT, asset-backed tokens are suitable instruments for accomplishing this.⁴⁰¹

In the context of DLT, a token is equivalent to "an exclusive, unique and nonreproducible entry in a database."⁴⁰² A token as such is ultimately merely a smart contract that, in addition to other attributes, has an "owner" field that can only be changed using the private key of the individual who currently has rights to it. In the context of merchandise logistics, a token reflects ownership of a particular real asset or, in the case of trading documents, a claim to a certain real asset, which is why it is referred to as an asset-backed token.⁴⁰³

In order to create an asset-backed token, a warehouse manager, carrier or forwarder must digitally merge the required information in a token via an interface to a DLT platform (API). This is added to a DLT platform as a smart contract after it has been validated and stored by all of its nodes.⁴⁰⁴ After a token has been added to a DLT platform, the information it contains is irreversibly linked to it. Because there can only be a relatively small number of nodes, such as cargo handlers and government agencies, a private permissioned blockchain (DLT platform)—as explained in section **Fehler! Verweisquelle konnte nicht gefunden werden.**—is an appropriate network structure.⁴⁰⁵

6.2.1.3.2 Evidentiary function

The evidentiary function of a bill of lading involves showing that the carrier has taken over the goods in the state described pursuant to Section 515 Subsection 1 nos. 7 and 8 as well as Section 517 Subsection 1 no. 1 of the German Commercial Code. This function can be adequately performed by digitally, i.e. via software, merging all required information in an asset-backed token.

6.2.1.3.3 Legitimation function

In the analog world, a bill of lading entitles the document's owner to exercise the contractual maritime freight rights that it confers.⁴⁰⁶ Pursuant to Section 519 Sentence 2 of the German Commercial Code, his entitlement is assumed if he or she is in possession of the formally legitimizing document. The nature of this legitimization depends on the type of bill of lading involved. A distinction is made among bearer, order (or negotiable), and straight bills of lading.⁴⁰⁷ As indicated in its name, in the first of these, according to Section 519, Sentence 3 No. 1 of the German Commercial Code any bearer of the document, even without being mentioned (by name) in the document, is legitimized; this type has no practical relevance owing to the impossibility of tracing the bearer's history.⁴⁰⁸ In the second type, as defined in Section 519, Sentence 3 No. 2, the bearer is legitimized by being named as the recipient (in some cases the words "to forwarder's order" or similar may be enough) or if he or she is identified by an unbro-

⁴⁰¹ Saive, TranspR, 2018, pp. 234-238 (237).

⁴⁰² Kaulartz/Matzke, NJW, 2018, pp. 3278-3283.

⁴⁰³ Kaulartz/Matzke, NJW, 2018, pp. 3278-3283 (3280).

⁴⁰⁴ Saive, TranspR, 2018, pp. 234-238 (237).

⁴⁰⁵ Saive, RdTW, 2018, pp. 85-89 (88).

⁴⁰⁶ MüKoHGB/Herber, § 519 Rn. 3.

⁴⁰⁷ Rabe/Bahnsen, § 519 Vor 481 Rn. 119.

⁴⁰⁸ MüKoHGB/Herber, § 519 Rn. 5.

ken chain of endorsements.⁴⁰⁹ In the third case, pursuant to Section 519, Sentence 3 No. 3, the bearer is only legitimized if his or her name appears in the document as the authorized recipient. When using a DLT application, the bearer is legitimized to the carrier via a user interface that clearly and unmisunderstandably indicates who the asset-backed token is assigned to (depending on the DLT application's design, possibly only to authorized users). It also frees the carrier from having to check it for visible signs of manipulation like in the case of paper-based bills of lading.⁴¹⁰

6.2.1.3.4 Blocking function

The principle follows from Section 519, Sentence 1 of the German Commercial Code that, alongside the rights bestowed by a bill of lading, claims based on the freight contract (contract of carriage) may not be additionally exercised if they are already conferred by the bill of lading.⁴¹¹ The bill of lading thus blocks claims derived from the freight contract, since the bill of lading takes precedence over it. This is because the freight contract may not necessarily reflect a legal relationship identical to that of the bill of lading.⁴¹² A bill of lading primarily documents claims against the carrier for carriage to the destination and delivery there to the party authorized by the bill of lading, as per Section 514, Subsection 1 (2) and Section 521, Subsection 1 (1) of the German Commercial Code.⁴¹³ Secondarily, it also entitles the bearer to damages in the event of loss of or damage to the goods.⁴¹⁴ The blocking of the freight contract by the bill of lading ends, for example, if the bearer refuses to accept the goods.⁴¹⁵ In that case, the carrier can once again exercise the rights conferred by the freight contract.⁴¹⁶ Because all of the nodes of a DLT application can verify the existence of the bill of lading, they are also aware of its blocking effect. If, taking the aforementioned example further, the bearer should refuse to take possession of the goods, the carrier would have to place this information on the DLT platform in order to reverse the blocking effect; this function can therefore also be modeled there.

6.2.1.3.5 Trading function

In the event that ownership⁴¹⁷ to cargo changes en route as a result of its being resold, this is equivalent to transferring a token to a new importer/buyer via a transaction on the DLT platform once it has been validated by all authorized nodes and stored in the distributed computer network.⁴¹⁸ The new ownership situation is then evident as already described.

⁴⁰⁹ Rabe/Bahnsen, § 519 Vor 481 Rn. 119.

⁴¹⁰ MüKoHGB/Herber, § 519 Rn. 9.

⁴¹¹ Ramming, RdTW, 2018, pp. 45-58 (50).

⁴¹² MüKoHGB/Herber, § 519 Rn. 11.

⁴¹³ Rabe/Bahnsen, § 519 Rn. 7.

⁴¹⁴ Rabe/Bahnsen, § 519 Rn. 7.

⁴¹⁵ MüKoHGB/Herber, § 519 Rn. 17.

⁴¹⁶ MüKoHGB/Herber, § 519 Rn. 17.

⁴¹⁷ On the controversial treatment of this under property law, cf. Baumbach/Hopt/Merk, § 448 Rn 2.

⁴¹⁸ Saive, TranspR, 2018, pp. 234-238. (237).

6.2.1.3.6 Signature

The wording of the saving clauses on electronic bills of lading in Section 443 Subsection 3, Section 475c Subsection 4 and Section 516 Subsection 2 (3) of the German Commercial Code is nearly identical, containing the phrase "authenticity and integrity of the record." The term "record" ("Aufzeichnung" in German) was translated from the Rotterdam Rules for Section 516 Subsection 2 and then reused in all of the other saving clauses for the sake of consistency.⁴¹⁹ The intention is to make it clear that a private record in the sense of Section 416 of the German Code of Civil Procedure (ZPO) is not involved.⁴²⁰ The requirement to lastingly ensure the authenticity and integrity of the record explicitly avoids stipulating that the electronic record must include a qualified electronic signature as per Section 126a of the German Civil Code. This takes account of the fact that the procedure for providing a qualified electronic signature according to the rules of the German Signature Act (now defunct) is quite laborious and costly, and in any case the present wording allows greater flexibility.⁴²¹

6.2.1.3.7 Unwinding of transactions

It is fundamentally possible to unwind DLT-based transactions. On this, please refer in particular to the general discussion of smart contracts (5.1.1). Where bills of lading are concerned, this would take place in such a way as to ensure that afterward, once again only the original owner would be able to access the asset-backed token using his or her private key. The continued existence of its transaction history on the DLT platform, as explained in the general section on smart contracts,⁴²² is harmless.⁴²³ The only plausible reason to require the deletion of a transaction history in connection with trading documents is in connection with critical goods etc., provided that the parties involved reach a consensus on this. This does not, however, detract from the fundamental equivalence of DLT- and paper-based trading documents.

6.2.1.3.8 Numerus clausus

In Germany the number of different types of securities is limited by a numerus clausus system, which initially hindered the insertion of the above-mentioned saving clauses on electronic trading documents. The legislature wanted to eliminate this "obstacle" with the latter.⁴²⁴ The empowerment clause of Section 516, Subsection 3 of the German Commercial Code (which reoccurs with identical wording in Section 443 Subsection 3 and Section 475c Subsection 4) also does not imply a restrictive assessment. The German federal government commented on the bill that "the extent to which use is made of this empowerment [...] [ought to] depend on whether suitable forms and procedures emerge in practice."⁴²⁵ The empowerment clause is only intended to ensure in practice the standardization of the details of issuing, presenting, returning and trans-

⁴¹⁹ BT-Drs. 17/10309 p. 93.

⁴²⁰ BT-Drs. 17/10309 p. 52.

⁴²¹ BT-Drs. 17/10309 p. 93.

⁴²² Siehe 5.1.1.

⁴²³ On data protection issues in this context, cf. 6.2.1.4.

⁴²⁴ BT-Drs. 17/10309 pp. 93.

⁴²⁵ BT-Drs. 17/10309 pp. 93; a.A. Rabe/Bahnsen/Rabe, § 516 Rn. 5.

mitting an electronic bill of lading, as well as the particulars of the process of posting retroactive entries to one.⁴²⁶

6.2.1.3.8.1 Presenting

The aspect of "presenting", which Section 516, Subsection 3 of the German Commercial Code empowers the Federal Ministry of Justice and Consumer Protection to regulate, does not necessarily imply a document, despite the wording. At first glance this also appears illogical in the context of electronic bills of lading, which are supposed to overcome the need for paper documents. What causes one to sit up and take notice in this context, however, is the law on stocks as a special category of securities. Although Section 10, Subsection 5 of the German Stock Corporation Act (Aktiengesetz) allows for limiting or excluding stockholders' right to demand individual share certificates, joint stock companies remain obliged to issue and store a global share certificate (Section 9a, Subsection 1 (1) of the German Safe Custody Act (Depotgesetz)).⁴²⁷ Despite this, the broad definition of securities given in Section 2, Subsection 1 of the German Securities Trading Act (Wertpapierhandelsgesetz) also encompasses securities as such if no corresponding certificate has been issued. As long as a security, and thus ultimately also a trading document, possesses the required characteristics, it is also valid in digital form, e.g. as a token.⁴²⁸

6.2.1.3.8.2 Subsequent additions

In the bill for the present Section 516 of the German Commercial Code, with regard to the foreseen empowerment to regulate the details of entries in electronic bills of lading, the German federal government explicitly cited cases in which a carrier might want to enter a reservation in an electronic bill of lading as described in Section 517, Subsection 2.⁴²⁹ Where DLT is concerned, the requirements for such reservations can be met with by a smart contract if the carrier permits the later addition of more information. In the case of a DLT platform, to an objective observer the entire trading document then appears to be a combination of original entries and subsequent additions. Consequently, there is no need to intervene in the DLT platform as such.

6.2.1.4 Use of DLT for data protection in the context of digital trading documents

If a token is to be used as equivalent to a trading document and transferred between the contractual parties to a trading transaction, protection of the data of affected natural persons must be ensured.

Like with any other application, the affected persons can be users of the system or third parties. Exporters, importers, carriers and forwarders enter into consideration as direct users of the system. These interact with the smart contract via DLT within the scope of the processes for transferring the token. Their interactions are documented in the DLT. Processing of these data is relevant under data protection law whenever an

⁴²⁶ BT-Drs. 17/10309 pp. 93.

⁴²⁷ Henssler/Strohn/Lange, AktG § 10 Rn. 15.

⁴²⁸ Parhofer/Klöhn et al., ZBB, 2018, pp. 89-106 (102).

⁴²⁹ BT-Drs. 17/10309 pp. 93.

involved exporter, importer, forwarder or carrier is a natural person.⁴³⁰ In the case of companies, if it is impossible to draw any conclusions about the natural persons behind them from the use of usernames alone, then transactions executed by the system's users are not relevant under data protection law.⁴³¹ Here too, however, it may be possible to identify persons from information contained in trading documents. Under certain circumstances this can include data on third parties who wish to be informed of the status of the shipping operation.⁴³² Nor can the possibility be ruled out a priori that conclusions might be drawn about third persons associated with a transaction from a description of goods in a paper-based document.

Consequently, modelling trading documents on a DLT platform requires appropriate adjustments to the architecture. It is necessary to make a distinction based on whether or not knowledge of the platform's users (exporters, importers, carriers, forwarders) can be used to deduce information on persons behind the company or companies.

6.2.1.4.1 No information on natural persons behind a company

It may be impossible to identify natural persons behind the participating companies. In this case, processing of information on the participating companies is not relevant under data protection law. However, in this case it must also be ensured that the digital equivalent of a trading document contains no personal information on third parties. Processing of these data via DLT can be prevented by storing them off-chain. The information in the trading document is not stored as plain text, instead remaining locally in a signed and encrypted form with the issuer, who may grant other participants in the transaction access to the document. The ability to view the document depends on receiving the key for unlocking the encrypted information. A token on a DLT platform only contains a hash value of this information.⁴³³ This ensures that the information cannot be retroactively altered. A hash value per se does not constitute personal information, since the hash function is such that it is impossible to reverse engineer a hash value to draw conclusions about the inputs. There is therefore no way to identify natural persons from on-chain data.⁴³⁴

Even when the possibility of obtaining information on natural persons associated with the participating companies can be ruled out, it is still necessary to ensure, by technical means, that the content of the trading document is stored off-chain and only linked to the DLT layer by hash values. This can ensure data-protection-compliant implementation. Nevertheless, it is important to keep in mind that the impossibility of learning about natural persons behind a company cannot be taken for granted. If a platform is by definition supposed to be open, also to importers, exporters, carriers and forwarders acting as small companies with a considerable associated risk of revealing information on natural persons,⁴³⁵ this approach cannot be sufficient. In such a case, the use of a username in connection with transferring the trading document via the DLT layer

⁴³⁰ See section 5.2.2.2.1.1.

⁴³¹ See section 5.2.2.2.1.1.1.

⁴³² See the description of the usual content of conventional trading documents.

⁴³³ See the explanation of hash values in 0.

⁴³⁴ See 5.2.3.4.2.2.1.2.

⁴³⁵ See also 5.2.2.2.1.1.1.

can by itself already constitute a relevant act under data protection law. Other solutions must then be found.

6.2.1.4.2 Information possible on natural persons behind the companies

If an exporter, importer, carrier or forwarder is a natural person or company behind which natural persons can be identified, the challenges already discussed in the general part arise when interacting with such a participant via DLT. In this case as well, data must be stored off-chain and linked by hash values. However, it is also necessary to take steps to eliminate any chance of identifying the persons behind usernames.

An “open solution”⁴³⁶ would require all system participants to have a legitimate interest in all information. But only the persons involved in a given shipping transaction have a legitimate interest in transmitting an individual trading document. Permitting all system participants to view all activities is therefore not compatible with data protection law. Consequently, an “open solution” cannot work here.

However, a “central solution”⁴³⁷ basically appears to be possible. This calls for a permissioned blockchain to be operated by a central entity, which can use a system of rights and roles to control which information is visible to which participants. The central entity is then the controller, in the sense of data protection law, responsible for on-chain data processing. An agreement concluded between the participants and the central authority enters into consideration as the legal basis for this processing.⁴³⁸ The central entity must have suitable erasure methods at its disposal. The possibilities include a “redactable blockchain”⁴³⁹ in which changes can be retroactively made by the central entity, and forks⁴⁴⁰ in which the nodes are required to erase unwanted data from the decentralized database.

If a “centralized solution” is impossible or unwished, an “anonymization solution”⁴⁴¹ can also be chosen. In this case it will not be possible to balance transactions,⁴⁴² since every transfer of the trading document must be traceable. Only technical anonymization solutions such as zero-knowledge proofs⁴⁴³ or stealth addresses in combination with ring signatures⁴⁴⁴ therefore enter into consideration. With anonymization, no data processing relevant to data protection law takes place on-chain. Consequently, no legal basis is required for it either, and there is no need to erase data.

6.2.2 Conclusions and recommendations for action

The saving clauses on electronic trading documents in the German Commercial Code requiring them to be equivalent to paper-based documents are already enabling the

⁴³⁶ On “open solutions”, see also 5.2.3.4.2.1.

⁴³⁷ On “centralized solutions”, see also 5.2.3.4.2.1.

⁴³⁸ On the legal basis for choosing a centralized solution, see 5.2.4.2.2.

⁴³⁹ On redactable blockchains, see 0.

⁴⁴⁰ On forks, see 5.2.5.2.2 and 0.

⁴⁴¹ On “anonymization solutions”, see 5.2.3.4.2.2.

⁴⁴² On balancing in general, see 5.2.3.4.2.2.2.

⁴⁴³ On zero-knowledge proofs, see 5.2.3.4.2.2.2.3 and 0

⁴⁴⁴ On the use of stealth addresses in combination with ring signatures, see 5.2.3.4.2.2.4.

use of DLT-based documents today. This legislative technique therefore provides flexibility and the legislature may also want to take advantage of it in other areas as well.

Data protection law requires a distinction to be made depending on the nature of the potential participants (exporters, importers, forwarders and carriers). In case they are exclusively companies and it is not possible to draw any conclusions on the natural persons behind them, it is sufficient to dispense with storing personal data in the DLT layer. The information must be stored off-chain instead and linked to the DLT platform by hash values. However, such a solution requires that the participants be checked beforehand to make sure that they meet the above-mentioned requirements. Smaller companies would probably not qualify.

If DLT-based trading documents can at least be transferred by and to exporters, importers, carriers and forwarders who are natural persons, or if knowledge of an involved company also reveals information on natural persons behind it, then an open DLT platform does not enter into consideration for data protection reasons, at least not without modifying its architecture. The required modifications could be made by creating a responsible central entity ("centralized solution") or by completely anonymizing usernames ("anonymization solution").



Digital Saving Clauses and Data Protection

The digital saving clauses in the German Commercial Code (Sections 476 ff.) already permit the use of DLT-based trading documents in maritime shipping provided that the paper-based original and the DLT-based version are equivalent. Owing to the flexibility of this rule, it may be possible for it to be incorporated into other laws. In the context of digital shipping documents, the requirements of data protection law depend on the potential participants in each case.

7 Electric Vehicle Charging

7.1 Economic and Technical Aspects: Technical Part

7.1.1 Definition and description of the application

Vehicle electrification, widely referred to in Germany as electromobility, electric mobility and electrified mobility, has experienced rapid technical advances in recent years. However, the numbers of both electric vehicles in use and new registrations have fallen short of expectations. As of January 1, 2018, Germany only had about 291,000 electric vehicles (including hybrids).⁴⁴⁵ It therefore now faces the challenge of accelerating the shift to sustainable forms of transportation by encouraging greater use of electric vehicles. It appears possible to meet expectations regarding the further spread of electromobility in the medium term. One essential prerequisite for this is the establishment of a publicly accessible charging infrastructure. This infrastructure must be designed to meet the requirements for all charging situations throughout the country and enable easy use and payment.⁴⁴⁶ The charging situations vary greatly and are very context-specific, but can be broken down into three broad categories:

- a) Charging at home
- b) Charging at the destination
- c) (Fast) charging on the road

Whereas (a) is typically possible in a familiar environment without the need for a charging system or user interface, namely by plugging into a household power outlet or wall-mount charger⁴⁴⁷, the processes for (b) and (c) can be very different. At the same time, there are barriers to greater adoption of all-electric cars, the chief ones being charging situations (b) and (c) and so-called "range anxiety", namely the fear that a vehicle will not have a sufficient charge to reach its destination and strand its occupants.⁴⁴⁸ The expansion of infrastructure for these two charging situations and the market penetration of electric cars are coupled. The still-low registration figures for e-vehicles in Germany pose considerable economic risks for (would-be) charging infrastructure operators. Due to the relatively small number of electric cars in use, many existing charge points are used too infrequently to be profitable. This applies especially to capital-intensive rapid charging infrastructure. Conversely, it is mainly the lack of (rapid) charging opportunities that is inhibiting sales of e-vehicles. This is driving a negative feedback loop.⁴⁴⁹

⁴⁴⁵ Kraftfahrt-Bundesamt, press release no. 06/2018 - Der Fahrzeugbestand am 1. Januar 2018.

⁴⁴⁶ Sächsische Energieagentur – SAENA GmbH, Kompetenzatlas Elektromobilität Sachsen.

⁴⁴⁷ Home wall-mount charger

⁴⁴⁸ Sun/Yamamoto et al., Transportation Research Part D: Transport and Environment, 2016, pp. 26-39.

⁴⁴⁹ Sun/Yamamoto et al., Transportation Research Part D: Transport and Environment, 2016, pp. 26-39.



Range Anxiety

Range anxiety is the fear that a vehicle will not have enough range to reach its destination, thus stranding its occupants without a straightforward way out of their predicament.

„[...] Range anxiety is a stressful experience of a present or anticipated range situation, whereby the range resources and personal resources available to effectively manage the situation (e.g., increase available range) are perceived to be insufficient.“ Rauh/Franke/Krems, Human factors, 2015, 177

Comparisons

To provide a basic supply and break this vicious circle, public charge points should be available to all e-vehicle drivers. Germany already has numerous charge points, many of which also support rapid charging.⁴⁵⁰ In the past, and to a limited extent today as well (in the case of older charge points), there have been challenges with regard to the accessibility of charging infrastructure. To improve this situation, the legislature has already passed ordinances to ensure discrimination-free access to public charge points. “Discrimination-free” means that every charge point can potentially be used by any e-vehicle and driver. The number and rapid charging capabilities of publicly accessible charge points are not adequate throughout the country for ensuring high market penetration of electric vehicles. They should therefore not be additionally partitioned and fragmented. The causes of partitioning basically involve three levels:

- The physical level (e.g. plug compatibility)
- The information level (e.g. protocols and information and communications technology (ICT))
- The economic/business level (payments and payment systems)

The information level in turn has several layers that need to be considered. For example, communication between the charge point and vehicle and between the charge point and backend systems of the charge point operator (CPO), and between CPOs and other market players involves different protocols and systems in each case. The first-mentioned are sometimes also called low-level protocols and the last as higher-level protocols or systems. A comprehensive overview of all common charging protocols and players is provided in the source listed below.⁴⁵¹

The core challenges posed by partitioning have increasingly shifted from the physical level to the information level (especially higher-level protocols) and the economic level. This will be illuminated further below. In the following, the relevance of partitioning and the consequences of the available charging infrastructure are discussed. Figure 26 illustrates the accessibility of charging infrastructure in Germany based on data from Open Charge Map, a global registry of electric vehicle charging locations.⁴⁵²

⁴⁵⁰ I.e. they provide more than 22 kW.

⁴⁵¹ V2G Clarity, IEC 63110 – Standardizing the Management of Electric Vehicle (Dis-)Charging Infrastructures.

⁴⁵² Openchargemap.io/site

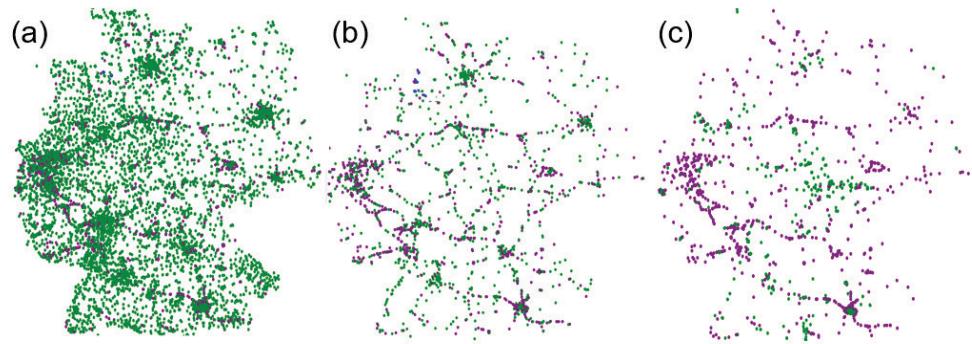


Figure 6: Charging locations in Germany: (a) all publicly accessible charge points, (b) all publicly accessible charge points with rapid charging capabilities, (c) all publicly accessible charge points from the user perspective

It is clear from this that Germany has already established a relatively dense network of charge points and made them publicly accessible (a). It is also apparent that only a small fraction of them has rapid charging capabilities, mainly along motorways (b). Considering the network of one leading provider that is active Germany-wide but does not operate any physical charging infrastructure itself, instead exclusively ensuring accessibility and uniform rates⁴⁵³ to drivers and owners of electric vehicles, the resulting picture shows very clearly that some drivers are likely to experience a (high) degree of partitioning. The players in the charging ecosystem are presented in detail below, since they have great relevance to the application under discussion. It is also apparent that, as of December 2018, only a minority of all physically available charge points provide a consistent charging experience that, ideally, is characterized by ease and convenience.⁴⁵⁴ Looking at other providers, similar results are obtained. While it is true that electromobility, which also includes electric commercial vehicles such as buses and trucks, is developing very dynamically, it is also extremely important to ensure a cross-provider charging infrastructure of sufficient scope and density to meet requirements.⁴⁵⁵ Especially in economic terms, possibilities for facilitating access to public charging infrastructure and counteracting partitioning also need to be investigated.

In the following, attention therefore concentrates on ways of reducing partitioning at the informational level and especially at the economic level, which comprises the subprocesses of authentication, authorization, billing and value transfer. In this context, it is particularly important to obtain an overview of the current situation at the economic level, which in everyday language is often simplified as "ways to pay". From the perspective of a driver, there are three different ways to pay for charging:

⁴⁵³ A widespread model is for providers to simply offer accessibility and send customers a monthly invoice, but pass on the price at the charger while adding a fee for access. Although this model corresponds to the one in place for vehicles with internal combustion engines, the pricing models applied to electric charging are far more heterogeneous and the prices themselves also exhibit much greater differences. They include prices per charging event, per minute, and per unit of electric power.

