



UNSW Law & Justice Research Series

Competing Claims to Cryptoassets

**Jannik Woxholth, Dirk A. Zetsche, Ross
Buckley and Douglas Arner**

[2023] *UNSWLRS* 26

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au

W: <http://www.law.unsw.edu.au/research/faculty-publications>

AustLII: <http://www.austlii.edu.au/au/journals/UNSWLRS/>

SSRN: <http://www.ssrn.com/link/UNSW-LEG.html>

COMPETING CLAIMS TO CRYPTOASSETS

*Jannik Woxholth**, *Dirk A. Zetzsche***, *Ross Buckley****, *Douglas Arner*****

ABSTRACT

At the height of the ‘crypto winter’, with several crypto-intermediaries filing for insolvency and subjected to schemes of arrangement, who owns what and who has a claim on what becomes all important. Meanwhile, Distributed Ledger Technologies (DLT) are frequently presented as a digital solution to these perennial problems of competing claims to the same asset. This article makes two contributions to the literature: First, we show that neither technology nor law solves the competing claims issue. Second, we suggest policy solutions based on a comparative legal analysis. In essence, the law must: (1) recognise property rights in cryptoassets, (2) provide for negotiability based on the assertion of control over private keys, and (3) facilitate the enforcement of titles in cryptoassets by the interplay of private and financial law.

* PhD; Senior Scientist, ADA Chair in Financial Law (Inclusive Finance), University of Luxembourg.

** Professor of Law, Dr. iur., Dr. iur. habil., LL.M., ADA Chair in Financial Law (Inclusive Finance), and Coordinator, Centre for Sustainable Governance and Markets, University of Luxembourg. Co-Chair, Fintech Working Group, European Banking Institute, Frankfurt.

*** KPMG Law - King & Wood Mallesons Professor of Disruptive Innovation, a Scientia Professor, and an Australian Research Council Laureate Fellow (FL200100007), at UNSW Sydney. This Australian government funding has supported this research. The views herein are of the authors and not necessarily of the Australian government or Research Council. We are grateful to the Australian government for their research assistance.

**** Kerry Holdings Professor in Law and Director, Asian Institute of International Financial Law, University of Hong Kong; Board Member, Centre for Finance, Technology & Entrepreneurship. We are thankful for comments provided by Professor Louise Gullifer and Professor Matthias Lehmann. Responsibility for any remaining errors is ours.

Contents

1. INTRODUCTION	3
2. COMPETING CLAIMS UNSOLVED BY TECHNOLOGY	5
<i>A. What Problem Did Nakamoto Set Out to Solve?</i>	5
<i>B. Remaining Issues Unaddressed by Technology</i>	5
<i>C. Competing Claims Facilitated by Technology</i>	7
3. COMPETING CLAIMS UNSOLVED BY LAW.....	7
<i>A. Cryptoassets as Property?</i>	7
<i>B. The Nemo Dat Rule Applied to On-Chain Transfers</i>	11
<i>C. Registration, Possession, and Negotiability</i>	12
<i>D. Competing Claims as an Issue Unsolved</i>	18
4. THREE PRINCIPLES TO ADDRESS COMPETING CLAIMS	19
<i>A. Property Rights</i>	20
<i>B. Negotiability</i>	20
<i>C. Enforcement</i>	23
<i>D. How our Solutions Solve the Competing Claims Issue</i>	27
5. CONCLUSION	29

1. Introduction

At the height of the ‘crypto winter’, with several crypto-intermediaries filing for insolvency and their assets are subjected to schemes of arrangement, who owns what and who has a claim on what becomes all important. This article contributes to these questions with a focus on the most pressing situation that, as we will show below, is adequately addressed neither by law nor by technology: competing claims to the same cryptoasset.¹

Cryptoassets were in fact invented specifically to address the competing claims issue for digital data entries, which are non-exclusive by nature and may be multiplied into a limitless number of exact, indistinguishable copies. For instance, the same email can be sent to two different recipients, and the two copies will be identical. This is why digitally recorded assets historically needed a trusted third party to preserve a master copy of who owned what – that is, until one or more developers under the pseudonym, Satoshi Nakamoto,² applied previous work in the areas of public transaction ledgers,³ peer-to-peer consensus algorithms,⁴ and computational expenditure (‘proof-of-work’)⁵ to prevent ‘double spending’ in digital payments.

Blockchain and, more broadly, Distributed Ledger Technologies (DLT) suggest there is a *technical* solution to the perennial problem of forgery and competing claims to the same asset. In effect, DLT prevents the same cryptoasset from being copied or transferred twice. However, the technology relies on private key authentication and cannot prevent the keys from being obtained through illicit acts, such as fraud, theft, and ransomware attacks – which represent three of the four principal means by which some USD 14 billion worth of cryptoassets were obtained by criminals in 2021.⁶ Similarly, the technology cannot protect against void

¹ In line with The Law Commission, *Digital Assets: Consultation Paper* (Law Com No 256, 2022), we use the term ‘cryptoasset’ for a subset of digital assets that are treated as tradeable objects by market participants.

² S Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ <<https://bitcoin.org/bitcoin.pdf>> accessed 17 October 2022; see E Schuster, ‘Cloud Crypto Land’ (2021) 84(5) MLR 974, 976-981; T Cutts, ‘Smart Contracts and Consumers’ (2019) 122 W Va L Rev 389, 402-410.

³ W Dai, ‘B-Money’ <<http://www.weidai.com/bmoney.txt>> accessed 23 October 2022.

⁴ V Vishnumurthy et al, ‘KARMA: A Secure Economic Framework for Peer-to-Peer Resource Sharing’ <<https://www.cs.cornell.edu/people/egs/papers/karma.pdf>> accessed 23 October 2022.

⁵ C Dwork and M Naor, ‘Pricing via Processing or Combatting Junk Mail’ in EF Brickell (ed), *Advances in Cryptology – CRYPTO ’92* (Springer 1993).

⁶ Chainalysis, ‘The 2022 Crypto Crime Report’ <<https://www.chainalysis.com/>> accessed 17 October 2022.

transactions, such as those conducted by underage or mentally impaired owners of cryptoassets. These examples all give rise to ‘competing claims’, that is the question of who now holds legal title to the cryptoassets – both immediately after the irregular transaction, and later when the cryptoassets have been passed to third parties without notice of the impairments in title.

Conventional asset transfers have faced similar issues for centuries, which our legal systems have developed ways to resolve. These rules, obviously, apply to cryptoassets as they do to any other asset class, so we now have both legal and technological solutions to the same problem. This is simply another evolutionary step in a story which stretches from the clay tokens and bullas of the ancient Sumerians through various precious metals, to the seals, stamps, signatures, and polymer notes used to prevent forgery today.⁷ Nonetheless, the blockchain community at times still suggests the code itself cures all ills.

We focus in this article on the most pressing situation: competing claims to the ownership⁸ of cryptoassets when transacted on-chain⁹ in the secondary market.¹⁰ We argue that the best solutions to competing claims in this dire situation require an interplay of private law, financial regulation and technology.

We do so in three steps. We first show in Part II that competing claims are still largely unsolved by technology. Bypassing an in-depth analysis of private international law (choice-of-law rules),¹¹ we argue in Part III, from a comparative perspective, that neither does the law adequately address competing claims to cryptoassets. Part IV looks out for policy solutions and provides three principles for national lawmakers

⁷ DW Arner, J Barberis and RP Buckley, ‘The Evolution of FinTech: A New Post-Crisis Paradigm?’ (2016) 47(4) *Georgetown J Int Law* 1271.

⁸ We discuss whether crypto-assets can be ‘owned’ (see Section III.A. below). We do not deal with collateral transactions or other limited rights to crypto-assets. On collateral transactions, see the forthcoming UNIDROIT Principles for Digital Assets and Private Law (WG8 draft of March 2023), s V; The European Law Institute, ‘ELI Principles on the Use of Digital Assets as Security’ (2022) <<https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/use-of-digital-assets-as-security/>> accessed 17 October 2022.

