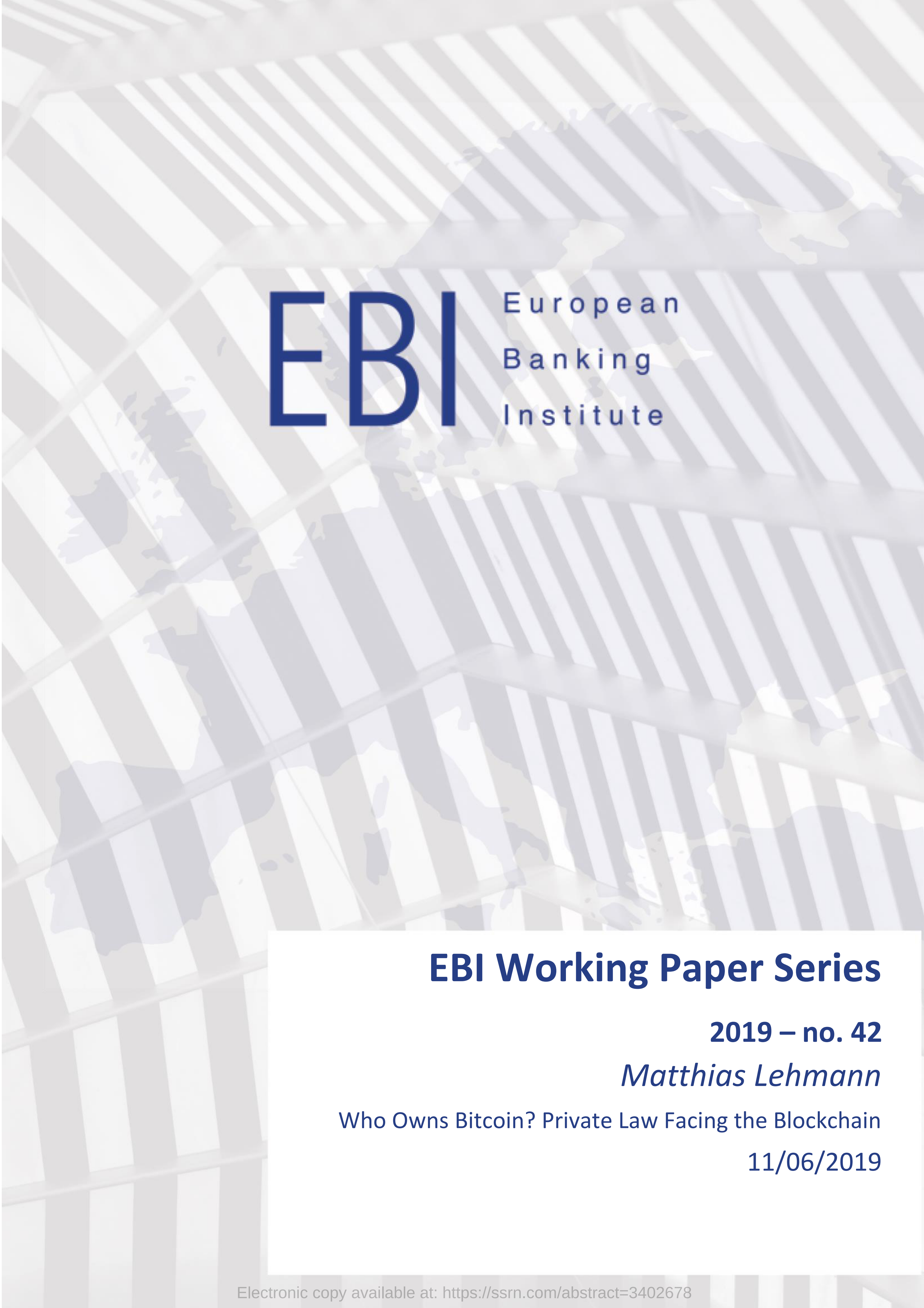

EBI
European
Banking
Institute

EBI Working Paper Series

2019 – no. 42

Matthias Lehmann

Who Owns Bitcoin? Private Law Facing the Blockchain

11/06/2019

Who Owns Bitcoin? Private Law Facing the Blockchain

by Matthias Lehmann[*]

Forthcoming publication in the Minnesota Journal of Law, Science, and Technology

Blockchain, or "distributed ledger" technology, 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 ignores 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.