⁴⁵⁴ In this case study, charging is addressed from the perspective of electric vehicle operators. It is also possible to talk about the customer experience from the standpoint of charging infrastructure operators. This is an important concept in modern business administration; it defines the customer relationship and therefore contributes to the success of a business venture.

⁴⁵⁵ Anderson, LADEN2020 Schlussbericht.

- (1) *Charging infrastructure operator-specific payment:* Drivers of electric vehicles can use an app of the charge point operator on their smartphones to initiate the charging process. The app also contains details on how to make payment, such as by direct debit or using an NFC (near field communication)-enabled credit card.
- (2) *Web-based direct payment:* The second German Charge Point Ordinance requires all new charging stations to enable ad hoc payments with a so-called Web-based direct payment procedure. This process must not discriminate against anyone or require a contract to be concluded with the operator beforehand. Credit cards are an accepted Web-based payment method.
- (3) *Payment via a third-party service provider:* Users of e-vehicles can also be enabled to access charging infrastructure without directly concluding a contract with the operator. Similarly to (1), these approaches involve the use of a charging card or smartphone with a charging app. The difference is that a third party, with whom the driver has concluded a contract, provides the app or charging card. In this scenario, the driver receives an invoice from the third-party service provider, to which the charging station operator sends an invoice for the consumed electricity.

In the application investigated here, payment via a third party has special interest as the focus of a possible DLT-based solution. The goal of this payment option is to offer drivers of electric vehicles a familiar, convenient charging experience across all charging situations and thus contribute to increasing the acceptance of electromobility.⁴⁵⁶

 Peer-to-peer charging at a neighbor's wall outlet

There is a new trend for home owners to allow others to charge their electric vehicles using a house socket or accessible wall outlet in return for payment. The idea is to derive greater benefits from one's own charging infrastructure and use the extra income to finance the original investment. In rural areas, this could also improve the availability of charging infrastructure. Although this case study does not examine this particular practice, there is an urgent need to look for ways to extend blockchain-based implementation to include it. At this time, wall outlets of this kind are still rare. But it would be worthwhile to investigate this possibility in greater depth, since the owners of such outlets can usually be identified, thus raising issues under data protection law.

The eRoaming model is a payment option belonging to the third category. Its goals are to unify all of the individual steps involved in charging and create a consistently customer-focused charging experience. The concept of roaming was invented by the mobile phone industry. Now, for example, when traveling to another EU country a user's smartphone almost always automatically connects to another network operator with which the home operator has concluded a roaming deal. Another example is ATMs, despite the fact that the term "roaming" is rarely used in this context. Multiple banks form a network with a shared IT system to offer —possibly for a fee—"roaming",

⁴⁵⁶ Grathwohl, Kartellrechtliche Bewertung von Standardisierungsstrategien, 2015, pp. 221-271.

in other words the ability to withdraw cash or execute other transactions using the machines of other banks. The same idea occurs in similar form in connection with electromobility, i.e. with different charging networks collaborating with one another. While the roaming fees for mobile phones are capped by European law within the EU, sharing of ATMs is usually regulated at the national level. Analogously, eRoaming strives to achieve a consistent, good-quality customer experience with maximum coverage. The quality of the customer experience is determined by many factors. From the perspective of electric vehicle drivers, the two most important are:

- Transparent, fair and, as far as possible, consistent rates and prices
- Standardized, straightforward authentication and authorization in every charging situation



Authentication and Authorization

When a computer program can grant access to a secured domain, a user can demonstrate his or her right to enter it by first entering a username. He or she then authenticates himself or herself by entering a password. The program then uses this information to identify the user and execute an authentication process to verify whether the user is in fact authorized. Only after the successful conclusion of this verification is the user allowed to access the domain in question, usually for the duration of a single session.

In order to keep this promise, new market players and roles have become established within the scope of eRoaming. These are sketched in the following. It should be kept in mind that a single company, and in general terms any legal person, can definitely perform several of the following sequentially listed roles.

A charge point operator (CPO) runs a pool of charge points at one or more locations, each of which can have one or more chargers and plugs. CPOs can, but in practice often do not, have an interface to customers. It is more common for their facilities to enable authentication with a dedicated card or app provided by the CPO. The pools are therefore commonly referred to as charging networks. The charging infrastructure itself is designed to meet the requirements of the charging situations sketched above. Stations for charging vehicles while they are traveling (case (c)) are often built and run by CPOs when this is their core business. In this case, the operator and owner of the infrastructure are identical. In the case of "charging at the destination", by contrast, ownership and operation are sometimes separate. Once again, various relevant scenarios can be distinguished. Three models are basically possible, geared to different kinds of operators and their interests:

1. *Proprietary operation:* In this case, the owner is also the operator (CPO). It runs the entire charging infrastructure on its own. The interfaces to IT systems must be individually implemented and maintained. This mode of operation is typical of players with a large number of charge points, such as corporations or municipal utilities.
2. *Contract operation:* In this case, the owner is not the charge point operator (CPO). Instead, another party such as a local municipal utility is contracted to do this. They are then integrated in a (CPO) charging network. Although this greatly reduces the

owner's workload, control over the details of the operation, such as rates, largely also passes to the contractor. Occasionally would-be owners of charging infrastructure purchase charging stations from large CPOs, which in turn buy the charging systems as "white label" solutions from "charge point manufacturers" (CPMs). In these cases it is not uncommon to supply electricity to e-vehicle drivers at cost price or even free as an incentive for taking advantage of another service such as a hotel. When power for charging is provided free, eRoaming is irrelevant.

3. *Partial third-party operation:* Some CPMs or CPOs that operate white label solutions also provide intermediate solutions. For example, the rates or access possibilities themselves can be fixed in considerable detail⁴⁵⁷ while interfaces and other services are provided by the CPM within the scope of charging management and billing protocols. In these cases, the owner is often responsible for providing first-level support.⁴⁵⁸ Because CPMs are not normally also CPOs, they typically do not enter into any eRoaming arrangements; in fact, like in the case of self-run operations, integration in eRoaming networks is a rarity. If a charge point can be integrated in a CPO charging network, authentication and authorization can be performed via it. Beyond that, the accessibility of the CPO charging network can be improved by taking advantage of any existing eRoaming arrangements.

[[Example: There is a rapid charge point on the parking lot of the SuperPrice supermarket in Anyville. Customers can use a card from the Anyville municipal utility to authenticate themselves and pay at a reduced rate of 10 cents a minute that has been set by SuperPrice. In addition, because the Anyville municipal utility has joined an eRoaming network, drivers from nearby Anytown who have obtained a flat rate from their provider can also charge their cars free of charge in Anyville.]]

The typical charge point owners that apply the three scenarios described above include hotels, parking facilities, companies and landlords. These players have an interest in providing charging services so that their guests, customers, employees or tenants can meet the requirements for starting or continuing their journeys from these typical destinations.

E-mobility service provider (eMSP): An especially important role is played by eMSPs, who have an interest in providing the previously described services to their customers. An eMSP is essentially the operator of a platform on which charge points and drivers of electric vehicles come together. The platform is accessed via human-machine interfaces (HMIs) that are installed at the charger or integrated in in-car entertainment systems or mobile phone and occasionally Web-based apps. The consumers, i.e. platform users, utilize the latter to select suitable charging locations when planning their routes. These intermeshed roles and players are depicted in Figure 27.

Not uncommonly, the underlying value proposition, in the guise of a platform economy, is supplemented by premium service components such as green electricity certificates, carbon offset or local power certificates, reservation of chargers (if permitted by other involved market players) or rentals of cars with internal combustion engines for driving longer distances. In this example application, we first focus on the aspect of the

⁴⁵⁷ E.g. exclusively private access, public access, public access on request etc.

⁴⁵⁸ First-level support refers to the first point of contact for all support requests.

accessibility and convenience of public charge points. Both enhance customers' charging experience and offset range anxiety, which is one of the greatest obstacles to e-mobility.⁴⁵⁹ Not uncommonly, eMSPs are simultaneous CPOs. But there are also numerous "dedicated" eMSPs, some of which only serve certain customer groups such as drivers of company cars. It is important for eMSPs to provide good coverage, i.e. a sufficient number of well-distributed charge points, via the platform interfaces. In keeping with the classic theory on platform economies, they are subject to positive networking effects and the concept of critical mass.

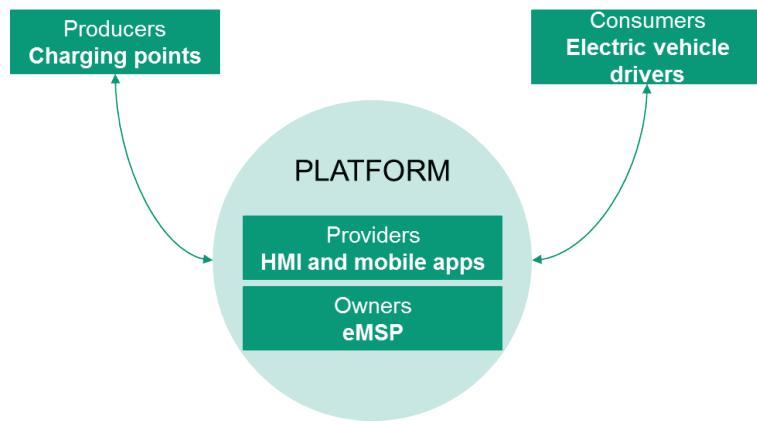


Figure 27: Representation of the roles and players involved in electric vehicle charging as a platform economy (based on van Alstyne et al. (2016))

Clearing and Roaming (C&R): While large CPO charging networks theoretically operate eMSP platforms and can therefore achieve the required critical mass, this is not technically feasible for dedicated eMSPs without networking and payment settlement. The same statement also applies to small and medium-sized CPO charging networks. In order for both producers and consumers to derive greater benefits from their platforms, the already discussed eRoaming model was studied, developed and introduced. Here we will use the term "clearing & roaming" (C&R) to designate the activity of implementing eRoaming networks. The name combines two essential services that C&Rs must be able to offer participants. "Clearing" refers to (partially) automated payment settlement, which takes place between eMSPs and CPOs across platforms. This depends on their being essentially roaming-enabled. Although automated payment settlement is not absolutely essential for roaming networks, a service that lacks it would have to rely on manual settlement of payments with the associated additional overhead. It should be noted that such a player could potentially collect data from all of the charging transactions conducted. Possession of this information can improve such a player's understanding of the market compared to individual eMSPs and CPOs. In this role, C&Rs provide a platform via which eMSPs can network with one another. Since eMSPs are themselves platforms, C&Rs in effect offer a platform for platforms. This is also referred to as a superplatform.⁴⁶⁰ Figure 28 visualizes the interconnected relationships. As a consequence, depending on the form that a given C&R role takes, market power can accumulate in the hands of these players, making it conceivable that others

⁴⁵⁹ Melliger/Vliet et al., *Transportation Research Part D: Transport and Environment*, 2018a, pp. 101-115.

⁴⁶⁰ Lang/Szczepanski et al., *The Emerging Art of Ecosystem Management*.

will become mistrustful of this form of intermediation. This is remarkable in the sense that the subprocesses described above presuppose trust in correct mediation and settlement by the C&Rs.

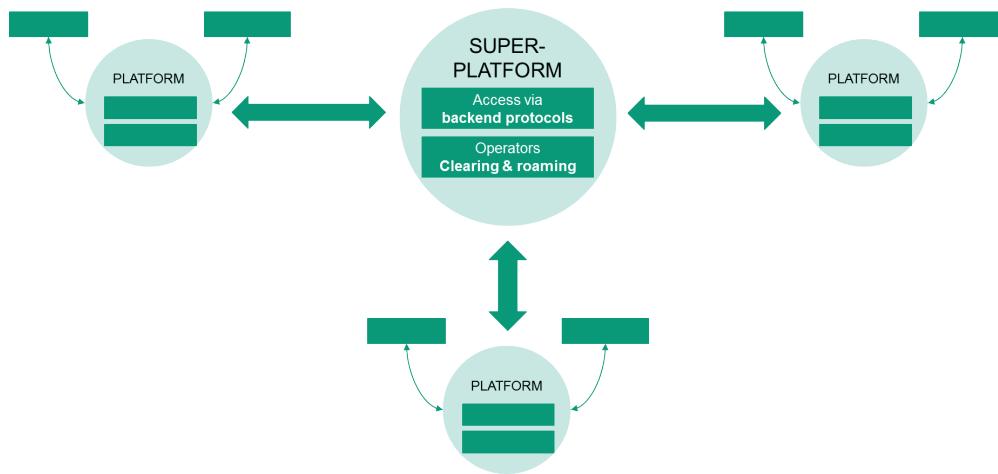


Figure 7: Superplatform acc. to Lang/Szczepanski et al., 2019.: a platform of eMSP platforms—a schematic depiction of a pure hub-and-spoke model for cooperation in eRoaming

In practice, several such intermediaries have developed, many of which in turn have CPOs among their shareholders. According to one study,⁴⁶¹ three idealized cooperation models can be distinguished in the context of eRoaming: (1) meshed networks, (2) hub-and-spoke networks, and (3) spoke-model interroaming networks.

A meshed network (1) is implemented in eRoaming by bilateral connections, which requires interfaces to proprietary systems and is therefore a slow and laborious process. In a hub-and-spoke network (2), analogously to a superplatform there is a central C&R provider with which all CPOs and eMSPs establish interfaces. In a spoke-model interroaming network (3) multiple C&R providers are interconnected by direct interfaces between all of them. It can be observed that in practice not all C&Rs collaborate bilaterally and that transitive relationships are not possible. Such transitive relationships would, for example, allow customers of an iMSP that has an interface with a C&R provider, which in turn has an interface with another C&R provider that has an interface with a third C&R provider to which a CPO C is connected, to charge at C. Figure 29 shows in idealized form the three prototypical cooperative models for charging of electric vehicles. In Germany, model (3) dominates. However, model (1) would be more desirable because it would encourage competition better, while model (2) is the least attractive since it would result in a single player dominating the market. In this sense, model (3) is an intermediate solution between these two extremes. It is unclear whether the previously mentioned network effects would lead to further market concentration.

⁴⁶¹ Begleit- und Wirkungsforschung Schaufenster Elektromobilität (BuW), Good E-Roaming Practice: Praktischer Leitfaden zur Ladeinfrastruktur-Vernetzung in den Schaufenstern Elektromobilität.

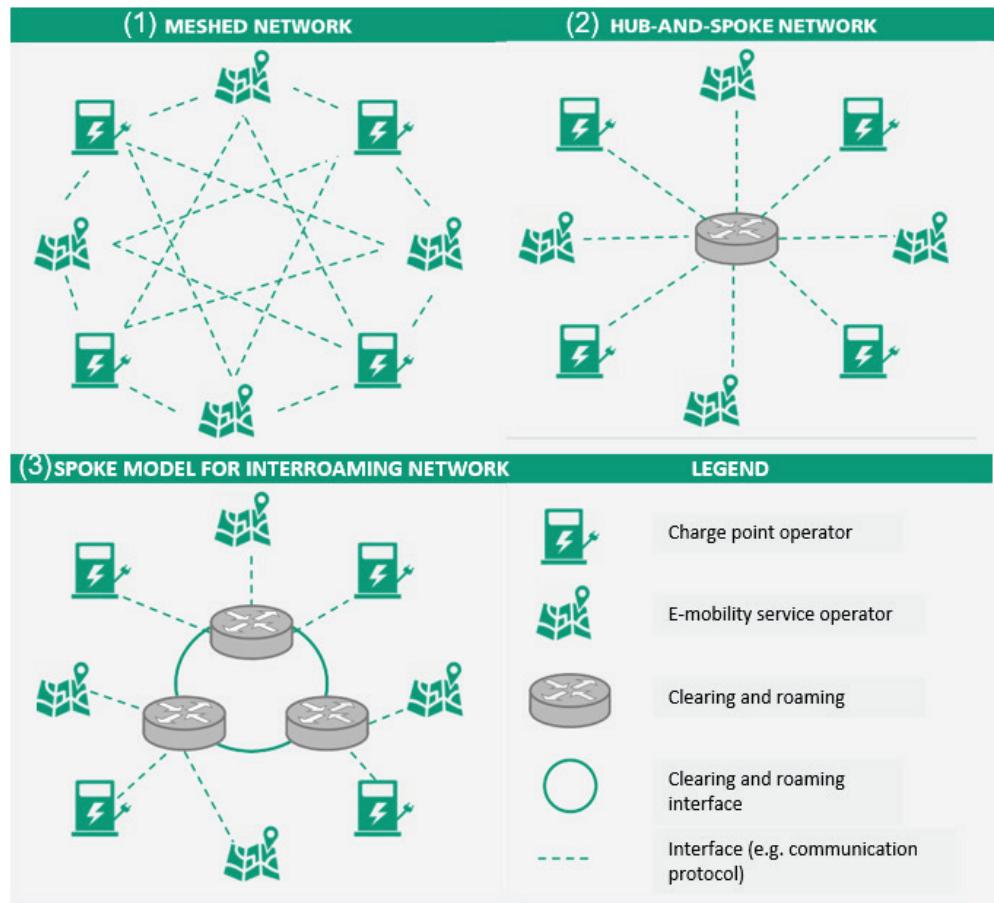


Figure 8: Cooperative models for eRoaming based on "Begleit- und Wirkungsforschung Schaufenster Elektromobilität" (BuW), 2015.

Alongside these three cooperative models, the above-mentioned C&R providers differ in terms of their vertical integration and whether or not they also provide clearing services in addition to roaming. This applies especially to model (3), in which multiple C&R providers ought to have implemented these functions end-to-end, i.e. from initiation of the process by the driver of an electric vehicle to the conclusion of charging. In practice, in relationships of this kind it is not always the case that all functions are performed. While the processes required for roaming need to be comprehensively modelled, this is not necessarily so with (semi-)automated clearing. It should also be noted that, for economic and other reasons, functions like premium services are optional and do not necessarily have to be taken advantage by a C&R provider's users.

The technical-functional processes are first sketched below before going on to describe their contractual relationships in general terms. The latter will be more thoroughly illuminated in the legal section.

In connection with implementing a C&R service, two process groups need to be distinguished:

- (1) Authentication, authorization and transfer of transaction data (roaming)
- (2) Invoicing⁴⁶² and execution of payments (clearing)

Process group (1) involves providing information at the charge point⁴⁶³, legitimizing a charging event that has been initiated by an identified e-vehicle driver (authentication and authorization), technically supplying electric power from the charger to the vehicle, and measuring the relevant performance parameters (e.g. time, energy flow, charging session, connection time, parking time etc.) and storing them in a charge detail record (CDR).

On the basis of these processes, bilateral settlement of charging services received is possible between the CPO and eMSP. Some roaming providers that do not also act as clearing houses base their service exclusively on these components. The CPO is responsible for documenting incurred costs. At the time of preparing this study, this still partly requires considerable manual work, a fact that is prompting many CPOs to invest in more complex backend solutions to increase their level of automation.

Process group (2) involves invoicing, settlement and offsetting of charging services between CPOs and eMSPs, and processing of invoiced charging services via payment services. For this purpose, monetary values are transferred between the eMSP and the CPO, which can take different forms depending on the payment method employed. This is accomplished with the aid of information from the CDR. Then agreed rates and prices are applied for invoicing the services. Process group (2) depends on the proper functioning of process group (1).

These processes are coordinated at the IT level using a wide variety of typically open communication protocols. While communication between an electric vehicle and the charger is nearly always based on the ISO/IEC 15118 standard and communication between the charger and the CPO typically uses the Open Charge Point Protocol (OCPP), which has been widely adopted in this market, a large number of other protocols are also in use. Competing C&R providers typically rely on different protocols. The largest C&R provider, intercharge, uses the Open Intercharge Protocol and e-clearing.net relies on the OCPP. Their names reveal that they have been largely shaped by their respective users. Newer, less prevalent protocols that mediate directly between eMSPs and CPOs are still in the development stage. However, these too require the existence of central registries that statically store relationships between eMSPs and CPOs for queries and approvals. In Germany, this task is performed by the Bundesverband der Energie- und Wasserwirtschaft (Federal Association of the German Energy and Water Industries).

The contractual situation can be summarized in simplified form⁴⁶⁴ as follows: so that eMSPs can work with CPOs via C&R providers, eRoaming contracts must be concluded between eMSPs and C&R providers as well as between C&R providers and CPOs to

⁴⁶² Invoicing: The process of creating an invoice with the result of the billing document (invoice), which contains the invoice value (invoice value= and its invoice components).

⁴⁶³ Charge point information such as price, maximum charging speed, charger availability etc.

⁴⁶⁴ Many other schemes exist, but the contractual setup described here is a widespread model.

define their relationships. In addition, eMSPs must also directly conclude contracts with CPOs in order to specify settlement terms. If there are n CPOs and m eMSPs, then potentially $n \times m$ contracts need to be concluded among the last-mentioned players. These contracts are needed because, even when a C&R provider meets the technical prerequisites for cooperation, this will not necessarily enable the settlement of services between an eMSP and a CPO. By way of conclusion, it should be mentioned that in practice a company can assume multiple roles. Larger CPOs in particular also provide eRoaming-capable electric vehicle charging services. Consequently, customers can also charge at other CPOs that have concluded contracts with the same C&R provider.

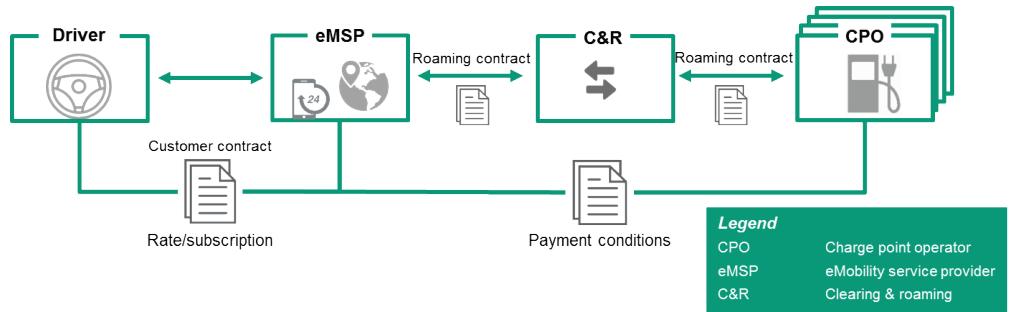


Figure 9: Market roles and players and contractual relationships (a simplified schematic depiction)

7.1.2 Status quo and challenges

The availability of suitable charging infrastructure for meeting demand being a vital requirement, it is important to analyze and understand the accessibility and other issues that public charge points face. This section therefore summarizes the situation from the viewpoint of drivers, i.e. electromobility users, before explaining the challenges of CPOs and eMSPs.

The chief value proposition of eMSPs is to provide customers with a consistent charging experience. This means providing as many (rapid) charge points as possible with transparent, attractively priced terms and smooth payment processes that require minimal effort on the part of drivers. Against this background, partitioning the theoretically available charge points is an unsatisfactory solution. Although Web-based direct payment processes like those described above have been possible at all installed charge points since 2017 thanks to the second German Charge Point Ordinance, they are not ideal from the driver perspective:

- *Comfort:* Direct payment is less than pleasant because drivers are generally obliged to interact with an unknown user interface at the charge point, often in bad weather. For another, many users are reluctant to reveal personal data and confidential credit card information (if they even have a credit card). In some cases, eRoaming providers enable Web-based direct payment using proprietary mobile apps or separate websites that the user must open in a browser in order to complete the transaction. Both approaches are widely perceived as user-unfriendly.⁴⁶⁵

⁴⁶⁵ Dudenhausen/Hahn, Herausforderung Utility 4.0, 2017, pp. 683-700.

In addition, instead of a single consolidated statement, e.g. at the end of each month like with the eMSP, users receive a separate receipt or invoice every time they charge.

- *Settlement modes:* It takes an additional effort to learn about rates and prices. It is common for clauses on possible roaming fees to be hidden away in fine print. And ad hoc charging rates tend to be high. It is therefore understandable that drivers or owners of slow-charging electric vehicles are more likely to choose a service provider whose prices are based not on elapsed time or a flat rate but instead on the amount of energy consumed (in kilowatt-hours). If the charge point that a driver wants to use only offers a time-based rate, he or she may go elsewhere to avoid paying more than users whose vehicles support rapid charging. This applies analogously to charge points where a higher price must be paid for ad hoc charging, and especially to those that require the payment of a fixed base rate to offset low variable costs (which in extreme cases can be none at all, effectively resulting in a flat rate).

The current situation poses challenges for CPOs, which are summarized in the following. Depending on their operational model, CPOs strive to make their charging infrastructure available to the largest possible number of electric vehicle drivers. The main motivation is to increase revenues. From today's perspective, this requires implementing multiple communication protocols, thus increasing the associated IT integration costs. Costs are also incurred for C&R services. These usually require the payment of three- or four-digit sums on a monthly or yearly basis, occasionally supplemented by one-off hookup fees that can run into thousands of euros. The use of multiple C&R services can impose an excessive IT and/or financial burden on smaller CPOs. The fact that, depending on the C&R service, it can be necessary to manually invoice every single eMSP at the end of each month makes the situation even more difficult. Worse still, the vast majority of established C&R services negotiate bilateral contracts with static pricing. In the event of a merger or the takeover of additional eMSPs, the terms have to be manually changed. This high overhead leaves many CPOs no choice but to charge roaming fees.

eMSPs face similar challenges. But because there are far more CPOs than eMSPs, it is very laborious to establish and maintain relationships with CPOs while negotiating different terms in each case. The technical challenges involved are also considerable for eMSPs. They have to make an enormous effort to mobilize enough capacity for checking the monthly invoices received from CPOs.

