Minnesota Journal of Law, Science & Technology

Volume 21 | Issue 1 Article 4

2-7-2020

Who Owns Bitcoin? Private Law Facing the Blockchain

Matthias Lehmann

Who Owns Bitcoin? Private Law Facing the Blockchain

by Matthias Lehmann*

ABSTRACT

Blockchain, or "distributed ledger technology" (DLT), has been devised as an alternative to the law of finance. While it has become clear by now that regulation in the public interest is necessary—for example to avoid money laundering, drug dealing, or tax evasion—the particularly thorny issues of private law have been less discussed. These include, for instance, the right to reverse an erroneous transfer, the ownership of stolen coins, and the effects of succession or bankruptcy of a bitcoin holder. All of these questions require answers from a legal perspective because the technology does not answer them.

Particular difficulties arise when one tries to apply a property analysis to the blockchain. Surprisingly, it is far from clear how virtual currencies and other crypto assets are transferred and acquired. The traditional requirements posed by private law, such as an agreement between the parties and the transfer of possession, are incompatible with the technology. Moreover, the idea of a "void" or "null" transfer is hard to reconcile with the immutability that characterizes the blockchain.

---

* Director of the Institute for Private International and Comparative Law, University of Bonn, Germany. This paper was presented at a joint seminar of the University of Tokyo and Sophia University Tokyo on April 6, 2018, at a staff seminar at the City University of Hong Kong Law School on April 11, 2018, and at the Digiweek organized by the University of Lausanne (Switzerland) on February 16, 2019. I wish to thank the participants for their helpful comments, in particular Akira Tokutsu, Keisuke Takeshita, Tsubasa Oguri, Tadashi Kanzaki, Takahito Kato, Kelvin Fatt Kin Low, and Pok Chin Stephenson Chow. I am also grateful to the organizers, Professor Hiroyuki Kansaku, André Janssen, Anne-Christine Fornage, Eva Lein, and in particular Tetsuo Morishita, who provided crucial comments. Special thanks go to Stephen Williams for advice on technical issues.

Before any such questions can be answered, it is necessary to determine the law governing blockchain transfers and assets. This is the point where conflict of laws, or "private international law," comes into play. Conflicts lawyers are used to submitting legal relations to the law of the country with the most significant connection. But seemingly insurmountable problems occur because decentralized ledgers with no physical connecting factors do not lend themselves to this type of "localization" exercise.

The issue of this paper therefore is: How can blockchain be squared with traditional categories of private law, including private international law? The proposal made herein avoids the recourse to a newly fashioned "lex digitalis" or "lex cryptographica." Rather, it is suggested that the problems can be solved by using existing national laws, supplemented by an international text. At the same time, the results produced by DLT should also be accepted as legally protected and corrected only where necessary under the applicable national rules. In this way, a symbiosis between private law and innovative technology can be created.

INTRODUCTION

By now, virtually everybody has heard about the blockchain, or "distributed ledger technology" (DLT), as it is called among professionals. Claims that DLT is about to change the world or trigger a new informational revolution may have been greatly exaggerated.[1] What the technology offers is a mechanism for the

1. *Cf., e.g.*, Interview by Rik Kirkland with Don Tapscott, CEO, Tapscott Grp. (May 2016), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-blockchains-could-change-the-world [https://perma.cc/N7HS-RDNS] (explaining how blockchains could "revolutionize the world economy"); Andrew Gazdecki, *Five Ways Blockchain Could Change the World*, FORBES (Sept. 7, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/09/07/five-ways-blockchain-could-change-the

transfer of assets between two parties at any place in the world with an internet connection.[2] Importantly, its use is not limited to the transfer of virtual currencies and other crypto assets, but can also extend—through so-called tokenization—to objects of the physical world, such as gold, land, or stocks.[3] The main advantage of DLT is that it dispenses with the necessity of trust between the parties and sharply reduces the need for intermediaries.[4] This is the result of three hallmark features of DLT: pseudonimity, resilience, and immutability.[5] Pseudonymity denotes that although each transfer is recorded on a ledger that is open to the public, the identity of the parties to the transfer is not revealed.[6] The resilience of DLT stems from the fact that the ledger is distributed over a large number of nodes that cannot be easily attacked at the same time.[7] Finally, immutability means that the transfers cannot be undone once they have been recorded on the blockchain.[8]

As is by now equally well-known, DLT raises a number of legal problems, such as the possibility of money laundering, drug and arms dealing, terrorism financing, and the circumvention of

---

-world/#1f4b831273d7 [https://perma.cc/6937-RQU4] (providing five examples of the revolutionary nature of blockchains).

2. *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 2 (2018) (explaining blockchains and their potential role in the modern economy).

3. *See* Joshua A. T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 826–827 (2014) (describing how ownership in commodities, land, and stock might be tied to coins within a blockchain).

4. *See* Adrian Blundell-Wignall, *The Bitcoin Question: Currency Versus Trust-Less Transfer Technology* 7 (OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, 2014) (arguing that cryptocurrencies avoid the need for a trusted third party); Fairfield, *supra* note 3, at 814 (emphasizing that trustless public ledgers can avoid the enormous costs of generating trust).

5. *See* DE FILIPPI & WRIGHT, *supra* note 2, at 134 ("blockchains can store records in a tamper-resistant, resilient, and nonrepudiable manner.").

6. *See id.* at 38 ("[B]lockchains make it possible for a person to store information or engage in transactions without revealing one's true identity.").

7. *See id.* at 36–37 (explaining how the distributed nature of blockchains makes them resilient and tamper-resistant).

8. *See id.* at 37 (describing the "nonrepudiable" nature of all transaction data stored on a blockchain: "[O]nce a transaction occurs on a blockchain-based network, parties subject to that transaction will have a hard time denying involvement.").

embargoes.[9] Much ink has been spilled on these problems.[10] This contribution deals with an issue that has been less studied: the private law rules that underpin a DLT transfer. It tries to answer a couple of fundamental questions: Who owns the transferred assets? How can a transfer be reversed in case of a mistake or fraud? What are the legal consequences if the code is hacked and the virtual assets are stolen? What happens in case of death or bankruptcy of the bitcoin holder?

In the world of physical objects, the answers to these questions are found in private law. Property law in particular enumerates exhaustively the methods by which ownership may be transferred from one party to another. It imposes certain conditions, such as an agreement between the present and the prospective owner.[11] DLT neither requires nor ensures that such an agreement exists.[12] It merely relies on the fulfillment of technological requirements, namely the use of the correct private and public key.[13] The result produced by DLT may thus clash with classic private law.

On a meta-level lies an even more fundamental problem: the determination of the national law applicable to the transfer. For each and every transaction, a governing national law must be identified.[14] As DLT is a global and virtual transfer mechanism, it is impossible to identify the state which has the closest connection to it. The underlying difficulty is that the technology

---

9. *See, e.g.*, FINANCIAL ACTION TASK FORCE, VIRTUAL CURRENCIES – KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 17 (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

10. *See, e.g.*, Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox*, 20 RICH. J.L. & TECH. 13 (2014) (exposing the links of virtual currencies to numerous types of crimes); Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015) (arguing for a holistic technology specific regulation to combat risks of virtual currencies); Sarah Hughes & Stephen T. Middlebrook, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813 (2014) (discussing enforcement actions by U.S. legislators and regulators).

11. *See, e.g.*, JESSE DUKEMINIER ET AL., PROPERTY CONCISE EDITION 426 (2nd ed. 2017) (describing the agreement between a seller and a bona fide purchaser at common law).

12. *See infra* Section A.2.

13. *See, e.g.*, DE FILIPPI & WRIGHT, *supra* note 2, at 14–15 (introducing the concept of public-private key encryption).

14. *See* PETER HAY ET AL., CONFLICT OF LAWS 5 (5th ed. 2010) (describing choice of law in a property law context).

is completely delocalized and a-national, while the law is first and foremost made on the national level. Therefore, trying to identify the law applicable to DLT seems like putting a square peg in a round hole.[15]

This article is organized in the following way: The first part will show why private law is relevant for the blockchain although it has been devised as an alternative mechanism to the law. It will outline the numerous types of legal questions that arise and to which precise answers are needed. On the other hand, one must not ignore the specificity of DLT, which produces technically irreversible transfers in a decentralized manner without being connected to a particular state. The second part will demonstrate that these specificities pose obstacles to the application of classic concepts of private law. The third part suggests a way to reconcile the technology with the law and combine them into a meaningful whole. The fourth part will address counterarguments and complications, such as the problems of succession and bankruptcy. The fifth part concludes.

A. DOES CODE NEED LAW?

1. A GLOBAL TRANSFER MECHANISM WITHOUT A LEGAL BASIS

DLT is often presented as an alternative to legal solutions. It was originally designed to surmount the shortcomings of the trust-based banking system that gives banks and states a prominent role.[16] Satoshi Nakamoto, the pseudonym used in the original bitcoin proposal, saw these institutions as being inherently corrupt.[17] His goal was to eliminate the need for them by creating a peer-to-peer system in which transactions are recorded by a decentralized network of computers rather than intermediaries.[18]

---

15. *See infra* Section B.3.

16. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG https://bitcoin.org/bitcoin.pdf (last visited Dec. 5, 2019) (calling for "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need of a trusted third party.").

17. *See* Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*, 5 INTERNET POL'Y REV. 1, 4 (2016) ("Bitcoin aimed at eradicating corruption from the realm of currency issuance and exchange.").

18. *See id.* ("Bitcoin is often presented as an alternative monetary system, capable of bypassing most of the state-backed financial institutions. . . .").

The philosophical underpinnings of the blockchain stand in sharp tension to the rule of law. Anarchists, like "cypherpunks" and "crypto rebels,"[19] are attracted to DLT because they see autonomous cryptocurrencies as a safeguard of civil liberties against a Big Brother state.[20] The idea also appeals to neoliberals because it might toll the bell for the state's monopoly to create money.[21] For both ends of the political spectrum, the right-wing and the left-wing, DLT is essential to reduce the role of the government and its rules.[22] The anti-legalistic tendency is epitomized in the formula "code is law," which was coined by Lawrence Lessig, albeit with precisely the opposite intention: to demonstrate that the state should intervene in the internet's architecture.[23] Some authors maintain that the blockchain

---

19. *See generally* Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html [https://perma.cc/KR2Y-CZG4] ("[P]rivacy in an open society requires anonymous transaction systems . . . an anonymous system empowers individuals to reveal their identity when desired and only when desired. . . ."). The Cyperpunk's Manifesto builds on the earlier Crypto Anarchist Manifesto by Timothy C. May. *See* Timothy C. May, *The Crypto Anarchist Manifesto*, ACTIVISM.NET (Nov. 22, 1992), http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html [https://perma.cc/6GEG-58Y8] (predicting new technologies that will "alter completely the nature of government regulation, the ability to tax and control economic interactions, [and] the ability to keep information secret. . . .").

20. For the story of "crypto rebels" beating the government and "Big Brother," *see generally* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE (2001) (describing various instances of individuals who succeeded in protecting personal data from the government using cryptography).

21. *See, e.g.*, Nikolei Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation*, 25 LOY. CONSUM. L. REV. 111, 171 (2012) ("Allowing bitcoin to operate unfettered by substantial regulation allows it to contribute toward job creation, economic growth, and opportunity."). Neoliberals have long argued for the need of a currency that is independent from the state, *see* FRIEDRICH AUGUST HAYEK, DENATIONALISATION OF MONEY: THE ARGUMENT REFINED 133–34 (3rd ed. 1990) (arguing for a "Free Money Movement" to overcome central-bank-induced inflation).