⁹ Accordingly, this article does not cover custody. See UNIDROIT Principles for Digital Assets and Private Law, s IV; J Sarra and L Gullifer, ‘Crypto-Claimants and Bitcoin Bankruptcy: Challenges for Recognition and Realization’ (2019) 28 *Int Insolv Rev* 233, 260-271; M Solinas, ‘Investors’ Rights in (Crypto) Custodial Holdings: *Ruscoe v Cryptopia Ltd (in Liquidation)*’ (2021) 84(1) *MLR* 155, 156, 162; H Liu, L Gullifer, and H Chong, ‘Client-Intermediary Relations in the Crypto-Asset World’ in Paul S Davies and Tan Cheng-Han, *Intermediaries in the Commercial World* (Hart 2022) 213-234; M Haentjens et al, ‘The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them’ (2020) *Sing J Legal Stud* 526, 527.

¹⁰ As opposed to the primary market which involves the origination, issuance, or ‘minting’ of new crypto-assets.

¹¹ See M Lehmann, ‘Who Owns Bitcoin? Private Law Facing the Blockchain’ (2020) 21(1) *Minnesota Journal of Law, Science & Technology* 93, 111-116.

along with prioritised areas for international collaboration. Part V concludes.

2. Competing Claims Unsolved by Technology

We argue in this section that competing claims remain largely unsolved by the technology underlying cryptoassets. To provide some context, we describe briefly the technology before we show that DLT was never designed to deal adequately with competing claims.

A. What Problem Did Nakamoto Set Out to Solve?

As explained by Satoshi Nakamoto, '[c]ommercer on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments' so '[c]ompletely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes'.¹² He, she, or they go on to propose Bitcoin as an electronic alternative to physical cash by solving 'the double-spending problem'.¹³

B. Remaining Issues Unaddressed by Technology





Competing claims arise (1) in transfers, such as a sale, gift, or succession, and (2) in enforcement of individual or collective creditor claims, as in the case of insolvency. In both cases, either the asset is transferred from its true 'owner' to multiple persons that have mutually exclusive claims to the same asset ('double spending' problem), or the asset is transferred from an apparent 'owner' to a third party who now has a competing claim to that of the true owner ('apparent owner' problem).

At the height of the 'crypto winter', with multiple crypto-intermediaries (often dubbed inadequately 'crypto-exchanges') filing for insolvency, one might hope that DLT, in its attempt to create 'an electronic payment system based on cryptographic proof instead of trust',¹⁴ would address the perennial issue of competing claims. This is however not the case: Nakamoto's solution merely addresses the 'double spending' problem and only in a certain situation: on-chain transfers. This has several implications (see Figure 1):

¹² Nakamoto (n 2) 1.

¹³ Ibid.

¹⁴ Ibid.

Type of claim	Consensual transfers			DLT provides a solution ✓
	Creditor claims			DLT provides <u>no</u> solution ✗
		Double spending	Apparent owner	
		Type of problem		

First, DLT provides no solution to the case of creditor claims because these by definition arise off-chain. If a creditor through legal proceedings acquires rights to the debtor's cryptoassets, there is no *technical* solution stopping the debtor from transferring the cryptoassets to a third party (double spending problem). Similarly, if the debtor is in possession of the private key and thereby appears to be the owner of an account belonging to someone else, there is no *technical* solution preventing those cryptoassets from being seized by creditors through legal proceedings (apparent owner problem). In fact, these matters have proven practical when wallet providers and other crypto-intermediaries file for bankruptcy.¹⁵

Second, DLT provides no protections against illicit transfers due to the apparent owner problem. This means that holders of cryptoassets obtained through illicit acts, such as hacks (theft), fraud, blackmail, and ransomware attacks, appear as owners on the ledger and have the *technical* means to pass the cryptoassets on to innocent third parties. The same applies to cryptoassets obtained through other void transactions, such as those by underage or mentally impaired owners.¹⁶

Third, even for the problem that DLT was designed to solve, namely the double spending problem for transfers, the technical solution extends to on-chain transfers only. In practice, however, many and

¹⁵ See Sarra and Gullifer (n 9) 260-271; Solinas (n 9).

¹⁶ See Lehmann (n 11) 103-104.

perhaps most transactions in cryptoassets now occur off-chain by debiting and crediting internal accounts with a wallet provider.¹⁷

C. Competing Claims Facilitated by Technology

While an ingenious solution to the on-chain double spending problem, DLT comes with five side-effects that in fact exacerbate the issue of competing claims: (1) individual wallets have proven prone to cyber-attacks (theft), (2) the pseudonymous nature of private keys implies that transferees cannot validate whether the transferor has legal capacity to conduct the transaction, (3) the ownership of cryptoassets may easily be hidden from creditors seeking redress, (4) anonymous accounts further make it notoriously difficult to identify which courts have jurisdiction and which laws apply, and, finally, (5) DLT is designed to be immutable, so it is rarely an option to return cryptoassets to their rightful owner by rewriting the ledger.¹⁸ Even if the entire transaction history of the ledger is open for anyone to read, private keys provide anonymity. For all these reasons, criminals have embraced a technology otherwise designed for transparency.¹⁹ Importantly for this article, the issue of competing claims not only remains unresolved by DLT but is in fact *facilitated* by DLT.

3. Competing Claims Unsolved by Law

If DLT does not prevent competing claims, but rather facilitates them, we would hope law has solutions. Yet, as we argue in this section based on examples from several jurisdictions, the law does not effectively address competing claims to cryptoassets.

A. Cryptoassets as Property?

All competing claims derive from mutually contradictory rights to the same property, and different rules apply for different types of property. The first question to consider then is whether rights to cryptoassets constitute property rights (*in rem*), contractual rights (*in personam*), or something else. This matters in an insolvency, for instance, where

¹⁷ Solinas (n 9) 156, 162; Haentjens et al (n 9) 527.

¹⁸ Yet this does happen sometimes, eg, following ‘the DAO hack’: see K Yeung, ‘Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law’ (2019) 82(2) MLR 207, 233-235.

¹⁹ See R Houben and A Snyers, ‘Crypto-Assets: Key Developments, Regulatory Concerns and Responses’ (European Parliament ECON Committee Study 25, 2020) <[https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2020\)648779](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648779)> accessed 5 July 2022.

proprietary rights generally have priority over claims by creditors. The distinction could also be decisive under international choice-of-law rules.²⁰ If rights to cryptoassets are neither proprietary (*in rem*) nor contractual (*in personam*), moreover, then there is a question of whether they are legally enforceable at all because ownership rights typically do not arise in data / information or, more generally, in intangibles that are not contractual rights.²¹ For instance, as authors we may have the copyright to this article but we do not own the information in it, and so cannot prevent anyone from using the information once they have read it.

Most cryptoassets fall neatly into conventional legal categories because they represent conventional rights. *Utility tokens*, for instance, typically represent a contractual right against the issuer to receive some future product or service, equivalent to a conventional paper-based gift card or voucher. The same is true for *financial tokens*, which represent underlying rights in the same way as do share or bond certificates, and some types of *stablecoins* that also represent a claim on an issuer. Similarly, some cryptoassets represent physical property, equivalent to a title deed. In all these cases, the data are not the asset itself, but merely a representation thereof and evidence of an entitlement thereto.

Meanwhile, other cryptoassets, such as Bitcoin and many other cryptocurrencies, are the asset in and of themselves: The data stored on the ledger are valuable purely because other people believe in their scarcity. They represent neither a contractual right (*in personam*) nor are they a physical object, which has traditionally been seen as the main characteristic of property (*in rem*). The question of how to treat such cryptocurrencies was first put to a court in Japan following the massive hack and subsequent insolvency proceedings of MtGox Co. Ltd. (MtGox), the world's largest Bitcoin exchange in 2013. Japanese law recognises property in tangible things only, unless specifically provided otherwise, and the Tokyo District Court concluded that Bitcoin lacked the required corporeality to qualify as property.²² In the aftermath of the MtGox insolvency, Japan introduced amendments to its Payment Services Act, explicitly recognising property in cryptocurrency.²³ In the same vein,

²⁰ See Haentjens et al (n 9) 546-550.

²¹ With some exceptions, such as trademarks. See JD Michels and C Millard, 'The New Things: Property Rights in Digital Files?' (2022) 81(2) CLJ 323, ch 2.1; Sarra and Gullifer (n 9) 245; HR Howe and J Griffiths (eds), *Concepts of Property in Intellectual Property Law* (CUP 2013).