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.

[*] 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.

Introduction

By now, virtually everybody will have 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. What the technology offers is a mechanism for the transfer of assets between two parties at any place in the world with an internet connection. 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.[1] The main advantage of DLT is that it dispenses with the necessity of trust between the parties and sharply reduces the need for intermediaries.[2] This is the result of three hallmark features of DLT: pseudonimity, resilience and immutability.[3] 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. 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. Finally, immutability means that the transfers cannot be undone once they have been recorded on the blockchain.

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 embargoes.[4] Much ink has been spilled on these problems.[5] 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

[1] 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).

[2] 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) (underlining that cryptocurrencies allow to avoid the need for a trusted third party); Fairfield, *supra* note 1, at 814 (emphasizing that trustless public ledgers can avoid the enourmous costs of generating trust).

[3] See PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 3 (2018) (describing the blockchain's nature as tamper-resistant, resilient and non-repudiable).

[4] 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 (last visited Mar 27, 2018).

[5] From the voluminous literature, 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 US legislators and regulators).

owns the transferred assets? How a transfer can 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. DLT neither requires nor ensures that such an agreement exists. It merely relies on the fulfillment of technological requirements, namely the use of the correct private and public key. 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. 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 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.

The paper 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 do 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 counter-arguments 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 solution to legal problems. It was originally designed to surmount the shortcomings of the trust based banking system that gives banks and states a prominent role.[6] Satoshi Nakamoto, the pseudonym used in the original bitcoin proposal, saw these institutions as being inherently corrupt.[7] His goal was to eliminate the need for them by creating a peer-to-peer system in which transactions are proven by a decentralized network of computers rather than intermediaries.

The philosophical underpinnings of the blockchain stand in sharp tension to the rule of law. Anarchists, like 'cypherpunks' and 'crypto rebels', are attracted to DLT because they see autonomous cryptocurrencies as a safeguard of civil liberties against a 'Big Brother' state.[8] But the idea also appeals to neoliberals because it might toll the bell for the state's monopoly to create money.[9] 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. The anti-legalistic tendency is epitomized in the formula "code is law", which was coined by Lawrence Lessig, albeit with precisely the opposite

[6] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, https://bitcoin.org/bitcoin.pdf (last visited Mar 20, 2018) (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).

[7] Primavera De Filippi & Benjamin Loveluck, *The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure*, 5 INTERNET POL'Y REV. 1, 4 (2016) (highlighting that Satoshi Nakamoto stated explicitly in various blogs posts and forums that Bitcoin aimed at eradicating corruption from the realm of currency issuance and exchange).

[8] A "cypherpunk's manifesto" insists that privacy in an open society would require anonymous transaction systems, which force individuals to reveal their identity only when desired, see Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html; The Cyperpunk's Manifesto builds on the earlier Crypto Anarchist Manifesto by Timothy May, see Timothy May, *The Crypto Anarchist Manifesto*, ACTIVISM.NET (Nov. 22, 1922), http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html (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); For the story of "crypto rebels" beating the government and "Big Brother" see STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE (2001).

[9] 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) (arguing that the unfettered operation of bitcoin would contribute towards 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 135 (3rd ed. 1990) (pleading for a "Free Money Movement" to overcome central bank induced inflation).

intention to demonstrate that the state should intervene in the internet's architecture.[10] Some authors maintain that the blockchain would be governed by a non-state and a-national law for the digital age, which they call *lex cryptographica*.[11]

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. A DLT transfer is initiated when the transferor enters a unique digital key that is only known to him ("private key") as well as the publicly known key of the transferee ("public key") to a chain of digital signatures on the internet.[12] The transfer is then broadcasted 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. Each of the nodes maintains its own copy of all transfers (the "ledger") against which it checks the new transfer. The nodes work on a decentralized basis and are dispersed around the world (therefore "distributed ledger"). They are assigned a fee to incentivize them to perform the verification work. 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. From this moment, the chain can no longer be altered without redoing all the verification work that has been done, which becomes even more difficult as new blocks are added.[13]

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. None of this requires the intervention of notaries, lawyers or intermediaries that could be supervised, e.g. banks, clearing agents or depositories. Nor does it need a contract or

[10] Lawrence Lessig, *Code Is Law*, HARV. MAG. (Jan. 1, 2000), https://harvardmagazine.com/2000/01/code-is-law-html (last visited Mar 20, 2018); see also LAWRENCE LESSIG, CODE: VERSION 2.0 1-9 (2006).