22. *See, e.g.*, Scott H. Kimpel, *House of Representatives Approves Bipartisan Blockchain Bill*, THE HUNTON ANDREWS KURTH BLOCKCHAIN BLOG, https://www.blockchainlegalresource.com/2019/10/house-of-representatives-approves-bipartisan-blockchain-bill/ (describing a blockchain bill with bipartisan support in the U.S. House of Representatives).

23. Lawrence Lessig, *Code Is Law*, HARV. MAG. (Jan. 1, 2000), https://harvardmagazine.com/2000/01/code-is-law-html (last visited Dec. 5, 2019); *see also* LAWRENCE LESSIG, CODE: VERSION 2.0 1–8 (2006) (arguing that absent some state regulation cyberspace will become a tool of control).

would be governed by a non-state and a-national law for the digital age, which they call *lex cryptographica*.[24]

A quick look at the technology seems to confirm the idea that code is indeed replacing the law: DLT permits to transfer assets on the internet without any intervention by banks or other intermediaries that can be controlled by the state.[25] A DLT transfer is initiated when the transferor enters a unique digital key that is only known to him (a "private key") as well as the publicly known key of the transferee (a "public key") to a chain of digital signatures on the internet.[26] The transfer is then broadcast via a unique "hash" (a string of numbers) to computer servers (so-called "nodes"), which verify the validity of the keys and the conformity to the previous transfers in the chain.[27] Each of the nodes maintains its own copy of all transfers (the "ledger") against which it checks the new transfer.[28] The nodes work on a decentralized basis and are dispersed around the world (therefore "distributed ledger").[29] The nodes are assigned a "fee" to incentivize them to perform the verification work.[30] Their verification effort results in the addition of a new block to the chain (therefore "blockchain"). Once it is proven that enough work has been invested into the verification process, the longest blockchain—representing the decision of the majority of nodes—will be accepted by all others.[31] From this moment, the chain can no longer be altered without redoing all the verification work

---

24. *See* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 48 (Mar. 10, 2015), https://papers.ssrn.com/abstract=2580664 (last visited Mar. 28, 2018) (describing *lex cryptographica* as "a set of rules administered through self-executing smart contracts and decentralized (and potentially anonymous) organizations."). *See also* DE FILIPPI & WRIGHT, *supra* note 2, at 52 (claiming that with *lex cryptographica* "national laws get pushed to the edges").

25. *See* De Filippi & Loveluck, *supra* note 17 and accompanying text.

26. Nakamoto, *supra* note 16, at 2; ("We need a way for the payee to know that the previous owners did not sign any earlier transactions.").

27. *See id.*

28. *See id.* at 3 ("New transactions are broadcast to all nodes.").

29. *See id.* at 3–4 (explaining how such a decentralized system operates).

30. *See id.* at 4 (explaining how this fee structure incentivizes network support).

31. *Id.* at 2 ("[W]e need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.").

that has been done, which becomes even more difficult as new blocks are added.[32]

This whole process is independent of any legal rules. The transfer comes about by the transferor combining its private key with the public key of the transferee and the following confirmation of the transfer through the verification process.[33] None of this requires the intervention of notaries, lawyers, or intermediaries that could be supervised, e.g. banks, clearing agents, or depositories.[34] Nor does it need a contract, or any other legal agreement or act. In this sense, the characterization of code as law seems to be entirely fitting.

2. PRIVATE LAW PROBLEMS THAT MAY ARISE FROM DLT TRANSFERS

Although many consider DLT as independent from the law or an underpinning legal system, they nevertheless seem to assume that the technology yields legally binding results. For instance, it is very often said that the recipient of a transfer becomes the "owner" of the bitcoin,[35] or that concepts such as "ownership" and "property" would also apply to cryptocurrencies.[36] Statements like these presuppose that DLT transfers have some effect on the level of property law. But it is wholly unclear whether bitcoin and other virtual currencies can indeed be conceptualized as property from the point of view of

---

32. *See id.* at 3 ("To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.").

33. *See id.* at 2 (explaining how transactions incorporate private and public keys).

34. *See* De Filippi & Loveluck, *supra* note 17 and accompanying text.

35. *See* Kaplanov, *supra* note 21, at 123 ("[O]wner transfers her bitcoins to the purchaser. . ."); Sarah Meiklejohn et al*., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC'13 - PROCEEDINGS OF THE 13TH ACM CONFERENCE ON INTERNET MEASUREMENT 127 (2013) ("[B]itcoin can be thought of as a chain of *transactions* from one owner to the next. . . .") (emphasis in original). Kevin V. Tu, *Perfecting Bitcoin*, 52 GA. L. REV. 505, 548 (2017) ("Owners access, manage, and use their virtual currency with digital keys.").

36. *See* Michael Abramaowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 414 (2016) (claiming that a legal system's refusal to allow cryptocurrency ownership "would be self-defeating"); Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22, 29 (2014) (calling direct ownership of bitcoin "a new class of private property"); Fairfield, *supra* note 3 at 842–54 (suggesting to reconceptualize property law as the "law of information" in order to cover virtual assets like cryptocurrencies).

the common law.[37] An even more problematic but often neglected point is that one cannot assume the blockchain is exclusively or predominantly subject to the common law.[38] Given the division of the world into different states with diverging legal systems, each and every form of property exists by virtue of its recognition under some applicable national law.[39] It is first necessary to identify this law through the mechanics of conflicts of law before it can be applied to any phenomenon of the real or virtual world.

To blockchain enthusiasts, the search for an applicable property law is anathema.[40] They consider DLT as guaranteeing the position of the acquirer with absolute certainty, something that a real-world transaction with tons of documentation, lawyers, and courts cannot provide.[41] From their point of view, the technology does not need law.[42]

Yet this belief is wrong. Blockchain is designed to avoid "double spending," i.e. that the same owner transfers the bitcoin twice. It provides no safeguards at all against other problems

---

37. *See* Tatiana Cutts, *Bitcoin Ownership and its Impact on Fungibility*, COINDESK (June 14, 2015, 3:00 PM), https://www.coindesk.com/bitcoin-ownership-impact-fungibility (claiming that there is "a good policy reason for the conclusion that one cannot, in a private law sense, 'own' bitcoin"); Kelvin F. K. Low & Ernie G. S. Teo, *Legal Risks of Owning Cryptocurrencies*, 1 HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION 225–47 (2018) (stating that "it is not entirely clear what, if any legal rights, attach to bitcoins and other private cryptocurrencies like bitcoin"); Bayern, *supra* note 36, at 25–29 (arguing that "owning" Bitcoin may be a contract right rather than a property right).

38. *See* Low & Teo, *supra* note 37, at 9 ("It may come as a shock . . . but there is no such thing as digital money as a matter of law."); Bayern, *supra* note 36, at 33–34 (explaining that Bitcoin "does not fit neatly into classical categories" of common law).

39. *See generally* Carol M. Rose, *Possession as the Origin of Property*, 52 U. CHI. L. REV. 73, 84–85 (1985) ("It is not enough, then, for the property claimant to say simply, 'It's mine' through some act or gesture; in order for the 'statement' to have any force, some relevant world must understand the claim it makes and take that claim seriously.").

40. Bayern, *supra* note 36, at 25 (questioning the meaning of "hold[ing] a bitcoin").

41. *Cf.* Fairfield, *supra* note 3, at 29–31 (explaining that courts often rely on imprecise and unhelpful distinctions, such as physicality, causing them to wrongly apply intellectual property law to digital objects, thereby denying the appropriate protections of law).

42. *See* May, *supra* note 19 (predicting that developments in information technology such as cryptographic protocols "will alter completely the nature of government"); Hughes, *supra* note 19 ("Even laws against cryptography reach only so far as a nation's border and the arm of its violence.").

that may occur.[43] The following provides some illustrations of such problems. In order to get a better overview, they will be divided into those that are endogenous, i.e. inherent to the transaction, and those that are exogenous, i.e. rooted in events outside the blockchain.[44]

a) Endogenous Transfer Problems

Many problems inherent to the transaction may plague a DLT transfer. One of them is that the transferor may have made a mistake.[45] He might, for instance, have entered the wrong number of bitcoin, e.g. "10" instead of "1." It is also conceivable that the transferor's assent to the bitcoin transfer was induced by fraud or material misrepresentation because the transferee has made false allegations to induce the transferor to use its private key. Furthermore, it is possible that the transferor acted under the influence of an improper threat by the transferee, thereby forcing her to make the transfer. This is by no means a farfetched possibility, given that many online blackmailers today demand payment in bitcoin, e.g. in exchange for abstaining from the publication of private information on the internet.[46]

From a legal point of view, in all of these situations the contract that entails the property transfer is voidable.[47] Yet

---

43. *See, e.g.*, Low & Teo, *supra* note 37, at 22 (explaining the blockchain protocols "only promise to prevent double-spending"); *see also* Nakamoto, *supra* note 16, at 1 (proposing "a solution to the double-spending problem using a peer-to-peer distributed time stamp server . . . .").

44. *See* PRIMAVERA DE FILIPPI & GREG MCMULLEN, GOVERNANCE OF BLOCKCHAIN SYSTEMS: GOVERNANCE OF AND BY DISTRIBUTED INFRASTRUCTURE 16 (2018), https://hal.archives-ouvertes.fr/hal-02046787/document (explaining the difference between endogenous and exogenous rules).

45. *See generally* DE FILIPPI & WRIGHT, *supra* note 2, at 44 (explaining "it can be difficult to unwind the transaction retroactively" if bitcoin is sent to the wrong address).

46. *See* Cristina Miranda, *How to Avoid a Bitcoin Blackmail Scam*, FEDERAL TRADE COMMISSION BLOG (Aug. 21, 2018), https://www.consumer.ftc.gov/blog/2018/08/how-avoid-bitcoin-blackmail-scam [https://perma.cc/Z7F6-J8MT] (describing a scheme in which payments in bitcoin were extorted from men in exchange for silence about an alleged affair).

47. *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 153, 164, 175 (AM. LAW INST. 1981) (providing that a contract made under the influence of a mistake, fraud, or an improper threat is voidable).

under the blockchain, the transfer is effective.[48] For an effective transfer, it suffices that the correct codes have been used.[49] Transfers of bitcoins are recorded as long as the correct private key of the transferor is combined with an existing public key of a transferee.[50] The technology does not take into account mistakes, fraud, or improper threats.[51] These are not part of the algorithm.

Even worse, the cryptocurrency transfer is also effective where it is not supported by any agreement at all. This may occur where the transferor or the transferee has been subject to some strong form of incapacity, for instance, because they suffer from a mental illness or defect.[52] One must also not discard the possibility that the parties to the transfer have never been in contact.[53] For example, the transferor could have confused the public key of the transferee with that of another person. Or the transferee could hack the computer of the transferor, copy his private key, and used it to transfer to bitcoin to himself. In these cases, no contract has been concluded between both sides.[54] Yet from a technological point of view, the transfers would be effective.[55]

b) Exogenous Transfer Problems

Exogenous events are those that have no relation to the blockchain but nevertheless have the potential to impact the

---

48. *See, e.g.*, DE FILIPPI & WRIGHT, *supra* note 2, at 21 (explaining the validity of Bitcoin transactions with the aid of a private key); *accord* Meiklejohn, *supra* note 35, at 2 (describing the basic Bitcoin protocol).

49. *See* DE FILIPPI & WRIGHT, *supra* note 2 and the accompanying text.

50. *Id.*

51. *Id.* at 4 (noting that the technology requires regulations to prevent it from being used for criminal and illicit activities).

