(How) Can Blockchain Contribute to the Management of Systemic Risks in Global Supply Networks?

Gilbert Fridgen[1,2], Marc-Fabian Körner[1], Johannes Sedlmeir[2],
and Martin Weibelzahl[1,2]

1 FIM Research Center, University of Bayreuth, Wittelsbacherring 10, Bayreuth, Germany
2 Project Group Business & Information Systems Engineering of the Fraunhofer FIT,
Wittelsbacherring 10, Bayreuth, Germany

gilbert.fridgen@uni-bayreuth.de,
marc.koerner@fim-rc.de,
johannes.sedlmeir@fit.fraunhofer.de,
martin.weibelzahl@uni-bayreuth.de

Abstract. Even though globalization has led to larger, faster, and more efficient supply chains, at the same time the new worldwide interconnection has also resulted in major challenges with respect to hidden systemic risks. In particular, there is a lack of a holistic perspective on the entire supply network. This missing global view prohibits the anamnesis and management of underlying risks. Against this backdrop, in this paper we discuss the potential contributions of Blockchain technology to systemic risk management in global supply chains and networks. Given the increasing number of recent initiatives of businesses in the context of Blockchain, we argue that Blockchain technology can lower the hurdle for the use of secure multiparty computation. Ultimately, it may be possible to implement a corresponding monitoring mechanism for systemic risks without (i) the need of a central authority and (ii) revealing competition relevant, confidential information to other supply network participants.

Keywords: Systemic Risks, Supply Networks, Blockchain, Secure Multiparty Computation.

1 Introduction

With the steady progression of globalization, supply networks expand globally and operate across borders. To address the growing global competition, companies are continuously increasing efficiency and speed, resulting in reduced inventory levels and just-in-time production [1]. In the past decades, digitalization has successfully contributed to expanding and managing the resulting complexity of modern supply network structures. However, while digitalization has helped to speed up business processes, systemic risks have simultaneously increased, since failures may rapidly propagate within fast-responding (supply) networks [2–5]. A prominent example for such propagating effects are the floods in Thailand in 2011: After several tropical storms and heavy rainfall, Thai manufacturers of hard disks were forced to shut down their production temporarily [6, 7]. In an ex-ante unexpected intensity, this finally affected the global production of notebooks and digital video recorders via different intermediate manufacturers [8]. In fact, an ex-post investigation revealed that the involved manufacturers have had a significant market share at that time. As this example demonstrates, an exogenous local event has led to a large global supply network disruption, where rising prices for end customers heavily influenced markets all around the world. Therefore, managing systemic risks is a major challenge in times of increased interconnection and complexity of supply networks [9].

As highlighted above, various suppliers and manufacturers that are worldwide distributed and connected characterize today's supply networks. However, there is no central institution that could take over the anamnesis, diagnosis, or therapy of underlying systemic risks. Given this lack of a global perspective and control, not only researchers but also customers and managers are well aware of the significant challenges posed by cascading risks and failures [10–13]. Ultimately, the results of the described developments may have highly negative consequences for end consumers, e.g., in form of rising prices or decreasing welfare.

On the other hand, Blockchain technology has caused a sensation with its first and most popular application to date, the Bitcoin, for almost ten years [14]. The Blockchain architecture unconditionally focusses on decentralization and hence for example enables a currency system with equal parties, i.e., without any central institution or intermediaries [15, 16]. Its key properties concerning forgery protection, transparency of rules, neutrality, and the already mentioned decentralization make Blockchain technology highly relevant for cross-organizational workflow management and particularly for applications in logistics and supply networks.

Against this background, it is conceivable that for the first time all relevant players of a supply network can meet on a common system with a uniform way of communication and a spirit of cooperation in competition (“coopetition”). In principle, such a meeting would make it possible to collect all relevant data in order to identify systemic risks with comparatively little effort. However, members of a supply network may still hesitate to share their typically confidential data. Given this potential hesitation, this paper discusses the opportunities of Blockchain technology for managing systemic risks in global supply networks by using secure multiparty computation. Of course, the latter technology has been known for quite some time, but practical applications in the supply sector have not been observed, yet. In this paper, we argue that with the presence of new Blockchain infrastructures, secure multiparty computation has the potential to derive different risk-related metrics of a supply network. In particular, for computing such metrics, inputs from various supply network participants can be used without any company gaining additional information except the final result.

This paper is organized as follows: We will first describe main Blockchain-related developments in supply networks in Section 2. Based on these developments, Section 3 will subsequently discuss the opportunities of Blockchain to address the challenges of systemic risks by being an economic enabler for secure multiparty computation. Finally, the paper concludes with a summary in Section 4.