[11] 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 smart contracts and decentralised as well as potentially autonomous organisations). See also FILIPPI AND WRIGHT, *supra* note 3, at 52 (claiming that with lex cryptographica "national laws get pushed to the edges").

[12] Nakamoto, *supra* note 6, at 2.

[13] *Id.* at 3.

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 legal results. For instance, it is very often said that the recipient of a transfer becomes the "owner" of the bitcoin[14] or that concepts such as "ownership" and "property" would also apply to cryptocurrencies.[15] 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 the Common law.[16] An even more problematic but often neglected point is that one cannot assume the blockchain is exclusively or predominantly subject to the Common law. 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. 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. They consider DLT as guaranteeing the position of the acquirer with absolute certainty, something that a real-world transaction with tons of documentation,

[14] Kaplanov, *supra* note 9, at 123 (describing that the "owner transfers her bitcoins to the purchaser"); Sarah Meiklejohn et al., A fistful of bitcoins: Characterizing Payments Among Men with No Names, *in* IMC'13 - PROCEEDINGS OF THE 13TH ACM INTERNET MEASUREMENT CONFERENCE 127–139 (2013) (assimilating bitcoin to a chain of transactions from one owner to the next); Kevin V. Tu, *Perfecting Bitcoin*, 52 GA. L. REV. 505,, 548 (2017) (stating that "[o]wners access, manage, and use their virtual currency with digital keys").

[15] 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 1 at 842-54 (suggesting to reconceptualize property law as the "law of information" in order to cover virtual assets like cryptocurrencies).

[16] 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 (last visited Mar 7, 2019) (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*, *in* 1 HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION 225–247 (2018) (stating that "it is not entirely clear what, if any legal rights, attach to bitcoins and other private cryptocurrencies like bitcoin").

lawyers and courts cannot provide. From their point of view, the technology does not need law.

Yet this belief is wrong. Blockchain is designed to avoid "double spending", i.e. that the same owner transfers the bitcoin twice.[17] It provides no safeguards at all against other problems that may occur.[18] 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.

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. He might, for instance, have entered the wrong number of bitcoin, e.g. "10" instead of "1". It is also not excluded 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.[19]

From a legal point of view, in all of these situations the contract that entails the property transfer is voidable.[20] Yet under the blockchain, the transfer is effective. For this, it suffices that the correct codes have been used. 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. The technology does not take into account mistakes, fraud or improper threats. This is not part of the algorithm.

[17] Nakamoto, *supra* note, 6 at 1 ("In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed time stamp server...").

[18] Low & Teo, *supra* note 16, at 22 (highlighting that the cryptographic protocols provide "zero protection" from other forms of fraud than double-spending).

[19] 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 (describing how payments in bitcoin are extorted from men in exchange for silence about an alleged affair).

[20] See RESTATEMENT (SECOND) OF CONTRACTS §§ 153, 164, 175 (1981) (providing that a contract made under the influence of a mistake, fraud or an improper threat is voidable).

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 have been subject to some strong form of incapacity, for instance because they suffer from a mental illness or defect.[21] One must also not discard the possibility that the parties to the transfer have never been in contact. 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. Yet from a technological point of view, the transfers would be effective.

b) Exogenous Transfer Problems

Exogenous events are those that have no relation to the blockchain but nevertheless have the potential to impact the ownership of crypto assets. 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.[22] 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.[23] Since the decedent is no longer able to dispose of these coins, his successors must

[21] See RESTATEMENT (SECOND) OF CONTRACTS § 13 (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).

[22] See e.g. 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); 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); M.J. de Waal, *Law of Succession*, *in*, INTRODUCTION TO THE LAW OF SOUTH AFRICA 169 (C.G. Van der Merwe and 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).