52. *See* RESTATEMENT (SECOND) OF CONTRACTS § 13 (AM. LAW INST. 1981) (providing that a person has no capacity to incur contractual duties if his property is under guardianship by reason of an adjudication of mental illness or defect).

53. *See* DE FILIPPI & WRIGHT, *supra* note 2, at 38–39 (explaining that blockchain technology allows transactions to occur without the parties to the transaction revealing their true identity or trusting each other as long as both parties "trust the underlying technical infrastructure").

54. *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 17, 18, 22 (AM. LAW INST. 1981) (providing that a contract requires mutual assent on behalf of both parties to the contract, and that the manifestation of mutual assent be in relation to the manifestation of the other).

55. *See* DE FILIPPI & WRIGHT, *supra* 2 and the accompanying text.

ownership of crypto assets.[56] One salient example is succession or inheritance law. In most legal systems, in case of death the assets of the decedent are vested in their entirety in the heirs or the executor of a will.[57] This transfer is automatic and not conditioned on any transmission of possession or other act. Arguably, it also includes any cryptocurrency that the decedent had acquired.[58] Since the decedent is no longer able to dispose of these coins, his successors must have become the "owners" outside of the DLT.[59] The question is how and under which national law does this transfer happen legally.

Exogenous problems may also occur in case of bankruptcy. Typically, the bankruptcy trustee steps into the shoes of the debtor and acquires the right to dispose of all of the latter's assets in order to satisfy the creditors.[60] This power arguably extends to virtual assets, such as bitcoin, which can make up a

---

56. *See* DE FILIPPI & MCMULLEN, *supra* note 44, at 16 (explaining exogenous rules).

57. *See e.g.*, M.J. de Waal, *Law of Succession*, *in* INTRODUCTION TO THE LAW OF SOUTH AFRICA 169 (C.G. Van der Merwe & J.E. Du Plessis eds., 2004) (describing the transformation of South African law from the Roman-Dutch concept of universal succession to the English system of executorship); HENRY DYSON, FRENCH PROPERTY AND INHERITANCE LAW: PRINCIPLES AND PRACTICE 313 (1st ed. 2003) (explaining the vesting of the decedent's assets in her lawful heirs under French law); WILLIAM M. MCGOVERN JR., SHELDON F. KURTZ & DAVID M. ENGLISH, WILLS, TRUSTS AND ESTATES, INCLUDING TAXATION AND FUTURE INTERESTS, 4TH 49–133 (4th ed. 2010) (outlining intestate succession and effects of wills); Catherine Rendell, *Payment of Expenses, Debts, and Pecuniary Legacies, in* LAW OF SUCCESSION 193 (Catherine Rendell ed., 1997) (describing the devolution of the decedent's assets on his personal representative under English law).

58. *See*, *e.g.*, Ana-Caterina Anitei, *Digital Inheritance: Problems, Cases and Solutions*, INT'L. CONF. EDUC. & CREATIVITY. FOR A KNOWLEDGE-BASED SOC'Y. 32 (2017) (characterizing bitcoin as part of the "digital inheritance"); Naomi Cahn, *Probate Law Meets the Digital Age*, 67 VAND. L. REV. 1697, 1702–05 (2014) (considering bitcoins as "digital assets" subject to probate law); L. A. G. M. van der Geld, *De Executeur in een Nalatenschap met Bitcoins en Andere 'Digitale Bezittingen'*, 8 TIJDSCHR. ERFRECHT 122 (2014) (discussing the executor's obligation to search for digital assets of the deceased, such as bitcoin, under Dutch law. This article was among the first to discuss the problem of inheritance of digital assets).

59. For an example of such inheritance under Dutch law, *see* Anna Berlee, *Digital Inheritance in the Netherlands*, 6 J. EUR. CONSUMER & MARKET L. 256 (2017).

60. *See* HENRY CAMPBELL BLACK, A TREATISE ON THE LAW AND PRACTICE OF BANKRUPTCY: UNDER THE ACT OF CONGRESS OF 1898 AND ITS AMENDMENTS 42 (3rd ed. 1922) ("Property, wherever situated, which is not exempt, passes to and vests in the trustee...").

sizeable proportion of the debtor's wealth. Furthermore, many legal systems endow the bankruptcy trustee with the power to avoid transactions made before the opening of the bankruptcy proceedings that favor particular creditors over others.[61] To achieve its goal of protecting the bankruptcy estate against fraudulent, biased, or suspect transfers by the debtor, this power must also extend to bitcoin and other virtual currency payments.[62] The treatment of cryptocurrencies in bankruptcy proceedings is the subject of intense legal discussion.[63] Independently of the correct characterization, it should be clear that crypto assets are part of the debtor's estate and, as such, must be used for the benefit of his creditors.

3. INTERMEDIATE CONCLUSION

The problems discussed, whether they are endogenous or exogenous to the blockchain, affect the private relationships between individuals. They concern the parties to a bitcoin transfer, but also third parties such as the heirs or creditors of a holder of crypto assets. None of these issues are taken into account by the functioning of DLT. The blockchain largely ignores them. Real-life problems like mistake, duress, death, or bankruptcy are not solved by decentralizing a ledger in which transactions are recorded. In all of these cases, a rational outcome cannot be ensured without the intervention of the law.

---

61. *See* 11 U.S.C. § 544 (2012) (giving the trustee the right to avoid certain transfers made by the debtor).

62. *See, e.g.*, Order on Motion for Partial Summary Judgment, HashFast Technologies LLC v. Lowe (*In re HashFast Technologies LLC)*, No. 14-30725-DM, (Bnkr N.D. Cal. Feb. 23, 2016) (granting, in a partial summary judgment, recovery of the value of the bitcoin at the time of the transfer to the defendant, in which case the bankruptcy trustee of the plaintiff sought to recover 3000 bitcoin that had been paid to the defendant before the plaintiff had gone into administration).

63. *See, e.g.*, David E. Kronenberg & Daniel Gwen, *Bitcoins in Bankruptcy: Trouble Ahead for Investors and Bankruptcy Professionals?*, 10 PRATT'S J. BANKR. L. 112, 116 (2014) (categorizing bitcoin as "property" for the purposes of the Bankruptcy Code); Chelsea Deppert, *Bitcoin and Bankruptcy: Putting the Bits Together*, 32 EMORY BANKR. DEV. J. 123 (2015) (defending a characterization as "currency"). The courts differ on whether bitcoin can be considered as property or currency, *see* United States v. Petix, 2016 WL 7017919 (W.D.N.Y. Dec. 1, 2016) (holding that bitcoin is not money in the ordinary sense of the term); United States v. Mansy, 2017 WL 9672554 (D. Maine May 11, 2017) (stating that the court is not persuaded by the reasoning in *United States v. Petix*).

B. CODE'S RESISTANCE TO THE LAW

To solve the problems mentioned, one could simply try to apply the concepts, principles, and rules of private law to DLT. This would entail determining for each and every operation on the blockchain the applicable national law and checking whether its requirements for the transfer of property are fulfilled. Yet such a legalistic approach cannot overcome the gap between law and technology. There are several stumbling blocks that stand in its way.

1. THE AUTONOMY OF THE BLOCKCHAIN VIS-À-VIS NATIONAL LAW

The first obstacle on the road to applying the law to DLT is its autonomy. The technology operates independently from the law.[64] It is also impossible for the law to impose its requirements on the blockchain.[65]

The problem is well illustrated by the case of stolen bitcoin that a thief transfers to his own public key.[66] Legally, this transfer should be invalid given that the holder of the bitcoin has never agreed to it.[67] But when the correct codes are entered and broadcast to the nodes, a new private key is created for the recipient in about ten minutes, the average time to confirm a bitcoin transaction.[68] This private key gives the transferee the factual power to dispose of the crypto currency despite the fact that there was no legal basis for the transfer.[69] Though the

---

64. *See* Fairfield, *supra* note 3, at 809 (discussing the insulation and autonomy of blockchain property).

65. *See* discussions *supra* Part A.1.

66. *See, e.g.*, Joey Garrison, *2 Men Arrested in Elaborate Plot to Steal $550K in Cryptocurrency by Hacking Social Media Accounts*, USA TODAY, https://www.usatoday.com/story/news/nation/2019/11/15/massachusetts-men-arrested-plot-steal-cryptocurrency-bitcoin-social-media-threats/4201763002/ [https://perma.cc/B62X-GTFS] (last updated Nov. 15, 2019, 3:19 PM) (reporting examples of stolen bitcoins); Michael Kaplan, *Hackers are Stealing Millions in Bitcoin—and Living Like Big Shots*, NY POST (Apr. 13, 2019, 2:43 PM), https://nypost.com/2019/04/13/hackers-are-stealing-millions-in-bitcoin-and-living-like-big-shots/ [https://perma.cc/G3EN-6ZUM] (reporting examples of stolen bitcoins).

67. *See* RESTATEMENT (SECOND) OF CONTRACTS *supra* note 47 and the accompanying text.

68. *See How Long Does It Take to Transfer Bitcoins and Why?*, COINSUTRA, https://coinsutra.com/bitcoin-transfer-time/ (last updated Aug. 6, 2019) (explaining why it takes ten minutes to confirm a transaction).

69. *See* DE FILIPPI & WRIGHT, *supra* note 2 and the accompanying text.

recipient cannot be considered the "owner" of the bitcoin in a legal sense, he has obtained the ability to transfer via the blockchain. It is impossible to prevent him from exercising this power by, for example, sending the bitcoin to a third party. Any transfer made by him leads to the creation of a new private key in the transferee's favor, who can be anywhere on the planet. This new key can then be used again to create a further new private key for anybody in the world, and so on. The process is legally unstoppable.

Another illustration of the blockchain's resistance to the law is the hypothetical of succession. Let us imagine "*A*," dying intestate with his private key stored on an office computer to which his employer has exclusive access. Legally, all of *A*'s assets belong to his estate.[70] Yet factually, the employer has the private key in his possession, which gives her unlimited power to send the crypto currency to anybody she wants. The legitimate heir or executor of the will, in turn, is unable to dispose of the crypto asset as he lacks the private key. There is no way to obtain it other than via the blockchain. The technology resists accounting for the death of the bitcoin holder because the event takes place outside of the blockchain.

What emerges in these cases is that the divide between law and technology cannot be easily overcome. DLT is a self-contained mechanism that works autonomously and is shielded from outside influences. A transfer of crypto assets is effective on the blockchain whenever the private and public keys are used, and only in this case. For this reason, the hacker who obtained bitcoins illegally can dispose of them, whereas an heir or executor who is legally entitled to them cannot. To make DLT compatible with the law would require a complete reconceptualization of the technology. This cannot be done under the protocol in its current form.

2. THE IRREVERSIBILITY OF BLOCKCHAIN TRANSFERS

One could attempt to avoid the clash between technology and the law by "correcting" the blockchain after a transfer is executed. Instead of requiring title or property as a condition of transfer, one might, for instance, consider the transfer made by the thief to himself in the example above as being invalid. As a

---

70. *See* MCGOVERN ET. AL., *supra* note 57, at 8 (defining "estate" as the property of the decedent).

consequence, the newly added block of the chain would have to be deleted and the original owner and victim of the theft would have to be reinstated as the rightful holder of the bitcoin. The same procedure could be used where someone other than the heir of the bitcoin holder or the executor of his will disposes of his assets. In other words, the blockchain would be changed *subsequent* to the transfer in such a way as to restore the parties to their original positions.