7.1.3 Possible solutions and roles of DLT

Role

DLT could potentially perform at least three functions for addressing the challenges described above. They are:

- 1) Authentication and authorization with DLT-based, autonomous identity solutions
- 2) Tamperproof documentation and storage of charging events

- This includes, above all, taking advantage of DLT's attributes of unchangeability and verifiability for invoicing charging services, from the eMSP all the way to the meter, for irrevocably documenting charging events⁴⁶⁶ in compliance with the applicable laws and ordinances on measures and calibration.

3) Prompt billing of and payment for charging events using tokens

By modeling these three functions, a DLT solution can assume the role of a C&R provider as described above for implementing a meshed network model of cooperation (3) that will "by design" eliminate the risks associated with a concentration of market power in the hands of individual C&R players. A DLT-based solution would, first and foremost, make available a (further) alternative in the form of a neutral platform⁴⁶⁷ alongside existing C&R players. If market power should then become excessively concentrated, more and more players can be expected to switch to this neutral platform.

Solution

The use of a platform based on a public DLT system such as Ethereum could, unlike existing C&R services, enable new players to enter and participate in this market faster and more easily. Ideally, each CPO and each eMSP would constitute a node. Detailed study is required to determine the extent to which IT integration costs can be reduced, since this greatly depends on how the DLT solution is designed. Because, at least theoretically, no (more) new roaming communication protocols have to be created, the required work would only involve applying established standards to communications between vehicles and charge points, charge points and CPOs, and CPOs and the DLT-based platform. Since not every charge point but only every CPO would constitute a node, no modifications to existing charging infrastructure are required, especially since currently existing C&R services already have Internet connectivity.⁴⁶⁸ From the perspective of electric vehicle drivers, charging conditions will become transparent, since this information, being part of the smart contract specifications, is stored in the DLT layer where it is publicly accessible. It could also be advantageous if drivers did not have to have their own wallet or a publicly known identity, instead being able to use a temporary pseudonym, provided that the eMSP in question keeps records of each combination of pseudonym, time stamp and customer. Charging events would then be easy for CPOs to authorize and would be lastingly documented when storing a CDR in the DLT layer in such a way that executing the smart contract triggers a value transfer from the eMSP to the CPO.

⁴⁶⁶ The required tamperproof sensors, for examples, are being developed (further) within the scope of the SecMobil project promoted by the German Federal Ministry for Economic Affairs and Energy.

⁴⁶⁷ Cf. section **Fehler! Verweisquelle konnte nicht gefunden werden..**

⁴⁶⁸ Cf. section 7.1.1.

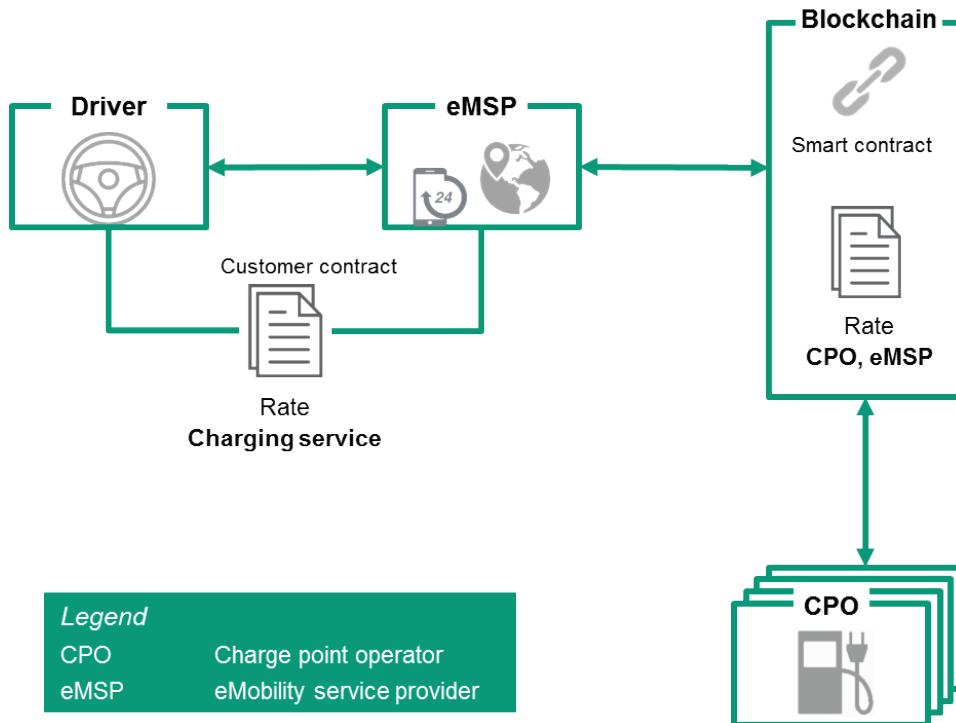


Figure 10: DLT flowchart showing how the roles interact

7.1.4 Process description

Authentication and authorization: Say that an e-vehicle driver has investigated the available charging facilities ahead of time, for example while planning her travel route, or obtained information via the in-car entertainment system, and selected an appropriate charge point along the way. There also may be predefined or user-defined profiles in the vehicle that include charging preferences. After the vehicle arrives at the charge point and is connected, it receives the charger ID straight from the CPO, e.g. according to the communication rules⁴⁶⁹ defined by the plug & charge⁴⁷⁰ protocol. This communication takes place via a direct channel—in other words, off-chain—since attributes such as speed take precedence and lack of trust has not yet been identified as an obstacle at this point. The vehicle uses the received information to log in with its eMSP, which checks the terms for that particular combination of driver and charger (and thus the CPO) and, if the result is positive, authorizes charging. The terms for starting the charging procedure can then be easily rechecked and either accepted or rejected. By tapping a button on a screen of the in-car entertainment system, a corresponding query can be initiated or a declaration of intent printed out as appropriate.

Documentation and maintenance: Within the scope of the documentation, the concluded agreements are specified before actual charging begins. These include the

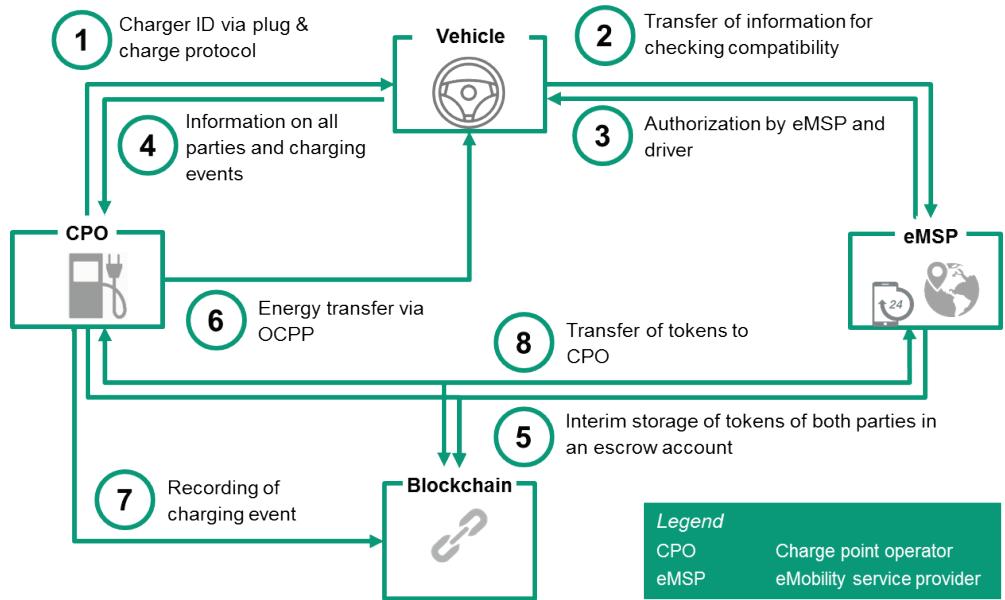
⁴⁶⁹ For example within the scope of ISO 15118.

⁴⁷⁰ Plug & charge allows an e-vehicle to self-authenticate (without needing a charging app or card at the charger).

terms of the impending charging event, such as the applicable rates and the signatures of the contractual parties. A posteriori, the charging parameters and, once again, the signatures are recorded. It is possible to divide up the charging process into sections, with this procedure being repeated in each one. This increases the strength of the documentation. In these cases, however, it is advisable to incorporate scalability and transaction costs into the decision-making process. This way, tamperproof storage of the CDR in the DLT can provide the basis for the required trust between two parties (in this case, the CPO and MPS) without the necessity for a C&R service to perform this role.

Settlement and value transfer: For settlement purposes, the eMSP makes partial payment⁴⁷¹ up front within the scope of an escrow smart contract⁴⁷² to give the CPO confidence that the eMSP possesses tokens for making payment, and then initiates the process. The tokens⁴⁷³ of both parties are kept in the escrow smart contract until the transaction has been completed. The energy transfer itself takes place in accordance with standard Open Charge Point Protocol (OCPP) specifications. Then the CPO stores the CDR, which ideally is based on data from tamperproof sensors, along with the driver's temporary pseudonym and the eMSP ID, in the distributed ledger to serve as a receipt. While acknowledging this, the tokens are transferred from the escrow smart contract to the CPO's wallet. Actual clearance for payment settlement takes place afterward—i.e. the remaining tokens are returned to the eMSP. Analogously to centralized C&R services, (automated) payment settlement is an additional service.

At the end of the month, the charging event is invoiced to the vehicle driver, who only has a contractual relationship with the eMSP.



⁴⁷¹ For the sake of simplicity, we are assuming that a sum up to a defined maximum (e.g. 60 euros in the case of chargeNow) is paid up front so that the eMSP will never have to transfer any additional tokens at the end of the charging process.

⁴⁷² See the general technical section.

⁴⁷³ The details of the token's design (cf. the section on digital documents 4.2.5.6) cannot be generalized and in any case are irrelevant at the level of abstraction chosen for this case study.

Figure 11: Schematic process description of a DLT-based implementation

7.1.5 Conclusions and recommendations for action

The use of DLT being investigated here is a scenario in which DLT results in disintermediation (i.e. reduces the use of intermediaries between producers and customers), counteracting the tendency of today's C&R providers to assume a typical intermediary role in the electromobility value creation network by setting up superplatforms. It is evident from the approach described here that technocultural solutions are possible and, analogously to neutral platforms, could make it more difficult for power to become concentrated in only a few hands. However, it remains quite doubtful that a DLT-based solution that only models existing functions could acquire a significant share of the market, considering that, especially in Germany, well-established players largely dominate it, with CPOs also participating by acquiring shares of them. These C&R services are already deriving enormous benefits from network effects. As a rule large CPOs have simultaneous access to all relevant C&R services via standardized interfaces. In addition, C&R services and their protocols are continuing to evolve rapidly. It remains to be seen whether roaming prices can and will fall with the advent of DLT-based solutions. A more detailed analysis than is possible within the scope of this study is needed in order to precisely assess this potential effect. In case a blockchain-based solution becomes established as a basis for other, similar applications such as the previously mentioned green and local power certificates, distribution of charging across multiple electric vehicles within the scope of smart charging, and home charging, a new situation will arise in which such a DLT solution could become a genuine alternative as a neutral platform in a market that has not yet been carved up.



Consumer Protection Portals

Owing to the complex nature of DLT, ordinary citizens should probably not be expected to understand every detail of the underlying technology. Nevertheless, it is important for there to be a broad basic understanding of it, since DLT as a digital infrastructure technology will potentially be used—at least indirectly—by many people. It is therefore extremely important for them to grasp the implications (e.g. of resistance to tampering etc.). Moreover, general mistrust or basic skepticism toward DLT in the population could hamper the spread of innovations. It should therefore be ascertained whether, in collaboration with consumer protection portals and institutions like TÜV, it is possible to promote greater understanding and acceptance of this technology.

7.2 Legal Discussion

The preceding comprehensive economic and technical analysis of the status quo in section 7.1.2 shows that charging of electric vehicles is currently only possible with the participation of multiple players. In the following, the aim is to legally define and fill in more details of the required contractual relationships. Although the use of DLT could reduce the number of contractual relationships, it also poses challenges under data protection law, which are also addressed in the following.

7.2.1 Contractual relationships

It follows from Section 4 of the Charge Point Ordinance (LSV) issued by the Federal Ministry for Economic Affairs and Energy⁴⁷⁴ that the relevant contractual relationships can be distinguished on the basis of the chosen payment method (as already discussed in 7.1.1). The LSV implements EU Directive 2014/94/EU on the deployment of alternative fuel infrastructure with the goal of advancing the establishment of charging infrastructure.⁴⁷⁵ The German legislature initially only implemented the directive's technical standardization requirements (as the first LSV) and later supplemented this, among other things by addressing the aspects of authentication and payment, which also need to be implemented (under the second LSV).⁴⁷⁶ If the operator of a charge point lets users charge their vehicles without authentication as per Section 4, No. 1, Letter a of the LSV without making a financial contribution or in return for cash payment as per Section 4, No. 1, Letter b of the LSV, then in the first case a gift is typically involved in the sense of Section 516 of the German Civil Code, and in the second case a purchase contract for electric power arises in accordance with Section 453, Subsection 1 and Section 433 of the German Civil Code.⁴⁷⁷ The latter also applies in the case of card- or web-based payment, both of which require authentication as per Section 4, No. 2 of the LSV.

What interests here is so-called roaming, with charging across multiple providers,⁴⁷⁸ instead of the just-described practice of charging at individual, unconnected charge points.⁴⁷⁹ Like in the case of mobile telephony, each customer concludes a single subscription-like vehicle charging contract in the form of an ongoing obligation⁴⁸⁰ with an eMSP (see Figure 30). The contract resembles conventional electric power supply contracts, since the purpose for which the purchased electricity is used—in this case, for operating a vehicle—is irrelevant.⁴⁸¹ Consequently, in accordance with Section 453, Subsection 1 and Section 433 of the German Civil Code it basically constitutes a contract for purchasing electricity, while differing from conventional electric power supply contracts in that it entitles the customer to use the charging infrastructure.⁴⁸² In order to enable charging across multiple providers, the R&C services conclude bilateral roaming contracts with individual eMSPs and CPOs (see Figure 30). The principal characteristic of these bilateral roaming contracts is that their conclusion also gives rise to separate multilateral (charging network) contracts among all participating eMSPs and CPOs (see Figure 30).⁴⁸³ This is necessary because no direct contract arises between a customer who signs up for a roaming scheme and a CPO.⁴⁸⁴ When the customer charges his or her electric vehicle, contractually it is the eMSP that uses the unrestricted access which a CPO has granted to the customer in each case.⁴⁸⁵

⁴⁷⁴ Section 49, Subsection 4, Sentence 1, Nos. 1 to 4 of the German Energy Industry Act (Gesetz über die Elektrizitäts- und Gasversorgung).

⁴⁷⁵ Directive 2014/94/EU, Recital 23.

⁴⁷⁶ Lehner, RAW, 2018, pp. 17-21. (18).

⁴⁷⁷ Graf von Westphalen/Schöne, 37. EL. Okt. 2015, Stromlieferverträge Rn. 369.

⁴⁷⁸ Overkamp/Schings, EnWZ, 2019, pp. 3-8..

⁴⁷⁹ Section 4 of the German Charge Point Ordinance (LSV).

⁴⁸⁰ Overkamp/Schings, EnWZ, 2019, pp. 3-8 (7).

⁴⁸¹ Graf von Westphalen/Schöne, 37. EL. Okt. 2015, Stromlieferverträge Rn. 369.

⁴⁸² Graf von Westphalen/Schöne, 37. EL. Okt. 2015, Stromlieferverträge Rn. 368.

⁴⁸³ Hahn/Grün, IR, 2013, pp. 293-296 (295).

⁴⁸⁴ Hahn/Grün, IR, 2013, pp. 293-296 (294).

⁴⁸⁵ Hahn/Grün, IR, 2013, pp. 293-296 (294).

In this constellation, the eMSP faces a price risk. While he or she may have agreed on a flat rate with his or her customers, toward the CPO involved in the roaming scheme he or she might have to pay the participating CPO a fee per kilowatt-hour or charging event. Comparable to conventional fueling agreements in the context of fleet leasing, eMSPs therefore have an incentive to conclude special agreements with CPOs in order to make their business calculable.⁴⁸⁶

Today, as shown, a large number of contracts is required to organize a roaming scheme. Over time it may then be possible to lower the number of participants, especially by substituting R&Cs, to simplify matters. In the medium term, however, smart contracts stored on a DLT platform could be integrated in the remuneration agreements to automate payment for charging by means of tokens.⁴⁸⁷

7.2.2 Blockchain-based data protection for electric vehicle charging infrastructure

In connection with making payments for using charging infrastructure, personal data of the system's users may be processed. The extent to which data protection laws come into play here depends on whether the information on users of the system includes information on natural persons. Where the system's users are concerned, it is necessary to distinguish between eRoaming schemes on the one hand and systems in which drivers directly pay the CPO on the other. In connection with eRoaming, it also matters whether knowledge of the eMSP and CPO can reveal information about the natural persons behind them.

7.2.2.1 Data protection in connection with eRoaming when no information can be obtained about natural persons behind the eMSP and CPO

In the case of eRoaming, it is usual to execute transactions at the blockchain level exclusively with a B2B solution between the eMSP and CPO. The driver approaches the CPO to initiate the charging process. The driver can also be authenticated at that time. The transactions required for payment to be made between the eMSP and CPO are executed in the blockchain. However, these transactions do not include any information on individual drivers. Problems under data protection law only arise if knowledge of the eMSP and CPO also reveals information on natural persons behind these companies.⁴⁸⁸ If this is not the case, on-chain processing does not raise any issues under data protection law.

7.2.2.2 Data protection with direct payment and eRoaming if information can be obtained on natural persons behind the eMSP and CPO

If a customer is supposed to directly execute the transaction with the CPO via a separate payment process, under existing laws it is necessary to choose one of the solutions explained in the general section. Such a solution is also required if the blockchain is exclusively operated by the eMSP and CPO but one or both of them is a small compa-

⁴⁸⁶ Hahn/Grün, IR, 2013, pp. 293-296 (295).

⁴⁸⁷ The website of the charge point operator Ionity, a joint venture of BMW, Daimler, Ford and VW, lists tokens as a possible means of payment: <https://ionity.eu/de/wo-und-wie.html> (last accessed on 26.02.2018).

⁴⁸⁸ See 5.2.2.2.1.1.1.

ny, thus making it easier to learn about the natural persons behind them. This is especially likely to be the case with CPOs. For example, if a CPO consists of a single individual, and if the key linking the username with the CPO is known, then the information associated with the username of the CPO in question is personal data. In this case, an appropriate solution must be chosen to satisfy the stipulations of data protection law.

An “open solution”⁴⁸⁹ would require all participants in the system to demonstrate a legitimate interest in all of the information. However, only the parties involved in the actual charging process have an interest in the payment transactions for operating electric vehicle charging infrastructure. It follows from this that it is contrary to data protection law for all system participants to be privy to all activities. Consequently, an “open solution” does not enter into consideration here.

By contrast, a “centralized solution” basically appears to be feasible.⁴⁹⁰ This would have to involve the operation of a permissioned blockchain by a central entity that is able to use a system of rights and roles to control which information is visible to which participants. The central entity would therefore be the “controller” (in the sense of data protection law) for on-chain data processing. A contract concluded between the participants and the central entity enters into consideration as the legal basis for this processing.⁴⁹¹ The central entity must also possess suitable means of erasing data. This could be enabled by a “redactable blockchain”⁴⁹² in which the central entity can insert chains or forks⁴⁹³ in which the nodes are obliged to erase unwanted data from the decentralized database.

If a “centralized solution” is neither possible nor wished, an “anonymization solution”⁴⁹⁴ could also be chosen. In the context of eRoaming, off-chain balancing is basically possible.⁴⁹⁵ In this approach, the participating eMSP and CPO do not enter every transaction in the blockchain; instead, each of them keeps a separate ledger off-chain. The offsetting payments due are then made between the participants at regular intervals. No patterns should be evident in these payments that could make it possible to deduce the identity of the CPO or eMSP behind a username.

Anonymization solutions enter into consideration for this, such as zero-knowledge proofs⁴⁹⁶ or stealth addresses in conjunction with ring signatures.⁴⁹⁷ In the case of anonymization, no data processing of relevance to data protection law is stored on-chain, and consequently no legal basis is required for doing so either. Nor does it have to be possible to erase data.

⁴⁸⁹ On “open solutions”, see 5.2.3.4.2.1.

⁴⁹⁰ On “centralized solutions”, see 5.2.3.4.1.

⁴⁹¹ On the legal basis for choosing a centralized solution, see 5.2.4.2.2.

⁴⁹² On redactable blockchains, see 0.

⁴⁹³ On forks, see 5.2.5.2.2 and 0.

⁴⁹⁴ On anonymization solutions, see 5.2.3.4.2.2.2.4.

⁴⁹⁵ On balancing in general, see 5.2.3.4.2.2.2.2.

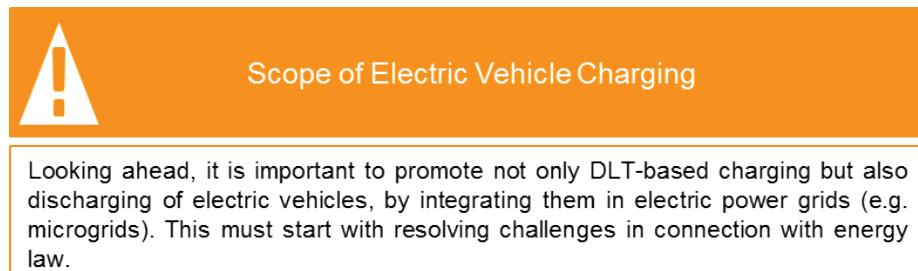
⁴⁹⁶ On zero-knowledge proofs, see 5.2.3.4.2.2.2.3 and 0.

⁴⁹⁷ On stealth addresses in conjunction with ring signatures, see 5.2.3.4.2.2.2.4.

7.2.3 Conclusions and recommendations for action

Vehicle charging is a potential application for DLT, especially in connection with eRoaming. In the medium term, its use can lead to payment with tokens and in the long term perhaps even to a reduction in the number of parties involved in providing the services, which is like to cut down the large number of contracts that are required today. Looking ahead, it is important to keep in mind that, besides charging, there is also discharging. Electric vehicles can also serve as energy storage modules, for example in a microgrid. Here the legal hurdles mainly have to do with energy law rather than DLT-specific issues.⁴⁹⁸ However, they are not part of the scope of this study.

If eRoaming is implemented via a DLT platform, this will be permissible under data protection law provided that the natural persons behind the participating eMSPs and CPOs are not identifiable. There can be a need to make adjustments, however, if information on transactions conducted by eMSPs or CPOs also reveal information on natural persons behind these companies. The same statement applies if, instead of an eRoaming scheme, an approach involving direct payment by drivers to CPOs is taken.



⁴⁹⁸ An introduction is provided among others by: Scholtka/Kneuper, IR, 2019, pp. 17-21.; Overkamp/Schings, EnWZ, 2019, pp. 3-8.

8 Ridesharing

8.1 Economic and Technical Aspects: Technical Part

8.1.1 Definition and description of the application

Consumers are increasingly resorting to shared means of transportation for getting around instead of traveling alone. This has potential for saving costs and resources, thus reducing environmental burdens. Whereas forms of public transportation such as buses, subways (underground trains) and railways are characterized by fixed routes and schedules, shared use of motor vehicles provides greater flexibility. In many cases, the benefits also include greater comfort and convenience and faster travel. This applies especially to rural areas, where it is more difficult to arrange dense, regular public transportation services.

Ridesharing is defined in this context as the shared use of a vehicle by several persons with similar travel needs, who typically also divide up the incurred costs.⁴⁹⁹ For the purposes of this study, it is immaterial whether the driver also travels in order to get somewhere (peer-to-peer) or does so as a commercial activity.

In Europe, the USA and China, the overall market for shared mobility is projected to grow by between 15 and 28 percent yearly until 2030. While in the United States and China monopolistic providers control more than 80% of the market, for regulatory reasons there is currently greater fragmentation in Europe.⁵⁰⁰ A survey of experts carried out by the German Aerospace Center revealed that approaches for the shared use of motor vehicles are still relatively unknown in Germany. It is expected, however, that these forms of mobility will gain in importance in several defined contexts and mainly among younger persons, but not in city centers.⁵⁰¹

The spread of shared mobility options is intimately linked to increasing digitalization. Digital platforms are a prerequisite for scalable real-time coordination of the supply of and demand for transportation opportunities, and these in turn depend on high availability of the Internet and advanced information and telecommunications technology.⁵⁰² In this context, digital platforms are undertakings in two- or multiple-sided markets that use the Internet to enable interactions among two or more different but mutually dependent user groups. Value should be created for at least one of these user groups.⁵⁰³ Specifically, this means that digital mobility platforms dynamically bring together providers and users of mobility opportunities. According to the German Federal Ministry for Economic Affairs and Energy, digital platforms can also be described as intermediaries that use digitized information on networked devices to simplify searches and reduce the cost of comparing offers.⁵⁰⁴ In the context of ridesharing, there are

⁴⁹⁹ Furuhata/Dessouky et al., *Transportation Research Part B: Methodological*, 2013, pp. 28-46..

⁵⁰⁰ Grosse-Ophoff/Hausler et al., *How shared mobility will change the automotive industry*.