²² See Issue 2, District Court, Tokyo, 5 August 2015, (Japan, 2014 (Wa) 33320), Reference number 25541521, Unofficial English translation at <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf> accessed 17 October 2022.

²³ See M Ishikawa, 'Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case' (2017) 3 J Financ Regul 125, 126.

legislation has been passed in other jurisdictions, such as Russia²⁴ and the US state of Wyoming²⁵.

If cryptoassets consist purely of information stored on a ledger along with information in the form of public and private keys, this information should in our view not be seen as constituting the cryptoassets, but rather as a record of them and of the means of accessing them.²⁶ This makes cryptoassets profoundly different from other digital assets such as a digital photograph or a copy of this article, the value of which is the information itself. Rather, cryptocurrencies are more like physical cash.²⁷ Since the end of the gold standard, fiat currencies can no longer be seen as a claim on any underlying asset. Neither is the value of fiat currencies derived from the metal or paper of which they are made nor from the information printed on that metal or paper. In effect, the difference between information on the one hand, and cryptoassets or cash on the other, lies in scarcity, because information can be copied, while cryptoassets and cash are exclusive by design.²⁸ Therefore, cryptoassets and cash both meet typical criteria to qualify as property, such as being definable, rivalrous, and identifiable by third parties.²⁹

A logical conclusion would seem to be that cryptoassets should qualify as contractual rights (*in personam*) insofar as they represent a claim against someone and otherwise qualify as property (*in rem*) in the same way as cash. Yet, this is clearly not the case across jurisdictions

²⁴ Under the new Article 141.1 of the Russian Civil Code, 1994, following the Federal Law of 18 March 2019 No 34-FZ, ‘Regarding amending parts of the first, second and third part 1124 of the Civil Code of the Russian Federation’ (in force since 1 October 2019), ‘digital rights’ are ‘obligations and other rights, the content and conditions of which are determined in accordance with the rules of the information system that meets the criteria established by law.’ See Haentjens et al (n 9) 551.

²⁵ Virtual currency is classified as ‘intangible personal property’ under Article 34-29-102(a) US, SB 125, Digital assets-existing law, 2019-65, Gen Sess, Wyo, 2019 (effective as of 1 July 2019) <<https://www.wyoleg.gov/Legislation/2019/SF0125>> accessed 17 October 2022.

²⁶ See UK Jurisdiction Taskforce, ‘Legal Statement on Cryptoassets and Smart Contracts’ (2019) para 60 <<https://lawtechuk.io/explore/cryptoasset-and-smart-contract-statement>> accessed 17 October 2022.

²⁷ In the same vein, see B Geva et al, ‘The e-Banknote as a “Banknote”: A Monetary Law Interpreted’ (2021) 41(4) OJLS 1119.

²⁸ See *ibid* paras 62-63; T Cutts, ‘Crypto Property? Response to Public Consultation by the UK Jurisdiction Taskforce of the LawTech Delivery Panel’ (LSE Policy Briefing 36, 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406736> accessed 17 October 2022; D Fox, ‘Cryptocurrencies in the Common Law of Property’ in D Fox and S Greed (eds), *Cryptocurrencies in the Public and Private Law* (OUP 2019), 145-148.

²⁹ Most jurisdictions have no comprehensive definition of property, yet case law typically points to some characteristics. For digital assets specifically, see Michels and Millard (n 21) ch 2.1.2.

because we tend to see cash as corporeal, which cryptoassets are not.³⁰ In reality, however, the value of cash is detached from its physical medium of metal or paper in much the same way as the value of cryptoassets is detached from the physical computers on which they are stored.

Under Common Law, a related but not identical dichotomy exists between things in possession and things in action, where the first represents property characterised by the physical control over tangible assets and the latter is generally used to mean property that can be enforced only by court action – that is, legal rights against another person.³¹ According to the UK Jurisdiction Taskforce, ‘[a] cryptoasset is not a thing in possession because it [is] not tangible and so cannot be possessed’.³² However, they argue, ‘the term thing in action has also been used more broadly as a kind of “catch-all” to refer to any property that is not a thing in possession’.³³ Following this statement and emerging case law, the prevailing view now seems to be that cryptoassets can be owned under Common Law,³⁴ albeit either as things in action or possibly as a new, third category of things.³⁵

³⁰ See K Low and E Teo, ‘Bitcoins and Other Cryptocurrencies as Property?’ (2017) 9(2) *Law, Innovation and Technology* 235, 245.

³¹ The division goes at least back to *Colonial Bank v Whinney* [1885] 30 ChD 261, [1885] 11 App Cas 426 (HL). See UK Jurisdiction Taskforce (n 26) paras 67-68.

³² UK Jurisdiction Taskforce (ibid) para 67.

³³ Ibid para 69.

³⁴ See UK Jurisdiction Taskforce (n 26) paras 66-84; *Vorotyntseva v Money-4 Ltd t/a Nebeus.com and Others* [England, 2018] EWHC 2596 (Ch) (where Birrs J noted that there ‘was no suggestion that cryptocurrency cannot be a form of property’); *Shair.Com Global Digital Services Ltd v Arnold* [Canada, 2018] BCSC 1512; *AA v Persons Unknown* [England, 2019] EWHC 3556 (Comm), [2020] 4 WLR 35 (which was the first English judgment to explicitly recognise Bitcoin as property); CL-2020-840, *Ion Science Ltd and D Johns v Persons Unknown*, England, EWHC (Ch), Judgment of 21 December 2020, not yet reported; *Fetch.AI Ltd v Persons Unknown Category A and Others* [England, 2021] EWHC 2254 (Comm); *Mr Dollar Bill Ltd v Persons Unknown and Others* [England, 2021] EWHC 2718 (Ch); *Wang v Darby* [England, 2021] EWHC 3054 (Comm), [2022] WTLR 327; *Tulip Trading Ltd v Bitcoin Association for BSV and Others* [England, 2022] EWHC 667; *Danisz v Persons Unknown and Huobi Global Ltd* [England, 2022] EWHC 280 (QB), [2022] All ER (D) 107; *Osbourne v (1) Persons Unknown and (2) Ozone Networks Inc* [England, 2022] EWHC 1021 (acknowledging property to non-fungible tokens); *Ruscoe and Moore v Cryptopia Ltd (In Liquidation)* [New Zealand, 2020] NZHC 728, [2020] 2 NZLR 809; *ChainSwap Ltd v Persons Unknown* [British Virgin Islands, 2022] BVIHC 31 (Comm); *B2C2 Ltd v Quione Pte Ltd* [Singapore, 2019] SGHC(I) 03, [2019] 4 SLR 17, but the issue was left open on appeal: [2020] SGCA(I) 02, [2020] 2 SLR 20. See now, however, *CLM v CLN and Others* [2022] SGHC 46. See also Sarra and Gullifer (n 9) 242-248; RR Condon, ‘Bit-Property’ (2020) 79(2) CLJ 224; Geva (n 27) 1129; A Loke, ‘Mistakes in Algorithmic Trading of Cryptocurrencies’ (2020) 83(6) MLR 1343; Solinas (n 9) 156-161; Cutts (n 28); Fox (n 28) 139, 142-155; K Low and M Hara, ‘Cryptoassets and Property’ in S van Erp and K Zimmermann (eds), Low and Teo (n 30).

³⁵ See UK Jurisdiction Taskforce (n 26) paras 69, 86; The Law Commission (n 1) paras 10.55-10.138; Michels and Millard (n 21) ch 4.4.

B. The Nemo Dat Rule Applied to On-Chain Transfers

Both proprietary (*in rem*) and contractual (*in personam*) rights can typically be transferred, so they may give rise to competing claims. For these situations, the legal starting point can be summarised by the principle of *nemo dat quod non habet* or ‘no one can give what they do not have’.³⁶ Applied to the apparent owner problem, this means that the rights of the true owner prevail over those who may receive the cryptoassets from an apparent owner. A version of the same principle also applies to the double spending problem, which is then often referred to as *prior tempore, potitur jure* or ‘first in time, greater in right’.