Such a corrective approach would, however, be inhibited by another feature of the blockchain: its immutability or "nonrepudiability."[71] Once a transfer has been added to the chain in the form of a block, the information can no longer be removed technologically. The chain has been transformed forever and can only be accepted by other nodes as such. Every transfer on the blockchain is, therefore, immutable, which is one of the major reasons why DLT is particularly tamper-proof and can dispense with trust.[72]

One must partially qualify the characterization of blockchain transfers as immutable. There are a great variety of DLT networks, which represent different trade-offs in terms of reversibility and finality of transactions.[73] They can be roughly divided into permissioned and permissionless networks.[74] Permissionless systems are those in which anybody can

---

71. *See* DE FILIPPI & WRIGHT, *supra* note 2, at 37 (stating that the data stored on the blockchain is nonrepudiable).

72. *See* discussion *supra* Part A.1.

73. *See, e.g.*, Xiwei Xu et al., *A Taxonomy of Blockchain-Based Systems for Architecture Design*, IEEE INT'L CONF. ON SOFTWARE ARCHITECTURE 246 (2017), http://ieeexplore.ieee.org/document/7930224/ (last visited Mar 26, 2018); Richard Gendal Brown, *A Simple Model to Make Sense of the Proliferation of Distributed Ledger, Smart Contract and Cryptocurrency Projects* (2014), https://gendal.me/2014/12/19/a-simple-model-to-make-sense-of-the -proliferation-of-distributed-ledger-smart-contract-and-cryptocurrency -projects/ (last visited Mar 27, 2018); Tim Swanson, *Consensus-as-a-service: a Brief Report on the Emergence of Permissioned, Distributed Ledger Systems* 12–14 (April 6, 2015), *available at:* http://www.ofnumbers.com/wp-content /uploads/2015/04/Permissioned-distributed-ledgers.pdf.

74. *See* Xu et al., *supra* note 73 at 246 (describing permissioned and permissionless blockchain as two design options for blockchains). *Cf.* Till Neudecker & Hannes Hartenstein, *Network Layer Aspects of Permissionless Blockchains*, 21 IEEE COMM. SURV. & TUTORIALS 838, 838 (2019) (characterizing permissionless systems as unstructured peer-to-peer networks that typically rely on the consensus of the participants, not a central operator).

participate and where consensus is thus highly distributed.[75] In contrast, permissioned systems feature one or more authorities that act as gatekeepers.[76] They allow participants into the network and sometimes also confirm transfers.[77] In a permissioned system of the latter type, i.e. one with confirmation powers limited to some nodes, it is relatively easy to reverse a transaction with the help of the authorities in charge.[78] Yet reversals are also not unthinkable in other types of permissioned and even in permissionless systems.[79] They are effectuated by creating a so-called hard fork that splits the blockchain protocol in two. This happened, for example, to the Bitcoin network when it was reorganized in 2013,[80] and with the Ethereum network after a considerable amount of the cryptocurrency was siphoned off by hackers in 2016.[81] In both instances, a new version of the blockchain was created. While the case of Bitcoin seems to have been relatively unproblematic, in the case of Ethereum, the old, hacked ledger refused to die, which resulted in the parallel existence of two separate currencies: Ethereum (One) and Ethereum Classic.[82]

The example of Ethereum illustrates that a reversal of the blockchain comes at a hefty price. Two parallel versions of the same ledger are far from ideal and may lead to many problems. Those who have invested in the "dying" ledger are deprived of the "real" cryptocurrency. All other participants will be confused

---

75. *See* Neudecker & Hartenstein, *supra* note 74 and the accompanying text.

76. *See* Xu et al., *supra* note 73, at 245 ("[A] blockchain may be permissioned in requiring that one or more authorities act as a gate for participation.").

77. *See id*. (including permission to "join the network . . . , permission to initiate transactions, or permission to mine").

78. *Cf*. Swanson, *supra* note 73, at 26 (discussing permissioned blockchains and accountability for reversals).

79. *See, e.g.*, *id*. at 21 (noting reversal possibility in a permissionless blockchain such as Bitcoin).

80. *See* Vitalik Buterin, *Bitcoin Network Shaken by Blockchain Fork*, BITCOIN MAG. (Mar. 12, 2013, 11:14 PM), https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ ("Starting from block 225430, the blockchain literally split into two . . . . For the next six hours, there were effectively two Bitcoin networks . . . .").

81. *See* Eduard Gómez, *The Ethereum Hard Fork & Ethereum Classic*, MERKLE (July 21, 2016), https://themerkle.com/the-ethereum-hard-fork-ethereum-classic/ [https://perma.cc/4PRJ-X59G].

82. *See* Low & Teo, *supra* note 37, at 19.

by the parallel existence of two versions of the same ledger.[83] Both effects undermine trust in the cryptocurrency. It is hard to overestimate the negative repercussions since the value of the cryptocurrency depends first and foremost on trust.[84] Therefore, a hard fork is not a viable option except for the most extreme and rare cases, such as the discovery of a major hack that corrupts a very large number of transfers. For all other purposes, undoing a DLT transfer is impracticable.

3. THE A-NATIONAL CHARACTER OF THE BLOCKCHAIN

Another problem that stands in the way of applying law to the blockchain is that before one could do so, it would first be necessary to determine *which* national law applies. The rules of private law are mainly made at the level of the state. Since the world is split into states with differing rules of private law, there is no such thing as a global law for private transactions. In order to assess any blockchain transfer in legal terms, one must, therefore, first determine the applicable national law. This is the task of conflict of laws, or "private international law" as it is called in many parts of the world.[85] Conflict of laws works by attributing sets of facts or "relations" to the law of the state with which it has the closest connection.[86] DLT presents a formidable challenge for this methodology.

The blockchain is a global or "transnational" transfer mechanism that has little to no connections with any particular state. Transfers are executed on the basis of private and public keys without determining the location of the parties.[87] The

---

83. *Id*.

84. *See supra* note 4 and the accompanying text.

85. *See, e.g.*, HAY ET. AL., *supra* note 14, at 1 (defining conflict of laws as "the body of law that aspires to provide solutions to international or interstate legal disputes between persons or entities other than countries or states *as such*") (emphasis in original); *See also* JAMES FAWCETT & JANEEN CARRUTHERS, CHESHIRE, NORTH & FAWCETT: PRIVATE INTERNATIONAL LAW 3 (Peter North ed., 14th ed. 2008) (explaining that private international law "comes into operation whenever the court is faced with a claim that contains a foreign element").

86. *See* FAWCETT & CARRUTHERS, *supra* note 85, at 682 (explaining the "most closely connected" test for determining which law governs in international contract law); HAY ET. AL., *supra* note 14, at 16–18 (providing a background of Savigny's theory of the seat); *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145 (1971) (regarding the applicable law for torts).

87. *See* Nakamoto, *supra* note 16, at 2 (illustrating the transaction process with respect to public and private keys).

protocols are stored on computers worldwide. Anybody can participate in permissionless systems like Bitcoin for there is no authority or server that controls access.[88] Confirmations take place through distributed consent from nodes all over the world.[89] It is thus not exaggerated to say that permissionless systems are completely de-nationalized and not connected to any particular country, which makes it impossible to determine the state with the closest connection.

A further problem is that most conflict-of-laws systems provide different rules for different types of relations. They distinguish between contracts, torts, property, and succession, to name but a few.[90] To fit the blockchain technology into of one of these categories is challenging, to say the least. On the one hand, there is clearly a transactional aspect to blockchain in the cases where the transfer is accompanied by an agreement between the transferor and the transferee.[91] On the other hand, a property law analysis may also seem apposite because the coins or other assets encrypted on the blockchain often have market value and can be assimilated to goods which are the object of property law.[92]

Let us consider for a moment the implications of one or the other qualification. A contractual qualification would lead to the principle of party autonomy, according to which the parties to a contract can freely select the law applying to their agreement.[93]

---

88. *See* Xu et. al., *supra* note 73, at 245 (explaining that permissionless systems are completely open to new users).

89. *See id*. at 244 (explaining that nodes in a network validate transactions and propagate them to their peers, potentially around the globe).

90. *See, e.g.*, HAY ET. AL., *supra* note 14, at 147–49 (explaining that subject matter characterization of the legal dispute at issue is "the natural and necessary starting point for the analysis of any conflicts case.").

91. Some authors therefore speak of the "transactions on a blockchain." *See* DE FILIPPI & WRIGHT, *supra* note 2, at 6 (describing the function of blockchain protocols in regard to transactions on a blockchain).

92. *See* Fairfield, *supra* note 3, at 843 (describing goods as property).

93. *See* Russell J. Weintraub, *Functional Developments in Choice of Law for Contracts*, 187 HAGUE ACAD. COLLECTED COURSES ONLINE 239, 271 (1984) (describing party autonomy as "perhaps the most widely accepted private international law rule of our time"). The principle has, for instance, been recognized in Commission Regulation 593/2008 of 17 June 2008, On the Law Applicable to Contractual Obligations, 2008 O.J. (L 177) 10, art. 3(1) [hereinafter *Rome I*]. *See also* Hō no Tekiyō ni Kansuru Tsūsokuhō [Act on the General Rules of Application of Laws], Law No. 78 of 2006, art. 7 (Japan), *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law

If followed strictly, this principle would allow the parties to choose the law applying to the transfer. As a result, a great variety of different laws would govern DLT. A different law could apply to each transfer recorded on the chain, depending on the choice made by the individual parties. This would be incompatible with the coherence of the chain. Also, the law that the transferor and the transferee have chosen would be unknown from the perspective of other participants, except where this choice had been coded into the blockchain, which is highly unusual and not easy from a technical point of view.

One could instead embed a *central* choice of law in the protocol of the cryptocurrency. The chosen law would then govern *all* transactions with the digital asset.[94] Yet it is very unlikely that such a choice of a national law would be made because it is contradictory to the explicit anti-legal philosophy underlying Bitcoin.[95] Such a choice is incompatible with the ideals of crypto aficionados,[96] and is therefore unlikely to be

---

/detail/?id=1970 (providing that "[t]he formation and effect of a judicial act shall be governed by the law of the place chosen by the parties at the time of the act"); Bundesgesetz über das Internationale Privatrecht [IPRG] [Federal Act on Private International Law] Dec. 18, 1987, SR 291, art. 116 (Switz.) [hereinafter *Swiss PILA*] (stating that "[i]n matters involving an economic interest, the task of establishing foreign law may be assigned to the parties"); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1210 (Russ) (providing that parties who enter into a contract "may select by agreement between them select [sic] the law that will govern their rights and duties under the contract") (http://en.smb.gov.ru/support/regulation/ccpart3/); Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和国涉外民事关系法律适用法) [Law of the People's Republic of China on Application of Law in Foreign-related Civil Relations] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2010, effective April 1, 2001), Chap. 6, art. 41 (China), *translated in* 2010 CHINA LAW LEXIS 3009 (stating that "[t]he parties may select by agreement the law applicable to a contract"); Inter-American Convention on the Law Applicable to International Contracts, Org. Am. St., art. 7, Mar. 17, 1994, 33 I.L.M. 732 (stating that "[t]he contract shall be governed by the law chosen by the parties"); Hague Conf. on Priv. Int'l L. [HCPIL], *Principles on Choice of Law in International Commercial Contracts*, art. 2 § 1, (Mar. 19, 2015) (stating that "[a] contract is governed by the law chosen by the parties.").

94. This option has been envisaged by the Financial Markets Law Committee (FMLC). *See Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*, FIN. MKTS. L. COMITY Mar. 2018, at 15 [hereinafter FMLC], http://www.fmlc.org/dlt-and-governing-law.html (last visited Mar. 27, 2018) (considering the law chosen by the network participants for the DLT system as "elective *situs*").

95. *See* May, *supra* note 19 and accompanying text.