2 Distributed ledger technologies and the rise of Blockchain-based initiatives in supply networks

Although Blockchain is the most commonly used term for the technology under consideration in this paper, we will place Blockchain in the more general context of "Distributed Ledger Technologies" (DLT). DLT is a collective term for distributed databases within a peer-to-peer network that typically employs a combination of cryptographic methods on the technical side and principles from game theory as economic incentives in order to create consensus between the participants [17]. Consensus refers to a commonly accepted definition of what the rules are, e.g., "append-only" or "no double spending". Such rules can then enforce immutability of data in the Blockchain, facilitate digital money (cryptocurrencies), or joint execution of scripts – so-called smart contracts – in a trusted way without the need for an intermediary [18, 19]. In DLT-based architectures, usually the same data is stored on every single node, resulting in complete transparency of the data in the ledger. In general, the concrete design of distributed ledgers can take various forms depending on reading or writing permission (permissioned vs. permissionless), efficiency, or the degree of centralization (public vs. private).

A special type of DLT is Blockchain technology. The latter employs a specific, linear data structure of blocks that are linked by inserting the hash-value of the previous block into each block. In fact, the first and most prominent representative of a distributed ledger application, namely the Bitcoin network for the well-known cryptocurrency [14], is a Blockchain. However, the number of applications of DLT has increased rapidly in the last years, as researchers and practitioners consider them to have a radical potential not only for cryptocurrencies, but also for various other areas [20], e.g., the energy sector [21] or general supply networks [22–24]. Since most of the applications so far have the structure of a Blockchain, the latter is the more popular term, and hence we will also mainly use the word "Blockchain" in this paper – even though most statements are also true for DLT in general.

The generic idea behind the use of Blockchain is the implementation of an IT architecture that ensures manipulation security and transparency of rules without the need of a trusted intermediary. In other words, Blockchain technology can facilitate so-called "neutral platforms". It could therefore also take on the role of a coordinating, trusted central authority that currently does not exist in global supply networks [16].

In this context, logistics and supply networks have long strived for improved digitalization, automation, and coordination, which is only possible if the relevant players agree to participate on some kind of common platform. However, participants may hesitate to entrust competition-relevant information (e.g., data on their suppliers or customers) not only to rivals, but also to a central institution – regardless of whether such an institution is represented by a government or by a private company. In particular, even if all participants in the network were to agree that a central authority would make sense to coordinate and monitor the network, this authority would possess a central market role and thus a considerable amount of market power. Finally, not only economic, but also political considerations might suggest a refusal of such a potential monopolist.

Already today, a non-negligible number of consortia and initiatives – often either consisting of or being supported by global players – aim at employing Blockchain to pursue the latter goal have been formed. These initiatives try to tackle practical problems in operation and management of modern supply networks with the help of Blockchain-based solution approaches, e.g., problems related to missing data integration, limited information about the manufacturing process, or the huge effort with respect to necessary paperwork [16, 22]. Ultimately, with the described initiatives, the involved companies aim at realizing positive effects on the efficiency of their supply networks, on product quality, and on customer confidence [25]. For example, IBM and Maersk created the so-called "TradeLens" initiative in 2018 to implement a Blockchain infrastructure within a global supply network. Furthermore, also Walmart implemented a Blockchain-based supply network platform to trace its pork and mangos for tackling food scandals [25, 26]. Given these well-known initiatives, further and more advanced Blockchain-based neutral platforms and new ecosystems are expected to evolve in the coming years.

3 Secure Multiparty Computation, its relation to Blockchain, and the corresponding potential for managing systemic risks

As described in the previous section, companies usually keep their suppliers and customers in the supply network secret and hesitate to give corresponding information to their competitors. One of the main reasons is that information asymmetries in supply networks are often an integral part of the business secret and therefore provide the foundation for profitability of companies. In particular, companies may also not be willing to give such information to a trusted central institution even if the resulting, aggregated information on the general state of the network would be highly relevant for individual decision making.

Against this backdrop, secure multiparty computation (SMC), which has already been a subject to research since the 1970s, provides the ability to perform computations which use data inputs from different participants without distributing the inputs among the participants or having to disclose any of them to a third party. The following example, which is inspired by [27], illustrates the basic idea behind secure multiparty computation by a simplified sketch of secure addition: Let us assume three involved companies denoted by A, B, and C. The associated private numbers of the companies are a, b, and c. In order to compute their sum by means of SMC, company A first generates a random number r in a sufficiently large range and gives $r + a$ to company B. In turn, company B adds its own number b and passes the result to company C, which then adds c and arrives at $r + a + b + c$. This subtotal is subsequently forwarded to company A, which is the only company which knows r. Company A can then subtract r from the last subtotal and gets the desired result a+b+c. Finally, A communicates this sum to the other companies. Note that this protocol makes sure that no single company can draw any conclusions about the others' individual inputs. Consequently, none of the three companies gets any additional information apart from the final sum *a*+*b*+*c*. Also, no central authority is needed to perform the protocol. Figure 1 summarizes this simple example for secure addition among the three companies.