This all builds on the assumption that multiple parties have claims on the same asset, which is not necessarily the case with on-chain transfers of cryptoassets: when A’s private-public key pair is used to send cryptoassets to an account represented by B’s public key, typically, no actual transfer of cryptoassets takes place between A and B. When Bitcoins are transferred, for instance, they are simply registered as ‘spent’ by the nodes in the network so they cannot be spent again, and an equivalent amount of new Bitcoins on the transferee’s account are acknowledged by the same nodes as available for new transactions.³⁷ For this reason, these coins are often referred to as ‘unspent transaction output’ (UTXO).³⁸ The technology varies across DLT protocols, yet the conclusion seems to persist: While perceived as a transfer of the same asset from one person to another by all parties involved, the cryptoasset passing from the transferor and that received by the transferee are technically not the same unit.³⁹

Thus, the UK Jurisdiction Taskforce argues that no transfer is taking place – the implication of which is that no competing claims exist to the same asset, the *nemo dat* rule and other legal principles for competing claims become irrelevant, and whoever gets the new cryptoassets recorded on their account in effect prevails.⁴⁰

We appreciate this de facto outcome, which somewhat resembles the rules we propose in this article (see Section IV.B. below). Yet, a substance over form argument should in our view prevail. Users of cryptocurrencies certainly view their transactions as transferring the same

³⁶ This Common Law principle is essentially equivalent to the Civil Law principle of *nemo plus iuris ad alium transferre potest quam ipse habet* or ‘one cannot transfer to another more rights than oneself has’.

³⁷ Fox (n 28) 143-145.

³⁸ See Sarra and Gullifer (n 9) 237; Cutts (n 2) 409; Fox (n 28) 143.

³⁹ The Law Commission (n 1) ch 12.

⁴⁰ See UK Jurisdiction Taskforce (n 26) paras 44-47.

units of value from one to another. It is also unclear how to draw the line between cryptoassets and other digitally recorded assets in this regard: certainly, securities that exist purely in the digital records of a custodian or central securities depository also do not change hands in the same way as do physical bearer securities. Yet, nobody has to our knowledge argued, in context of the *nemo dat* rule, that securities leaving the account of the seller are entirely different units from those reaching the account of the buyer even if they are recorded as completely different entries on the ledger.

C. Registration, Possession, and Negotiability

The *nemo dat* rule is a mere starting point and all jurisdictions allow for significant exceptions, as in the cases of property registers and negotiable instruments. For transfers, exceptions from the *nemo dat* rule are grounded in the need for well-functioning markets that protect the reasonable expectations of a bona fide purchaser for value.⁴¹ Similar exceptions are granted for creditor claims, with rules to prevent proforma or antedated transfers that seek to shield the debtor's assets from creditors seeking redress. Cryptoassets are designed to be negotiable, but this is typically not (yet) reflected in the law because exceptions from the *nemo dat* rule may be established only by statute or mercantile usage.⁴²

(i) Negotiability by statute

Some countries have adopted laws that make cryptoassets negotiable, essentially equating recording on a distributed ledger to physical possession or registration in central registries:

The first Common Law jurisdiction to adopt an Act on cryptoassets was the US state of Wyoming in 2019 – by which virtual currency is considered ‘money’, digital securities are considered ‘securities’, other cryptoassets may be considered ‘financial assets’, and all are treated as negotiable instruments under articles 8 and 9 of the *Uniform Commercial Code* (UCC).⁴³ The Act further treats ‘control’ over cryptoassets through a private key or multi-signature arrangement as equivalent to ‘possession’ under article 9 of the UCC.⁴⁴ Similar rules will most likely soon apply across the United States, as states adopt the 2022

⁴¹ See A Clarke and P Kohler, *Property Law: Commentary and Materials* (CUP 2005), 396-402.

⁴² See, eg, *Dixon v Bovill* [1856] 3 Macq HL 1, 16.

⁴³ Article 34-29-102(a) US, SB 125, Digital assets-existing law, 2019-65, Gen Sess, Wyo, 2019 (effective as of 1 July 2019) <<https://www.wyoleg.gov/Legislation/2019/SF0125>> accessed 17 October 2022.

⁴⁴ Article 34-29-103 (e) and (f) US, SB 125, Digital assets-existing law (ibid).

amendments to articles 9 and 12 of the UCC on ‘controllable electronic records’ (CERs).⁴⁵

France had earlier introduced its ‘DLT Order’ in 2017,⁴⁶ allowing issuers of some securities to register them on a distributed ledger with the same legal effect as if they were registered on a conventional securities registry. Similarly, the Luxembourg Blockchain I and II legislation allowed in 2019 and 2021,⁴⁷ respectively, securities first to be registered on DLT-based accounts and then the issuance and circulation of dematerialised securities directly using DLT. In principle, the Blockchain Laws requires DLT-based ledger entries to be treated analogously to book entries of dematerialised securities.

Meanwhile, the Liechtenstein Parliament adopted in 2019 an act applying to all ‘tokens’,⁴⁸ defined as representing claims or membership rights against a person, rights to things, or other absolute or relative rights.⁴⁹ Such tokens were made negotiable in the sense that a bona fide purchaser acquires good title when transacting with someone who has access to the private key.⁵⁰ Later, in 2020, the Swiss parliament passed the so called DLT Act,⁵¹ which amends ten existing acts to accommodate cryptoassets.⁵² For instance, new Articles 973d to 973i were added to the Code of Obligations,⁵³ which let all rights that can otherwise be represented by securities (as bearer securities or intermediated securities)

⁴⁵ See Uniform Law Commission, ‘2022 Amendments to UCC’ <<https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac>> accessed 22 November 2022.

⁴⁶ Order no 2017-1674 dated 8 December 2017 <<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036171908>> accessed 18 October 2022.

⁴⁷ See Law of 1 March 2019 amending the General Securities Law (Blockchain I) and Law of 22 January 2021 modifying (1) the law of 5 April 1993 on the financial sector and (2) the law of 6 April 2013 on dematerialised securities (Blockchain II).

⁴⁸ Gesetz vom 3.10.2019 über Token und VT-Dienstleister (VTG), Official Journal of Liechtenstein (Liechtensteinisches Landesgesetzblatt) 2019, No 301, 2 December 2019, 950.6. The act entered into force on 1 January 2020.

⁴⁹ Article 2(1)(c) VTG.

⁵⁰ Article 9 VTG.

⁵¹ Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register.

⁵² See RH Weber, ‘Neue Blockchain-Gesetzgebung in der Schweiz’ (2021) 4 *Recht Digital* 186; C Zellweger-Gutknecht and B Seiler, ‘Country Report Switzerland’ in P Maume, L Maute, and M Fromberger (eds), *The Law of Crypto Assets - A Handbook* (Bloomsbury 2020), 475–491.

⁵³ Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911, SR 220.

also be represented by securities recorded on a distributed ledger.⁵⁴ Finally, Germany adopted in 2021 a new act on electronic securities (eWpG). The Act essentially equates registration of bearer bonds in electronic form to the transfer of physical certificates, meaning that electronic registration allows for negotiability.⁵⁵ Further, the act entails a whole section on ‘crypto securities registries’,⁵⁶ and distributed ledgers are considered securities registries on equal terms with conventional, custodial ones.⁵⁷

For jurisdictions without specific legislation for DLT, a first question will be whether some cryptoassets may still be treated as negotiable under existing laws. For instance, cryptoassets that represent rights to tangible goods may qualify as electronic documents of title that may be recognised as negotiable in many jurisdictions,⁵⁸ following the recommendations of the UNCITRAL Model Law on Electronic Transferable Records.⁵⁹ For financial tokens, moreover, some jurisdictions may consider applying statutory rules for conventional securities registries by analogy – or even rules for paper-based negotiable instruments, for instance by interpreting terms like ‘possession’ of ‘documents’ as encompassing the control over cryptoassets through the possession of a private key.

A second question is whether existing laws may *prevent* certain cryptoassets from being treated as negotiable. In Scandinavia, for instance, the concept of negotiable, physical share certificates is now partly replaced by a rule stating that the right prevails of which the company was first notified, when shares in a limited liability company are transferred to several bona fide purchasers.⁶⁰ This rule presumably applies also to shares that are registered on a distributed ledger and thereby qualify as cryptoassets, with the consequence that notification to the company prevails over whatever is recorded on the distributed ledger – thereby undermining the main advantage of DLT as a technological solution to the double spending problem.