96. *See supra* Section A.1.

made. Moreover, it would give a single state plenary power over the blockchain, which lends itself to abuse. Applying one national law exclusively may be appropriate for some permissioned systems that are backed up by one or several authorities sitting in a certain country, yet it seems inappropriate for permissionless systems that are open to the whole world and not connected to any particular state.

In case no law has been chosen, a contractual qualification would lead to the applicability of default conflicts rules. Many legal systems point to the law at the habitual residence of the party that is to perform the characteristic obligation as the law governing contracts in the absence of a choice.[97] But such a default rule would not work for the anonymous transfers on the blockchain, in which neither the identity nor the address of the transferor is known.

These difficulties in applying classic conflict rules for contracts point to a larger problem: These rules are designed for the exchange of goods or services between parties that know each other, not for pseudonymous transfers of crypto assets in a computer system. It is not even justified to assume that a DLT transfer is supported by an agreement, since it can also be the result of a mistake or coercion.[98] In this sense, a contract conflicts-of-laws analysis creates many issues that are insurmountable.

If one instead characterizes crypto transfers as property, the law that would normally apply is the *lex rei sitae*, which is the law of the state where the object of the property right—"the thing"—is located.[99] Such a locational exercise would be all but impossible for a virtual object stored in the blockchain. These objects "exist" only in the ledger that is distributed among numerous computers around the world. The simple truth is that a bitcoin has no geographical home and is impossible to locate.

There are, however, variations and adaptations of the *lex rei sitae* rule that one could attempt to follow. For instance, many states apply the so-called PRIMA rule for incorporeal securities, which refers to the law in force at the place of the relevant

---

97. *See Rome I*, *supra* note 93, at art. 4(1), (2); *Swiss PILA*, *supra* note 93, at art. 117.

98. See *supra* Section A.2.b.

99. *See, e.g.*, HAY ET. AL., *supra* note 14, at 1253–54 (applying the law of the *situs* to tangible moveable property).

intermediary.[100] This approach could be used, e.g., for permissioned systems without an explicit choice of law. One could submit them, e.g., to the law of the relevant operator, even though its role is not precisely the same as that of an intermediary administering "accounts" of securities.[101] But while such an approach may perhaps work for permissioned systems, it is not feasible in a permissionless environment, which gives no special status to any of the participants spread around the world. The PRIMA rule therefore does not fit blockchains such as those for Bitcoin.[102]

A third route between contract and property could be to use the conflict-of-laws rules for assignment. Assignment is a special technique whereby the assignor transfers a nonphysical claim to the transferee.[103] It is usually effectuated by a simple agreement between both parties. Once perfected, the transfer of the claim is effective against third parties, such as creditors of the transferor or competing transferors.[104] Hence, assignment can, to a certain extent, be assimilated to the transfer of property in intangible objects. The conflict-of-laws rules that apply to assignment are, however, notoriously uncertain and oscillate between different solutions, such as applying the law in force at the domicile of the transferor, the law governing the assignment, or the law underlying the claim.[105] Moreover, any analogy

---

100. Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary art. 4, adopted July 5, 2006, 17 T.I.A.S. 401. The Convention has been signed by the United States and Switzerland.

101. *FMLC*, *supra* note 94, at 18–19 (suggesting two approaches: the Place of the Relevant Operating Authority/Administrator (PROPA) approach or the Primary Residence of the Encryption Private Master Key Holder (PREMA) approach).

102. *See id.* at 11 (noting that the *lex situs* does not translate well when applied to a DLT ledger).

103. *See, e.g.*, HAY ET. AL., *supra* note 14, at 1279–81 (discussing the assignment of intangibles).

104. *See id.* at 1280–81 (discussing assignment for the benefit of creditors).

105. *See, e.g.*, Harry C. Sigman & Eva-Maria Kieninger, *The Law of Assignment of Receivables: in Flux, Still Uncertain, Still Non-Uniform*, *in* CROSS-BORDER SECURITY OVER RECEIVABLES 1, 43–74 (Harry C. Sigman & Eva-Maria Kieninger eds., 2009) (discussing various solutions to determine the law applicable to assignment); AXEL FLESSNER & HENDRIK VERHAGEN, ASSIGNMENT IN EUROPEAN PRIVATE INTERNATIONAL LAW: CLAIMS AS PROPERTY AND THE EUROPEAN COMMISSION'S "ROME I PROPOSAL" 77–78 (2006) (defending the application of the law chosen by the parties to the assignment); Francisco Garcimartín Alférez, *Assignment of Claims in the Rome I Regulation: Article 14*, *in* ROME I REGULATION: THE LAW APPLICABLE TO CONTRACTUAL

between blockchain and assignment is bound to fail because the scope of application of the blockchain is much wider than that of assignment. Besides incorporeal claims, it can be used to transfer virtual assets, like cryptocurrencies, or intellectual property rights, e.g. copyrights in pictures. One can even employ DLT to transfer physical assets, whether movables or immovables, through tokenization.[106] These assets are very different from claims and call for different conflict rules.

In sum, none of the received conflict-of-laws solutions lends itself to DLT. This problem is fundamental because it stands in the way of developing new substantive rules that are specific to the blockchain. Proposals such as those to reconceptualize property law[107] or to recognize bitcoin as a new kind of property[108] are built on the implicit assumption that a certain national law governs the blockchain (often the common law). Yet they fail to address the primary question of how this law is determined, or which version of the common law they mean, and why it is this and not another national law that applies. A set of substantive rules that could eliminate conflicts issues and govern the blockchain as a whole would have to be global in scope. We are, however, far away from having such a law. In fact, it is nowhere in sight.

C. HOW TO RECONCILE DLT AND PRIVATE LAW

The law that applies to blockchain transfers and the resulting positions presents a conundrum. In the following, a proposal will be made. Before doing so, this article will explain the outer constraints that every proposal must respect regarding the application of private law to DLT.

1. UNDERPINNINGS OF THE PROPOSAL

Any suggestion for combining the blockchain with private law must take into consideration all three problems that have been identified in the preceding section: the autonomy of DLT, the immutability of transfers, and the a-national character of the blockchain. What is needed is a mechanism that respects the

---

OBLIGATIONS IN EUROPE 217, 217 (Franco Ferrari & Stefan Leible eds., 2009) (discussing the impact of *Rome I* on the law applicable to assignment).

106. *See* Fairfield, *supra* note 3, at 826–27.

107. *Id.* at 842–63.

108. *See* Bayern, *supra* note 36, at 29.

result of bitcoin transactions—in particular, one that does not try to reverse them and press them into the *Procrustes* bed of national law—while at the same time responds to the requirements of private justice. In addition, such an approach should not require the elaboration of uniform global rules, which at the moment seem elusive. Instead, it should be fully compatible with the division in national laws that currently exists.

The forthcoming proposal respects all four conditions. It suggests an application of the law that respects the autonomy of DLT, the immutability of transfers and abstains from imposing one national law on the whole blockchain, all without requiring the development of new global rules. Even though this may seem like a perfect solution, the proposal risks coming under fire from both the proponents of the technology as well as from lawyers, because it is based on certain underpinnings that either of them may dislike. To reduce this risk, these fundamental underpinning shall be disclosed in the following. Basically, the proposal is driven by two convictions for which it should not be attacked.

The first conviction is that the blockchain is a useful innovation that can yield significant societal benefits and should therefore be allowed to continue to flourish.[109] DLT provides a stable, nonrepudiable and largely tamper-proof mechanism to transfer assets around the world. In the great majority of cases, and provided it is not abused for illegal purposes, it works perfectly without the law.[110] This is an advantage that should be maintained. The attractiveness of DLT would greatly suffer if lawyers tried to change the code. Even indirect changes should be avoided, such as a requirement to include a choice of law in the blockchain, for these changes would gravely compromise the functioning of DLT.

The second conviction is that code is not law and that the positions obtained on the blockchain cannot be the end point of

---

109. *See, e.g.*, Fairfield, *supra* note 3, at 874 (characterizing DLT as trustless ledgers tracking transactions in real time at comparatively low cost).

110. At the end of the third quarter of 2019, a total number of 311,396 Bitcoin daily transactions were recorded world-wide. *See Number of Daily Bitcoin Transactions from 1st Quarter 2016 to 3rd Quarter 2019,* STATISTA, https://www.statista.com/statistics/730806/daily-number-of-bitcoin -transactions/ (last visited Feb. 2, 2019). This number contrasts with the very few instances in which legal problems or disputes have arisen.

ownership analysis but instead require supplementation and additions. Though it works in the majority of cases, in exceptional situations the law must correct the result achieved by the use of DLT. This article has identified above the instances of mistake, fraud, and improper threat, but also those of theft, bankruptcy and succession. From a legal point of view, all of these circumstances require a solution different from that of the blockchain. As the technology does not provide it, the law must step in. It should do so not by invalidating the transfer—something which would be technologically unfeasible. Instead, another means must be established to achieve a balanced and just result.

In sum, there is undeniably a tension between the law and the blockchain. Nevertheless, they must be reconciled if one shares the two convictions just outlined. The thesis of the following proposal is that the blockchain and private law are not mutually exclusive but can exist beside each other. Law and technology must neither ignore nor fight one other. They should live in a symbiosis with each leaving to the other its own field of competence.

2. ACCEPT DLT AS A FACT

The first step of the new solution is that the law should not interfere with the blockchain. The technology should essentially continue to function as it currently does without the law and without the intervention of lawyers. Transfers should be done on the basis of private and public keys only. Any introduction of legal conditions or requirements should be omitted.

This means that the law should not question the validity of blockchain transactions. This would be a hopeless enterprise anyway. The power of the holder of bitcoin resides in his knowledge of the private key. This and the public key of the recipient is all that is needed to initiate a transfer. To call such a transfer "invalid" from a legal point of view would not change the factual power of the private key's holder to initiate a new transfer, which will then result in a corresponding power of the recipient, and so on. Importantly, this result comes about by technology, not by the law. The legal system is unable to avoid

the passing on of crypto assets, and it should not try to inhibit it.[111]

Instead, the immutability of the transfer from a technical point of view is a fact that lawyers must accept. Choosing to ignore it would come at the cost of failing to provide a solution that is workable in real life.

One may compare the situation to that of a cash payment: The transfer in this case comes about by a factual element, the delivery of one or more banknotes or coins. The law accepts and confirms the transfer because the transferee becomes the owner of the banknote from a legal perspective. This is not the case where an agreement supporting the transfer is lacking, e.g., because the money has been stolen. Yet even a thief can provide title to cash to a bona fide creditor.[112] The fact that he possesses the notes or coins allows him to transfer title to a transferee in good faith. The original owner keeps his title and can demand the cash back only as long as the illegal possessor has not spent the money.[113]

A similar type of legal analysis should also be applied to DLT. The entry into the blockchain is a fact that reveals the current holder of the crypto asset. This position allows him factually and legally to procure title to another recipient. In order to determine this power, it is unnecessary to investigate the validity of the previous transactions recorded on the blockchain. Specifically, one should not go back in time by conducting a "title search" to find out whether the transferor had a position she can transfer, and her predecessor, and so on. As in the case of cash, such a title search is counterproductive because of the fungibility of coins and their function as means of

---

111. *See* WRIGHT & DE FILIPPI, *supra* note 2 at 184 (stressing that any attempt by the government to introduce a technological backdoor or other access control on both hardware and software makes the technology weaker).