⁵⁰¹ Heinrichs/Thomaier et al., *Arbeitsberichte zur Verkehrsorschung: Ko-Automobilität*.

⁵⁰² Cohen/Kietzmann, *Organization & Environment*, 2014, pp. 279-296..

⁵⁰³ European Commission, *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*.

⁵⁰⁴ Bundesministerium für Wirtschaft und Energie (BMWi), *Grünbuch Digitale Plattformen*.

both digital platforms that themselves provide transportation and/or have drivers under contract, and such that merely capture and coordinate supply and demand.⁵⁰⁵ In both types, as a rule for each trip there is someone offering transportation and one or more persons who ride with him or her.

In practice, three distinct ridesharing models have emerged, which differ in terms of the time dimensions of the offers they list.⁵⁰⁶ The first two types resemble one another closely in terms of how their platforms are structured.

- *One-off ride offers*: Most common are platforms on which someone places an offer to carry passengers well in advance. In this scenario, interested persons can use the digital platform to book the trip.
- *Regular commutes*: There are also models in which someone offers to regularly carry passengers, for example to their place of work. These offers can also be booked by others; typically only the initial contact is made via the ridesharing platform.
- *Ad hoc ridesharing*: In addition, there are platforms offering dynamic ad hoc ridesharing. Drivers and potential passengers are directly and spontaneously brought together on the digital platform, with the latter typically using mobile devices to search for rides. This model has been gaining in popularity in recent years while benefiting from the spread of mobile devices and mobile Internet services. In practice, most platforms combine two or all three of these models.

8.1.2 Status quo and challenges

In Germany, the passenger transportation sector is currently divided between traditionally highly regulated and organized taxi services on the one hand and new digital mobility platforms offering ridesharing opportunities on the other. Because the vehicles of private individuals offering transportation are in heavy demand, many ridesharing providers charge lower prices than regular taxi services. According to one study,⁵⁰⁷ increased competition in the market is generating price benefits for consumers, at least for the time being. As a result of these economic incentives, as well as increasing flexibility for choosing transportation, overall the demand for ridesharing services is surging. In addition, this trend may possibly generate other benefits for society such as reduced emissions and overall lower traffic volumes.⁵⁰⁸ This is offset, however, by various challenges that have not yet been resolved⁵⁰⁹ and call for new ways of thinking.

1. Formation of monopolies

Ridesharing platforms generate greater benefits for everyone involved as the number of participants—both providers and consumers—increases on both sides as a result of so-called network effects.⁵¹⁰ The downside to this is a risk that monopolies will form, since coordination of the market inevitably concen-

⁵⁰⁵ Furuhata/Dessouky et al., *Transportation Research Part B: Methodological*, 2013, pp. 28-46..

⁵⁰⁶ Andersson/Hjalmarsson et al., *The 34th International Conference on Information Systems. ICIS 2013*, pp. 1-15..

⁵⁰⁷ Haucap/Pavel et al., *List Forum für Wirtschafts- und Finanzpolitik*, 2017, pp. 139-183.

⁵⁰⁸ Hahn/Metcalfe, *The Ridesharing Revolution: Economic Survey and Synthesis*.

⁵⁰⁹ Furuhata/Dessouky et al., *Transportation Research Part B: Methodological*, 2013, pp. 28-46..

⁵¹⁰ Alstyne, Marshall W., Eisenmann, Thomas/Parker, *Harvard business review*, 2006, pp. 92-104..

trates in the hands of a small number of platform operators.⁵¹¹ Initially there are various providers jostling for business, but eventually one or a small number of platforms wind up dominating the market. After that point, the monopolists can leverage their market power to block competing ridesharing providers from accessing customers and eventually exclude them completely from the market. The dominant platforms can then set prices almost however they please, since they alone are in possession of customer data in isolated silos. These additionally strengthen their position and make it increasingly difficult for new rivals to penetrate the market. Over the long term, this poses serious risks for free competition and also hurts customers as a result.

2. Identity management and generation of trust

Operationally, ridesharing also poses problems with regard to identity management and trust among the involved parties. One major challenge, for example, is instilling mutual trust among travelers who typically do not know one another, which is a necessary prerequisite for the trip to go smoothly. For this purpose, platform users typically need to reveal quite a bit of personal information to the platform operator etc. This often includes information that is not relevant, such as place of residence and date of birth.

It is also necessary to ensure that payment is only made for services that are actually provided as agreed, in order to prevent fraud.⁵¹² In other words, trust must be established regarding the willingness to pay of the individual parties involved in the process. It is common for so-called reputation systems to be used for this, despite the fact that they suffer from various weaknesses. The most critical aspect is how to provide an incentive for users to truthfully provide the requested information.⁵¹³ Escrow services are also used to reliably ensure payment for adequately provided transportation. This involves a third party freezing a sum of money for the trip and not disbursing it until confirmation is received that the service has actually been provided in an appropriate manner.⁵¹⁴ These services also require information to be passed on to a third party, in addition to requiring extra work and possibly additional fees.

Because customers must open a separate account for each available platform service, moreover, it becomes more difficult or inconvenient for them to switch to another provider or take advantage of any available cross-provider services. This circumstance additionally amplifies the problems discussed above in connection with monopolies.

3. Payment settlement

Another critical aspect of current ridesharing platforms has to do with processing payments for transportation services. In practice, there are two main alternatives for this: direct payment (in cash) by passengers to the driver, and

⁵¹¹ Bundesministerium für Wirtschaft und Energie (BMWi), Grünbuch Digitale Plattformen.

⁵¹² Furuhata/Dessouky et al., Transportation Research Part B: Methodological, 2013, pp. 28-46.

⁵¹³ Ibid.

⁵¹⁴ Ibid.

payment via a third party such as an online payment service provider.⁵¹⁵ Bilateral cash payments pose the risk that passengers may not carry enough cash in sufficiently small bills with them or will simply fail to turn up, while the driver has costs in any case.⁵¹⁶ What is more, in the case of an argument it is impossible to realistically check whether or not payment has been made. Payment settlement via a third party has the drawback of incurring transaction fees that increase the overall cost for the provider and consumer⁵¹⁷ and have the additional disadvantage that data are relayed to yet another party. This payment method is usually employed by ad hoc ridesharing platforms.⁵¹⁸ And if, as described in point 2, escrow services are used, additional work and expense also result.

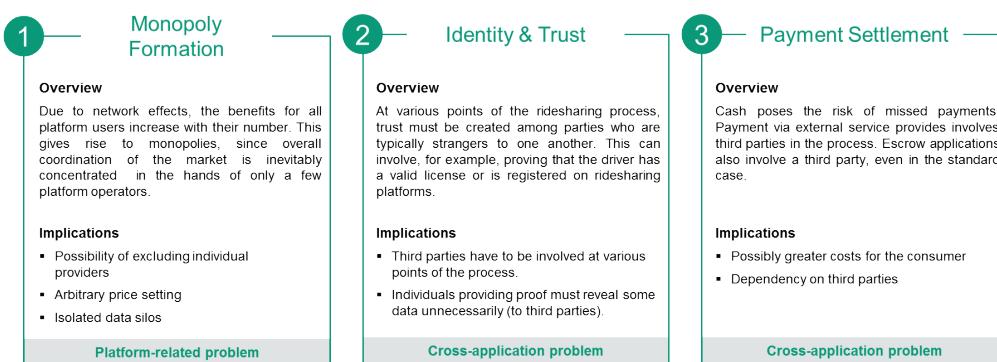


Figure 12: Summary of the problems of the existing situation

The upshot is that, in order to address the challenges sketched in the foregoing, there is a need for novel approaches to designing ridesharing platforms. To avoid the problems associated with the formation of monopolies, it appears desirable to strive for an open platform solution that will not exclude any providers or consumers from the market. There is also a need for alternatives to current practices for creating a sense of security and trust between travelers. It is particularly important to create identity management systems that span multiple providers and allow selective release of information on passengers. Finally, alternative approaches for efficient and secure settlement of payments between trip providers and passengers.

8.1.3 Possible solutions involving DLT

1. Monopolistic tendencies

To add value for users, it is essential for digital platforms to generate strong network effects.⁵¹⁹ This also applies to the market for ridesharing platforms. Generally speaking, however, it can be observed that the profits generated by a platform are not or not fairly distributed among the platform participants; in-

⁵¹⁵ Ibid.

⁵¹⁶ Ibid.

⁵¹⁷ Ibid.

⁵¹⁸ Furuhata/Dessouky et al., *Transportation Research Part B: Methodological*, 2013, pp. 28-46.

⁵¹⁹ Bundesministerium für Wirtschaft und Energie (BMWi), *Weißbuch Digitale Plattformen*.

stead, in many cases the intermediaries who run the platform retain an excessive share.⁵²⁰ In order to prevent the market from becoming concentrated in the hands of just a few providers, it appears to be essential to create an open platform that will not exclude any providers or customers from participating and is not controlled by a single institution.

DLT, because of its distributed nature and possibilities for automating business processes with smart contracts, is inherently well-suited for rendering individual institutions obsolete as intermediaries for bilateral relationships.⁵²¹ The specific case of ridesharing, however, poses challenges for identifying solutions that can be conceptually and technically implemented while adding value.

One core function of ridesharing platforms is coordinating supply and demand, in other words matching ride providers and passengers.⁵²² For this purpose, it is continually necessary to analyze, update and process large data volumes. Especially with dynamic ad hoc ridesharing, this is an extremely complex task, since diverse, frequently changing parameters (such as GPS data) need to be processed.⁵²³ It is therefore doubtful that DLT, in its current stage of technological development, would be suitable for ridesharing, at least for this type, for several reasons. Due to the high (monetary) costs of performing computational operations with smart contracts in today's public DLT systems, as well as the general limitations of smart contracts in terms of storing, querying and processing large data volumes, it does not appear to be feasible to implement appropriate algorithms with smart contracts. Other constraints are the high latency times and maximum data throughput, in terms of transactions processed per second, of currently available public DLT systems.⁵²⁴ Although several initiatives are striving to create ad hoc ridesharing platforms with DLT, the status of their technical implementation is difficult to assess to a lack of precise information. According to what little is known, however, in many cases matching of supply and demand does not take place directly on a DLT system.⁵²⁵ It is also necessary to ascertain how much value could actually be added by tamperproof storage of all posted ride offers and searches. Where this is concerned, it may also be difficult to comply with data protection requirements (see the general legal discussion). The use of DLT for matching supply and demand must therefore also be critically regarded in this context as well.

In the case of ad hoc ridesharing, presumably one or more locally oriented, neutral and centralized entities are needed for capturing and coordinating supply and demand in real time. This layer could then serve as a platform on which various ridesharing providers could post their offers while continuing to operate customer interfaces. With this approach, it would no longer be possi-

⁵²⁰ DeFilippi, Harvard Business Review Digital Articles, 2017, pp. 2-5..

⁵²¹ Schweizer/Schlatt et al., 38th International Conference on Information Systems (ICIS), 1.

⁵²² Hahn/Metcalfe, The Ridesharing Revolution: Economic Survey and Synthesis.

⁵²³ Mukherjee/Banerjee et al., Proceedings of the 21st International Conference on World Wide Web, 579.

⁵²⁴ Cf. section 4.3.2.1.

⁵²⁵ Johnson, Can La'Zooz Take Ridesharing to the Moon?

ble to exclude other providers or certain customers. Within this scenario, the possible business models encompass the use of anonymized utilization data and provision of customer interfaces, for example, which could also be integrated in other systems if expedient. Overall, a combination of on-chain and off-chain process is therefore the probable outcome for this application. Aspects that can be handled via a DLT system will be discussed in greater detail below.

Ridesharing platforms for regular routes (commuter services) and one-off ride offers with long lead times, by comparison, involve relative static listing of ride offers and requests that are displayed to users in response to corresponding searches. DLT-based decentralized marketplaces could be used in these cases to coordinate supply and demand.⁵²⁶ Decentralized and distributed storage systems such as the Interplanetary File System⁵²⁷ are generally used for this, in order to bypass the data storage constraints of DLT systems. Multiple providers can then use defined interfaces to run applications ridesharing customers, with all of them accessing the same open data layer and the ride offers and searches stored there. Despite the coexistence of different customer interfaces, this approach permits the creation of an open and decentralized data layer.

DLT can also assume other roles to pave the way for open ridesharing platforms that are accessible to various providers. In order to achieve a critical mass of platform participants (and thus also network effects), it could, for example, be used to create an incentive system that rewards them for their active participation by giving them tokens representing shares of the platform or allowing them to help design it.^{528,529} For the technical reasons explained above, it may not be feasible to implement the matching algorithms themselves in a DLT-based system.⁵³⁰ Instead, there would only be an interface for issuing tokens for each action performed on the platform. Tokens could also be used to pay for services via the platform. Finally, tokens could potentially facilitate and document payments for the services of individual providers on the open platform. This would be especially relevant if, for example, services are booked via external user interfaces.

2. Identity management and creation of trust

One possible use of DLT in this context is selective identification and authentication of individual parties in a way that respects their privacy.⁵³¹ This approach could, for one, potentially be used to authenticate and register individual users vis-à-vis multiple ridesharing platforms without the need for them to open more than one account. It would also make it easy for them to switch to another provider. For another, DLT could be used to resolve a previously identified trust issue⁵³² between drivers and passengers. For example, a driver

⁵²⁶ Origin Protocol, ORIGIN - Decentralized marketplaces on the blockchain.

⁵²⁷ Protocol Labs, IPFS is the Distributed Web.

⁵²⁸ Beck/Müller-Bloch et al., Journal of the Association for Information Systems, 2018, pp. 1020-1034.

⁵²⁹ DeFilippi, Harvard Business Review Digital Articles, 2017, pp. 2-5.

⁵³⁰ Johnson, Can La'Zooz Take Ridesharing to the Moon?

⁵³¹ Dunphy/Petitcolas, IEEE Security & Privacy, 2018, pp. 20-29..

⁵³² Furuhata/Dessouky et al., Transportation Research Part B: Methodological, 2013, pp. 28-46.

could directly and verifiably inform selected passengers or a platform that he or she has a valid driver's license without, for instance, having to disclose his or her date of birth.⁵³³

3. Payment services

Another possible use for DLT in connection with ridesharing is a history function for storing metadata on the business relationships between drivers and passengers. This would make it possible to verify the originally agreed conditions for a ride at a later time. This application is similar to one discussed in the next section in the context of platooning.

Tokens are currently an integral part of nearly all DLT systems.⁵³⁴ Such tokens, corresponding to values in fiat currencies, could, for example, be integrated in ridesharing platforms as an alternative to conventional means of payment. Credit card payments require an existing contract with corresponding (third-party) payment service providers. In practice, however, at least when taking a global perspective, fewer persons have concluded a contract of this kind than own a smartphone⁵³⁵ (which is needed to pay in a cryptocurrency), a fact that could encourage the spread of ridesharing platforms. The general part of this study contains a detailed discussion of payment functions. Although in many cases current DLT technology incurs higher transaction costs than the use of conventional payment service providers, considerable work is now being devoted to the development of alternative consensus mechanisms such as proof of stake for reducing the transaction costs of public DLT systems.

The use of smart contracts for implementing escrow contracts⁵³⁶ appears to be especially promising in the context of payment settlement for ridesharing. Generally speaking, conventional platform solutions involve sending a certain sum of money to a third party. After receipt of the service is confirmed, this sum is disbursed to the driver.⁵³⁷ DLT could automate this process without the need to involve intermediaries. In the standard case,⁵³⁸ the involvement of an additional intermediary could be prevented by automatically disbursing the agreed sum after the parties have signed off with their private keys. In addition, the selection of one of several verified mediators via a DLT system (using public keys, for example) could be used to automatically trigger the resolution of possible disputes⁵³⁹ and record the process in an understandable form in a DLT system.

8.1.4 Process description

The process varies for different kinds of ridesharing mainly in how supply and demand are matched. On ridesharing platforms that coordinate ride offers ahead of time, pro-

⁵³³ See also sections 0 and 0.

⁵³⁴ Cf. section 0.

⁵³⁵ Hahn/Metcalfe, The Ridesharing Revolution: Economic Survey and Synthesis.

⁵³⁶ Cf. section **Fehler! Verweisquelle konnte nicht gefunden werden..**

⁵³⁷ Furuhata/Dessouky et al., Transportation Research Part B: Methodological, 2013, pp. 28-46.

⁵³⁸ In other words, when there is no need to involve an intermediary for resolving conflicts.

⁵³⁹ Goldfeder/Bonneau et al. in Kiayias, Financial Cryptography and Data Security, 321.

viders use a (mobile) application to upload an offer for a precisely specified route at a certain time on a particular date. This applies to both one-time rides and regular commutes. In the next step, potential passengers use a (mobile) application to search for available rides for a precisely specified route. If the routes partly or entirely coincide in time and space, matching offers are displayed to the searchers, who can choose one of them. This gives rise to a bilateral connection between a driver and a passenger. Additional details, such as the meeting place, can then often be discussed and coordinated via the same platform.

While it continues to be possible to offer interfaces to users (of (mobile) applications) via various centralized providers, the data storage layer and the protocols for coordinating offers can be implemented in a decentralized manner with the aid of DLT systems. From the perspective of customers, however, this does not initially alter the process.

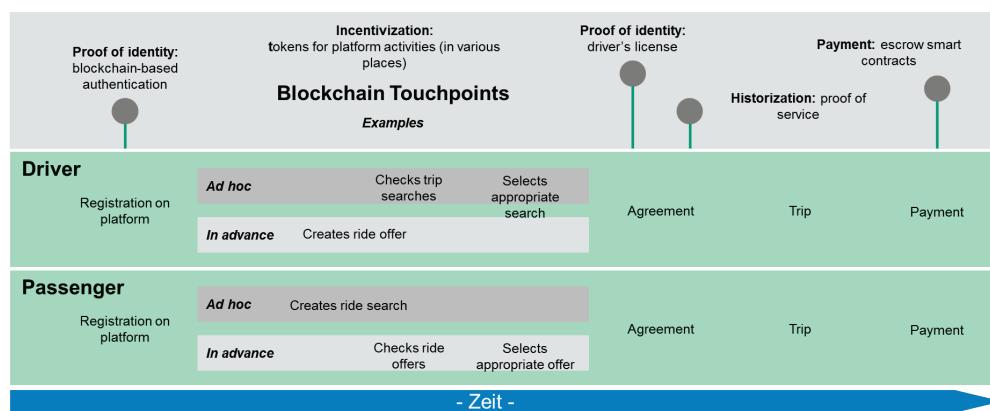


Figure 13: DLT partially supports the ridesharing process.

In the case of ad hoc ridesharing, by contrast, potential passengers first use a (usually mobile) application to post a request for a ride on a certain route. A matching algorithm, which at this time usually runs on the IT infrastructure of a given platform operator, then looks for offers that match the search. These can be from drivers who are geographically available to the potential passengers. The corresponding ride requests are then displayed to these drivers (typically also via a mobile application). If a driver accepts one or more of them, an agreement arises between the driver and the passenger or passengers, and he or she picks them up at the place specified by the application. In this scenario as well, as a minimum it is desirable to openly design the data layer, and if possible also the matching algorithm. In view of the performance requirements described above, however, it is questionable whether DLT could be used for this. What is needed is a neutral platform, and DLT could potentially support its implementation in various ways (cf. the possible solutions for and role of DLT). It also matters whether or not tamperproof storage of all posted offers and searches (along with the associated costs) is required.

Up to this point, DLT could possibly, as described in the previous section, be used as a digital infrastructure for registering users of the various (mobile) ridesharing applications. It is important to stress, however, that the DLT systems used in the application scenario of an open ridesharing platform should also be public systems (see section 3.3.1 on public permissionless DLT systems), since interactions among many parties (in actual practice, often private individuals) are modelled. The use of DLT is also conceiv-

able for selective identity management after supply and demand have been matched. A driver can use his digital identity to prove to his passengers that he or she has a valid driver's license. This claim would have already been digitally signed by the responsible authority and an anonymized pointer to a public blockchain stored without permitting any conclusions to be drawn about the actual person behind the driver's license.

After supply and demand have been matched, a smart escrow contract can be used. This involves creating a standardized smart contract containing metadata on the ride (e.g. date, route, price and number of passengers). Provided that all participating parties agree, they can then use their private keys to sign in to the corresponding DLT system, whereupon the smart contract is written into the DLT system and becomes executable there. After the ride service has been provided, each of the parties must once again send a signed message to this effect to the corresponding smart contract, whereupon the agreed price for the ride can be disbursed to the driver in each case. If a party refuses to sign, it is possible to deploy a mediator who has been previously chosen and defined in the smart contract. Alternatively, it is conceivable to integrate an interface that lets customers pay via DLT using a (mobile) application. In this case, cryptocurrencies can be used as an alternative means of payment. From the user perspective, this closely resembles conventional online payment services and in practice would presumably supplement them. Section 0 contains a more detailed discussion of the advantages and disadvantages of paying with cryptocurrencies.

If DLT is used to implement a system with incentives in the form of share tokens, then tokens are disbursed for each action on the platform (e.g. willingness to drive, the actual trip, and submission of an evaluation via a reputation system). These tokens represent shares in the open platform and could, for example, be used in turn to pay for or provide compensation for services provided on the open platform.

8.1.5 Conclusions and recommendations for action

To prevent the formation of monopolies and associated data silos, it is necessary to create an open, distributed ridesharing platform that does not exclude anyone offering or searching for rides from participating. Comparing the practical requirements of such systems with the special technical features of public blockchains, the exclusive use of DLT for this purpose appears questionable, at least where ad hoc ridesharing is concerned. Protocols for implementing DLT-based decentralized marketplaces can be used for static offers and searches, like in the cases of single rides and commuting services. DLT is basically well-suited for modelling direct relationships and processes among different parties and also for irreversibly documenting past events. However, these bilateral and multilateral relationships do not exist until after supply and demand have been matched, when it can also be important to securely store historical data. It follows that DLT as a digital infrastructure can assume important supporting functions in connection with ridesharing activities. These include, for example, extended identity management at several points of the process, provision of trust-generating mechanisms, and implementation of an incentivization and settlement structure for open platform systems.

If this application is extended, for example by integrating providers of different modes of transportation besides those that offer ridesharing services on an open multimodal platform,⁵⁴⁰ DLT could also potentially add value there. In this scenario, existing relationships among multiple suppliers would have to be modeled, e.g. in order to facilitate guaranteed settlement of provided multimodal transportation services. Examples include the OMOS⁵⁴¹ (Open Mobility System) initiative for creating an open, decentralized transportation system and the proposed Germany Ticket. Integration in multimodal transportation systems could also generally promote the spread of ridesharing.⁵⁴²



Study of Multimodal Mobility Platforms

The possibilities for and implications of implementing open and decentralized platforms should be studied in order to prevent the rise of monopolistic platform operators. Because it is for DLT to be used at various points along processes on a mobility platform, and various alternative technologies are also available, an open-minded study should be carried out first. It should also include multimodal platforms, since they require the transactions and interactions of multiple companies to be modeled and coordinated. DLT appears to be excellently suited for this.

8.2 Legal Discussion

As already shown in the preceding economic and technical analysis, certain characteristics of current DLT platforms—above all, the latency of data processing and energy costs for executing transactions—tend to make it unsuited for implementing ridesharing platforms without intermediaries. From a legal perspective there are also obstacles that, while being DLT-specific in terms of their data protection implications, mainly arise from ridesharing as such.

8.2.1 Passenger transportation law

In Germany, commercial transportation of passengers by motor vehicles for consideration is regulated by the Passenger Transport Act (Personenbeförderungsgesetz) (Section 1, Subsection 1, Sentence 1). A fundamental precept of this law is a “numerus clausus of types and forms of transportation [requiring approval]”, for which reason only specifically recognized forms of transportation may be licensed.⁵⁴³ Ridesharing services, unless they are already covered by the Passenger Transport Act because their use is free of charge or the revenues they generate do not exceed the operating costs (Section 1, Subsection 2, No. 1) or because they are subject to approval during a defined time period because they are new and still in a trial phase within the scope of a saving clause (Section 1, Subsection 7), can therefore only be licensed as rental cars used to transport passengers (Section 49, Subsection 4).⁵⁴⁴ The problematic aspect here is that,

⁵⁴⁰ Deakin/Frick et al., *Transportation Research Record*, 2010, pp. 131-137.

⁵⁴¹ MotionWerk GmbH, Open Mobility System (OMOS).

⁵⁴² Heinrichs/Thomaier et al., *Arbeitsberichte zur Verkehrsforschung: Ko-Automobilität*.

⁵⁴³ Linke/Jürschik, NZV, 2018, pp. 496-506 (498f.).

⁵⁴⁴ Linke/Jürschik, NZV, 2018, pp. 496-506 (499).

according to Section 49, Subsection 4, Sentence 2 of the Passenger Transport Act, rental cars may only be used to carry passengers if a request to provide this service is received at the entrepreneur's place of business or home. Furthermore, Section 49, Subsection 4, Sentence 3 prescribes that a rental car must return without delay to the entrepreneur's place of business after meeting a transportation request unless it has received another request before leaving the place of business or home or by telephone while traveling. Both requirements conflict with ridesharing practice.⁵⁴⁵ The underlying idea of ridesharing, namely pooling of trips, also contradicts Section 49, Subsection 4, Sentence 1, according to which rental cars may only be rented in their entirety for transportation purposes. Only a passenger may request a pooling of trips, having the sole right to determine the purpose, destination and route of a trip according to Section 49, Subsection 4, Sentence 1.