Finally, most cryptoassets do not fall neatly into existing legal categories like those of shares, bonds, or other negotiable instruments. Yet, if they resemble a conventional category, this raises a third question

⁵⁴ This comprises most asset tokens (including many stablecoins) and utility tokens (see Articles 620 et seq and 764 et seq CO), but not fiat-like payment tokens that constitute no claim on anyone.

⁵⁵ Article 26 eWpG.

⁵⁶ s 3 eWpG.

⁵⁷ Article 4(1) eWpG.

⁵⁸ See, eg, UCC § 7-106 and § 7-501; §§ 443(III), 475(c), and 516(II) of the German *Handelsgesetzbuch*.

⁵⁹ See, eg, Article 7 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf> accessed 17 October 2022.

⁶⁰ See Article 65 of the Danish Companies Act; Article 4-13(2) of the Norwegian Limited Liability Companies Act.

of whether the existing rules for that category apply. For instance, the PAquarium cryptoasset comes with a right to 20% of normal dividends and voting rights on the choice of location for the issuer's proposed aquarium. These cryptoassets therefore resemble shares, but they also provide lifetime free entry to the aquarium and may be used to purchase yet undefined goods at the aquarium premises.⁶¹ This raises the question of whether the rules for competing claims to shares apply to such cryptoassets, either directly or by analogy, and what the implications would be.

(ii) Negotiability by mercantile usage

In the absence of statutory rules, courts may also recognise exceptions from the *nemo dat* rule by mercantile usage. Under English law, for instance, this has been the norm for negotiable documents,⁶² and even in codified Civil Law systems legislative recognition was typically preceded by mercantile usage.⁶³

The situation with cryptoassets today is similar to that when *lex mercatoria* (merchant law) was adopted by legal systems across medieval Europe.⁶⁴ Since at least the 14th Century merchants developed a practice where intrinsically worthless pieces of paper were treated as representations of proprietary and contractual rights, which then gradually were accepted first by courts and then by legislators.⁶⁵ Just like today's tokenisation, anonymous wallets, and near immutable ledgers, early bearer instruments often entailed clever elements of financial engineering to overcome the *nemo dat* rule. For instance, in Lombardy the earliest ancestors of current bearer instruments were apparently seen neither as the contract itself nor even as evidence of the underlying contract, but rather as a document providing access to the assets pledged as security for fulfilment of the contract – so that, in effect, no contractual relationship was required between the debtor and the de facto creditor for the latter to invoke the security.⁶⁶ Similarly, in France, bills were drawn in blank to

⁶¹ See ESMA, 'Annex 1: Legal Qualifications of Crypto-Assets – Survey to NCAs' (ESMA50-157-1384, 2019) 24 <[esma50-157-1384 annex.pdf \(europa.eu\)](https://esma.europa.eu/press-material/press-news/press-news-details/esma50-157-1384-annex.pdf)> accessed 5 July 2022.

⁶² See UK Jurisdiction Taskforce (n 26) paras 113-122.

⁶³ See UNIDROIT Issues Paper, Study LXXXII – WG4 – Doc 2 (2021), 61.

⁶⁴ See Schuster (n 2) 995.

⁶⁵ See E Jenks, 'On the Early History of Negotiable Instruments' (1893) 9 LQR 70; JS Rogers, *The Early History of the Law of Bills and Notes* (CUP 1995); M Lobban, 'Negotiable Instruments' in W Cornish et al (eds), *The Oxford History of the Laws of England: Volume XII: 1829-1914 Private Law* (OUP 2010).

⁶⁶ See Jenks (ibid) 81-82.

conceal the fact that the document had indeed changed hands.⁶⁷ Yet, over time, such circumvention of the *nemo dat* rule became superfluous as negotiability was legally recognised.

The history of negotiable documents shows that legal systems often adapt to market practice in a process that can take centuries. In modern times the speed of technological and market developments is higher, of course, and thus mercantile usage can develop more quickly.⁶⁸ Even if the duration of a given practice is of relevance to establish mercantile usage, the number of transactions and the perception among participants in the market matter more.⁶⁹

A critical element here is what constitutes a relevant market: In our view, we are today much closer to an established mercantile usage in the market for pure payment tokens, for instance, than for tokens that represent underlying assets with an already established market practice. At least for Bitcoin and other non-stablecoin payment tokens, it is natural to view these either as a completely new asset class or somehow analogous to fiat currencies, which are already negotiable.⁷⁰ Given the high trading volumes in such coins today and the fact that market participants largely perceive the control over a private key as evidencing ownership of the coins, it should not be too difficult for a court to acknowledge an established mercantile usage of negotiability.

However, essentially all other cryptoassets represent conventional assets, where tokenisation to date represents but a very small fraction of the overall market for that asset class. This is obvious for financial tokens as part of the conventional market for financial instruments. With utility tokens it is worth asking if they represent something entirely new or are merely a different representation of gift cards or vouchers, for instance, where long held market practices already prevail and the establishment of an entirely new mercantile usage therefore would take time. This is the case with electronic documents of title, for example, where contracts now commonly provide for certain electronic documents to be treated as negotiable bills of lading. Yet at least under English law such clauses may be enforced only as between the parties because the new practice is not yet seen as amending the old mercantile usage of paper documents.⁷¹

⁶⁷ See *ibid* 85.

⁶⁸ See UK Jurisdiction Taskforce (n 26) para 122.

⁶⁹ See *Edelstein v Schuler & Co* [England, 1902] 2 KB 144 (KBD), 154.

⁷⁰ See *Miller v Race* [1758] 97 Eng Rep 398, 401; *Atlantic Cotton Mills v Indian Orchard Mills* [Mass 1888] 17 NE 496, 501; *Transamerica Insurance Co v Long* [WD Pa 1970] 318 F Supp 156; Clarke and Kohler (n 41) 399.

⁷¹ See UK Jurisdiction Taskforce (n 26) para 119; Aikens et al, *Bills of Lading*, (2nd edn, Informa 2015) para 2.119.

(iii) Negotiability by consent?

An agreement between the parties cannot establish negotiability, as this deals with the rights of third parties and is thus incompatible with the doctrine of privity of contract. However, an intriguing question is whether this could still be possible if *all* the relevant market participants somehow agree. Indeed, one could argue that since blockchains were made to solve the double spending problem, anyone that voluntarily participates in the network has agreed that ‘code is law’ for this purpose. Essentially, blockchains would then be considered multi-party contracts to which participants become parties by opting to use the network, and where the content of the contract is entailed in the information stored on the ledger together with the open source code.⁷²

We believe participation in the network could be seen as sufficient for consent under general principles of contract law. In fact, there is nothing new in the establishment of legally binding contracts through actions, such as taking a bite of an apple in a store or parking on a metered street – both of which require you to pay. Given the general expectation among market participants of ‘ownership’ as evidenced by control over a private key, it is easy for the participants to understand the rules of the game before setting up a wallet account and engaging in transactions. In some jurisdictions there are also examples of courts recognising the act of entering into a transaction as sufficient acceptance of contractual rules about the negotiability of the transacted goods.⁷³

Negotiability through such multi-party contracts would naturally bind only voluntary participants in the network.⁷⁴ Essentially, it would imply that cryptoassets become negotiable with regard to on-chain transactions, but not creditor claims, for instance. Even among network participants, moreover, courts may be reluctant to extend the effects of such contractual negotiability to the most extreme cases such as theft, fraud, and the like – either by arguing that there are limits to the freedom of contract or by requiring a more explicit form of consent to such far-reaching contractual terms.

⁷² See P Paech, ‘The Governance of Blockchain Financial Networks’ (2017) 80(6) MLR 1073, 1096; Haentjens et al (n 9) 552.

⁷³ For instance, in two consecutive cases (Rt 1940 p 450 and Rt 1955 p 536) the Supreme Court of Norway upheld that purchasers of LP records were bound by a prohibition against radio broadcasting that was printed on the record itself, thereby setting aside the Norwegian rule that a good faith purchaser for value gets full title by taking over the possession of physical goods.

⁷⁴ UK Jurisdiction Taskforce (n 26) para 134.