112. *See* Miller v. Race, (1758) 97 Eng. Rep. 398, 401 ("[I]n the case of money stolen, the true owner can not recover it, after it has been paid away fairly and honestly upon a valuable and bona fide consideration . . . "); *see also* Transamerica Insurance Co. v. Long, 318 F. Supp. 156 (W.D. Pa. 1970) (denying restitution of money that a bank robber had paid to tax authorities); Atlantic Cotton Mills v. Indian Orchard Mills, 17 N.E. 496, 501 (Mass. 1888) ("There is no doubt that a thief may use stolen money . . . to pay his debts, and in such case an innocent creditor may retain the payment."). *See generally* Andrew Kull, *Defenses to Restitution: The Bona Fide Creditor*, 81 B.U. L. REV. 919, 937 (2001) (providing further cases and commentary on stolen money used for debts).

113. Miller v. Race, (1758) 97 Eng. Rep. 398, 401 ("[B]ut before money has passed in currency, an action may be brought for the money itself . . . . ").

payment. Lawyers should not second-guess the blockchain by controlling each and every transfer, either giving it their stamp of approval or denying its validity. This approach would make DLT essentially useless; it would become an expensive record system without any practical value. One should therefore accept the record on the blockchain as a fact which creates the power to transfer. This also means that those that have obtained a private key via DLT should, without any showing to the contrary, be seen as the legitimate holders of the crypto asset. As such, their position deserves to be protected by the law.[114]

An exception should apply only where it can be proven that the crypto asset has been obtained illegally, in particular by hacking, blackmailing, or fraud. In these cases, the presumption of a legal effect is rebutted. The exceptional situation is similar to that of a stolen banknote and will be dealt with in more detail later.[115] Apart from such an event, a transfer on the blockchain should be accepted as such.

3. FOCUS ON THE REVERSE TRANSACTION

The fact that transfers recorded on the blockchain cannot be undone does not mean, however, that one would have to consider the situation as presented by the blockchain as final.[116] Though it is impossible to delete a block once it has been added to the chain, the law can reverse *the effects* of such transfer. The means for doing this is ordering a reverse transfer.[117] For instance, though the record of a transfer of bitcoin cannot be undone and deleted from the blockchain, the recipient of an erroneous transfer can be obliged to transfer the cryptocurrency back to the sender. The same obligation can be imposed on the party that has not effectuated its counter-performance under a transaction.

---

114. *See infra* Section D1.

115. *See* discussion *infra* Section D1.

116. *See* Nakamoto, *supra* note 16, at 1, 8 (indicating that transactions will be computationally irreversible but that subsequent transactions can occur provided they satisfy the consensus mechanism of the DLT network).

117. For example, such reverse transfer may take the form of a judgment ordering replevin of stolen or fraudulently conveyed cryptocurrency. *See* Angela Morris, *Judge Orders $ 30 Million in Bitcoin to Be Returned in Cryptocurrency Class Action*, MIAMI DAILY BUS. REV. (Aug. 3, 2017) (summarizing a default judgment against Project Investors Inc. in a class action case regarding stolen cryptocurrency); *see also* Leidel v. Project Inv'rs, No. 9:16-cv-80060-MARRA (S.D. Fla. July 27, 2017), ECF No. 123 (ordering a default judgment of 11,325.0961 BTC against Project Investors Inc.).

Even in the case of hacking, blackmailing, or fraud, it makes sense to force the tortfeasor to return the illegally obtained assets because the ineffectiveness of the transfer from a legal point of view does not bestow a private key to the victim. The reverse transfer restores the parties to the same positions they had been in before the transfer. For all practical purposes, it cancels the effects of the first transfer.

It is important in this context to note a certain ambiguity of the term "reversible." Insofar as it means annulling a transfer as if it had never happened, it is not a workable option for most DLT networks. But insofar as it refers to a reverse transfer as a result of which a new private key is created for the victim, it is certainly feasible with the help of the law. The law cannot undo a fact, but it can provide remedies aiming to reverse the situation that had been achieved. What comes to the fore here is the difference between a set of facts and a normative order. The law as a normative order cannot undo a fact, e.g., a tort that has been committed, a document that has been handed over, or work that has been performed. Yet it can remedy the consequences of these facts rectroactively. Just as the effects of an unjust enrichment can be compensated by a restitution claim, the law can impose an obligation on the recipient of virtual assets recorded on the blockchain to return what has been received.[118]

The idea of a reverse obligation to correct legally incorrect transfers marries the dominant features of the technology, its autonomy, and nonrepudiability, with the practical need for correcting unjust and societally unbearable results. This is achieved by imposing an obligation to return, which can be complied with by using the methods of DLT. In this way, the blockchain is not "invalidated" but supplemented with an additional reverse transfer. The reversal takes place in the form that the DLT provides and thus does not create any contradiction or upheaval. The law is adapted to the particularity of the technology to achieve its aims.

Yet, there is a catch. The actual performance of the reverse transfer depends on the will of the recipient.[119] He must make

---

118. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 54(2)(a) (2008) ("Rescission requires a mutual restoration and accounting in which each party restores property received from the other, to the extent such restoration is feasible . . . .").

119. *See* Andrew W. Balthazor, Comment, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. Rev. 1207 (explaining the challenges of recovering

use of his private key to send the crypto assets back to the sender. It is by no means sure that he will comply with his obligation.[120]

But this peculiarity does not make the reverse transfer improbable or unlikely.[121] The legal system has mechanisms to force the use of keys or any other human action. Examples include a court order and the obligation to pay a fine in case of its violation for "contempt of court."[122] Of course, these legal mechanisms are not as certain to succeed as would be the technical deletion of the transfer, which would restore the transferred asset directly to the former holder. Yet such a deletion is not possible, or only possible at a high cost.[123] Moreover, the obligation to use a private key to retransfer assets is not very different from other court orders, say, to restore a physical asset or perform another act, e.g., providing testimony as a witness. Legal enforcement works at least in many, if not in most, cases. The undeniable truth that the law is sometimes broken or disobeyed does not mean that it is useless to impose a normative order.[124]

The consequences of the "reverse transfer approach" shall be illustrated using a practical example: Let us imagine that *A* wants to exchange a bitcoin in U.S. dollars and enters into an online transaction with *B*, who is a fraudster. A transfers the bitcoin via the blockchain to *B*, but *B* never transfers U.S. dollars. A court of law would order *B* to transfer the bitcoin back to *A*. If *B* does not comply, he will be in contempt of court and

---

cryptocurrency even when ordered by a court). *See also* Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 969, 975 (2015) (explaining how the possessor of a cryptocurrency account's private key has total control over the account).

120. *See* Balthazor, *supra* note 119, at 1219 (describing methods of enforcing judgements against defendants that hold cryptocurrency).

121. *See id*. at 1235 ("Cryptocurrency asset recovery poses challenges surmountable under the right conditions.").

122. *See id*. at 1226 ("Cryptocurrency may be seized, pursuant to a levy or writ of replevin."); *see also* FED. R. CIV. P. 70(e) ("The court may also hold the disobedient party in contempt.").

123. *See* Nakamoto, *supra* note 16, at 8 (showing that for the bitcoin blockchain, it is computationally impractical to reverse a transaction without controlling the majority of computing power in the network).

124. *See* HANS KELSEN, PURE THEORY OF LAW 113 (2005) (explaining that a law or norm is not invalidated by the existence of contrary behavior); *see also* H. L. A. HART, THE CONCEPT OF LAW 84 (2012) (distinguishing the normative rules of law from predictive language).

ordered to pay a fine. The same obligation to retransfer could be imposed on the recipient of cryptocurrency from a transferor who subsequently is declared bankrupt. If the transfer is done during the suspect period, the assets would have to be restored to the bankruptcy estate through a new transfer.

4. STOP THINKING ABOUT PROPERTY TRANSFERS

The essence of the proposal made here is to substitute a conceptualization of the transfer in terms of property law by an analysis that is based on remedies under the law of obligations. No longer is it necessary to enquire into the ownership of bitcoin or other cryptocurrencies. For the vast majority, the law accepts and protects the results produced by the blockchain.

The abandonment of a property law analysis of the transfer has two main advantages. The first is that it is no longer necessary to probe and second-guess the validity of every DLT transfer. The distributed ledger is accepted as is. This not only allows the technology to operate without disturbances, it also spares the useless effort to "correct" the blockchain.

The second advantage is that the holder of a private key whose bitcoin has been hacked or stolen can rely on the law's protection. She is not obliged to prove title to the bitcoin by relying on circumstances outside of the blockchain, specifically that the person she obtained the coins from was the "owner" who legitimately obtained it from the former "owner" and so on. Such a parallel "title search" would indeed be impossible given the decentralized and pseudonymous working of DLT. The blockchain itself is the ledger that confers legitimacy.

A further advantage becomes visible at the international level. Excluding a property analysis dispenses with the need to look for *the* one national law that governs the transfer. As has been shown above, it is impossible to identify such a law for completely distributed ledgers.[125] In addition, it is also a futile analysis, as the law cannot in any sense "validate" a blockchain transfer. The "validity" is certified by technology. Its result cannot be annulled or voided by law.[126] It is thus not only impossible, but also useless to search for the law that "governs" a transfer on the blockchain. There is no need for such law, as DLT is a factual and global process.

---

125. *See supra* Section A.3.
126. *See supra* Section A.3.

The many legal questions raised by such transfers cannot be answered by one legal system, but only by a plurality of different laws. These laws concern, for instance, the right of the victim of a fraud or theft to have the assets returned, the obligation to restore assets transferred by mistake, or the fate of crypto assets in the event of the death or bankruptcy of their holder. Why should *one* national law govern all of these questions? It conforms much more to the current reality of split legal systems to answer these questions by simultaneously applying different national laws.

Take the example of an agreement for the transfer of bitcoin. Such an obligation will usually only be undertaken against some consideration. The transfer is thus part of the performance of a contract. It is important to pay attention to the precise wording of the previous statement: The bitcoin transfer is *not* a contract but the performance of a contract. The transfer serves to fulfill an obligation arising under a contract concluded outside the blockchain, such as a sales contract for some object that is paid for in bitcoin. This contract is submitted to some national law in accordance with the ordinary rules of conflict of laws. The law governing the contract determines whether the agreement is invalid, e.g., in case of mistake. The same law will also determine the consequences if the transfer made in the contract's execution has to be returned.[127] Since the agreement is concluded outside the blockchain, it is not difficult to determine the contract's governing law. This law is identified by the usual rules of private international law: in the case of a sale, for instance, the parties can agree to the applicable law to their contract;[128] in the absence of a choice by the parties, many tribunals would apply the law of the habitual residence of the seller.[129]

---

127. It is generally agreed that the law applicable to a contract also governs the consequences of its invalidity. *See Rome I*, *supra* note 93, at art. 12(1)(e) ("(1) The law applicable to a contract . . . shall govern in particular: . . . (e) the consequences of the nullity of the contract."); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 221(1) (1971) (stating that rights and liabilities of the parties to a contract in actions for restitution are governed by the state law which "has the most significant relationship to the occurrence and the parties under [choice-of-law principles]."); HAY ET AL., *supra* note 14, at 1218–22 (providing a more nuanced discussion of the Second Restatement § 221).

128. *See* sources cited *supra* note 119 and the accompanying text.

129. *See, e.g.*, Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和国涉外民事关系法律适用法) [Laws Applicable to Foreign-Related Civil Relations] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2010, effective April 1, 2001) art. 41 (China) ("Where

It is thus both easy and appropriate to apply the law governing a contract (if there is any) to the obligation to restore the crypto assets in case of nullity of that contract. Determining this law is easy because the contract is a phenomenon *outside* the blockchain. One can rely on the connecting factors supplied by the usual conflicts rules that point to circumstances beyond the chain, e.g., the choice of law by the parties or the habitual residence of one of them, to determine the law that governs the reversal obligation. It is not necessary to identify a law governing the blockchain as such.