[23] 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); Ana-Caterina Anitei, *Digital Inheritance: Problems, Cases and Solutions*, *in* 2017 THE INT'L. CONF.: EDUC. AND CREATIVITY. FOR A KNOWLEDGE-BASED SOC'Y. 32–39 (2017) (characterizing bitcoin as part of the "digital inheritance"); 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).

have become the "owners" outside of the DLT.[24] The question is, however, 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.[25] This power must arguably also extend to virtual assets, such as bitcoin, which can make up a 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.[26] 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.[27] The treatment of cryptocurrencies in bankruptcy proceedings is the subject of intense legal discussion.[28] 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

[24] From the point of view of Dutch law, see Anna Berlee, *Digital Inheritance in the Netherlands*, 6 J. EUR. CONSUMER & MARKET L. 256 (2017) (describing how the heir succeeds on the death of a person to the rights capable of transmission and to whatever the deceased possessed or held).

[25] 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...").

[26] See e.g. 11 U.S.C. § 544 (1978) (giving the trustee the right to avoid certain transfers made by the debtor).

[27] 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); Order on Motion for Partial Summary Judgment, Kasolas v. Lowe (*In re HashFast Technologies LLC*), No. 14-30725-DM (Bankr. N.D. Cal. June 17, 2016). In this case, the bankruptcy trustee of the plaintiff sought to recover 3.000 bitcoin that had been paid out to the defendant before the plaintiff had gone into administration. In a summary judgment, the court granted the request for the recovery of the value the bitcoin had at the time of transfer to the defendant.

[28] 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"). In the case *In re HashFest Technologies* LLC, *supra* note 27, the court decided for a classification as "intangible personal property".

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.

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 law. It is also impossible for the law to impose its requirements on the blockchain.

The problem is well illustrated by the case of stolen bitcoin that the thief transfers to his own public key. Legally, this transfer should be invalid given that the holder of the bitcoin has never agreed to it. But when the correct codes are entered and broadcasted to the nodes, a new private key is created for the recipient in about 10 minutes, the average time to confirm a bitcoin transaction. 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. Though the recipient cannot be considered the "owner" of the bitcoin in a legal sense, he has obtained the ability to transfer under 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.[29] 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 it 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 asset 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 the bitcoin illegally can dispose of them, whereas an heir or executor who is legally entitled to them cannot. To make the technology compatible with the law would require a complete reconceptualization. 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 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 re-instated 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 *subsequently* 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".[30] Once that a transfer has been

[29] See references footnote 22.
[30] Filippi & Wright, *supra* note 11, at 37 (stating that the data stored on the blockchain is nonrepudiable).

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.[31]

One must partially qualify the characterization of blockchain transfers as immutable. There is a great variety DLT networks, which represent different trade-offs in terms of reversibility and finality of transactions.[32] They can be roughly divided in permissioned and permissionless networks.[33] Permissionless systems are those in which anybody can participate and where consensus is thus highly distributed. In contrast, permissioned systems feature one or more authorities that act as gatekeepers. They allow participants into the network and sometimes also confirm transfers. 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. Yet reversals are also not unthinkable in other types of permissioned and even in permissionless systems. They are effectuated by creating a so-called hard fork that splits the blockchain protocol into two. This happened for example with regard to bitcoin when the network was reorganized in 2013[34] and with regard to Ethereum after a considerable amount of the cryptocurrency had been siphoned off by hackers in 2016[35]. In both instances, a new version of the blockchain

[31] See *supra* A 1.

[32] For an overview, 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 (visited April 2, 2019).

[33] Xu et al., *supra* note 32 at 246 (describing permissioned and permissionless blockchain as two design options for blockchains). Permissionless systems typically rely on the consensus of the participants, see Till Neudecker and Hannes Hartenstein, *Network Layer Aspects of Permissionless Blockchains*, 99:1 IEEE COMMUNICATIONS SURVEYS & TUTORIALS 1 (characterizing permissionless systems as unstructured peer-to-peer networks). While it is not excluded that there is a central operator, creator or sponsor who has the possibility to control or reverse transfers, this would be rather unusual given that the network are designed to distribute consensus as much as possible.

[34] See Vitalik Buterin, *Bitcoin Network Shaken by Blockchain Fork*, BITCOIN MAGAZINE (Mar. 12, 2013, 11:14 PM), https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ (accessed 22 March 2018).