Due to the associated licensing problems, the current Passenger Transport Act has come under criticism.⁵⁴⁶ During the 19th legislative period of the German Bundestag, the parliamentary coalition comprising the CDU, CSU and SPD therefore announced its intention to amend this law.⁵⁴⁷

Amending the Passenger Transport Act is no easy task,⁵⁴⁸ however, since conflicts have to be resolved between public passenger transportation and taxi companies on the one hand, both of which have the status of public services, and the economic interests of new providers of transportation services, including some that carry considerable weight such as Uber, on the other. With regard to the possible use of DLT for ridesharing, it is important not to lose sight of the fact that it renders intermediaries obsolete, making it essential for any future licensing requirements to apply not only to large providers but also to drivers. In the future, the latter could conclude transportation contracts with smart contract-based remuneration agreements (as per Section 631 of the German Civil Code) without an intermediary.

8.2.2 Data protection

A DLT-based ridesharing solution intended to eliminate the need for centralized intermediaries will typically require drivers and passengers to directly interact on the blockchain. These will often be natural persons, so processing of their data will be subject to data protection law. Appropriate mechanisms to ensure compliance will therefore be required. Either a "centralized solution"⁵⁴⁹ or an "anonymization solution"⁵⁵⁰ could conceivably be used for this. However, in view of the fact that a DLT platform does not currently appear to be a very promising approach for ridesharing services, there is no need for any further discussion here of how to implement one in a manner that is consistent with data protection.

⁵⁴⁵ Ludwigs, NVwZ, 2017, pp. 1646-1653 (1648).

⁵⁴⁶ BT-Drs. 19/726.

⁵⁴⁷ Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Zeile 2140.

⁵⁴⁸ On possible specific aspects of an amendment, cf. Linke/Jürschik, NZV, 2018, pp. 496-506 (501 ff.).

⁵⁴⁹ On centralized solutions in general cf. section 5.2.3.4.1, on legal foundations section 5.2.4.2.2 and on implementing erasure obligations section 5.2.5.2.

⁵⁵⁰ On anonymization solutions, cf. section 5.2.3.4.2.2.2.

8.2.3 Conclusions and recommendations for action

The current German Passenger Transport Act poses problems for ridesharing. There are plans to amend it, however. In anticipation of DLT, the new law should take into account that both intermediaries and platform operators and agents could eventually become obsolete, making it essential for any licensing requirements to also include drivers.

Ridesharing also poses challenges with respect to data protection law. Since the participants include natural persons, an open DLT solution (at least, without modifications to the architecture) is not an option. Instead, a responsible central entity would have to be created or else direct links between usernames and participants eliminated by means of an anonymization solution.



Amendment of the German Passenger Transport Act and Data Protection

When amending the German Passenger Transport Act, it is important to keep in mind that DLT intermediaries may become obsolete once current technological constraints are eliminated. Licensing requirements should therefore also apply to drivers. Because the participants in ridesharing schemes are natural persons, the DLT architecture will also have to be adjusted to comply with data protection law. Various possibilities for dealing with this are presented here.

9 Platooning

9.1 Economic and Technical Aspects

9.1.1 *Definition and description of the application*

Platooning involves a closely packed group of two or more road vehicles driving in single file. It includes a system for sharing the cost savings that this generates. Accordingly, a "platoon" is a convoy of two or more vehicles that drive together for a generally not previously determined time period over a shared portion of their respective routes.⁵⁵¹ Platooning requires the use of various technologies that typically also play a role in (fully) autonomous driving,⁵⁵² such as distance sensors and automatic control systems for steering wheels, accelerator pedals etc. Platooning also depends on digital infrastructures for coordinating and executing technical processes among the participating vehicles and for implementing (monetary) exchanges. Platooning activities are currently (still) in a precompetitive stage. Competitive implementation is technically conceivable with either a centralized architecture⁵⁵³ in conjunction with an appropriate central coordinating market player or a DLT⁵⁵⁴-based architecture without the involvement of any intermediaries.

Independently of the IT architecture used to implement it, platooning is regarded as a promising approach⁵⁵⁵ that may have considerable potential for implementing major improvements in connection with the steadily increasing truck traffic on Germany's roads.⁵⁵⁶ Truck platooning in particular is regarded as providing opportunities not only to realize significant cost savings but also to improve the safety⁵⁵⁷ and efficiency⁵⁵⁸ of traffic while reducing environmental burdens at the same time.

The economic rationale for combining vehicles in a platoon has to do with the anticipated reduction in expenditures for fuel, personnel (i.e. drivers, especially in commercial applications) and insurance.

⁵⁵¹ Platooning is generally suited for highways, and especially motorways due to the ease of passing on them.

⁵⁵² McKinsey & Company, Lkw-Industrie: Jeder dritte Lastwagen bis 2025 teilautonom.

⁵⁵³ The terms "architecture" and "platform" are defined in the general section.

⁵⁵⁴ DLT (distributed-ledger technology) is described in the general section.

⁵⁵⁵ Deutsches Zentrum für Luft- und Raumfahrt (DLR), Automatisiertes und vernetztes Fahren im Güterverkehr - Auswirkungen auf die Logistikbranche.

⁵⁵⁶ Bundesministerium für Verkehr und digitale Infrastruktur (BMVI), Verkehrsverflechtungsprognose 2030; Sutter/Maibach et al., Finanzierung einer nachhaltigen Güterverkehrsinfrastruktur.

⁵⁵⁷ Up to 90% of all accidents are due to human error (Janssen/Zwijnenberg et al., Truck Platooning: Driving the Future of Transportation.

⁵⁵⁸ It is regarded as possible that the capacity of existing roads could be doubled. (Flämig, Autonomes Fahren, 2015, pp. 377-398.

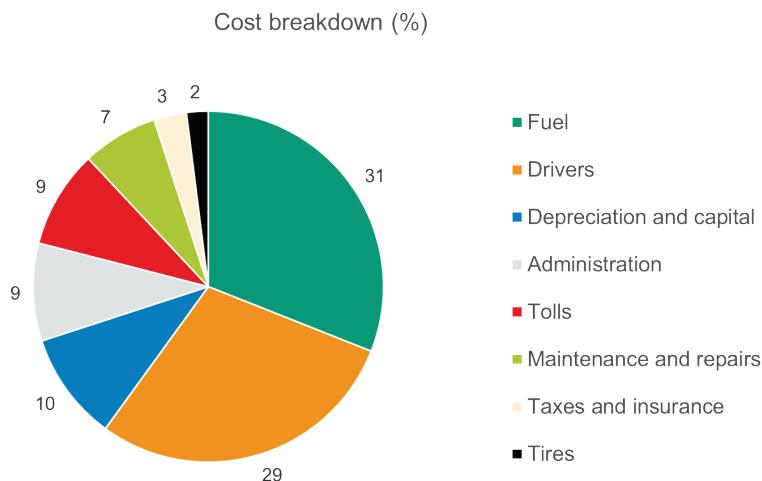


Figure 14: Cost breakdown for road haulage companies⁵⁵⁹

The prospects for improving fuel economy are especially promising, in terms of both magnitude and immediacy. The vehicles following the lead vehicle consume less fuel as a result of reduced wind resistance; this is commonly referred to as drafting, slip-streaming or tailgating. Surprisingly, even the vehicle heading up the convoy can cut down on fuel consumption as a result of reduced turbulence, although this effect is considerably less pronounced. It is only possible to estimate the magnitude of potential savings, since it depends on the spacing and speed of the vehicles, among other factors. Parameters such as road and environmental conditions (paving, temperature, elevation and slope) also have to be taken into account. Various experts predict average savings of around five percent for the lead vehicle, roughly 10% for the last vehicle of a platoon, and about 15% for the vehicles in the middle.⁵⁶⁰ Trials conducted by the company of Scania have shown, for example, that truck platooning can potentially generate savings of up to 12%.⁵⁶¹

The following back-of-the-envelope calculation of fuel savings shows that platooning has considerable potential for delivering economic and environmental benefits. Each year, trucks travel a total of about 35 billion kilometers on toll roads.⁵⁶² If all routes were driven in platoons of two vehicles (which actually overstates the potential, since it is not feasible to form such small platoons on sparsely traveled roads at night, and also overestimates the number of leading (and following) vehicles, which reduces the estimated fuel saving per vehicle), it appears plausible that an average fuel saving of 10% could be achieved on half of the mentioned 35 billion kilometers. At today's typical diesel fuel prices of around 1.30 euros per liter⁵⁶³ and average consumption of 30 liters per 100 km, the potential total saving in Germany is on the order of

⁵⁵⁹ Schwerberger, Cross Innovationen im KV: Platooning 2017.

⁵⁶⁰ Tsugawa, Energy ITS: What We Learned and What We should Learn.

⁵⁶¹ Scania, Platooning saves up to 12 percent fuel.

⁵⁶² Bundesamt für Güterverkehr (BAG), Entwicklung der gefahrenen Mautkilometer in Deutschland von 2005 bis 2017 (in Milliarden Kilometer).

⁵⁶³ <https://de.statista.com/statistik/daten/studie/779/umfrage/durchschnittspreis-fuer-diesekraftstoff-seit-dem-jahr-1950/>

$$35 \text{ bn km} \times 50\% \times 10\% \times \frac{30 \text{ l}}{100 \text{ km}} \times 1.30 \frac{\text{€}}{\text{l}} \approx \text{€}683\text{m}$$

However, it remains to be seen whether the hoped-for fuel savings will actually be as large as manufacturers and scientists predict. At the CES technology trade show in Las Vegas in January 2019, Daimler Trucks announced that past estimates of expected fuel savings had turned out to be inaccurate⁵⁶⁴ and it had therefore decided not to pursue this business model any further. Instead, the company plans to focus on developing autonomously driving trucks further to SAE level 4 to enable platoons of two so that the driver of the second vehicle can rest during the trip.⁵⁶⁵ The potential of this approach is explained in greater detail in the paragraph after next.

Diminished fuel consumption also reduces CO₂ emissions.⁵⁶⁶ This is a major benefit, since trucks account for a large share of emissions caused by road traffic. In the EU, about six percent of all emissions and roughly a quarter of the CO₂ emitted by road vehicles come from heavy commercial vehicles like trucks and buses.⁵⁶⁷ To get an idea of how platooning could curb CO₂ emissions in Germany, like in the calculation above it is assumed that 10% less fuel would be consumed on half of the 35 billion kilometers that trucks travel on toll roads. In addition, according to information provided by the German Association of the Motor Vehicle Industry, 2.65 kg of raw CO₂ are emitted for every liter of diesel fuel consumed⁵⁶⁸ (without considering the effect of catalytic converters etc.). This means that, with average fuel consumption of 30 liters per 100 km, about 1.39 million tonnes of CO₂ emissions can be prevented each year.

$$35 \text{ bn km} \times 50\% \times 10\% \times \frac{30 \text{ l}}{100 \text{ km}} \times 2.65 \frac{\text{kg}}{\text{l}} \approx 1.39\text{m tonnes}$$

Apart from cost savings for fuel and the positive effect on CO₂ emissions, it is frequently noted that electric vehicles could also increase their range as a result of energy savings. Increased range has been identified as one of the key prerequisites for advancing electromobility.⁵⁶⁹

Personnel costs can be reduced in truck platooning with the aid of automated support systems, which are already sufficiently advanced to enable such a high degree of autonomy that the driver of a following vehicle in a platoon could theoretically use the time to rest or engage in other activities instead of steering. The resulting greater flexibility could open up new possibilities for drivers to plan upcoming logistical activities such as unloading and the return trip. If plans change, the driver could also communicate with the dispatcher or use the time to prepare required electronic documents for handover of merchandise at the destination.⁵⁷⁰ This aspect is regarded as one of the most important drivers of cost savings. It is probably also the one that will take the longest to implement, since certain technical and legal prerequisites have to be met. In

⁵⁶⁴ This is apparently due to the additional acceleration and braking required to let cars drive into and out of the gaps between the trucks of a platoon, for example when entering or exiting the motorway.

⁵⁶⁵ Hoffmann, Paukenschlag aus Las Vegas.

⁵⁶⁶ Scora/Barth, Comprehensive Modal Emissions Model (CMEM).

⁵⁶⁷ Europäische Kommission, Vorschlag für eine Verordnung europäischen Parlaments und Rates zur Festlegung von CO₂-Emissionsnormen für neue schwere Nutzfahrzeuge.

⁵⁶⁸ Deutsche Handwerkszeitung, Kraftstoffverbrauch: So viel CO₂ stößt Ihr Auto aus.

⁵⁶⁹ Mellinger/Vliet et al., Transportation Research Part D: Transport and Environment, 2018b, pp. 101-115.

⁵⁷⁰ Reus, Interview: Platooning wird Nerven und Kraft der Fahrer schonen.

particular, current German law forbids drivers of following vehicles in a platoon to use the time to rest.⁵⁷¹ Studies have also cast doubt on whether drivers could actually relax during a platooning trip, since they have to be ready to intervene or take over at any time, calling for a level of concentration comparable to what is required when actually driving. It is safe to assume, however, that once the technology matures sufficiently it will no longer be essential for drivers to be constantly alert and ready to go into action at a moment's notice.

Another potential benefit of platooning is greater traffic safety as a result of using support systems to automatically maintain the right distance between vehicles and regulate their speed. In general, support systems can respond to unexpected events faster than human operators, thus preventing rear-end collisions etc.⁵⁷² The resulting reduction in serious traffic accidents could, over the long term, not only decrease the number of injuries and fatalities but also bring down insurance premiums. Current insurance models that also apply telemetric data for calculating rates anticipate such a trend.⁵⁷³ However, the financial savings from lower insurance premiums will definitely be less than those from the other benefits of platooning, considering that insurance payments currently only account for less than a tenth of trucking companies' costs.⁵⁷⁴

9.1.2 Status quo and challenges

The European Truck Platooning Challenge, organized by the Netherlands in 2016 to promote platooning, demonstrated the technical feasibility of truck convoys under realistic conditions.⁵⁷⁵ Six European truck manufacturers—Daimler, MAN, DAF, IVECO, Scania and Volvo—formed truck platoons that drove via different routes to the Port of Rotterdam. For the most part, they drove during daylight hours under normal traffic conditions. R&D projects in Germany are currently also testing truck platooning under realistic conditions. One example is a project promoted by the Federal Ministry of Transport and Digital Infrastructure. Called "Electronic Platooning – Digital Innovation EDDI", it is being conducted in cooperation with MAN and DB Schenker and involves tests on the A9 motorway between Munich and Nuremberg

It should be stressed, however, that the mentioned initiatives have only tested platooning on a precompetitive basis. The commercial success of this technology depends to a large extent on enabling trucks to form "mixed platoons" independently of their owners (e.g. trucking companies) and manufacturers. This is based on the realization that, for economic reasons (i.e. whether additional investments, e.g. for sensor systems, pay off), platoons will only be sufficiently often if the involved players are able to agree on a technology and/or standard that permits any truck to form or join a convoy with any other truck or trucks. This ability is regarded as essential by those in charge of numerous research and development projects, despite the fact that it has not yet been possible to implement it. This problem was also acknowledged in the EU document "On the

⁵⁷¹ See the legal section for more information.

⁵⁷² Alam/Besselink et al., jurisPR-BKR, 2015, pp. 34-56.

⁵⁷³ For example <https://emil.de/>, EMIL Deutschland AG, Wer wenig fährt, sollte wenig zahlen.

⁵⁷⁴ Schwerberger, Cross Innovationen im KV: Platooning 2017..

⁵⁷⁵ Alkom/Vliet et al., European Truck Platooning Challenge.

road to automated mobility: An EU strategy for mobility of the future",⁵⁷⁶ which led to the ENSEMBLE initiative for advancing communication protocols for multi-brand truck platooning.⁵⁷⁷

In platooning, the trucks can, for example, communicate via a Wi-Fi link based on the IEEE 802.11p standard⁵⁷⁸ for their support systems to exchange sensor data on the positions and speeds of surrounding vehicles. Technically speaking, semi-automated driving in a platoon (with SAE level 4 automation of trailing vehicles) requires protocols for trucks to communicate with one another and surrounding road infrastructure. These must be able to model various maneuvers that may be required during a platooning trip, such as forming and dissolving a platoon. They must also include mechanisms for ensuring safety in traffic situations at all times, both for the truck drivers and for drivers of other vehicles. To make sure that trucks and their proprietary "IT systems can communicate with one another despite the wide variety of different makes and models in use, it is necessary to standardize the communication protocols and interfaces in keeping with the goals of ENSEMBLE. Road markings that are difficult for the support systems to read and interpret, as well as dense traffic and traffic jams, also pose technical challenges. There is a risk that incorrect interpretation of what is going on around the trucks might cause accidents. This calls for advances in automated driving.

So that truck platooning can become reality, however, apart from resolving the described technical challenges it is also important to clarify other economic issues. Economically speaking, there is no incentive to lead a platoon: the savings from reduced fuel consumption are larger for trailing vehicles, and if it should someday become possible to spend less time actually steering vehicles, the lead truck and the company it belongs to will not benefit from this either. If trucks of one company lead platoons more often than those of other enterprises, it will be at a competitive disadvantage compared to rivals that travel further back in the platoon and therefore experience greater cost savings. Regularly taking turns in the lead, as is usual in bicycle racing, appears to be complicated and can even reduce fuel savings or, worse, interfere with the flow of traffic. The logical answer would appear to be a system of monetary incentives for compensating the lead truck for the cost savings it sacrifices. This in turn calls for a suitable settlement system.

In such a scenario, the obvious solution would seem to be a centralized platform that serves as an intermediary between the individual trucking companies. Like on other digital platforms such as Airbnb, this intermediary would regulate the interplay of the independent competing participants. In so doing, the intermediary ensures that all of them obey a fixed set of rules (for calculating compensatory payments and ensuring that they are made) that, ideally, adds value for all of the involved user groups. The business model of the platform itself is based on charging the participants utilization fees, as a rule in the form of transaction fees, for interactions that take place over the network.

⁵⁷⁶ Europäische Kommission, Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran.

⁵⁷⁷ Cordis, ENSEMBLE: Enabling Safe Multi-Brand platooning for Europe.

⁵⁷⁸ Bergenhem/Hedin et al., Procedia - Social and Behavioral Sciences, 2012, pp. 1222-1233.

It is possible that other, independent solutions will evolve, with each of them assuming a platform role of this kind. In the long term, however, it is to be expected that only a few, or just one, technologically superior (or market-dominating) solution will prevail. The reason for this is that the benefits of a platform crucially depend on so-called network effects. In this case, this means that the overall savings a given participant can expect will initially grow disproportionately faster with each additional participant that joins, because this also increases the probability that they can all form and operate platoons.

The problem with this is that, in the long term, individual platforms develop into monopolistic providers and, as experience in other areas has shown, take advantage of their dominance to erect barriers to the market entry of new competitors or raise the fees for using the platform so far that they no longer maximize the welfare of the individual participants (see the general economic section or the section on ridesharing).

Particularly in the case of B2B, manufacturers and/or road haulers must fear a world in which a platform operator, of which direct competitors may also own (considerable) shares, comes to dominate the market. Analyses by consultancies⁵⁷⁹ express the expectation, in agreement with the observations in the general part of this study, that both vehicle manufacturers and technology corporations will vie for the central role of platform operator.

9.1.3 Possible solutions and the role of DLT

As already explained, a central platform potentially constitutes a solution to the fundamental problem of how to settle payments among mutually mistrustful players in the case of truck platooning. In this case as well, DLT appears to be a good way to prevent the formation of a monopoly, as discussed in the general section.⁵⁸⁰ To enable a differentiated analysis of the possibilities for its use, at this point a distinction will be made between two different versions of platooning: planned platooning and ad hoc platooning.⁵⁸¹ These differ in terms of their degree of spontaneity and the amount of trust that DLT can create. In planned platooning, the bringing together of various vehicles to form a platoon is planned in advance of the actual platoon trip itself.⁵⁸² In this type of platooning, in contrast to ad hoc platooning, the individual parties have less need to establish mutual trust because they already know one another and may even be able to work out how to distribute the costs and savings in advance of the platoon trip and possibly even record this modus operandi in a smart contract or offline payment channel. In the case of ad hoc platooning, a platoon is formed spontaneously at short notice without prior planning. Ad hoc platooning therefore presupposes a greater need for trust, since the costs and savings must be distributed without agreeing in advance on the particulars.

Participants stand to benefit from DLT particularly for reciprocally settling their respective compensations. In addition to impeding the formation of a monopoly, it has the advantage of permitting automated real-time settlement of microtransactions without

⁵⁷⁹ Nowak/Viereckl et al., The era of digitized trucking Nowak/Viereckl et al., The era of digitized trucking

⁵⁸⁰ See also the example application of a “neutral platform”.

⁵⁸¹ Bhoopalam/Agatz et al., Transportation Research Part B: Methodological, 2018, pp. 212-228.

⁵⁸² Ibid.

the need for subsequent clearing, thanks to its peer-to-peer structure. Real-time settlement presupposes continual Internet access. On German roads, however, it can also be absent for long periods of time. This theoretically opens up the possibility that new platoons could form during offline phases without the rear vehicles making payments (when Internet access is restored). During the offline phases it may not be possible to verify whether a vehicle in back is solvent. However, it should be stressed here that this fraud scenario is purely theoretical, since it would require a great deal of effort and, when small sums are involved, probably not be worthwhile. There are also various ways to technically avoid this problem.



Expansion of Broadband Services

Intelligent expansion of the Internet and improved accessibility would greatly increase the chances of implementing various (economic) applications for DLT. The case of platooning vividly presents the advantages of omnipresent, high-speed Internet access, which makes it possible to consistently and efficiently execute all of the involved processes. Blockchain, as a manifestation of DLT, is based on the Internet, which in turn depends on telecommunications networks. Promising DLT projects are particularly likely to materialize in highly digitalized sectors. Expectations in connection with targeted support for projects should be guided by this fact. Where DLT is concerned, attention should focus on areas that have already been (or could be easily) digitalized to keep the threshold for its introduction as low as possible while maximizing potential benefits.

Planned platooning, for example, can avoid this issue with the aid of so-called offline channels: if the platoon is planned sufficiently in advance, a smart contract can be written into the DLT and, if there is Internet access, written into a smart contract before it starts. This would involve freezing a certain sum (escrow contract). If a transaction that has been digitally signed by both platooning participants is then sent to the address of this smart contract, the appropriate fraction of a token or amount of cryptocurrency is transferred to the participant concerned. This ensures that the lead vehicle, as a result of the rear vehicle regularly signing platooning data or corresponding transaction claims, receives a guarantee of fair compensation, also offline. In view of the large number of trucks (more than 100,000) using Germany's roads, it is essential to make sure that a technical solution of this kind is sufficiently scalable. This also highlights the fact that road traffic is especially prone to unexpected delays, making planned platooning, i.e. based on an agreement concluded well in advance, challenging to organize. Although it is overall technically relevant, in actual practice its role will be minor.

Ad hoc platooning should be able to overcome this weakness and permit the formation of platoons without a lead time (i.e., in "real time") by giving the participants a guarantee that they will also receive ad hoc compensation payments. The following discussion is therefore restricted to the case of ad hoc platooning. This platooning type is hypothetically also vulnerable to the above-mentioned fraud scenario, but there are various ways to prevent it from happening. For example, each participant could be required to keep a certain minimum sum in their account, or reputation mechanisms

could be implemented. Owing to the low economic relevance of this scenario, no further attention will be paid to it. Regarding the prerequisites of spontaneity, scalability, and low transaction costs, a DLT system that permits feeless microtransactions and high scalability is a good choice. The Berlin-based IOTA Foundation,⁵⁸³ for example, is studying a protocol of this kind. A technology of this kind would be an apt approach for enabling settlements in connection with ad hoc platooning.

A sensible figure for the number of kilometers driven in both platooning cases (with long-term planning and ad hoc) without changing positions is around 100 km. For the entire distance, this yields transactions amounting to approximately (assuming fair distribution of platooning revenues, i.e. both participants receive 50% of the savings achieved by the rear vehicle):

$$100 \text{ km} * 10\% * 30 \frac{l}{100 \text{ km}} * 1.30 \frac{\text{€}}{l} * 0.5 = \text{€}1.95$$

For longer platoons, e.g. consisting of five vehicles, the typical distance traveled without changing the constellation (at least in the case of ad hoc platoons), will be shorter (by about a factor of 5). At the same time, each following vehicle must only pay a fraction of the total compensation for the lead vehicle (1/4 of the saving in each case). The amount of the transaction will then be significantly less than the value above, namely by about 10 euro cents. It is essential for the transaction costs to be sufficiently small so that such a transaction is also worthwhile.

9.1.4 Process description

In the following, the principal phases of ad hoc platooning with settlement of payments via a DLT infrastructure are briefly presented. For the sake of simplicity, the descriptions are limited to the case of a two-truck platoon. As a rule of thumb, they can be extended to longer platforms by treating a platoon of a given size as a unit and iteratively adding one more truck at a time.

1. *Platoon search and contract conclusion:* A vehicle or its driver can generate a platooning bid either completely automatically or using an app while offering to be the lead or trailing vehicle. This can take the form of an "invitation to bargain" (*invitation ad offerendum*) or a binding offer. Alternatively, existing offers to platoon can be addressed to other trucks within the range of its own local Wi-Fi. Identification must then take place in the sense of linking the company or truck to the address assigned in the DLT system. In addition, an agreement must be reached on how to calculate the compensation payment, for example by bilaterally negotiating parameters such as speed, spacing etc. or by setting a flat rate (euros/km). Analogies to ridesharing can be drawn here, since in a certain sense this involves a local, free "marketplace" or ecosystem in which apps can negotiate and conclude formal agreements with one another. It has been observed that in the proprietary systems of vehicle manufacturers, "calculation and invoicing of the value added by a platoon [are] of-

⁵⁸³ IOTA Foundation, IOTA.

ten opaque and hard for users to understand".⁵⁸⁴ This problem does not have to occur in a DLT-based implementation.