If there is no contract because, for instance, the transferor has been blackmailed into making the transfer, then the conflict rules for torts apply. Most legal systems in the world refer to the law in force at the place of the tort, the so-called *lex loci delicti*.[130]

---

the parties do not so select [the law applicable to a contract], the law of the habitual residence of the party whose performance of contractual obligations can most reflect the characteristics of the contract [shall govern]."); Hō no Tekiyō ni Kansuru Tsūsokuhō [Act on the General Rules for Application of Laws], Act No. 78 of 2006, art. 8(2), (*translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=1970 ("In the case [where the parties of a contract do not choose a governing law], if only one of the parties is to provide a characteristic performance involved in a juridical act, the law of the habitual residence of the party providing said performance . . . shall be presumed to be the law of the place with which the act is most closely connected."); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1211(1) (Russ.) (stating that the governing law is the law of the country in which the primary activity occurs or where the principle actor is located); *Swiss PILA*, *supra* note 93, at art. 117(1)–117(2) ("(1) Failing a choice of law, contracts are governed by the law of the state with which they have the closest connection [such as where the performing party habitually resides]."); *Rome I*, *supra* note 93, at art. 4(2) ("Where the contract [has not established jurisdiction through art. 4(1) or is covered by multiple parts of art. 4(1)], the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence.").

130. *See, e.g.*, Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和国涉外民事关系法律适用法) [Laws Applicable to Foreign-Related Civil Relations] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2010, effective Apr. 1, 2011) art. 44 (China) ("Tort liability shall be governed by the law of the place where the tort occurs."); Hō no Tekiyō ni Kansuru Tsūsokuhō [Act on General Rules for Application of Laws], Law No. 78 of 2006, art. 17, *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp (Japan); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1219(1) (Russ.) (stating that the law of the country where the action occurred applies); *Swiss PILA*, *supra* note 93, at art. 133(2) (describing how the law of the state where the tort occurred generally applies); Commission Regulation 864/2007, On the Law Applicable to Non-Contractual Obligations (Rome II), pmbl. (15), 2007 O.J.

Challenging for this approach are cross-border torts, in which the damage and the harmful conduct occur in different countries. Some states give prominence to the place of damage.[131] Others consider the place of conduct as more important, but make an exception where the tortfeasor could foresee that the conduct would have harmful effects in another country; in this case, they equally follow the law of the place of damage.[132] A good case could be made that such damage occurs at the place of the victim's domicile. The same result may be obtained using the governmental interest analysis that is followed by many states in the United States because arguably the country of residence of the victim has the strongest interest in regulating this tort.[133] The blackmailer would therefore be subject to the law of the victim's country, which would oblige him to restore the crypto assets.

In sum, it is unnecessary to analyze DLT transfers in terms of property law. Rather, the entries on the blockchain should be accepted as they are. This does not mean that they are conclusive with regard to the final distribution of crypto assets. Where they are the result of a void contract or a tort, the crypto assets must be restored under the applicable contract or tort law. The advantage of such an approach can hardly be overestimated. Not only does it avoid the need for title search for crypto assets and the factually impossible deletion of a transfer from the ledger, it also spares the vain search for the law applicable to the blockchain as such because it accepts the ledger for what it is:

(L 199) 40 [hereinafter *Rome II*] ("The principle of the *lex loci delicti commissi* is the basic solution for non-contractual obligations.").

131. *See, e.g.*, Hō no Tekiyō ni Kansuru Tsūsokuhō [Act on General Rules for Application of Laws], Law No. 78 of 2006, art. 17, translated in (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp (Japan) ("The formation and effect of a claim arising from a tort shall be governed by the law of the place where the result of the wrongful act occurred."); *Rome II*, *supra* note 130, at art. 4(1) ("[T]he law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs.").

132. *See* GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1219(1) (Russ.) ("In cases when the action or other circumstances caused harm in another country, the law of that country may be applied if the person causing the harm foresaw or should have foreseen the onset of the harm in that country."); *Swiss PILA*, art. 133(2) ("However, if the result occurred in another state, the law of such state applies if the tortfeasor should have foreseen that the result would occur there.").

133. *See* HAY ET AL., *supra* note 14, at 808–22 (discussing governmental interest analysis and torts).

an autonomous, self-contained, global transfer mechanism. The technology is allowed to flourish and any doubling with a legal analysis is avoided. Consequently, no national law governs blockchain transfers, but rather the autonomous rules of the protocol, if need be, are supplemented with a remedy under an easily identifiable national law.

D. COUNTER-ARGUMENTS AND COMPLICATIONS

Every solution to a problem creates a heap of new issues. The proposal made here is no exception. The relinquishment of the traditional property analysis presents a challenge for classic legal thinking and will raise many eyebrows. These concerns deserve to be seriously addressed.

1. THEFT WITHOUT OWNERSHIP?

The first concern is whether abandoning a property law analysis foregoes the legal protections of crypto asset holders. Many authors see the need for submitting virtual currencies to property law to obtain such protection. For instance, Joshua Fairfield has called for a reconceptualization of property law as the "law of information" so as to allow it to cover intangible objects.[134] Others have qualified Bitcoin as a "new class of private property".[135] An expert in criminal law has stressed the societal expectation that "cryptotheft" must not go unpunished.[136] Uniting all of these statements is the conviction that the law must protect the holders of bitcoin and other crypto assets like traditional property owners.

The demands for property or property-like protection are not at variance with the proposals made here. The above statement that one should replace the property analysis with a return obligation merely concerns the *transfer* of crypto assets. It does not preclude the holder of such assets being protected by the law. Indeed, such protection is indispensable if one seriously strives for a symbiosis between the legal and the technological perspective. If the blockchain is to be endowed with legal effects, the holder of bitcoin and other assets recorded must be shielded against hacking, fraud, extortion, and similar torts. This can

---

134. Fairfield, *supra* note 3, at 849–54.

135. Bayern, *supra* note 36, at 29.

136. Henry S. Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 N.C. L. REV. 395, 401 (2019).

necessarily be done only by recognizing her position with some form of legal status. Such status is also necessary for the creation of a security right over the crypto asset, e.g., a lien or a pledge, which necessarily requires some type of legal right to the asset. We can leave it to the applicable tort, contract, or security law whether to call this status "property," "possession," or by another term. What matters is that the factual position of the holder of the private key receives protection by the law.

On a theoretical level, it may seem unsatisfying to grant protection to someone who cannot prove that he has acquired ownership under an applicable national law. What the "holder" of the bitcoin has is merely the private key, i.e., a string of numbers produced by an algorithm. Yet to protect such information is not without parallels. For instance, personal data and business secrets are protected as well,[137] despite the fact that they do not relate to physical objects and that they can be infinitely multiplied. There is consensus that they merit protection independently of their precise legal categorization and their invisibility in the real world.[138] These examples forcefully demonstrate that the protection by private law can go beyond traditional conceptions of property in physical objects. One should accept the private key as being reserved or "private" only to the holder. This protection must be independent of any showing of legal title. The mere factual situation that the private key was created for some person should suffice as a basis for a claim of return.

2. THE CASE OF HACKED OR ILLEGALLY OBTAINED CRYPTO ASSETS

This article argues that the results obtained by the operation of DLT merit legal protection independently of how they are qualified under national law. It is, however, necessary to make an exception: The holder of the cryptocurrency or other virtual asset should not be able to rely on his position recorded on the blockchain where it can be proven in a court of law that

---

137. *See, e.g.*, California Consumer Privacy Act 2018, CAL. CIV. CODE §§1798.100–.199 (Deering 2019) (requiring protection of personal data); *See also* Rivendell Forest Prods. v. Georgia-Pacific Corp., 28 F.3d 1042 (10th Cir. 1994) (discussing trade secrets and the Uniform Trade Secrets Act, a widely adopted uniform law which protects business secrets).

138. *See, e.g.*, Fairfield, *supra* note 3, at 849–54; Bayern, *supra* note 36, at 29; Zaytoun, *supra* note 136, at 401.

he has obtained the private key without the will of the former holder. This exception applies to cases in which the holder of the private key has hacked or copied the private key of another person and carried out a transfer to himself.[139]

In this case, a mere obligation to retransfer would be insufficient. This can be illustrated by the case of bankruptcy: If the "stolen" crypto assets—i.e. the new private keys—were deemed to belong to the hacker, they would fall into the hacker's bankruptcy estate.[140] The former holder would merely have a claim against the bankruptcy administrator, which he would have to pursue as a creditor in the ordinary bankruptcy proceedings. This means that he would have no guarantee of getting his assets back even if he could prove the wrongdoing. The other creditors in the insolvency proceedings should not, however, benefit from the illegal maneuvers of the insolvent debtor. The only way to avoid this result is to consider the holder as lacking legal title to the assets.

What if the hacker or fraudster has transferred the crypto assets to a recipient who knows about the hack? In this case, the result must be the same. The bad faith recipient should not be able to rely on his recording on the blockchain. Those who share the knowledge of his illegal undertaking deserve no protection. The situation is similar to that of the stolen banknote, which has been discussed before.[141] The thief can only transfer property to good faith recipients.

The same treatment should be applied in case of fraud or blackmail. A fraudster does not deserve the protection of the law, in line with the old Latin adage "*fraus omnia corrumpit"* (fraud negates everything); nor do the creditors of his bankruptcy estate or those who know about the fraudulent obtainment of the private key. There is no reason to treat blackmailers and their creditors differently.

It is important not to weaken the blockchain record beyond these exceptional situations. Otherwise, one would run the risk of paralleling the DLT with a largely futile and inefficient legal

---

139. In case the hacker has merely obtained the private key of the victim and has not yet used it to do a transfer to himself, the situation is somewhat easier. There is no invalid position that the holder could rely on. Yet there may be a confusion as to who is the "true holder" of the crypto asset. This should obviously be the victim of the hack.

140. *See* discussion *infra* Section A.3.

141. *See* discussion *supra* Section A.3.

analysis. Beyond a case in which the private key was hacked, obtained by fraud, or obtained by blackmail from the defendant, there should not be any analysis of the property situation before the suit. Where a person has willfully typed the private key into a computer, she should not be able to attack the position of the recipient. In cases where a person made a mistake or has not received a counter performance, she must rely on the reverse transfer to vindicate her rights.[142] The function of the DLT would be greatly compromised if the title of the recipient or third parties would depend on the validity of an underlying contract or the correct rendering of a counter-performance. Furthermore, the onus of proving that the crypto asset has been illegally obtained should be on the victim. The transfer should only be considered as not having occurred where she can prove that the holder of the private key has taken the information from her without her consent.

3. TRANSFERS OUTSIDE THE BLOCKCHAIN

Further issues raised by the proposal made here concern the possibility that crypto assets may be transferred outside the blockchain. These issues have been described above as "endogenous" problems.[143] Consider the example of succession: Upon death, legal systems typically vest the ownership of the decedent in his representative or heir.[144] This legal transfer comprises all of the decedent's assets, thus it should also include her crypto assets.[145] The transfer happens by mere operation of the law without regard to whether the representative or heir has knowledge of the private key or access to it.[146] This means that, legally, a person who is not the holder of the private key must nevertheless have a legal right to the crypto assets recorded on the blockchain.