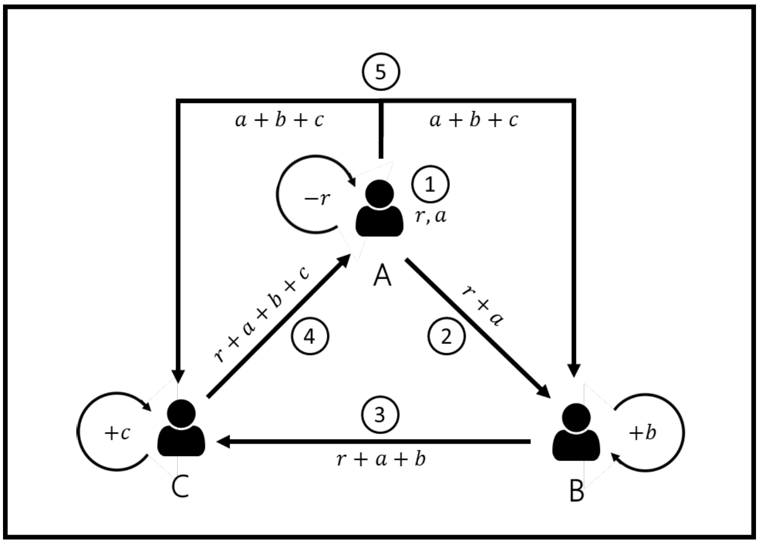

Figure 1: Secure addition among three companies A, B, and C

Even though the example is quite simple, it gives an illustrative way of describing the main functioning of SMC. In its standard version, "curious-but-honest" participants are assumed. More advanced problems often employ further mechanisms such as permuting the roles of A, B, and C in order to detect potential misbehaviour by checking whether the result is the same for each permutation. For even more enhanced security, such as ruling out collusion among a subset of the participants or ensuring tap-proof information exchange, cryptographic methods can be employed.

Academic literature already suggests several metrics for measuring systemic risks in supply networks: Among the most common examples is the "betweenness centrality" [28, 29]. The latter metric is calculated as a weighted sum of market shares of a specific good along shortest paths (with respect to suitable metrics) in a network. By using an appropriate secure multiparty computation protocol, such metrics can be computed in complex supply networks, too [30]. However, it remains to be analyzed how much information about the network can be reconstructed from the explained quantities such as betweenness centrality. In particular, the extent to which the results of a SMC protocol should be published needs to respect the degree of anonymity in the network or the severity of a systemic risk.

From a technical perspective, it is not necessary to have a Blockchain architecture set up in order to perform SMC protocols. Rather, a network is required in which the involved participants can meet and exchange data, ideally securely. Up to now, no such system of relevance with the purpose of SMC has been formed in practice. The advent of Blockchain-based platforms can significantly lower the barrier to establish and utilize SMC applications in supply networks. First examples are already being tested on Hyperledger Fabric, which is the Blockchain IT-architecture behind TradeLens [31]. It is therefore conceivable that the addressing of systemic risks in supply networks may soon become a realistic scenario.

To sum up, Blockchain may provide the basic infrastructure on which companies can (pseudonymously) identify themselves and exchange data under a certain degree of standardization. Given current Blockchain initiatives, there is a realistic chance of establishing decentralized and far-reaching networks where SMC protocols can be executed to compute critical risk metrics. Taking on the task of a trustworthy central authority, the latter metrics may then be used to monitor the risks of global supply systems. In this respect, Blockchain in combination with SMC may have the potential of better managing and regulating entire supply networks without pillorying individual companies.

4 Conclusions

Being a catalyst for globalization, digitization allows to trade faster across borders and to operate global supply networks more efficiently. With a growing global interdependency and interconnection, there is an increasing threat of systemic risks at the same time. Ultimately, such risks may result in failures that spread faster and more extensively in modern supply networks than ever before.

As we argue in this paper, distributed ledgers like Blockchains in combination with secure multiparty computation may have the potential to tackle the challenges of detecting and managing systemic risks in large supply networks. In particular, Blockchain technology could take on the role of a central authority, which does currently not exist in global supply networks, and grant access to data that is relevant for an anamnesis, diagnosis, or therapy of systemic risks.