2. *Coupling*: The platoon is formed: the two trucks position themselves one in back of the other and begin exchanging sensor data that are crucial for actual platooning and/or calculating the compensation as agreed, such as speed or spacing. The vehicles drive in this formation and gradually travel the agreed distance before swapping positions.
 - a. *Driving together* (leading and following): Sensor data continue to be continuously exchanged to ensure the platoon's safety in traffic. Transparency and provability can be ensured in the event of a later dispute by signing and temporarily storing sensor data locally prior to transmission. There is presumably no point in storing these data (also as hash values) in the blockchain, since in the event of an accident any disputes would only involve the most recently exchanged data. For compensation received, at certain contractually specified intervals (or possibly not until the end of the platooning phase) the system of the trailing vehicle signs transactions with the lead vehicle and sends them to it. These can be sent to the DLT either immediately (if there is Internet access) or later (if not) and—provided the corresponding account has sufficient funds—executed. It may occasionally be necessary to increase the distance between the vehicles to let cars in or respond to a changing weather situation.
3. *Uncoupling*: If, when the platoon has arrived at the arranged location, another vehicle wants to join or the platoon needs to end earlier than planned, e.g. because the lead driver does not meet the expectations of the driver in second place or because the second driver has not met his promises (in the sense of not signing transactions), the platoon must end. Manually as in (1) or automatically, a command is given for the vehicles to uncouple and the spacing of the trucks is increased to the normal minimum distance prescribed by the German Road Traffic Regulations (Straßenverkehrsordnung). If the driver of the trailing vehicle has engaged in other activities while traveling in the platoon (to the extent permitted by law), the system must check whether that driver has regained full control over his vehicle.

After the fourth phase, final settlement may take place or, as soon as an Internet connection is reestablished, the backlog of transactions uploaded to the DLT system. Apart from that, both vehicles are now free to join new platoons or leave the motorway. If a driver has violated the contractual terms (by not paying), his vehicle's license plate number can be used to take legal action.

9.1.5 Conclusions and recommendations for action

As already indicated, both the physical formation of platoons and communication between participating vehicles are currently being tested independently of DLT. A DLT-based solution can make it possible for mutually unfamiliar market players to fully automatically make fair compensatory payments to one another without the need for a

⁵⁸⁴ Sänn/Richter et al., Wirtschaftsinformatik & Management, 2017, pp. 60-71.

central third party to act as intermediary, while enjoying adequate safeguards against fraud. In addition, ongoing documentation of driving mistakes or technical problems of the vehicles in a platoon could ensure their verifiability for clarifying liability issues. DLT can thus generate the trust required for the lead vehicle to count on receiving fair compensation for services provided, also when forming a platoon with direct competitors (i.e. trucks of other road haulage companies). This last aspect will probably be crucial for enabling the breakthrough of platooning technology. It could, for example by speeding up the standardization process for car-to-X communications and the development of highly automated vehicles, encourage technological advances while simultaneously increasing the potential for adding value as described above, mainly in the form of fuel savings, less time spent steering (eventually), and lower insurance premiums.

In practice, the compensation payments made for platooning will be in the range between a few cents and several euros. In Germany as a whole, they will add up to a high three-digit or low four-digit sum per second. Due to the large number of trucking companies (around 15,000 in Germany alone⁵⁸⁵), a DLT-based solution would tend to resemble a public blockchain in terms of performance and efficiency. Further efforts are therefore required to develop a DLT technology with the scalability needed to process a five-digit number of nodes while keeping transaction costs very low. In addition, DLT raises not only legal questions but also ones of a general nature. These are addressed in the following legal section.



Promotion of International Standardization

Efforts must be made to advance the international standardization and acceptance of electronic documents, especially as regards the use of DLT in connection with shipping documents. Today's supply chains and logistical operations typically involve multiple countries, making it important for Germany to leverage its role as an exporting nation that is playing a pioneering role in introducing the required changes.

9.2 Legal Discussion

Platooning, both per se and in the context of DLT, touches on many areas of law, although the focus is on road traffic law, contract law, and data protection owing to their direct practical relevance. These are addressed in greater detail in the following.

9.2.1 Road traffic law

Currently, trucks weighing over 3.5 tonnes that travel at speeds faster than 50 km/h are required by Section 4, Subsection 3 of the German Road Traffic Regulations (StVO) to maintain a minimum distance of 50 meters from the next vehicle. So unless a special permit is obtained (allowed by Section 46), on German roads it is not currently possible to save fuel or reduce steering time by driving in the slipstream of a preceding truck.

⁵⁸⁵ Statistisches Bundesamt, Anzahl der Speditionen in Deutschland in den Jahren von 2009 bis 2016.

Before making adjustments to this rule, however, in case there are distance checks by the police it is also necessary to find a way to make it quite clear, without leaving any room for doubt, whether or not a given truck is driving in a platoon. A solution could be provided by Section 63a, Subsection 1 of the German Road Traffic Act, which requires information to be stored on places and times when drivers in a platoon relinquish control over their vehicles. However, although Section 63a, Subsection 2, Sentence 1 permits these data to be provided to state-level authorities for investigating traffic violations, it is still unclear who exactly these data must be provided to⁵⁸⁶ and where they should be stored,⁵⁸⁷ among other things.

From a traffic safety perspective, it must also be asked whether it is acceptable to interpret driving in a platoon as constituting a break in the sense of Article 7, Paragraph 1 and Article 4, Letter d of Regulation (EC) No. 561/2006, considering that the driver of a vehicle equipped with a highly or fully automated driving function is required by Section 1b, Subsection 1 in conjunction with Subsection 2 of the German Road Traffic Regulations to remain sufficiently alert at all times in order to be able to immediately resume steering the vehicle whenever required, which could rule out the breaks required by Article 4, Letter d of Regulation (EC) No. 561/2006.⁵⁸⁸ However, it could possibly be recognized as a break, since Article 8, Paragraph 8 of Regulation (EC) No. 561/2006 only explicitly requires the vehicle to be stationary.⁵⁸⁹

9.2.2 Contract law

Smart contracts enter into consideration for financially balancing the efficiency gains that vehicles driving in a platoon achieve by reducing fuel consumption and steering times. They involve (payment) software that is stored across a large number of computers in a P2P network (DLT platform or blockchain).⁵⁹⁰ The input values required for calculating a balancing sum, such as fuel consumption, GPS data etc., are processed off-chain (i.e. in the platoon) for data protection reasons.⁵⁹¹ On-chain (i.e. on the DLT platform), merely a (micro-)transaction equal in amount to the balancing sum is executed.⁵⁹² In the following, the contractual basis for executing these transactions is analyzed in greater detail.

9.2.2.1 Conclusion of a contract

Every platoon must be based on a contractual relationship that regulates balancing among the participating parties in a way that does justice to their interests. For example, it must be clear from the outset who drives the lead vehicle and provides the following vehicles with the data they need in order to follow automatically in the lead vehicle's slipstream. It must also be clarified in advance exactly how the payments made by the trailing vehicles to the lead vehicle to offset their fuel savings will be calculated.

⁵⁸⁶ Wagner/Goeble, ZD, 2017, pp. 263-269 (268).

⁵⁸⁷ Brockmeyer, ZD, 2018, pp. 258-263.

⁵⁸⁸ See Fn. 2 in Ylinen, RdTW, 2018, pp. 121-125.

⁵⁸⁹ See Fn. 2 in Ylinen, RdTW, 2018, pp. 121-125.

⁵⁹⁰ On smart contracts in general, see sections 0 and 5.1.1.

⁵⁹¹ On data protection, see section 0.

⁵⁹² See section 9.1.3.

It is unclear how and when these agreements should be concluded. Every contract arises on the basis of at least two coinciding declarations of intent, corresponding to an offer and its acceptance. A declaration of intent constitutes an expression of the will to establish, alter the content of, or terminate a legal transaction. It is therefore necessary to determine which actions or conduct of platoon participants may be regarded as legally relevant expressions of will. Which declarations are made at which points in time depends, first of all, on the circumstances under which a platoon is formed in a given case. There may be a prior agreement between the participating companies and/or drivers (with a planned platoon). In this case, as a rule the relevant declarations of intent will have already been made in connection with concluding said agreement. If ad hoc platoon formation is to be possible, the problem arises that on the routes driven there may not always be a connection to the Internet and thus to the DLT platform.⁵⁹³ The possibility of guaranteeing payments by "freezing" a certain sum beforehand is then not available. Despite this, there may be an interest in using smart contracts to execute payments. In this case, the parties can conclude an agreement that includes both a payment obligation and the obligation to induce settlement payments as soon as an Internet connection is reestablished by sending signed transactions to the smart contract. In ad hoc platoons of this kind, a signal from a vehicle prepared to lead the convoy can initially constitute an offer to an undefined group of persons, which is then accepted by the drivers of the participating vehicles.⁵⁹⁴ A scenario also appears possible in which a potential lead vehicle issues an invitation to submit offers (invitation ad offerendum) by initially merely signaling its willingness to lead the platoon and enter into a corresponding contractual relationship. Other vehicles interested in following it can then reply with their offers, which can be confirmed (= accepted) by the lead vehicle. The respective drivers naturally act as agents of their employers in the sense of Sections 164 ff. of the German Civil Code. The contractual relationship thus does not arise between the drivers personally, but instead between the logistics companies they work for.

This agreement is concluded prior to use of the smart contract for executing balancing payments. The content and effectiveness of the contract therefore legally depend on this agreement and not, for example, on the programming code of the smart contract.⁵⁹⁵

9.2.2.2 Type of contract

There is no clear answer to the question as to which type of contract should be used for platooning. The possibilities include a service contract or a contract to produce a work, but an internal (i.e. civil-law) partnership agreement as defined by the German Civil Code is probably the best choice.

⁵⁹³ See section 9.1.2 on dealing with sporadic Internet connections.

⁵⁹⁴ This possibility is likely to reach its limit at a platoon's technical maximum (in terms of computing power) and legal maximum (i.e. length).

⁵⁹⁵ On smart contracts in general, see sections 0 and 5.1.1.

9.2.2.2.1 Differentiation from a service contract as per Sections 611 ff. of the German Civil Code

A service contract requires exchanging a service for a remuneration. This might apply here in the sense that the driver of the lead vehicle accepts the following vehicles into his slipstream, continually supplies them with driving data, and receives (for example) a flat rate per kilometer in return. In the case of platooning, however, the main priority of all participants is to reduce fuel consumption⁵⁹⁶ and, at some future time, steering times as well. A partnership agreement is better-suited to this shared goal.

9.2.2.2.2 Differentiation from a contract to produce a work as per Sections 631 ff. of the German Civil Code

In view of the just-described goal of a platoon's members, the option of a success-oriented work contract can also be eliminated, since the point of an agreement to form a platoon is not to successfully transport goods.

9.2.2.2.3 Partnership agreement as per Sections 705 ff. of the German Civil Code

The purpose of a partnership agreement is to achieve a common purpose, and it obliges the partners to promote the achievement of this purpose. It does not need to take any particular form and can therefore also be impliedly concluded.⁵⁹⁷ Nor is it necessary for the participants to be aware that they are forming a partnership in accordance with the German Civil Code; their will to legally join forces is sufficient.⁵⁹⁸

9.2.2.2.3.1 Common purpose

The participants' goal of reducing fuel consumption and steering times by teaming up in a platoon is a permitted, durable and self-benefiting purpose, since it is directed at promoting the interests of all of the partners, i.e. the companies behind the drivers.⁵⁹⁹

9.2.2.2.3.2 Obligation to promote the achievement of a common purpose, contributions

In order to achieve the envisaged savings, the driver of the lead vehicle, as already explained, accepts one or more other vehicles into the slipstream behind his vehicle, makes his vehicle continually send them data of relevance to driving such as speed, braking, GSP position and acceleration via Wi-Fi, and otherwise watches over the platoon. The performance of services being acceptable as contributions by a partner as per Section 706, Subsection 3 of the German Civil Code, he or she thus makes the largest contribution to the platoon. In addition, the drivers of all following vehicles contribute to achieving the common purpose by entering the slipstream and completing the platoon. They also provide financial compensation to the lead vehicle.

⁵⁹⁶ Note: A platoon's lead vehicle also saves fuel, although less than the following vehicles driving in its slipstream, because of reduced turbulence in its wake.

⁵⁹⁷ Staudinger/Habermeier, § 705 Rn. 4.

⁵⁹⁸ BeckOGK/Geibel, Stand: 1.1.2019, BGB § 705 Rn. 17.

⁵⁹⁹ Staudinger/Habermeier, 705 Rn. 17 f.

9.2.2.2.4 Position of the partnership toward third parties

Because the sole purpose of the partnership is the internal goal of reducing fuel consumption and steering times, it may be assumed that the partners have no other outwardly directed interest in having their civil-law platooning partnership engage in legal transactions with third parties.⁶⁰⁰ It is therefore safe to assume that the technically justified authorization of the driver of the lead vehicle to manage the partnership's affairs does not extend to representing the partnership toward third parties outside of the platoon, and Section 714 of the German Civil Code will be waived in the partnership agreement.⁶⁰¹

Due to the lack of engagement with third parties, it follows that a civil-law platooning partnership would be a strictly internal partnership devoid of legal capacity.⁶⁰² The relationship of the participants is thus limited to debt balancing among themselves without any additional organization.⁶⁰³

Furthermore, an internal partnership typically has no joint assets.⁶⁰⁴

When financial balancing among a platoon's members takes place via a DLT-based smart contract, the latter executes the payments fully automatically provided that the instructions from the platoon vehicles match. It is not the partners' will for the tokens used for this purpose to constitute joint assets, since the smart contract is only intended to serve as the virtual escrow agent of each of the platoon members.

The fact that balancing instructions are sent from the vehicles to the DLT platform could imply joint assets and external civil-law partnership, since the platoon is visible from the outside in this respect. To avoid liability risks here, it would be advantageous for the transfer of balancing requests to the smart contract to coincide with the dissolution of the platoon (i.e. direct liquidation of the civil-law partnership). Alternatively, the platoon's members could agree among themselves on joint assets that would be held in rem, for example by the lead vehicle, which would outwardly act under its own name.⁶⁰⁵ This would also be advantageous for settlements in the event that a participant leaves a platoon consisting of multiple vehicles sooner than expected. Apart from this, the fact that the lead vehicle separately and bilaterally settles with each other vehicle is evidence against joint assets and an external civil-law partnership. For liability reasons, an internal civil-law partnership is preferable, because it, as already explained, does not perform any actions with legal consequences and therefore cannot be held accountable for violating legal obligations to do or refrain from doing anything, which also eliminates its liability.⁶⁰⁶

⁶⁰⁰ MüKo BGB/Schäfer, § 714 Rn. 8.

⁶⁰¹ Staudinger/Habermeier, § 714 Rn. 7.

⁶⁰² Palandt/Sprau, § 705 Rn. 33; MüKo BGB/Schäfer, § 705 Rn. 279.

⁶⁰³ BeckOK BGB/Schöne, 47. Ed. 01.08.2018, § 705 Rn. 159.

⁶⁰⁴ In MüKo BGB/Schäfer, § 705 Rn. 277 this is also regarded as a prerequisite for an internal partnership, despite the fact that it is disputed whether an internal partnership can also have joint assets. Cf. MüKo BGB/Schäfer, § 705 Rn. 280 ff.

⁶⁰⁵ MüKo BGB/Schäfer, § 705 Rn. 280.

⁶⁰⁶ MüKo BGB/Schäfer, § 714 Rn. 8.

With regard to the partners' liability⁶⁰⁷ within the scope of their internal relationships with one another, the principle of contractual freedom takes precedence.⁶⁰⁸ The members of a platoon can therefore freely conclude agreements to restrict or eliminate liability, e.g. in connection with their financial balancing obligations.

9.2.2.2.5 Departure of a partner

Depending on where trucks are loaded or unloaded, a platoon can lose one or more vehicles at any motorway exit. Leaving the platoon could constitute a classic termination in the sense of Section 723, Subsection 1 of the German Civil Code. Assuming that a civil-law platooning partnership will usually be formed for a certain length of time, for example for the duration of a trip from Munich to Nuremberg, Section 723, Subsection 1, Sentence 2 of the German Civil Code requires the existence of compelling grounds for termination. If a member has to load or unload somewhere along the way, e.g. in Ingolstadt, it would be impractical and ineffective to require him to first continue driving to Nuremberg and then turn around and drive back to Ingolstadt. If the partnership agreement includes a continuation clause based on Section 736 of the German Civil Code, the member concerned would retire from the partnership for good reason. If it is possible to reach a given destination via different routes without any appreciable difference in the required time, it is often likely to be the case that a member will, on the basis of his own experience (number of construction sites, traffic jams, frequency of accidents, landscape etc.), have a different preference than the driver of the lead vehicle. On the basis of a purely objective assessment, this is highly unlikely to constitute a compelling reason for leaving the platoon. However, it has to be possible for a truck to flexibly leave a platoon for purely economic reasons, for example because the dispatcher has arranged for it to take on an additional load elsewhere at short notice.

To ensure this flexibility, it is essential for the partnership agreement to accommodate departures from the platoon and ensure its continuation with the remaining vehicles afterward.⁶⁰⁹ If only one partner is left after the departure of another, the partnership is dissolved without the need for liquidation, due to the lack of joint assets. The smart contract automatically executes the financial settlement with the departure of the last following vehicle. This closely corresponds to the idea underlying Section 721, Subsection 1 of the German Civil Code, which describes the distribution of profits and losses after dissolution of a partnership. If settlements are already continually performed for every kilometer traveled, despite this not being practical, this provision would have to be waived to preserve fundamental personal freedoms.⁶¹⁰

9.2.2.2.6 Joining of a new partner

It follows from the principle of contractual freedom and Section 727, Subsection 1 of the German Civil Code, according to which a partnership is not dissolved upon the death of a partner if its agreement states otherwise, that at any time an additional

⁶⁰⁷ Acc. to the German Road Traffic Regulations (Straßenverkehrsordnung), the vehicle's driver or keeper is liable for accident-related damages, also in the case of a following vehicle that is driving completely automatically (Section 1b, Subsection 4).

⁶⁰⁸ MüKo BGB/Schäfer, § 705 Rn. 133.

⁶⁰⁹ Staudinger/Habermeier, § 736 Rn. 5.

⁶¹⁰ Staudinger/Habermeier § 721 Rn. 3.

following vehicle can join an existing platoon if it concludes an admission agreement with the existing members.⁶¹¹ In the partnership agreement, the platooning participants can create an obligation to accept additional following vehicles and authorize one partner, who in practice will be the driver of the lead vehicle, to conclude any admission agreements with them.

9.2.2.7 Replacement of a partner

It is also possible to replace a platoon member with another. This can be accomplished either with a double agreement, i.e. the departing and entering partners each conclude an agreement with the other partners without giving rise to a direct legal relationship between the departing and entering partners, or else the switch is made by transferring the departing member's share to the new member in accordance with Sections 398 and 413 of the German Civil Code. The second possibility appears less likely due to the interactions with the smart contract and the settlements executed by it.

9.2.2.8 Liquidation

In the case of an inwardly directly civil-law platooning partnership without joint assets, there is no room for winding it up in accordance with Sections 730 ff. of the German Civil Code.⁶¹² If only the lead vehicle remains in a platoon, the partnership is dissolved, which equates to its complete termination.⁶¹³ The continued existence of the partnership is not a prerequisite for internal settlement. In fact, the participants' postcontractual obligations include bringing about the settlement,⁶¹⁴ which is executed by the smart contract.

9.2.2.3 Malfunctions and unwinding of transactions

The use of smart contracts that is considered here is only for the purpose of balancing out the benefits that the members of a platoon derive from its use. If the software for calculating the settlements works flawlessly, remuneration is only made for cost savings that have actually been achieved. Poor performance as such, for instance in the form of insufficient participation in the platoon, is therefore not considered.⁶¹⁵ It is possible, however, that technical problems or discrepancies between agreed and programmed content could result in payments that are too low or too high. In such a case, the difference must be paid if too little was received (in lieu of fulfilling existing primary claims) or returned if too much was received (to avoid unjust enrichment). Rescission issues also arise in the event that the concluded contract is voided, for example after being contested. In this connection, the reader is referred to the general discussion of smart contracts in section 5.1.1.

⁶¹¹ Jauernig/Stürner, § 737 Rn. 10.

⁶¹² MüKo BGB/Schäfer, § 730 Rn. 12.

⁶¹³ BeckOGK/Koch, § 730 Rn. 50.

⁶¹⁴ MüKo BGB/Schäfer, § 730 Rn. 2.

⁶¹⁵ Liability for technical malfunctions of vehicles etc. is not blockchain-specific and therefore not covered by this study.

9.2.3 Data protection

When using a DLT platform to execute transactions in connection with platooning, special attention must be paid to data protection laws. The affected persons are primarily the users of the blockchain application. In the case of platooning, the application will be used by trucking companies. A distinction must be made on the basis of whether knowledge of a trucking company can also be used to obtain or derive information on natural persons behind it. If this is not the case, processing of the users' data has no relevance under data protection law, and a DLT platform can be used to execute transactions within the scope of platooning.

The situation is more problematic if information about a trucking company can be used to reveal information on natural persons behind it. Besides the managing directors or owners of smaller companies, these can also be drivers of larger trucking companies, to the extent that they can be deduced from the activity of a username. If the participation of trucking companies that meet these conditions cannot be ruled out, then processing of usernames on the blockchain falls under data protection law. In this case, use of the blockchain must be modified in order to comply with legal requirements. In doing so, a distinction must be made between exchanging driving data for determining the balancing payments due and exchanging data for actually making the payments.

9.2.3.1 Exchange of driving data

Data for determining the balancing payments among a platoon's members can be exchanged locally between the participating trucks. While doing so, the data can also be evaluated by smart contracts to calculate the compensatory payments that are due. If a temporary blockchain is created for this purpose, it can be managed as an "open solution"⁶¹⁶ among the platoon's members. All of them then share responsibility for the data processing done. The data processing operations are limited to the time period during which that specific platoon existed. Data may only continue to be stored after the platoon has ceased to exist if and only as long as they are required for evidentiary purposes. All of the platoon's members delete data as soon as they are no longer need for calculating the balancing payments.

9.2.3.2 Exchange of data for executing the balancing payments

The balancing payments themselves may not be made on the local blockchain, however. If it is also wished to execute them on the basis of DLT, the technology used for this must include a solution for ensuring compliance with data protection law, to the extent that it would otherwise be possible to draw conclusions about the natural persons behind the participating trucking companies. An open solution may not be used, since not all participants in the payment system have an interest in all transaction data.

However, it basically appears possible to use a "centralized solution".⁶¹⁷ It would have to involve a permissioned blockchain operated by a central entity. The central entity

⁶¹⁶ On open solutions, cf. 5.2.3.4.2.1.

⁶¹⁷ On "centralized solutions", cf. also 5.2.3.4.2.1.

can use a system of rights and roles to control which information is visible to which participants. The central entity would be the controller, in the sense of data protection law, for on-chain data processing. A contract concluded between the participants and the central entity could constitute the legal basis for this processing.⁶¹⁸ The central entity must provide suitable erasure methods; these could include, for example, a "redactable blockchain"⁶¹⁹ in which all changes made by the central entity can be stored, or forks⁶²⁰ in which the nodes are required to delete unwanted data from the decentralized database.

If a "centralized solution" is impossible or not wanted, another option is an "anonymization solution".⁶²¹ This would enable off-chain balancing.⁶²² In this case, the participating trucking companies do not enter every transaction in the blockchain; instead, each of them keeps a separate off-chain ledger. The balancing payments among the participants are executed on-chain at regular intervals. Here it is important to avoid any recognizable patterns in the payments that might make it possible to identify the trucking company behind a username or natural persons associated with it. To accomplish this, the companies should only use each username for a single interaction. The possibilities here also include technical anonymization solutions such as zero-knowledge proofs⁶²³ and stealth addresses in combination with ring signatures.⁶²⁴

If anonymization is successful, no more data processing of relevance under data protection law will take place on-chain, and consequently no legal legitimization will be required for it either. Nor will it be necessary to erase any data.

9.2.4 Conclusions and recommendations for action

A nationwide rollout of platooning will require a change to Section 4, Subsection 3 of the German Road Traffic Regulations (Straßenverkehrsordnung), which requires trucks to maintain a minimum distance of 50 meters from the vehicle in front on motorways. First, however, a way must be found for the responsible authorities to reliably tell whether or not trucks are driving closer together because they are in a platoon. It makes sense to use the location and time data that must be stored according to Section 63a, Subsection 2 of the German Road Traffic Act for this, since they permit deduction of the driving mode (manual vs. automatic). Although Sentence 1 permits these to be provided to the authorities, this solution is only a viable alternative if it is specified in greater detail, in particular by defining the addressee and where the data will be stored. The authorizations provided to the German Federal Minister for Transport and Digital Infrastructure by Section 63b of the German Road Traffic Act should be exercised for this purpose.

Legally speaking, it is not entirely out of the question for platooning to be categorized as a break from driving in the sense of Article 7, Paragraph 1 and Article 4, Letter d of

⁶¹⁸ On the legal foundations for a centralized solutions, cf. 5.2.4.2.2.