How can such a result be obtained without compromising the working of DLT? The easiest solution is to consider the crypto assets as the "property" of the holder; since in case of death, all property of the decedent vests in the trustee, heir, or devisees of testament, the characterization as property would

142. *See* discussion *supra* Section A.3.
143. *See* discussion *supra* Section A.2.a.
144. *See supra* note 56 and the accompanying text.
145. *See supra* note 57 and the accompanying text.
146. *Id*.

explain why the crypto assets now "belong" to the latter. This explanation is possible even though the transfer is not analyzed in terms of property law. A property qualification may not be necessary in those legal systems in which *all* rights of the decedent are transferred to the representative or heir, whether they are proprietary, contractual, or other.[147] The legal construction is ultimately up to the national law governing the succession to decide. It suffices to say that the bitcoin were assets of the deceased to justify their automatic transfer to his representative or heirs.

Practical problems may occur where the key is not accessible to the heirs. If it is, for instance, stored on the office computer of the deceased, it may be difficult for the heir or representative to dispose of the crypto asset. However, the novelty of the problem should not be exaggerated. Similar difficulties arise where physical objects are in the possession of third parties, e.g. china in the care of the maid or an expensive watch in the hands of a nurse. Many legal systems give the successor a claim against the third party to turn over the possession to them.[148] In the case of crypto assets, this entails the duty to provide the private key.

---

147. For French law, *see* CODE CIVIL [C. CIV.] art. 724(1) (Fr.) ("Heirs designated by legislation have seizin by operation of law of the assets, rights, and actions of the deceased."), For German law, *see* Bürgerliches Gesetzbuch [BGB] [German Civil Code], Jan. 2, 2002, BGBL. I at 42. § 1922 (Ger.) ("Upon the death of a person, that person's inheritance passes as a whole to one or more than one other person. . . ."). An exception applies only to highly personal rights such as personality rights, *see* FRANÇOIS TERRÉ, YVES LEQUETTE & SOPHIE GAUDEMET, DROIT CIVIL. LES SUCCESSIONS. LES LIBÉRALITÉS margin no. 50 [2013], but this exception is not applicable to crypto assets.

148. Some legal systems still allow the Roman *hereditatis petitio*, i.e. the claim of the heir against the possessor of any object belonging to the estate. *See, e.g.*, Bürgerliches Gesetzbuch [BGB] [Civil Code], § 2018 (Ger.) ("The heir may request every person who, on the basis of a right of succession that he does not really have, has acquired something from the inheritance (possessor of the inheritance) to surrender the item or items acquired.") Others follow the doctrine "le mort saisit le vif" developed by the *ius commune*, according to which the heirs are considered to be the owners and possessors of the estate at the moment of ownership. *See, e.g.*, LA. CIV. CODE ANN. art. 936 (1997) ("The possession of the decedent is transferred to his successors, whether testate or intestate, and if testate, whether particular, general, or universal legatees. A universal successor continues the possession of the decedent with all its advantages and defects, and with no alteration in the nature of the possession. A particular successor may commence a new possession for purposes of acquisitive prescription."); CODE CIVIL [C. CIV.] [CIVIL CODE] art. 724(1) (Fr.) In both cases, the heir has a cause of action against any person that possesses an object belonging to the estate.

However, a pure duty of information would not suffice. One must also fight the risk that the person in possession of the private key first uses it for a self-interested transfer before handing it over to the heir or representative. This can easily be achieved by supplementing the obligation to transfer the private key with the obligation to abstain from any use, disposition, or sharing of the information with third parties.

Similar obligations as those in succession cases also arise in other cases in which a party steps into the shoes of another. As illustrations, one may think about the new company in a merger transaction or the bankruptcy administrator after the opening of a bankruptcy proceeding. In both of these cases, it is necessary to provide the successor with a legal claim against the person that currently holds the private key and thus the information necessary to dispose of and otherwise administer the crypto asset.

4. APPLICABLE LAW

One may ask which legal system provides for all of these consequences. Is it necessary to create a proper blockchain regime for them?

The answer is no. One may derive the protection in cases of erroneous transfers by using the normal conflict rules for unjust enrichment, which refer, *inter alia*, to the place of the enrichment.[149] Where problems under a contract occur, the obligation to perform a reverse transaction will result from the applicable contract law.[150] In the case of hacking, blackmail, or

149. *See, e.g.*, Council Regulation 593/2008, On the Law Applicable to Contractual Obligations, 2008 O.J. (L 177) 6, art. 10. (stating that the existence and validity of a contract are determined by the law which would govern it if the contract or term were valid); RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 221(2)(b)(1971) (providing that, for restitution, the local law of the state with the most significant relationship to the particular issue is used to determine rights and liabilities of the parties for that issue and "the place where the benefit or enrichment was received" can be used to determine which state has the most significant relationship to the issue); HAY ET AL., *supra* note 14, at 1218–22 (discussing choice-of-law alternatives for preexisting contractual relationships).

150. *See, e.g.*, RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 54(2)(a) (2008) ("Rescission requires a mutual restoration and accounting in which each party restores property received from the other, to the extent such restoration is feasible . . . .").

fraud the transfer has no legal effect.[151] Nevertheless, the victim may claim the restoration of the private key under tort law.[152] The applicable national law can be determined according to the ordinary conflict-of-laws rules, which point to the place of the tort.[153] National law is capable of protecting positions deriving from the blockchain, as is demonstrated by the fact that other incorporeal rights are also protected, such as personal data[154] or business secrets.[155] Where a national law does not currently afford similar protection to crypto assets, it needs to be developed further in this direction. Otherwise, the citizens of the country in question will be in danger of losing their crypto assets due to hacking, fraud, or coercion.[156]

The consequences of a succession, merger, or bankruptcy proceeding are determined by the applicable national law. This

---

151. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS §§ 175–76 (1981) (stating that a "threat to make public embarrassing information concerning the recipient unless he makes a proposed contract" may result in a voidable contract, along with contracts induced by fraud or misrepresentation).

152. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 922 (1979) (discussing the return of converted chattel); RESTATEMENT (SECOND) OF TORTS § 222A (1965) (defining conversion).

153. *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145 (1971) ("The rights and liabilities of parties with respect to an issue in tort are based on the local law of the state which, with respect to that issue, has the most significant relationship to the occurrence and parties . . . .").

154. *See, e.g.*, Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, 2016 O.J. (L 119) 1 (instituting the General Data Protection Regulation (GDPR) with the purpose to "respect [the] fundamental rights and freedoms [of natural persons], in particular their right to the protection of personal data").

155. *See, e.g.*, 18 U.S.C. § 1836(b)(1) (2016) ("An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.").

156. *See, e.g.*, Timothy G. Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, ECON. STUD. AT BROOKINGS, Mar. 2019, at 2, available from https://www.brookings.edu/wp-content/uploads/2019/03/Timothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf ("There is a gap in the regulation of crypto-assets that Congress needs to fix. The gap is contributing to fraud and weak investor protection in the distribution and trading of crypto-assets."); *cf.* Ivan Novikov, *The Three Layers of Crypto Security*, FORBES (May 3, 2018, 7:15 AM), https://www.forbes.com/sites/forbestechcouncil/2018/05/03/the-three-layers-of-cryptocurrency-security/#2680bb6029aa (recommending methods of protecting cryptocurrency assets).

law can be determined using the normal conflict rules.[157] For instance, the law applicable to succession is usually determined based on the nationality or habitual residence of the deceased,[158] the law applicable to mergers by the law of the entities in question,[159] and the law applicable to bankruptcies by the law of the country in which the bankruptcy proceedings are opened.[160] Where this law contains a provision on universal transfers, it should also be applied to the private keys of blockchain assets. Where it does not contain such a provision, the legal issue does not arise.

Some confusion may still arise due to the fact that the conflict rules regarding all of these issues are not the same around the world. However, this is not unusual. The same issue arises all the time in other situations as well.[161]

More problematic is that national laws may take a view that is different from the one in this article. In particular, they may not accept DLT as a fact and try to double it with an analysis of the legal "validity" of blockchain transfers under their property law.[162] A good way to provide more certainty would be an international text that endows a blockchain record with some legal protection.[163] It could also provide for the exceptions in case

---

157. *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145 (1971) (discussing that the rights and liabilities of parties with respect to an issue of tort are based on the local law that has the most significant relationship to the occurrence and parties).

158. *See, e.g.*, *id.* at § 260 ("The devolution of interests in movables upon intestacy is determined by the law that would be applied by the courts of the state where the decedent was domiciled at the time of his death.").

159. *See, e.g.*, *id.* at § 302 (discussing the applicable law with respect to powers and liabilities of corporations).

160. *See, e.g.*, CLARK A. NICHOLS ET AL., CYCLOPEDIA OF FEDERAL PROCEDURE § 2:192 (3rd ed. 2019) ("American courts have consistently recognized the interest of foreign courts in liquidating or winding up the affairs of their own domestic business entities.").

161. *See, e.g.*, Donald Earl Childress III, *International Conflict of Laws and the New Conflicts Restatement*, 27 DUKE J. OF COMP. & INT'L L. 361, 374–76 (discussing application of foreign comity in a suit filed in California for a bombing that occurred in Santo Domingo, Dominican Republic).

162. *Cf.* Katie Szilagyi, *A Bundle of Blockchains? Digitally Disrupting Property Law*, 4 COLUM. L. REV. 9, 24–28 (arguing that blockchain should be treated as property under conventional property law and arguing that using a Hegelian property framework to validate a property owner's status with respect to the property is incompatible with Bitcoin).

163. *See* Jonathan Cardenas, *The Rise of the Crypto Asset Investment Fund: An Overview of the Crypto Fund Ecosystem*, in 1 BLOCKCHAIN & CRYPTOCURRENCY 149, 150 (Josias Dewey ed. 2019) (stating that institutions

of theft, blackmail, and fraud that have been advocated here. Such an international text could take the form of a convention, a legislative guide, or a model law. Possible fora could be the Hague Conference on Private International Law, UNIDROIT in Rome, or UNCITRAL in Vienna. The treatment of these issues by one of these international fora would be in line with the global nature of DLT. As long as they have not acted, one must hope for the reasonableness of national courts in applying their national law to blockchain transfers.

CONCLUSION

This article has proven that it is possible to maintain the hallmarks of DLT, namely its autonomy, nonrepudiability, and a-nationality, while arriving at just and socially acceptable outcomes from a legal perspective. This symbiosis has been achieved by respecting the results of blockchain transfer as a fact and imposing an obligation for a reverse transfer in case they are incompatible with the requirements of justice. The correction that is necessary from a legal perspective is thus done in a form that is compatible with the technology.

Unless it can be proven that such a corrective obligation exists, the distribution of assets foreseen by the technology should be presumed to be legitimate. The private key should therefore be legally protected against hacking, fraud, coercion, or other forms of misappropriation. These cases can be solved by using the general rules of tort law.[164] There is thus no need to define a national law governing the blockchain or developing a special *lex cryptographica*.

The solution proposed here can also solve the problem of crypto asset transfers outside of the blockchain (e.g., in case of a succession). The transfer is done by virtue of the applicable law. Any person that is illegally in possession of the private key is under an obligation to turn over the key to the legitimate successor and desist from any use.

In sum, there is no law applying to the blockchain transaction as such. Yet there are laws surrounding it, like

---

around the world are attempting to develop international norms for blockchains and the "crypto ecosystem").

164. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 922 (1979) (discussing return of converted chattel); RESTATEMENT (SECOND) OF TORTS § 222A (1965) (explaining what constitutes conversion); RESTATEMENT (FIRST) OF TORTS § 223 (1934) (describing ways of committing conversion).

contract law, tort law, or succession law. These laws must accept the social reality that is created by the blockchain transfer. They should regard such transfer as a fact, but not necessarily as conclusive with regard to the legal situation. Law as a normative system has the power to require reverse transfers. Indeed, it must use this power where injustice looms. But otherwise, it should abstain from interfering with the functioning of the self-contained transfer system that is DLT.