References

1. Manuj, I., Mentzer, J.T.: Global Supply Chain Risk Management. Journal of Business Logistics 29, 133–155 (2008)
2. Mertens, P., Barbian, D.: Die Wirtschaftsinformatik der Zukunft–auch eine Wissenschaft der Netze? HMD Praxis der Wirtschaftsinformatik 51, 729–743 (2014)
3. Buhl, H.U., Penzel, H.-G.: The Chance and Risk of Global Interdependent Networks. Business & Information Systems Engineering 2, 333–336 (2010)
4. Fridgen, G., Stepanek, C., Wolf, T.: Investigation of exogenous shocks in complex supply networks – a modular Petri Net approach. International Journal of Production Research 53, 1387–1408 (2015)
5. Mertens, P., Barbian, D.: Researching "Grand Challenges". Business & Information Systems Engineering 57, 391–403 (2015)

6. Haraguchi, M., Lall, U.: Flood risks and impacts: A case study of Thailand's floods in 2011 and research questions for supply chain decision making. International Journal of Disaster Risk Reduction 14, 256–272 (2015)
7. Abe, S.: Impact of the Great Thai Floods on the International Supply Chain. Malaysian Journal of Economic Studies 51, 147–155 (2017)
8. Chongvilaivan, A.: Thailand's 2011 flooding: Its impact on direct exports and global supply chains (2012)
9. Helbing, D.: Globally networked risks and how to respond. Nature 497, 51 (2013)
10. Little, R.G.: Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. Journal of Urban Technology 9, 109–123 (2002)
11. Watts, D.J.: A simple model of global cascades on random networks. Proceedings of the National Academy of Sciences 99, 5766–5771 (2002)
12. Lorenz, J., Battiston, S., Schweitzer, F.: Systemic risk in a unifying framework for cascading processes on networks. The European Physical Journal B 71, 441 (2009)
13. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature 464, 1025 (2010)
14. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
15. Schweizer, A., Schlatt, V., Urbach, N., Fridgen, G.: Unchaining Social Businesses – Blockchain as the Basic Technology of a Crowdlending Platform. ICIS 2017 Proceedings (2017)
16. Fridgen, G., Radszuwill, S., Urbach, N., Utz, L.: Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. Hawaii International Conference on System Sciences 2018 (HICSS-51) (2018)
17. Ferdinando M. Ametrano: Bitcoin, Blockchain, and Distributed Ledgers: Between Hype and Reality. SSRN (2016)
18. Peter H, M.A.: Blockchain-applications in banking & payment transactions: Results of a survey. European financial systems 2017: Proceedings of the 14th International scientific conference, 141–149
19. Davidson, S., Filippi, P. de, Potts, J.: Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. SSRN (2016)
20. Beck, R., Müller-Bloch, C.: Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization (2017)
21. Mylrea, M., Gourisetti, S.N.G.: Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: Proceedings 2017 Resilience Week (RWS). Chase Center on the Riverfront/Wilmington, DE, Wilmington, DE, 18-22 September 2017, pp. 18–23. IEEE, Piscataway, NJ (2017)
22. Korpela, K., Hallikas, J., Dahlberg, T.: Digital Supply Chain Transformation toward Blockchain Integration. Hawaii International Conference on System Sciences 2017 (HICSS-50) (2017)
23. Tian, F.: An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: Yang, B. (ed.) 2016 13th International Conference on Service Systems and Service Management (ICSSSM), pp. 1–6. IEEE, Piscataway, NJ (2016)
24. Nærland, K., Müller-Bloch, C., Beck, R., Palmund, S.: Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. ICIS 2017 Proceedings (2017)

25. Kamath, R.: Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. The JBBA 1, 3712 (2018)
26. Hackius, N., Petersen, M.: Blockchain in logistics and supply chain : trick or treat? Proceedings of the Hamburg International Conference of Logistics (HICL), 23 (2017)
27. Schneier, B.: Applied Cryptography. Protocols, Algorithms and Source Code in C. John Wiley & Sons Incorporated, New York (2015)
28. Newman, M.: Networks: An Introduction. Oxford University Press, Oxford (2010)
29. Kim, Y., Choi, T.Y., Yan, T., Dooley, K.: Structural investigation of supply networks: A social network analysis approach Journal of Operations Management, 194–211 (2011)
30. Zare-Garizy, T., Fridgen, G., Wederhake, L.: A Privacy Preserving Approach to Collaborative Systemic Risk Identification: The Use-Case of Supply Chain Networks. Security and Communication Networks (2018)
31. Benhamouda, F., Halevi, S., Halevi, T.: Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. 2018 IEEE International Conference on Cloud Engineering (IC2E), 357–363 (2018)