D. Competing Claims as an Issue Unsolved

From the above analysis, it is obvious that competing claims to cryptoassets remains an unsolved legal issue that needs to be addressed. Options include (1) not recognising property rights at all, (2) adhering to the *nemo dat* rule, (3) acknowledging negotiability (with further specification of its exact implications), and (4) avoiding the problem altogether by viewing the cryptoassets sent by the transferor and those received by the transferee as completely separate units of value so no competing claims exist to the same asset.

Each option has repercussions. For instance, to the extent that legal ownership or negotiability are *not* acknowledged, there would be a significant mismatch between the law and the general expectations of market participants. The situation may result in further confusion if the rules vary across different types of cryptoassets, as a result of existing legislation and mercantile usage diverging for different asset classes. To the extent negotiability can be founded on acceptance by the parties transacting on the ledger, different rules would even apply in the relationship between them and towards third parties, such as their creditors. With truly global cryptoasset markets and anonymous accounts, the legal uncertainty is amplified by the near practical impossibility of determining which country's laws apply and which courts have jurisdiction. With ambiguity as to the nature of property rights to cryptoassets, it is even uncertain whether international private law for property, contracts, or torts should be applied to resolve the matter.⁷⁵

All in all, this degree of legal uncertainty will be harmful to the further development of cryptoasset markets. Even though they represent billions of dollars in transaction value every day, the current 'crypto winter' indicates a certain lack of trust in cryptoasset markets.⁷⁶ This supports our view that more rather than less legal certainty is desirable: In the absence of good solutions to the competing claims issue, cryptoassets will remain unfit for large scale institutional investments and are doomed to remain a niche asset class.

How do we get where we need to be? One option is law-making *ex post*, i.e., by leaving the matter to the courts, which seems to be favoured by the UK Jurisdiction Taskforce.⁷⁷ Indeed, many of the desirable results can be achieved with purpose-oriented application of (that is: minor modifications to) the *lex lata*, and courts may be particularly good at identifying the nuances in the particular cases that come before them.

⁷⁵ See Lehmann (n 11) 111-116.

⁷⁶ See Reuters, 'Regulators Propose First Global Rules Before "Crypto Winter" Thaw' <<https://www.reuters.com/technology/regulators-propose-first-global-rules-before-crypto-winter-thaw-2022-10-11/>> accessed 18 October 2022.

⁷⁷ See UK Jurisdiction Taskforce (n 26) para 3.

Yet, developing case law takes times, and – most importantly – many cases. The legal uncertainty we have highlighted will reflect in the calculus of the claimants, thereby translating into higher legal costs and fewer suits. Where legal uncertainty prevails, we may see cases of outright fraud and theft being filed in court, but these may well not provide the finely tuned guidelines that are needed for crypto-transactions massive in scale and scope. All in all, fewer cases will likely come to court than will be needed to accompany and guide a fast-developing industry.

On the other hand, we do not necessarily argue for tightly drafted rules adopted by Parliament *ex ante*, which could well be harmful for innovation. Instead, we propose in the next section to adopt three broad principles that would address the issue of competing claims to cryptoassets.

4. Three Principles to Address Competing Claims

With DLT facilitating instead of mitigating competing claims, and with the law providing no remedy, the question arises of how holders of cryptoassets can be reasonably protected against competing claims to those assets? This section looks into potential solutions.

Competing claims to cryptoassets raise far-reaching political questions: Lawyers often underplay the significance of the technical solution to the on-chain double-spending problem, while technologists often underplay the importance of the broader competing claims issue. Many technologists see decentralisation as not just a feature, but as the entire purpose, of DLT.⁷⁸ This view – which rejects at its core the centralisation inherent to *any* legal system – is incompatible with *any* regulatory intervention other than an outright recognition of ‘code is law’.

While lawmakers in many jurisdictions are moving inexorably towards financial regulation of cryptoassets,⁷⁹ similar efforts to address the competing claims issue by legislation will be far more contentious because they undermine the very idea of a decentralised solution to the double spending problem. The question is of ideology: code vs. law, decentralised vs. centralised, and trustless vs. trust in institutions.⁸⁰ Today, this ideological divide finds its de facto resolution with cryptoasset

⁷⁸ See Fox (n 28) 140.

⁷⁹ On EU legislation, see DA Zetzsche, F Annunziata, RP Buckley, and DW Arner, ‘The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy’ (2021) 16(2) Cap Mark Law J 203; DA Zetzsche and J Woxholth, ‘The DLT Sandbox under the Pilot-Regulation’ (2022) 17(2) Cap Mark Law J 212.

⁸⁰ See Yeung (n 18).

proponents claiming to operate above or beyond the reach of the law.⁸¹ While they have something of a point to the extent law enforcement has proven very difficult, this approach is unacceptable in any society governed by law.

We need a legal framework that recognises the benefits of DLT and supports continued technological innovation yet addresses the problems that technology does not (yet) solve. In this spirit, we propose a solution centred on three broad principles: (1) laws must recognise property rights in cryptoassets, (2) negotiability must be linked to the control over private keys, and (3) laws must facilitate enforcement of rights in cryptoassets.

A. Property Rights

Market participants clearly believe and act as if they ‘own’ their cryptoassets, and this position should be supported by law. Recent history has shown that cryptoasset markets can work reasonably well without undisputed legal protection of property rights but that at times this leads to chaos, for instance in bankruptcy proceedings such as with Mt. Gox (see Section III.A. above). Therefore, the law must acknowledge property rights in cryptoassets.⁸²

The *type* of property rights is of lesser importance. They may vary indeed: cryptoassets that represent a claim on someone clearly constitute rights *in personam* and the similar things in action under Common Law, while typical cryptocurrencies represent no claim on anyone. From a pure *de lege ferenda* point of view, it is natural to view the control over such cryptocurrencies as a new digital equivalent to possession of physical things and, hence, categorise them as property *in rem* and the Common Law equivalent of a thing in possession.⁸³ Yet, for legal certainty, cryptoassets must simply be acknowledged as property, regardless of classification.

B. Negotiability

Our second principle is that the law must acknowledge negotiability in cryptoassets. While one could take the view that the current *de facto* negotiability of ‘code is law’ works in the vast majority of cases, as very

⁸¹ See AS Cloots, ‘Blockchain and the Law: The Rule of Code’ (2019) 78 CLJ 213, 214.

⁸² This approach is supported by the forthcoming UNIDROIT Principles for Digital Assets and Private Law, Principle 3(1).

⁸³ See Sarra and Gullifer (n 9) 244-246; D Carr, ‘Cryptocurrencies as Property in Civilian and Mixed Legal Systems’ in D Fox and S Greed (eds), *Cryptocurrencies in the Public and Private Law* (OUP 2019), 177-190.

few legal claims arise relative to the number of cryptoasset transactions,⁸⁴ the low number of cases could equally signal legal uncertainty, as market participants wonder whether law or technology will eventually prevail. The obvious solution is to bring the law closer in line with the underlying technology, essentially by acknowledging negotiability for cryptoassets and treating ‘control’ of the private key as equivalent to ‘possession’ for negotiable documents.⁸⁵

The next question is then *how much* the law should be brought in line with technology or, differently put, the exact *implications* of acknowledging negotiability. This is in part a question of which, if not all, cryptoassets to treat as negotiable and in part a matter of what such negotiability entails. The analogy with negotiable documents is illuminating:

As we have seen, negotiability entails an exception from the *nemo dat* rule, which can be established only by statute or mercantile usage (see Section III.C. above). A document representing an underlying asset may be treated as negotiable with effect to the title of that underlying asset only to the extent provided by either statute or mercantile usage. For instance, share or bond certificates are typically accepted as negotiable but a document pretending to represent legal title to a car or a basket of groceries is not. The context may also be relevant. For instance, the same car could be represented by a negotiable bill of lading in the context of transport by sea. The same logic must necessarily apply to cryptoassets, or existing laws could simply be circumvented by issuing crypto representations of conventional assets. Essentially, the law could provide for cryptoassets to represent underlying assets to the extent it currently does for conventional negotiable documents. When not representing underlying assets, as in the case of Bitcoin and most other payment tokens, cryptoassets should be treated as negotiable outright.⁸⁶

Even for conventional negotiable documents, moreover, legal systems do, to varying degrees, impose limits upon their negotiability. While the *nemo dat* rule protects the property rights of the rightful title holder, negotiability seeks to facilitate trade by protecting the expectations of market participants. Hence, negotiability is stronger where the rightful owner is somehow to blame for the emergence of competing claims and generally for asset classes where a well-functioning market is of particular

⁸⁵ In the same vein, see UNIDROIT Principles for Digital Assets and Private Law, s III; The Law Commission (n 1) ch 11 and 13.