[35] See Eduard Gómez, *The Ethereum Hard Fork & Ethereum Classic*, THE MERKLE (July 21, 2016), https://themerkle.com/the-ethereum-hard-fork-ethereum-classic/ (accessed 22 March 2018).

was created. While the case of bitcoin seems to have passed relatively unproblematic, in the Ethereum case, the old, hacked ledger refused to die, which resulted in the parallel existence of two separate currencies, Ethereum (One) and Ethereum Classic.[36]

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" crypto currency. All other participants will be confused by the parallel existence of two versions of the same ledger. Both effects undermine the trust in the cryptocurrency. It is hard to overestimate the negative repercussions since the value of the crypto currency depends first and foremost on trust. 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 w*hich* 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.[37] Conflict-of-laws works by attributing sets of facts or “relations” to the law of the state with which it has the closest connection.[38] DLT presents a formidable challenge for this methodology.

[36] Low & Teo, *supra* note 18.

[37] See e.g. PETER HAY ET AL., CONFLICT OF LAWS 1 (5th ed. 2010); JAMES FAWCETT, JANEEN CARRUTHERS & PETER NORTH, CHESHIRE, NORTH & FAWCETT: PRIVATE INTERNATIONAL LAW 3 (James Fawcett & Janeen Carruthers eds., 14th ed. 2008); DOMINIQUE BUREAU & HORATIA MUIR WATT, DROIT INTERNATIONAL PRIVÉ (4 ed. 2017); GERHARD KEGEL & KLAUS SCHURIG, INTERNATIONALES PRIVATRECHT (9 ed. 2004).

[38] See e.g. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145 (1971), (regarding the applicable law for torts) CHESHIRE, NORTH & FAWCETT: PRIVATE INTERNATIONAL LAW, 682 (Paul Torremans & J. J. Fawcett eds., 15th ed. 2017) (regarding the applicable law for contracts in the absence of a choice by the parties); BUREAU AND WATT, *supra* note 37, at 340 (about the *principe de proximité*); KEGEL AND SCHURIG, *supra* note 37, at 184 (on Savigny's theory of the seat).

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. The protocols are stored on computers worldwide. Anybody can participate in permissionless systems like bitcoin for there is no authority or server that controls access. Confirmations take place through distributed consent from nodes all over the world. 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.[39] 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.[40] 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.

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.[41] 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

[39] See e.g. CHESHIRE, NORTH & FAWCETT, *supra* note 38. at 681-888 (distinguishing conflicts rules for contracts, non-contractual obligations, family law and the law of property).

[40] Some authors therefore speak of the "transactions on a blockchain", see Wright and De Filippi, *supra* note 11 at 6.

[41] See Russell J. Weintraub, *Matière préliminaire*, *in* FUNCTIONAL DEVELOPMENTS IN CHOICE OF LAW FOR CONTRACTS, 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 No 593/2008 (Rome I), on the law applicable to contractual obligations, 2008, art. 3(1), O.J. (L177) 6 [hereafter Rome I]; Hō no tekiyō ni kansuru tsūsokuhō [Act on the General Rules of Application of Laws], Law No. 78 of 2006, art. 7 (Japan); Bundesgesetz über das Internationale Privatrecht [IPRG] [Swiss Federal Private International Law Act] Dec. 18, 1987, SR 291, art. 116 [hereafter Swiss PILA]; GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1210 (Russ).; Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和合国外围民俗法轮关西石永发) [Laws Applicable to 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).;, *Inter-American Convention on the Law Applicable to International Contracts* art. 7, reprinted in 33 IL.M. 732 (1994). See also Hague Principles on Choice of Law in International Commercial Contracts (approved on Mar. 19, 2015), art. 2 § (1).

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 indefinite 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.[42] 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.[43] Such a choice is incompatible with the ideals of crypto aficionados[44] and is therefore unlikely to be 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.[45] 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 points 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.[46] In this sense, a contract conflicts law analysis creates many issues that are insurmountable.

[42] This option has been envisaged by the Financial Markets Law Committee (FMLC), *see* FIN. MARKETS L. COMM. DISTRIBUTED LEDGER TECH. AND GOVERNING L.: ISSUES OF LEGAL UNCERTAINTY 15 (2018), 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') [hereafter FMLC].

[43] See May, *supra* note 8 and accompanying text.

[44] See *supra* A 1.

[45] See Rome I, art. 4(1), (2); Swiss PILA, art. 117.

[46] See *supra* A 2 b.

If one characterizes crypto transfers instead 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. 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 intermediary.[47] 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.[48] 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.[49]

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. 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. 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.[50] Moreover, any analogy between blockchain and

[47] Hague Conference on Private International Law, Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary, art. 4 (2006) (The Hague) (the Convention has inter alia been signed by the US and Switzerland).