⁶¹⁹ On redactable blockchains, cf. also 0.

⁶²⁰ For more on forks, cf. 5.2.5.2.2 and 0

⁶²¹ For more on anonymization solutions, cf. 5.2.3.4.2.2.

⁶²² For more on balancing, cf. 5.2.3.4.2.2.2.

⁶²³ For more on zero-knowledge proofs, cf. 5.2.3.4.2.2.2.3 and 0

⁶²⁴ On stealth addresses in combination with ring signatures, cf. 5.2.3.4.2.2.2.4.

Regulation (EC) No. 561/2006. However, it has not yet been conclusively studied whether the obligation of every driver to remain sufficiently alert to immediately resume driving (acc. to Section 1b, Subsection 1 with Subsection 2 of the Road Traffic Regulations) permits genuine recuperation. There is therefore a need for additional research here. Broadly speaking, platooning with DLT-based payment handling is based on an internal partnership.

There are also challenges with respect to data protection law. In many cases, knowledge of companies using the platooning platform can be used to learn about the natural persons behind them (proprietors, drivers etc.). If these are active with a username on a public DLT platform, data processing may take place that falls under data protection law. In these cases, it will be necessary to adjust the architecture. This can be done by implementing a central entity that is able to influence the processing of data (a "centralized solution"). Alternatively, technologies can be used that remove the link between a username and the user's identity (an "anonymization solution").

In case the participants are exclusively companies and it is not possible to draw conclusions about the natural persons behind them, then it is sufficient to dispense with storing personal data in the DLT layer. The information should instead be stored off-chain and linked to the DLT platform by hash values. However, with a solution of this kind it is essential to check the participants in advance to determine whether they meet the above-mentioned requirements. Smaller companies in particular would probably have to be excluded from the system.



Road Traffic Law and Data Protection

The nationwide introduction of platooning in Germany will require a few adjustments to road traffic law (especially Section 4, Subsection 3 of the German Road Traffic Regulations and Sections 63a and 63b of the German Road Traffic Act). In order to also reduce steering times and thus generate additional savings apart from reducing fuel consumption, it needs to be determined whether, despite the obligation of every driver in a platoon to be ready to take the wheel at any time, it is also possible for them to take breaks. Where data protection is concerned, it may be necessary to adjust the DLT architecture in the event that personal data are processed. Various possible solutions for this are presented here.

10 Final Considerations

Distributed-ledger technology, which is still relatively young, is now on its way to market maturity after having passed the peak of the Hype Cycle in 2017/18. At this time—due to its diverse potential applications in the public sector and in business—a large number of public institutions (e.g. the European Blockchain Observatory and Forum, the German Federal Office for Migration and Refugees, and the German Federal Ministry for Transport and Digital Infrastructure), companies (e.g. IBM, Maersk, and BMW), foundations (e.g. IOA, Sovrin, and Share&Charge), and research institutions (e.g. universities and Fraunhofer Societies) are actively developing this technology further, using it, or assessing it from a wide range of perspectives. Yet DLT is not a technology that, if appropriately fostered, could produce a “European champion”, in other words a monopolist with a DLT-based business model. Rather, it is essentially a digital infrastructure. In combination with other key technologies such as artificial intelligence or the Internet of Things, DLT solutions have potential for providing the technological and economic foundations for a plethora of applications. It should be stressed that, as a rule, the reasons for using a DLT solution are not purely technological in nature; a centralized system is typically more efficient than a distributed one. Rather, it is because DLT can digitally support and increase the efficiency of processes for which no central platform has yet become established, for various reasons that include avoiding the risk of monopolies or endangering federalist organizational principles. Especially in fragmented markets like Germany’s, which is characterized by a large number of small and medium-sized enterprises, and also in German and European administrations, DLT has enormous potential—and not just for benefiting individual market players, but also for raising the efficiency and competitiveness of entire industries. It therefore very possibly constitutes a libertarian alternative to purely capitalist societies dominated by a small number of large corporations, state-controlled economies, and centralized digital states. But it also requires, and deserves, special help for getting off the ground. The costs of setting up a DLT system can be considerable, but it does not only confer a competitive advantage on its initiator—it also benefits all other participants. Targeted assistance and startup funding from the state are essential to ensure the critical mass that is typically required for these systems to fulfill their potential and deliver benefits to society and the economy. Ultimately, it is the responsibility of the state to make sure that the advantages inherent in DLT materialize, including prevention of monopolistic structures but also societal aspects such as anchoring European values in a digital infrastructure.

DLT should therefore be regarded as digital infrastructure, not as a disruptive business model *per se*: it is only in conjunction with other technologies that it can unfold its potential and provide a foundation for new business models while boosting efficiency within and across industries.

The unique nature of DLT also poses some fundamental questions. Technically, the issue of scalability has yet to be resolved. The aspects being studied range from approaches for increasing scalability to concepts that reduce the need for it (e.g. sharding, pruning, on-chain and off-chain approaches, hierarchies, and interoperability), and all of these are basically still in their infancy. In view of DLT’s infrastructural character and considerable complexity, moreover, it also needs to be clarified whether it is necessary to rate or certify it.

A great many legal obstacles also remain. To be sure, the use of smart contracts has a sound basis in civil law. Fundamental reservations concerning their rescission are being dispelled, due to the fact that DLT transactions are not identical to the underlying legal transactions. Agreements that integrate smart contracts are not fundamentally different, since the parties to them must also obey the law. The bottom line is that the only real constraints are imposed by the current state of the technology.

Independently of issues in connection with contract law, it is to be expected that greater attention will focus on legitimizing tokens. The principal aspects requiring clarification are rights to tokens, the extent to which they enjoy protection under civil law, and whether there is a need for legislative action here.

Also notable are the data protection challenges associated with the use of DLT. The GDPR assumes the existence of a central controller, while DLT is inherently based on distributed storage of data in a large number of nodes. This contradiction can be partly resolved by appropriately designing a system's architecture. It is becoming clear, however, that it is not feasible to entirely dispense with the use of intermediaries. Coordinating central entities can be tempting targets for those affected by data processing. But the only way for data to be openly exchanged without such central entities while still complying with data protection law is to completely refrain from storing personal data in the DLT layer. This poses formidable challenges. While third-party data can be stored off-chain and linked by means of hash values, data attributable to direct users are still present in the DLT layer in the form of their public keys, at least when the DLT application is used by natural persons or companies backed by natural persons whose identities can be deduced. There is a need to anonymize usernames, which can be accomplished by using them only once and, under certain circumstances, by also employing technical methods such as zero-knowledge proofs. In practice, implementations also have to be protected from misuse. It is worth noting that conflicting interests must be weighed when employing an anonymization solution. A DLT application that ensures the complete anonymity of users also potentially provides opportunities for it to be misused for illegal activities. The interest that governments have in, for example, monitoring payment flows must also be taken into account when choosing an alternative; in cases of doubt, it can tip the scales toward an anonymization solution.

It is also necessary to resolve the conflict between the immutability of DLT on the one hand and the right of affected individuals to demand the correction or erasure of their personal data on the other. A controller can easily make retroactive changes in ordinary databases, but in the case of DLT platforms this is neither possible nor desired. The possible solutions include technically creating a backdoor to permit an authorized individual to make retroactive corrections or, again, simply not storing any personal data in the DLT layer, since this would rule out any later changes.

The four case studies presented cover a wide spectrum of potential uses for DLT. In the cases of electric vehicle charging, ridesharing and platooning, pragmatic use of DLT can increase efficiency and optimize processes. However, the actual savings are either fairly minor or difficult to quantify. The bill of lading case study stands out; it reveals opportunities for achieving enormous improvements and savings with the aid of DLT.

Overall it can be safely assumed that in the near future at least, distributed ledger technology is unlikely to fulfill many of the great expectations that have arisen in connection with cryptocurrencies and all the associated hype. In the long term, however,

many technological hurdles and legal problems will be overcome by technical or legislative solutions. This also makes it clear that an interdisciplinary approach involving cross-company consortia, as well as considerable patience, will be required. The state should realize that it also stands to greatly benefit from distributed ledger technology and therefore take all required steps to promote its use for the benefit of society and business. Otherwise the further evolution of this technology will shift to other countries. Germany optimally meets the social and technological-creative prerequisites for shaping the development of DLT and leveraging its benefits. If Germany and Europe miss this opportunity, there is reason to fear that future advances in DLT will take place elsewhere in other countries and societies, before being ultimately adopted in Europe as well. This would have negative consequences, since it always takes longer to regulate new technologies than it does to develop them in the first place. Regulation typically does not begin until a demand for it arises, in order to provide legal security for our society's creative minds. This can be prevented by providing sandboxes, real-world laboratories, and competent partners at public institutions and ministries. These are essential prerequisites for systematically creating a fertile ground for new ideas and developments to sprout and grow.

Bibliography

Acs, Blockchain Innovation 2018, available at: https://www.ipaustralia.gov.au/sites/default/files/reports_publications/acs-blockchain-report_o.pdf.

Alam/Besselink/Turri/Martensson/Johansson, Heavy-Duty Vehicle Platooning for Sustainable Freight Transportation: A Cooperative Method to Enhance Safety and Efficiency, jurisPR-BKR 2015, 34-56.

Ali/Awad, Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, Sensors (Basel, Switzerland) 2018, 1-17.

Alkom/Vliet/Aarts/Eckhardt 2016 European Truck Platooning Challenge (European Truck Platooning, Hrsg.), available at: <https://eutruckplatooning.com/PageByID.aspx?sectionID=131542&contentPageID=529927>.

Alstyne, Marshall W., Eisenmann, Thomas/Parker, Strategies for two-sided markets, Harvard business review 2006, 92-104.

Ammann, Bitcoin als Zahlungsmittel im Internet, Rechtliche Fragestellungen und Lösungsansätze, CR 2018, 379-386.

Anderson, LADEN2020 Schlussbericht 2016, available at: https://elib.dlr.de/111054/2/LADEN2020_Schlussbericht.pdf.

Andersson/Hjalmarsson/Avital, Peer-to-Peer Service Sharing Platforms: Driving Share and Share Alike on a Mass-Scale, The 34th International Conference on Information Systems. ICIS 2013, 1-15.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, 01248/07/DE 2007, available at: https://www.lda.bayern.de/media/wp136_de.pdf.

Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 00264/10/DE 2010.

Ateniese/Magri/Venturi/Andrade, Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. in: 2017 IEEE European Symposium on Security and Privacy (EuroS&P) 2017, S. 111-126.

Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2nd edition, Munich, 2016.

Baird/Mance/Madsen 2018 Hedera: A Governing Council & Public Hashgraph Network, available at: <https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.0-180313.pdf>.

Bajpai, IBM and Blockchain: What It Did In 2018, And Where It's Going In 2019 2019, available at: <https://www.nasdaq.com/article/ibm-and-blockchain-what-it-did-in-2018-and-where-its-going-in-2019-cm1100102>.

Baliga/Subhod/Kamat/Chatterjee 2018 Performance evaluation of the quorum blockchain platform, available at: <https://arxiv.org/abs/1809.03421>.

Bamberger/Roth/Hau/Poseck, Beck'scher Online Kommentar of the German Civil Code, 48th edition, Munich, 2018.

Bambrough, A Gold Standard Of ICOs Is Needed -- But It Won't Be Easy 2018, available at: <https://www.forbes.com/sites/billybambrough/2018/07/04/a-gold-standard-of-icos-is-needed-but-it-wont-be-easy/#7d652a5b4600>.

Bechtolf/Vogt, Datenschutz in der Blockchain – Eine Frage der Technik, Technologische Hürden und konzeptionelle Chancen, ZD 2018, 66-71.

Beck 2011 Die Finanzkrise ist auch eine Vertrauenskrise (Max-Planck-Institut für Gesellschaftsforschung (MPIfG), Hrsg.), available at: http://www.mpifg.de/pu/ueber_mpifg/mpifg_jb/JB1112/MPIfG_11-12_06_Beckert_Vertrauen.pdf.

Beck/König, Bitcoin: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld, JZ 2015, 130-138.

Beck/König, Bitcoins als Gegenstand von sekundären Leistungspflichten, Erfassung dem Grunde und der Höhe nach, AcP 2015, 655-682.

Beck/Müller-Bloch/King, Governance in the blockchain economy: A framework and research agenda, Journal of the Association for Information Systems 2018, 1020-1034.

Beecher, Can the Electronic Bill of Lading Go Paperless?, The International Lawyer 2006, 627-647.

Begleit- und Wirkungsforschung Schaufenster Elektromobilität, Good E-Roaming Practice: Praktischer Leitfaden zur Ladeinfrastruktur-Vernetzung in den Schaufenstern Elektromobilität 2015, available at: https://schaufenster-elektronomobilitaet.org/media/media/documents/dokumente_der_begleit_und_wirkungsforschung/Ergebnispapier_Nr_5_Good_E-Roaming_Practice.pdf.

Bergenhem/Hedin/Skarin, Vehicle-to-Vehicle Communication for a Platooning System, Procedia - Social and Behavioral Sciences 2012, 1222-1233.

Bernstein/Buchmann, J. (Hrsg.), Dahmen E., Introduction to post-quantum cryptography, Post-Quantum Cryptography 2009, 1-14.

Bernstorff, Das "reine Konnossement" im Seefrachtverkehr und die Ersatzmöglichkeit durch das elektronische "Bolero - bill of lading", RIW 2001, 504-512.

Bertram, Smart Contracts, Praxisrelevante Fragen zu Vertragsabschluss, Leistungsstörungen und Auslegung, MDR 2018, 1416-1421.

Beyerer/Müller-Quade/Reussner, Karlsruher Thesen zur Digitalen Souveränität Europas, DuD 2018, 277-280.

Bhoopalam/Agatz/Zuidwijk, Planning of truck platoons: A literature review and directions for future research, *Transportation Research Part B: Methodological* 2018, 212-228.

Binns/Lyngs/Kleek/Zhao/Libert/Shadbolt, Third Party Tracking in the Mobile Ecosystem, *Proceedings of the 10th ACM Conference on Web Science* 2018, 23-81.

Bitkom, Blockchain und Datenschutz – Faktenpapier Bitkom 2017, available at: <https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf>.

Bitkom, Künstliche Intelligenz 2017.

Blockchain Bundesverband, Blockchain, data protection and the GDPR 2018, available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.

Blockchain Bundesverband Finance Working Group 2018 Statement on Token Regulation with a Focus on Token Sales, available at: http://bundesblock.de/wp-content/uploads/2019/01/180209_Statement-Token-Regulation_blockchain-bundesverband.pdf.

BMVI, Ethik-Kommission: Automatisiertes und Vernetztes Fahren 2017.

BMW Group. 13.02.2019 Blockchain: Developing standards for universal application in the mobility sector, Munich, available at: <https://www.press.bmwgroup.com/global/article/detail/T0291855EN/blockchain-developing-standards-for-universal-application-in-the-mobility-sector?language=en>.

BMWi, Energiekonzept für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung BMWi, BMU 2010.

Böhm (2019, 21. Januar), Google soll 50 Millionen Euro Strafe zahlen, DSGVO in Frankreich, Spiegel Online, available at: <http://www.spiegel.de/netzwelt/netzpolitik/dsgvo-50-millionen-euro-strafe-fuer-google-in-frankreich-a-1249171.html>.

Boom, Certain legal aspects of electronic bills of lading, *European Transport Law (ETL)*, 1997, 9-24.

Borgia, The Internet of Things vision: Key features, applications and open issues, *Computer Communications*, 2014, 1-31.

Brandt, Neue Kryptoprojekte bald so effizient wie Visa 2018.

Brink/Wolff, Beck'scher Online-Kommentar Datenschutzrecht, 26th edition, Munich, 2018.

Brockmeyer, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG, ZD 2018, 258-263.

Bruckner, Organisationales Vertrauen initiieren, Wiesbaden, 2015.

BTC-Echo, Der deutsche Blockchain Index 2018, available at: <https://wwwbtc-echo.de/blockchain-studie-oekosystem-deutschland-2018/>.

Bundesamt für Güterverkehr, Entwicklung der gefahrenen Mautkilometer in Deutschland von 2005 bis 2017 (in Milliarden Kilometer) 2019, available at: <https://de.statista.com/statistik/daten/studie/202642/umfrage/entwicklung-der-gefahrenen-mautkilometer-in-deutschland/#0>.

Bundesanstalt für Finanzdienstleistungsaufsicht, Merkblatt Finanzinstrumente vom 20.12.2011, geändert am 26.07.2018 2011, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_1112_20_finanzinstrumente.html.

Bundesanstalt für Finanzdienstleistungsaufsicht, Virtuelle Währungen/Virtual Currency (VC) 2016, available at: https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel.html.

Bundesanstalt für Finanzdienstleistungsaufsicht, Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs) 2017, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html?nn=11056122.

Bundesanstalt für Finanzdienstleistungsaufsicht, Hinweisschreiben vom 20.02.2018, GZ: WA 11-QB 4100-2017/0010 2018.

Bundesministerium für Verkehr und digitale Infrastruktur, Verkehrsverflechtungsprognose 2030 2014, available at: https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/verkehrsvverflechtungsprognose-2030-zusammenfassung-los-3.pdf?__blob=publicationFile.

Bundesministerium für Verkehr und digitale Infrastruktur, Elektronische Deichsel – Digitale Innovation – EDDI Bundesministerium für Verkehr und digitale Infrastruktur 2019, available at: <https://www.bmvi.de/SharedDocs/DE/Artikel/DG/AVF-projekte/eddi.html>.

Bundesministerium für Wirtschaft und Energie, Grünbuch Digitale Plattformen 2016, available at: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/gruenbuch-digitale-plattformen.pdf?__blob=publicationFile&v=20.

Bundesministerium für Wirtschaft und Energie, Weißbuch Digitale Plattformen 2017, available at: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v=24.

Buterin 2018 Ethereum White Paper, available at: <https://github.com/ethereum/wiki/wiki/White-Paper>.

Christine Lagarde (2018, November), Winds of Change: The Case for New Digital Currency, Singapore Fintech Festival.

Christopher/Lee, Mitigating supply chain risk through improved confidence Emerald Group Publishing Limited 2013, available at: <https://www.emeraldinsight.com/doi/full/10.1108/09600030410545436>.

Cohen/Kietzmann, Ride on! Mobility business models for the sharing economy, *Organization & Environment* 2014, 279-296.

CoinMarketCap, Historical Snapshots 2019, available at: <https://coinmarketcap.com/historical/>.

Cong/He, Blockchain disruption and Smart Contracts 2018, available at: <https://www.nber.org/papers/w24399.pdf>.

Cordis 2018 ENSEMBLE: ENabling SafE Multi-Brand pLatooning for Europe, available at: <https://cordis.europa.eu/project/rcn/216001/factsheet/en>.

Customs, Saudi Customs Pilot Sees the Integration of Customs Tracking Feature with IBM and Maersk TradeLens Blockchain Solution 2018, available at: <https://www.customs.gov.sa/en/node/1022>.

Danwerth, The Regulation of Bitcoin and Other Virtual Currencies under Japanese Law in Comparative Perspective, *ZVglRWiss* 2018, 117-155.

Dauner-Lieb/Langen, Bürgerliches Gesetzbuch - of the German Civil Code, 3rd edition, Baden-Baden, 2016.

Dead Coins, Curated List of cryptocurrencies forgotten by this world...and more 2019, available at: <https://deadcoins.com/#>.

Deakin/Frick/Shively, Markets for Dynamic Ridesharing?, *Transportation Research Record* 2010, 131-137.

DeFilippi, What blockchain means for the sharing economy, *Harvard Business Review Digital Articles* 2017, 2-5.

Deutsche Handwerkszeitung, Kraftstoffverbrauch: So viel CO₂ stößt Ihr Auto aus 2018, available at: <https://www.deutsche-handwerkszeitung.de/kraftstoffverbrauch-in-co2-ausstoss-umrechnen/150/3097/57956>.

Deutsches Zentrum für Luft- und Raumfahrt, Automatisiertes und vernetztes Fahren im Güterverkehr - Auswirkungen auf die Logistikbranche 2017, available at: https://www.dlr.de/dlr/presse/desktopdefault.aspx/tabcid-10172/213_read-25203/#/gallery/29204.

Diepenbrock/Sachweh, Ein konzeptionelles Rahmenwerk für die Integration Digitaler Souveränität in Softwarearchitekturen, *DuD* 2018, 281-285.

Dittmer (2017, 29. November), Gigantischer Schwund: Millionen Bitcoins sind für immer verloren, n-tv, available at: <https://www.n-tv.de/wirtschaft/Millionen-Bitcoins-sind-fuer-immer-verloren-article20158230.html>.

Djazayeri, Rechtliche Herausforderungen durch Smart Contracts, *jurisPR-BKR* 2016, Anm. 1.

Dudenhausen/Hahn, Ganzheitliche Digitalisierungsansätze im Stadtwerk: Von der Strategie bis zur Umsetzung, Herausforderung Utility 4.0 2017, 683-700.

Dunphy/Petitcolas, A First Look at Identity Management Schemes on the Block-chain, IEEE Security & Privacy, 2018, 20-29.

DuPont, Experiments in algorithmic governance, A history and ethnography of "The DAO," a failed decentralized autonomous organization, Bitcoin and Beyond, 2017, 157-177.

Ehmann/Selmayr, DS-GVO, Beck'sche Kurz-Kommentare, 2nd edition, Munich, 2018.

EMIL Deutschland AG, Wer wenig fährt, sollte wenig zahlen EMIL Deutschland AG 2019, available at: <https://emil.de/>.

Engelhardt/Klein, Bitcoins – Geschäfte mit Geld, das keines ist, Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355-360.

Ernst & Young, Initial Coin Offerings (ICOs): The Class of 2017 – one year later 2018.

Etherscan, www.etherscan.io Etherscan 2019, available at: <https://etherscan.io/address/oxbb9bc244d798123fde783fcc1c72d3bb8c189413#>

EU Blockchain Observatory and Forum, About the European Union Blockchain Observatory and Forum 2019, available at: <https://www.eublockchainforum.eu/about>.

Europäische Kommission, Blockchain Technologies, available at: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>.

Europäische Kommission, COM(2018) 109 final 2018.

Europäische Kommission 2018 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von CO₂-Emissionsnormen für neue schwere Nutzfahrzeuge, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:93c5b96c-7ed6-11e8-ac6a-01aa75ed71a1.0009.02/DOC_1&format=PDF.

Europäische Kommission 2019 Künstliche Intelligenz: Kommission treibt Arbeit an Ethikleitlinien weiter voran (Europäische Kommission, Hrsg.). : Europäische Kommission.

European Commission, Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy 2015, available at: <https://ec.europa.eu/digital-single-market/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud>.

European Commission, European countries join Blockchain Partnership 2018, available at: <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>.

European Securities and Markets Authority, ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements 2017, available at: unter

https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

European Securities and Markets Authority, Own Initiative Report on Initial Coin Offerings and Crypto-Assets 2018, available at: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf.

European Securities and Markets Authority, Advice Initial Coin Offerings and Crypto-Assets 2019, available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

Falkon, The Story of the DAO—Its History and Consequences Medium 2017, available at: <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>.

Filippi/Hassan, Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code, First Monday 2016, 1-23.

Finck, Blockchains and Data Protection in the European Union, EDPL 2018, 17-35.

FINMA, Faktenblatt Virtuelle Währungen, Stand 30.08.2018, available at: <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-virtuelle-waehrungen.pdf?la=de>.

FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16.02.2018, available at: <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=de&hash=6518A4B3067554A0E22600E167601EF59AA20542>.

Flämig, Autonome Fahrzeuge und autonomes Fahren im Bereich des Gütertransports, Autonomes Fahren, 2015, 377-398.

Frantz/Nowostawski, From institutions to code: Towards automated generation of smart contracts, IEEE 1st International Workshops on Foundations and Applications on Self* Systems 2016, 210-215.

Fridgen/Guggenmos/Lockl/Rieger/Urbach 2018 Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain: Eine Machbarkeitsstudie des Bundesamtes für Migration und Flüchtlinge, Nürnberg: Bundesamt für Migration und Flüchtlinge, Bundesamt für Migration und Flüchtlinge (S. 1-32), available at: <https://eref.uni-bayreuth.de/46480/>.

Froitzheim, Code is Law, isn't it?, Rechtsfragen digitaler Transformationen, 311-325.

Furuhat/Dessouky/Ordóñez/Brunet/Wang/Koenig, Ridesharing: The state-of-the-art and future directions, Transportation Research Part B: Methodological 2013, 28-46.

Fußwinkel/Kreiterling, Blockchain-Technologie – Gedanken zur Regulierung 2018, available at:

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Fusswinkel.html?nn=11056122#U33.

Glatz, What are Smart Contracts? In search of a consensus. 2014, available at: <https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad>.

Global Agenda Council on the Future of Software & Society 2015 Deep Shift: World Economic Forum, available at: www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

Goldby, Electronic bills of lading and central registries: what is holding back progress? Routledge 2008, available at: <https://www.tandfonline.com/doi/abs/10.1080/13600830802239381>.

Goldfeder/Bonneau/Gennaro/Narayanan, Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. in: *Kiayias (Hg.) Financial Cryptography and Data Security*, Cham 2017, S. 321-339.

Grassi, Letter of Credit Transactions: the Banks' Position in Determining Documentary Compliance. A Comparative Evaluation Under U.S., Swiss and German Law, 7 *Pace Int'l Rev.*, 1995, 81-128.

Grathwohl, Die Rolle einer Roaming- und Clearing-Stelle für Elektrofahrzeuge im System der Elektromobilität, Kartellrechtliche Bewertung von Standardisierungsstrategien 2015, 221-271.