⁸⁶ Another framing of the same concept is to acknowledge negotiability of the crypto-token itself, but not necessarily with effect on the title to any underlying real asset. See The UNIDROIT Principles for Digital Assets and Private Law, Principles 6 to 9, cf Principle 4; The Law Commission (n 1) paras 13.84-13.93.

importance to society. Consequently, legal systems tend to protect a title holder who has not (yet) acted to take possession of a negotiable document *less* than one who is an innocent victim of forgery, theft, fraud, or blackmail, or who lacks legal capacity.⁸⁷ On the contrary, as compared with other negotiable instruments, cash is typically treated as ‘super-negotiable’, reflecting the importance of legal tender in the functioning of all markets, so ‘even a thief can provide title to cash to a bona fide creditor’.⁸⁸ Even the super-negotiability of cash, however, is not unlimited as it does not apply to bad faith purchasers.⁸⁹ When assessing the reach of negotiability for cryptoassets, it is again natural to treat cryptoassets that reference other assets in the same way as their conventional negotiable document equivalents. For Bitcoin and other cryptocurrencies that reference no underlying asset, DLT proponents would certainly note the analogy to cash as an argument for something akin to the super-negotiability of legal tender.⁹⁰ In our view, however, the super-negotiability of cash is and should remain a narrow exception, so that cryptocurrencies should rather be treated like negotiable instruments more broadly.

The analogies to negotiable documents and legal tender beg the question of why legal systems accepted exceptions from the *nemo dat* rule for such instruments in the first place. In the case of cash, bank notes (first issued by private banks, not central banks) were certainly a more practical and secure way to transport large amounts of value than the precious metals that then constituted money.⁹¹ This facilitated trade and thus economic growth, which legal systems naturally wanted to promote. Similarly, negotiable documents provided a liquid market in bearer securities and, hence, cheaper financing for the emerging development of trading and, later, industrial companies. The negotiability of such documents proved to be profound financial and legal innovations of their time, which were recognised by courts and, later, legislatures. Yet, it is fair to assume that the same legal status would not be granted to such essentially worthless pieces of paper today if the issue were to arise *de novo*, because we now have better alternatives such as digital bank transfers and asset registries.

The answer, then, to what extent we should allow negotiability for cryptoassets may well depend on their societal benefits relative to the

⁸⁷ See Schuster (n 2) 996.

⁸⁸ Lehmann (n 11) 119.

⁸⁹ See note 70 above.

⁹⁰ This view is in line with the UNIDROIT Principles for Digital Assets and Private Law, Principle 8(4), which according to its commentary is intended specifically for cases of theft and hacks.

⁹¹ See Clarke and Kohler (n 41) 400.

alternatives.⁹² We will limit ourselves to three essential points: First, many of the proposed benefits of DLT deserve close scrutiny as they may be equally or better achieved by centralised ledgers. For instance, a central database can and should have back-ups, thereby realising many of the same data security benefits as DLT where data is stored in multiple nodes. The second point is that DLT can provide the benefits of trusted registries where none presently exist. Governments or private enterprises could well unlock the same benefits by setting up conventional, centralised ledgers to register rights in unlisted securities, pre-paid digital services, artefacts in video games, or digital art. Yet, governments typically do not respond quickly to such market demands, and private enterprise may struggle to generate the trust required for managing a centralised ledger. Hence, the trustless, decentralised nature of DLT can produce the same positive outcomes as centralised registers in areas where centralised registers are rarely established due to market failure. Third, in some developing countries people do not trust government-run land or other registries and recent political history sadly proves that even long-standing democracies are not immune from institutional decay. In such contexts, those who see decentralisation and independence from central authority as a goal in itself do have a point, even if it is typically somewhat overblown.

Potential future benefits of DLT would be compromised by a strict enforcement of the *nemo dat* rule. To unleash the full potential of cryptoassets, we must accept negotiability in most cases by acknowledging control of a private key as sufficient proof of legal title. This does not require full acceptance of ‘code is law’, so that negotiability would attach to the claims of bad faith purchasers – that would go even further than the super-negotiability of cash. Instead, we argue for treating the various kinds of cryptoassets like their negotiable document equivalents, if any, and for the drawing of broad analogies between the physical and the digital.

C. Enforcement

While we have advocated for the acknowledgment of property rights and negotiability for cryptoassets, the enforcement gap we have identified will compromise these private law principles. We see as core of this issue (1) how cryptoassets may be returned to their rightful owner, (2) how the holder of cryptoassets may be identified, (3) how to resolve cross-border

⁹² The literature on how to secure social benefits of Blockchain and DLT is abundant. Instead of many see C Brummer and Y Yadav, ‘Fintech and the Innovation Trilemma’ (2019) 107 *Georgetown Law Journal* 235; K Werbach, ‘Trust, but verify’ (2018) 33(2) *Berk Techn L J* 487.

situations, and (4) how to support enforcement through international coordination. We address each of these questions below.

(i) Reverse-transfer and 'tainting' of cryptoassets

Given the de facto immutability of DLT records, the theoretical option that legal title is restored by demanding from all nodes a rewrite of the ledger is unrealistic: too many countries and parties are involved. Instead, enforcement of claims may take place either by the return of private key(s) or a reverse-transfer of the cryptoassets to an account controlled by the rightful title holder.⁹³ This problem is not unique to cryptoassets but applies also to physical goods, cash, and negotiable documents.⁹⁴ When creditors claim the physical belongings of the debtor, for instance, they must be provided either with keys to the storage facility or outright physical possession of the assets.⁹⁵ Such court orders are typically enforced through fines for disobedience. The same can be used for claims to cryptoassets.

Notably, a reverse-transfer of cryptoassets to their rightful owner may often be claimed only as damages in kind, rather than as a proprietary claim, as it may be impossible to specify the individual identity of each token. Although DLT is designed for transparency, criminals frequently use dedicated mixing services to inhibit the tracing of individual cryptoassets.⁹⁶ This leaves the claimant with only an unsecured contractual claim in the debtor's estate in bankruptcy.⁹⁷ However, this is no different from the situation with other fungible assets that may be mixed and therefore become difficult to trace, if not outright untraceable.⁹⁸

The similarities between cryptoassets and negotiable documents support the idea of a legal framework by which control of the private key confers the same rights as possession of bearer instruments. Yet, the same similarities should not prevent the law from using features of DLT to go one step further in support of efficient enforcement. Given the transparent transaction history of open blockchains, one such opportunity lies in the 'tainting' of individual cryptoassets that are unlawfully controlled by someone other than their rightful owner. This would operate much like the automatic ink-staining of bank notes by anti-theft devices when criminals open protected cash containers such as ATMs or transport vehicles. Essentially, cryptoassets obtained by criminals could be identified and

⁹³ See Cutts (n 2) 434.

⁹⁴ See Lehmann (n 11) 131-132.

⁹⁵ Of course, the return of a private key for a blockchain account provides no assurance against copies of the same key still being in circulation – as is the case also with the return of physical keys to a storage facility for goods.

⁹⁶ See Fox (n 28) 163-136.

⁹⁷ See Paech (n 72) 1096.

⁹⁸ See Fox (n 28) 163-174.

added to a public register. If market participants over time develop a generally recognised register of this kind, supported by software to identify prospective transactions in the listed assets, it would be difficult for anyone to act in good faith and thereby obtain legal title as a bona fide purchaser for value.⁹⁹ While we believe market participants will eventually develop such practices, a register of tainted cryptoassets might more swiftly and usefully be established by legislation.

(ii) KYC and licensing of intermediaries

Even with perfectly written laws, it is often impossible to know *whom* to sue due to the prevalence of anonymous accounts. This anonymity may also translate into legal uncertainty over *where* to sue, given that court jurisdiction may be linked to the residence of the defendant(s). While the same is true for negotiable documents and physical goods, the mere act of physical delivery and possession often indicates which persons were involved. Further, the lack of enforcement in one area is clearly no good argument for allowing the same in a new field – particularly when the technology allows for enhanced transparency.

Hence, we ask parliaments to take two supporting steps by way of *financial regulation*. The first step is to mandate the licensing of crypto-custodians that hold assets for clients residing in their country; this type of legislation is already underway in several jurisdictions.¹⁰⁰ The mandatory license facilitates the second step, which is a strict ‘know-your-customer’ (KYC) requirement. These steps are not too far-reaching given that anti-money-laundering legislation applies a ‘KYC approach’ anyway to an intermediary’s *own* clients.¹⁰¹ But the approach may be taken further, as exemplified by the EU legislators’ efforts to demand from intermediaries the use of technology for *tracing* of cryptoasset flows.¹⁰² We encourage

⁹⁹ Ibid 172-174.

¹⁰⁰ For the UK, see Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, reg 56(1) (f) and (g); for the EU, see European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology, COM (2020) 594 final, at Article 53(1).

¹⁰¹ For the UK, see Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, reg 27, cf reg 8(1) (j) and (k); for the EU, see European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, COM (2021) 420 final, at Articles 3(3)(g) and 58(1).

¹⁰² See European Commission, Proposal for a Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets (Recast), COM (2021) 422 final.

the UK and US to follow suit.¹⁰³ Working together the US, UK, and EU could adopt the role of *global* standard setters.

The KYC and tracing approach rests on the fact that distributed ledgers register all transactions in blocks anyway. Under the rules just cited, the crypto-custodians need to make these data accessible for *public* enforcement. As an important step to reduce enforcement costs in cryptoassets, we therefore propose to mandate the provision of the data also for *private* enforcement.

(iii) *Jurisdiction and choice of law*

Even if the defendant(s) cannot be identified, as frequent case law shows,¹⁰⁴ courts may assert jurisdiction and facilitate law enforcement even when the defendant(s) are utterly unknown. In these cases, courts referred, for instance, to the domicile of crypto-intermediaries or asserted jurisdiction over known defendants as well as the persons unknown. Transparency of DLT-stored transactions assisted in proving what happened on-chain and which accounts were involved, even if the persons behind the accounts remain unknown. We appreciate this pragmatism and are inclined to go even further, for example by arguing that courts in any country where a node in a DLT network is located can assert jurisdiction.

Slightly differently and even more beneficially for claimants, English courts through several cases have applied English law with reference to *lex situs*, that is the law of the country where the object of a property right ('the thing') is located.¹⁰⁵ For lack of a definitive physical location, the courts have determined the *lex situs* of a cryptoasset to be the domicile or residence of its alleged owner.¹⁰⁶ Law enforcement was facilitated by the English courts' interim proprietary injunction paired with a 'Bankers Trust order', meaning that cryptoasset custodians must freeze the assets and disclose information about account holders.¹⁰⁷ While no panacea, these approaches have yielded encouraging results. Following the 'LCX Hack', for instance, around 60 per cent of the USD 8 million worth of stolen cryptoassets were frozen as a result of concerted law

¹⁰³ The UK was first proposing regulation similar to that of the EU but then modified the proposal: HM Treasury, 'Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022 – Response to the Consultation' para 6.21.

¹⁰⁴ See n 34 above.

¹⁰⁵ See *Ion Science Ltd and D Johns v Persons Unknown* (n 34); *Osbourne v (1) Persons Unknown and (2) Ozone Networks Inc* (n 34); *Tulip Trading Ltd v Bitcoin Association for BSV and Others* (n 34).

¹⁰⁶ Following *Tulip Trading Ltd v Bitcoin Association and Others* (ibid) the residence rather than the domicile now seems to be the appropriate determining factor.

¹⁰⁷ See *Ion Science Ltd and D Johns v Persons Unknown* (n 34); *Osbourne v (1) Persons Unknown and (2) Ozone Networks Inc* (n 34).

enforcement in four different countries.¹⁰⁸ These and similar actions by courts within existing international private law frameworks are strong foundations of a rule of law over cryptoassets.¹⁰⁹ Nevertheless, the licensing and KYC-rules just proposed herein, would grant the courts stronger powers over competing claims.

(iv) International coordination

Two issues remain for effective enforcement: On the one hand, unclear and diverging rules on jurisdiction and choice of law may prove costly to claimants. On the other hand, some countries may seek to adopt the status of libertarian ‘free havens’ to attract crypto business and thereby undermine efforts by other jurisdictions to promote law enforcement. We may also see blockchain networks themselves adopting terms of use with explicit choice-of-law clauses in favour of *laissez faire* jurisdictions.¹¹⁰ This may be challenged by courts on the basis of *ordre public* limitations,¹¹¹ resulting in a costly back-and-forth of legal actions.

While *full* harmonisation of national private laws is out of reach, some level of international consensus would strengthen the impact of the three principles outlined in this article. Efforts that highlight and analyse legal options for harmonisation deserve support.¹¹²

D. How our Solutions Solve the Competing Claims Issue

In this article, we posit that a combination of DLT and three broad legal principles effectively address the issue of competing claims to cryptoassets. Drawing on the main situations in which competing claims arise (see Section II.B. above), we now illustrate how this interplay between law and technology may play out.

In the apparent owner problem, the *nemo dat* rule applies and, as a default, the true owner prevails. Yet, a bona fide purchaser for value would prevail instead with exceptions for negotiable cryptoassets. In either case, the purchaser would assert de facto control over the cryptoassets, so *nemo dat* would ask courts to enforce law by the means

¹⁰⁸ See <<https://www.lcx.com/lcx-hack-update/>> accessed 14 June 2022.

¹⁰⁹ For alternative choice-of-law rules, see Lehmann (n 11) 111-116, 132-135.

¹¹⁰ Cf *ibid* 113.

¹¹¹ See Schuster (n 2) 1002.

¹¹² See in particular, the UNIDROIT Principles for Digital Assets and Private Law; The European Law Institute, ‘ELI Principles on the Use of Digital Assets as Security’; further, the ‘ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection’ put forward clauses on court jurisdiction and preference for reverse transactions.

described in Section IV.C. such that the true owner effectively prevails. Victims of fraud, hacks (theft), and ransomware attacks, to take the three most prominent examples, could recover their cryptoassets *unless* the law protects a bona fide purchaser for value to whom the assets have been transferred. Such a transfer, moreover, could be prevented by ‘tainting’ the assets in question.

If the law recognises property rights in cryptoassets, insolvency laws apply to these assets – as do laws that regulate creditor claims more broadly. The licensing of crypto-custodians, KYC and tracing rules proposed herein then support claimants in identifying the cryptoassets held by (potential) defendants. Proforma or antedated transactions could further be addressed by acknowledging the transfer of control on the ledger as providing the required notoriety in the same way as a transfer of possession does for negotiable documents.

Finally, the double spending problem for off-chain transfers would be resolved by the principle of *first in time, better in right* – unless a subsequent bona fide purchaser for value is first to assert control over the private key.

5. Conclusion

For most practical purposes, competing claims to cryptoassets are today resolved in practice by the ‘code is law’ impact of the software because it is difficult to enforce laws against market participants who hide behind anonymous accounts. While the technology effectively addresses on-chain double spending of cryptoassets, we have shown that neither technology nor law so far deals at all well with the broader issue of competing claims. This will provide significant uncertainty as crypto-intermediaries are being wound-up and are subjected to schemes of arrangement.

Our solution to this challenge requires three steps by legislatures, regulators and possibly courts: assign property rights to cryptoassets, establish that negotiability derives from control over the private key, and implement initiatives to lower enforcement cost. The latter includes licensing rules for custodians, KYC and tracing rules, and injunctive remedies addressed towards crypto-custodians.

With the ‘crypto winter’ at full height, each of these steps should be taken swiftly and effectively by national legislators to solve the most pressing issues. Beyond short-term crisis relief, such steps create a strong foundation for more holistic reforms over the years to come. However, as is so often the case with the law of commerce, the legal certainty the crypto-markets so desperately need today would be better delivered if these national efforts were to follow international coordination and harmonisation of laws along the lines proposed herein.