Gratzke/Schatsky/Piscini, Banding together for blockchain 2017, available at: <https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html#endnote-sup-2>.

Grosse-Ophoff/Hausler/Heineke/Möller, How shared mobility will change the automotive industry 2017, available at: <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/how-shared-mobility-will-change-the-automotive-industry>.

Gsell/Krüger/Lorenz/Reyman, beck-online GROSSKOMMENTAR, Munich.

Gtreview, New blockchain shipping consortium to rival Maersk and IBM's TradeLens 2018, available at: <https://www.gtreview.com/news/fintech/new-blockchain-shipping-consortium-to-rival-maersk-and-ibms-tradelens/>.

Habersack, Münchener Kommentar zum Bürgerliches Gesetzbuch, 7th edition, Munich, 2017.

Hahn/Grün, Modell eines eRoaming-Systems für die Elektromobilität, IR 2013, 293-296.

Hahn/Metcalfe, The Ridesharing Revolution: Economic Survey and Synthesis 2017, available at: <https://www.brookings.edu/wp-content/uploads/2017/01/ridesharing-oup-1117-v6-brookings1.pdf>.

Hahn/Wons, Initial Coin Offering (ICO), Wiesbaden, 2018.

Haucap/Pavel/Aigner/Arnold/Hottenrott/Kehder, Chancen der Digitalisierung auf Märkten für urbane Mobilität: Das Beispiel Uber, List Forum für Wirtschafts- und Finanzpolitik 2017, 139-183.

Hazard/Haapio, Wise contracts: smart contracts that work for people and machines, Proceedings of the 20th International Legal Informatics Symposium IRIS 2017, 425-432.

Heinrichs/Thomaier/Parzonka, Arbeitsberichte zur Verkehrsorschung: Ko-Automobilität 2017, available at: https://elib.dlr.de/112759/1/Autoteilen-Abschlussbericht%20%28final%29%20_2017_08_22.pdf.

Henssler/Strohn, Gesellschaftsrecht, 4th edition, Munich, 2019.

Herber, Münchener Kommentar zum Handelsgesetzbuch, 3rd edition, Munich, 2014.

Hochhold/Rudolph, Principal-Agent-Theorie, Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende 2011, 131-145.

Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 47th edition, Munich, 2019.

Hofert, Regulierung der Blockchains, Tübingen, 2018.

Hoffmann, Paukenschlag aus Las Vegas 2019, available at: <https://www.eurotransport.de/artikel/paukenschlag-aus-las-vegas-daimler-kehrt-sich-von-platooning-ab-10644852.html>.

Hopt/Kumpan/Merk/Roth, Handelsgesetzbuch, 38th edition, Munich, 2018.

Hyland-Wood/Khatchadourian, A Future History of International Blockchain Standards, The JBBA 2018, 3724.

ICodata.io, ICO Status 2019, available at: <https://www.icodata.io/ICO>.

International Chamber of Shipping, Shipping and World Trade Shipping and World Trade, available at: <http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade>.

International Organization for Standardization, Standards catalogue ISO/TC 307 2019, available at: <https://www.iso.org/committee/62666o4/x/catalogue/p/o/u/1/w/o/d/o>.

IOTA Foundation, IOTA 2019, available at: <https://www.iota.org/>.

Janssen/Zwijnenberg/Blankers/Kruijff, Truck Platooning: Driving the Future of Transportation 2015, available at: <https://www.tno.nl/en/about-tno/news/2015/3/truck-platooning-driving-the-future-of-transportation-tno-whitepaper/>.

Jentzsch 2016 Decentralized autonomous organization to automate governance. White paper, November., available at: <https://download.slock.it/public/DAO/WhitePaper.pdf>.

Joblift, Nach Startups entdecken auch Konzerne die Blockchain: über 1.500 Stellen rund um die innovative Technologie in Deutschland 2018, available at: <https://joblift.de/Presse/blockchain-jobs>.

Johnson, Can La'Zooz Take Ridesharing to the Moon? 2015, available at: <https://cointelegraph.com/news/can-lazooz-take-ridesharing-to-the-moon>.

Joos/Karlstetter, Blockchain-as-a-Service im Unternehmen nutzen 2018, available at: <https://www.cloudcomputing-insider.de/blockchain-as-a-service-im-unternehmen-nutzen-a-763985/>.

Kaulartz, Die Blockchain-Technologie, CR 2016, 474-480.

Kaulartz, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, Taeger (Hg.) – Smart world 2016, 1023-1037.

Kaulartz/Heckmann, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618-624.

Kaulartz/Matzke, Die Tokenisierung des Rechts, NJW 2018, 3278-3283.

Keding, Die aufsichtsrechtliche Behandlung von Machine-to-Machine-Zahlungen unter Rückgriff auf Peer-to-Peer-Netzwerke, WM 2018, 64-72.

Klein/Kottbauer, Strategien erfolgreich entwickeln und umsetzen, Munich, 2017.

Klein/Prinz/Gräther, A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities, Reports of the European Society for Socially Embedded Technologies, 2018, 1-10.

Kling, Sprachrisiken im Privatrechtsverkehr, Tübingen, 2008.

Kraftfahrt-Bundesamt, Pressemitteilung No. 06/2018 - Der Fahrzeugbestand am 1. Januar 2018 Kraftfahrt-Bundesamt 2018, available at: https://www.kba.de/DE/Service/Nachrichten/2018/PM/PM_Nr_06_2018_Bestand_2018.html.

Kshetri/Voas, Blockchain-Enabled E-Voting 2018, available at: https://www.researchgate.net/publication/326239528_Blockchain-Enabled_E-Voting.

Kühling/Buchner, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2nd edition, Munich, 2018.

Kütük/Sorge, Bitcoin im deutschen Vollstreckungsrecht, Von der "Tulpenmanie" zur "Bitcoinmanie", MMR 2014, 643-646.

Lamberti/Gatteschi/Demartini/Pranteda/Santamaria, Blockchain or not blockchain, that is the question of the insurance and other sectors, IT Professional (Early Access) 2017, 1-13.

Lang/Szczepanski/Wurzer, The Emerging Art of Ecosystem Management 2019, available at: https://www.bcg.com/publications/2019/emerging-art-ecosystem-management.aspx?utm_medium=Email&utm_source=201902&utm_campaign=20190

z_NoVal_EALERT_NONE_GLOBAL&utm_usertoken=6f68b280do6f3c5d6d5ba
db9dfaf98414c9fa6e&redir=true.

Lehner, Der rechtliche Rahmen der Elektromobilität, Eine Betrachtung der Ladesäulenverordnung und des Messstellenbetriebsgesetzes unter Berücksichtigung der Blockchain-Technologie, RAW 2018, 17-21.

Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau 2017 Blockchain und Smart Contracts: vbw Die Bayerische Wirtschaft.

Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Munich, 2008.

Lin/Liao, A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security 2017, 653-659.

Linke/Jürschik, Analog trifft digital - Neuigkeiten bei den rechtlichen Rahmenbedingungen zum Ridesharing, NZV 2018, 496-506.

Ludwigs, Rechtsfragen der Sharing Economy am Beispiel der Modelle Uber und Airbnb, NVwZ 2017, 1646-1653.

Lyons/Courcelas/Timsit, Blockchain for Government and Public Services 2018, available at: <https://www.eublockchainforum.eu/reports>.

MaaS Alliance, Guidelines & recommendations to create the foundations for a thriving MaaS Ecosystem 2017.

Macaulay/Buckalew/Chung 2015 Internet of Things in Logistics: DHL Trend Research, Cisco Consulting Services, available at: http://www.dpdhl.com/content/dam/dpdhl/presse/pdf/2015/DHLTrendReport_I nternet_of_things.pdf.

MarketsandMarkets, Blockchain Market by Provider, Application (Payments, Exchanges, Smart Contracts, Documentation, Digital Identity, Supply Chain Management, and GRC Management), Organization Size, Industry Vertical, and Region - Global Forecast to 2023 2018, available at: <https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html>.

Markl, Eine nationale Daten- und Analyseinfrastruktur als Grundlage digitaler Souveränität, Informatik Spektrum 2018, 433-439.

Marnau, Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung. in: *Eibl & Gaedke (Hg.) INFORMATIK* 2017, Bonn 2017, S. 1025-1036.

Marquette, Crypto-based funds crawl toward mom and pop 2019, available at: <https://www.rollcall.com/news/congress/the-future-holds-cryptocurrency-based-funds-says-secs-jackson>.

Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251-1259.

Martin-Jung (2019, 4. Februar), Passwort für 190 Millionen Dollar fehlt, Süddeutsche Zeitung, available at: <https://www.sueddeutsche.de/digital/kryptowaehrung-passwort-tod-bitcoin-blockchain-1.4315793>.

Mattila/Seppälä 2016 Digital trust, platforms, and policy. (no. 42). : ETLA Brief.

Mattila/Seppälä, Distributed Governance in Multi-sided Platforms: A Conceptual Framework from Case: Bitcoin, Collaborative Value Co-Creation in the Platform Economy 2018, 183-205.

McKinsey & Company, Lkw-Industrie: Jeder dritte Lastwagen bis 2025 teilautonom McKinsey & Company 2016, available at: <https://www.mckinsey.com/de/news/presse/lkw-industrie-jeder-dritte-lastwagen-bis-2025-teilautonom>.

Melliger/Vliet/Liimatainen, Anxiety vs reality – Sufficiency of battery electric vehicle range in Switzerland and Finland, Transportation Research Part D: Transport and Environment 2018a, 101-115.

Melliger/Vliet/Liimatainen, Anxiety vs reality-Sufficiency of battery electric vehicle range in Switzerland and Finland, Transportation Research Part D: Transport and Environment 2018b, 101-115.

MotionWerk GmbH, Open Mobility System (OMOS) 2019, available at: <https://www.omas.io/>.

Mühle/Grüner/Gayvoronskaya/Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review 2018, 80-86.

Mukherjee/Banerjee/Misra, Ad hoc ridesharring application using continuous sparql queries. in: Proceedings of the 21st International Conference on World Wide Web 2012, S. 579-580.

Müller, Studie über internationalen Arbeitsmarkt 2018, available at: <https://www.datacenter-insider.de/deutschland-stark-bei-bitcoin-blockchain-und-dlt-a-782634/>.

Mulligan/Scott/Warren/Rangaswami 2018 Blockchain Beyond the Hype (World Economic Forum, Hrsg.), available at: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf.

Nærland/Müller-Bloch/Beck/Palmund, Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. in: 38th International Conference on Information Systems (ICIS) 2017, S. 1-16.

Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2008, available at: <https://bitcoin.org/bitcoin.pdf>.

Narayanan/Bonneau/Felten/Miller/Goldfeder, Bitcoin and cryptocurrency technologies: A comprehensive introduction, Princeton, 2016.

Natoli/Gramoli, The blockchain anomaly, 2016 IEEE 15th International Symposium 2016, 310-317.

Nowak/Viereckl/Kauschke/Starke, The era of digitized trucking 2018, available at: <https://www.strategyand.pwc.com/media/file/The-era-of-digitized-trucking-charting-your-transformation.pdf>.

Oberländer/Röglinger/Rosemann/Kees, Conceptualizing business-to-thing interactions – A sociomaterial perspective on the Internet of Things, European Journal of Information Systems, 2018, 486-502.

Oliveira/Zavolokina/Bauer/Schwabe, To Token or not to Token: Tools for Understanding Blockchain Tokens 2018, available at: <https://www.zora.uzh.ch/id/eprint/157908/>.

Origin Protocol, ORIGIN - Decentralized marketplaces on the blockchain 2019, available at: <https://www.originprotocol.com/en>.

Osterland/Rose, Engineering sustainable blockchain applications, Proceedings of 1st ERCIM Blockchain 2018, 1-8.

Otte, Die Finanzmärkte und die ökonomische Selbstbehauptung Europas, Wiesbaden, 2019.

Overkamp/Schings, Blockchain im Strom- und Verkehrssektor, Potenziale und rechtliche Herausforderungen, EnWZ 2019, 3-8.

Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentare, 2nd edition, Munich, 2018.

Palandt, Bürgerliches Gesetzbuch, 78th edition, Munich, 2019.

Panetta, Gartner Top 10 Strategic Technology Trends for 2019 2018, available at: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>.

Parhofer/Klöhn/Resas, Initial Con Offerings (ICOs), ZBB 2018, 89-106.

Paulus/Matzke, Digitalisierung und private Rechtsdurchsetzung, Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?, CR 2017, 769-778.

Paulus/Matzke, Smart Contracts und das of the German Civil Code - Viel Lärm um nichts?, ZfPW 2018, 431-466.

Pike/Capobianco/Gomes 2018 Blockchain Technology and Competition Policy - Issues paper by the Secretariat (Organisation for Economic Co-operation and Development, Hrsg.), available at: [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf).

Popov 2018 The tangle, available at: https://assets.ctfassets.net/r1dr6vzfxhev/zt4uxvslqkoEUau6g2swog/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

Port of Rotterdam, ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a container logistics blockchain pilot 2018, available at: <https://www.portofrotterdam.com/en/news-and-press-releases/abn-amro-samsung-sds-and-the-port-of-rotterdam-authority-are-launching-a>.

Porter/Heppelmann, How Smart, Connected Products Are Transforming Competition, Harvard business review, 2014, 1-23.

Prinz 2018 Blockchain and CSCW – Shall we care? (European Society for Socially Embedded Technologies (EUSSET), Hrsg.), Proceedings of 16th European Conference on Computer-Supported Cooperative Work - Exploratory Papers, available at: <https://hdl.handle.net/20.500.12015/3124>.

Protocol Labs, IPFS is the Distributed Web 2019, available at: <https://ipfs.io/>.

Rabe/Bahnsen, Seehandelsrecht, 5th edition, Munich, 2018.

Ramming, Die Sperrwirkung von Ladeschein und Konnossement, RdTW 2018, 45-58.

Redeker, IT-Recht, 6. Auflage, Munich, 2017.

Reiff, Bitcoin ETFs Explained 2018, available at: <https://www.investopedia.com/investing/bitcoin-etfs-explained/>.

Reiter/Methner, Bitcoin und Blockchain-Technologie: Rechtliche Aspekte für Verbraucher und Anbieter beim anonymen Bezahlen. in: *Taeger* (Hg.) Rechtsfragen digitaler Transformationen. Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 359-370.

Reus, Interview: Platooning wird Nerven und Kraft der Fahrer schonen 2017, available at: <https://logistik-aktuell.com/2017/02/23/interview-platooning/>.

Reuters, Barclays says conducts first blockchain-based trade-finance deal 2016, available at: <https://www.reuters.com/article/us-banks-barclays-blockchain/barclays-says-conducts-first-blockchain-based-trade-finance-deal-idUSKCN11D23B>.

Römer/Tscheulin, Die Bedeutung von Vertrauen in risikoreichen Kooperationsentscheidungen — Analyse der theoretischen Grundlagen und empirische Überprüfung, Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 2008, 434-458.

Rowan/Clear/Gerla/Huggard/Goldrick 2017 Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels, available at: <http://arxiv.org/pdf/1704.02553v1>.

Saberhagen, CryptoNote v 2.0 2013, available at: <https://cryptonote.org/whitepaper.pdf>.

Sächsische Energieagentur – SAENA GmbH, Kompetenzatlas Elektromobilität Sachsen 2016, available at: http://www.saena.de/download/Broschueren/BEMob_Kompetenzatlas.pdf.

Säcker/Rixecker/Oetker/Limperg et al., Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7th edition, Munich, 2018.

Saive, Blockchain in der Transportwirtschaft, RdTW 2018, 85-89.

Saive, Das Blockchain-Traditionsstück, Die transportrechtlichen Traditionspapiere vor dem Hintergrund neuer Technologien, TranspR 2018, 234-238.

Saive, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764-767.

Sänn/Richter/Fraunholz, Car-to-X als Basis organisationaler Transformation und neuer Mobilitätsleistungen, Wirtschaftsinformatik & Management 2017, 60-71.

Sasson/Chiesa/Garman/Green/Miers/Tromer et al., Zerocash: Decentralized Anonymous Payments from Bitcoin. in: The Institute of Electrical and Electronics Engineers (Hg.) IEEE Symposium on Security and Privacy 2014, S. 459-474.

Scania, Plaunoing saves up to 12 percent fuel 2015, available at: <https://www.scania.com/group/en/plaunoing-saves-up-to-12-percent-fuel/>.

Schneier, Applied Cryptography, Indianapolis, 2015.

Scholtka/Kneuper, Lokale Energiemärkte auf Basis der Blockchain-Technologie, IR 2019, 17-21.

Schrey/Thalhofer, Rechtliche Aspekte der Blockchain, NJW 2017, 1431-1436.

Schulze, 'We are about to see massive disruptions': IMF's Lagarde says it's time to get serious about digital currency CNBC 2017, available at: <https://www.cnbc.com/2017/10/13/bitcoin-get-serious-about-digital-currency-imf-christine-lagarde-says.html>.

Schulze, Bürgerliches Gesetzbuch, 10th edition, Baden-Baden, 2019.

Schütte/Fridgen/Prinz/Rose/Urbach 2017 Blockchain und Smart Contracts (Wolfgang Prinz, Axel T. Schulte, Hrsg.): Fraunhofer, available at: https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf.

Schweizer/Schlatt/Urbach/Fridgen, Unchaining Social Businesses: Blockchain as the Basic Technology of a Crowdensing Platform. in: 38th International Conference on Information Systems (ICIS) 2017, S. 1-21.

Schweizer Bundesrat, Bericht Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, available at: https://www.mme.ch/fileadmin/files/documents/Publikationen/2018/181207_Bericht_Bundesrat_Blockchain.pdf.

Schweizer Bundesrat, Medienmitteilung vom 18.01.2018, available at: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69539.html>.

Scora/Barth 2006 Comprehensive Modal Emissions Model (CMEM), University of California, USA.

Securities and Exchange Commission, Statement on Digital Asset Securities Issuance and Trading 2018, available at: <https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading>.

Securities Exchange Comission 2017 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO: Securities and Exchange Commission, available at: <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

Seitz, Distributed Ledger Technology - Die Revolution hat begonnen und das Recht muss folgen. in: *Taeger (Hg.) Recht 4.0. Innovationen aus den rechtswissenschaftlichen Laboren*, Edewecht 2017, S. 777-791.

Shah, Global Blockchain Market Could Reach \$60 Billion by 2024, Shows Report 2018, available at: <https://blokt.com/news/global-blockchain-market-could-reach-60-billion-by-2024-shows-report>.

Shen/Pena-Mora, Blockchain for Cities—A Systematic Literature Review, IEEE Access 2018, 76787-76819.

Shermin, Disrupting Governance with Blockchains and Smart Contracts, Strategic Change 2017, 499-509.

Shmatenko/Möllenkamp, Digitale Zahlungsmittel in einer analog geprägten Rechtsordnung, A bit(coin) out of control - Rechtsnatur und schuldrechtliche Behandlung von Kryptowährungen, MMR 2018, 495-501.

Simmchen, Blockchain (R)Evolution, Verwendungsmöglichkeiten und Risiken, MMR 2017, 162-165.

Simpson/Cooke, Blockchain: competition issues in nascent markets 2016, available at:
<https://www.nortonrosefulbright.com/en/knowledge/publications/81f70b38/blockchain-competition-issues-in-nascent-markets>.

Sovrin Foundation 2018 A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, available at: <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>.

Spiegel Online, Merkel und Steinbrück im Wortlaut 2008, available at: <http://www.spiegel.de/wirtschaft/merkel-und-steinbrueck-im-wortlaut-die-spareinlagen-sind-sicher-a-582305.html>.

Spindler/Bille, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357-1369.

Spindler/Schuster, Recht der elektronischen Medien, 3rd edition, Munich, 2015.

Statista, Blockchain 2018, available at: <https://www.statista.com/study/39859/blockchain-statista-dossier/>.

Statista, Trends in global export volume of trade in goods from 1950 to 2017 2018, available at: <https://www.statista.com/statistics/264682/worldwide-export-volume-in-the-trade-since-1950/>.

Statistisches Bundesamt, Anzahl der Speditionen in Deutschland in den Jahren von 2009 bis 2016 statista 2019, available at: <https://de.statista.com/statistik/daten/studie/422098/umfrage/anzahl-der-speditionen/>.

Staudinger, J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch. Buch 2: Recht der Schuldverhältnisse: §§ 705 - 740 (Gesellschaftsrecht), Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Berlin, 2003.

Staudinger, J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Neubearb. 2013, Berlin, 2013.

Staudinger, J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Neubearb. 2017, Berlin, 2017.

Stürner, Bürgerliches Gesetzbuch, 17th edition, Munich, 2018.

Sun/Yamamoto/Morikawa, Fast-charging station choice behavior among battery electric vehicle users, Transportation Research Part D: Transport and Environment 2016, 26-39.

Sutter/Maibach/Bertschmann/Ickert/Peter/Doll et al., Finanzierung einer nachhaltigen Güterverkehrsinfrastruktur 2016, available at: https://www.umweltbundesamt.de/sites/default/files/medien/376/publikationen/texte_53_2016_finanzierung_einer_nachhaltigen_gueterverkehrsinfrastruktur_aktualisiert.pdf.

Sydow, Europäische Datenschutzgrundverordnung, 2nd edition, Baden-Baden, 2018.

Tamm/Tonner/Bergmann, Verbraucherrecht, 2nd edition, Baden-Baden, 2016.

The Linux Foundation 2017 Hyperledger Architecture, Volume 1, available at: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.

Thomas Halleck, Facebook: One Out Of Every Five People On Earth Have An Active Account 2015, available at: <https://www.ibtimes.com/facebook-one-out-every-five-people-earth-have-active-account-1801240>.

Thüsing/Westphalen, Vertragsrecht und AGB-Klauselwerke, 41st edition, Munich, 2018.

Tobin/Reed, The Inevitable Rise of Self-Sovereign Identity Sovrin Foundation 2016.

Todd, Dematerialisation of shipping documents, Journal of International Banking Law 2000, 410-418.

Tractica, Enterprise Blockchain Revenue to Surpass \$20 Billion by 2025 2018, available at: <https://www.tractica.com/newsroom/press-releases/enterprise-blockchain-revenue-to-surpass-20-billion-by-2025/>.

Tradelens, The Power of the Ecosystem 2019, available at: <https://www.tradelens.com/ecosystem/>.

Tsugawa, Energy ITS: What We Learned and What We should Learn TRB Road Vehicle Automation Workshop 2012, available at: <http://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Tsugawa.pdf>.

Tual, Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir announced amongst exceptional DAO Curators Medium 2016, available at: <https://blog.slock.it/vitalik-buterin-gavin-wood-alex-van-de-sande-vlad-zamfir-announced-amongst-stellar-dao-curators-44be4d12dd6e>.

Tulpule, Enforcement and Compliance in a Blockchain(ed) World, CPI Antitrust Chronicle, 2017, 45.

Ulmer/Brandner/Hensen, AGB-Recht, 12th edition, Saarbrücken, 2016.

UN News, World Book Day: new UN report spotlights potential of mobile technology to advance literacy 2014, available at: Grundsätzlich abzugleichen_ https://www.acatech.de/wp-content/uploads/2018/10/acatech-HORIZONTE_Blockchain.pdf.

Underwood, Blockchain beyond bitcoin, Communications of the ACM 2016, 15-17.

V2G Clarity, IEC 63110 – Standardizing the Management of Electric Vehicle (Dis-)Charging Infrastructures 2017.

Valenta/Sandner 2017 Comparison of Ethereum, Hyperledger Fabric and Corda (Frankfurt School Blockchain Center, Hrsg.) (FSBC Working Paper).

Virmani, 18 blockchain consortia you should know about 2019, available at: <https://medium.com/blockchain-blog/18-blockchain-consortia-you-should-know-about-6262b6a30ba9>.

Vukolic, Rethinking Permissioned Blockchains, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts 2017, 3-7.

Wagner/Goeble, Freie Fahrt für das Auto der Zukunft, Kritische Analyse des Gesetzentwurfs zum hoch- und vollautomatisierten Fahren, ZD 2017, 263-269.

Werbach, Trust, But Verify: Why the Blockchain Needs the Law, Berkeley Tech. L.J. 2018, 491-552.

Wieske, Transportrecht, 3. Auflage, Berlin, 2012.

Yermack, Corporate Governance and Blockchains 2016, available at: <https://www.nber.org/papers/w21802.pdf>.

Ylinen, Zusammenarbeit beim Platooning zu Lande und zur See – kartellrechtliche Gesichtspunkte, RdTW 2018, 121-125.

YouGov, Umfrage zur Bekanntheit von Einsatzmöglichkeiten einer Blockchain im Mittelstand 2017, available at: <https://de.statista.com/statistik/daten/studie/683657/umfrage/umfrage-zur-bekanntheit-von-blockchain-einsatzmoeglichkeiten-im-mittelstand-in-deutschland/>.

Zare-Garizy/Fridgen/Wederhake, A Privacy Preserving Approach to Collaborative Systemic Risk Identification: The Use-Case of Supply Chain Networks, Security and Communication Networks 2018, 1-18.

Publication Data

Published by

Federal Ministry of Transport and Digital Infrastructure
Invalidenstr. 44
D-10115 Berlin

As at

Mai 2019

Picture credits

Cover picture: © logicbomb - stock.adobe.com
Fraunhofer Institute for Applied Information Technology FIT

Text

Fraunhofer Institute for Applied Information Technology FIT

This brochure is part of the Federal Government's public relations work.
It is issued free of charge and may not be sold..