[48] FMLC, *supra* note 40, at 18–19 (suggesting the Place of the Relevant Operating Authority/Administrator [PROPA] or alternatively the Primary Residence of the Master Key Holder Approach [PREMA]).

[49] In the same sense *Id.* at 11. (noting that the lex situs does not translate well when applied to a DLT ledger).

[50] The discussion has been particularly heated in Europe, 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 42-75 (Harry C. Sigman & Eva-Maria Kieninger eds., 2009) (presenting the various solutions to determine the applicable law to assignment); AXEL FLESSNER &

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.[51] 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[52] or to recognize bitcoin as a new kind of property[53] 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, the outer constraints that every proposal must respect regarding the application of private law to DLT will be explained.

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

HENDRIK VERHAGEN, ASSIGNMENT IN EUROPEAN PRIVATE INTERNATIONAL LAW: CLAIMS AS PROPERTY AND THE EUROPEAN COMMISSION'S "ROME I PROPOSAL" (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 OBLIGATIONS IN EUROPE 217 (Franco Ferrari & Stefan Leible eds., 2009) (discussing the impact of the Rome I Regulation on the law applicable to assignment).

[51] See Fairfield, *supra* note 1, at 826-27.

[52] *Id.* at 842-63..

[53] Bayern, *supra* note 15 at 29.

autonomy of DLT, the immutability of transfers and the a-national character of the blockchain. What is needed is a mechanism that respects the 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 does respond to the requirements of private justice. In addition, such an approach should not require the elaboration of uniform global rules, which at the moment seems 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 need development of new global rules. Even though this may seem like a perfect solution, the proposal risks coming under fire from both the sides of 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.[54] 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. 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 the requirement to include a choice of law in the blockchain, for they 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 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. We have identified above the instances of mistake, fraud, improper threat, but also those of theft, bankruptcy and succession. From a legal point of view, all of these

[54] See e.g. Fairfield, *supra* note 1 at 874 (characterizing DLT as trustless ledgers tracking transactions in real time at comparatively low cost).

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 each 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.

Instead, the immutability of the transfer from a technical point of view is a fact that lawyers must accept. If they chose to ignore it, this 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 is becoming 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.[55] 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.[56]

A similar type of legal analysis should also be applied to DLT. The entry into the blockchain is a fact that shows 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 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.[57]

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.[58] Apart from it, the transfer on the blockchain should be accepted as such.

[55] See already Miller v. Race, [1758] 97 Eng. Rep. 398 (K.B.) (Lord Mansfield) ("...in 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 Atlantic Cotton Mills v. Indian Orchard Mills, 17 N.E. 406, 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."); Transamerica Insurance Company v. Long, 318 F. Supp. 156 (W.D. Pa. 1970) (denying restitution of money that a bank robber had paid to tax authorities). For further cases, see Andrew Kull, *Defenses to Restitution: The Bona Fide Creditor*, 81 B.U. L. REV. 919, 937 (2001).

[56] See Miller v. Race, [1758] 97 Eng. Rep. 398 (K.B.) (Lord Mansfield) ("...but before money has passed in currency, an action may be brought for the money itself...").

[57] On this protection see *infra* D 1.

[58] See *infra* part D 1.

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. 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. 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 counterperformance under a transaction. 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 have 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 with hindsight. 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.

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. He must make 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.

But this peculiarity does not make the reverse transfer improbable or unlikely. 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". 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 at a high cost. Moreover, the obligation to use a private key to retransfer assets is not very different from other courts 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 it.

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 US$ 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 US$. 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 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 it 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 decentralised 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. 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. 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.

The many legal questions raised by such transfers cannot be answered by one legal system, but only by a plurality of different laws. This concerns, 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 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. It serves to fulfill an obligation arising under a contract that is 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. This law determines whether the contract is invalid, e.g. in case of mistake. It will also determine the consequences if the transfer made in its execution has to be returned.[59] Since the contract is concluded outside the blockchain, it is not difficult to determine its 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.[60] In the absence of a choice by the parties, many tribunals would apply the law at the habitual residence of the seller.[61]

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 very 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 insofar to the law in force at the place of the tort, the so-called *lex loci delicti*.[62] Challenging for this approach is cross-border torts, in which the damage and the harmful conduct occur in different countries. Some states give prominence to the place of damage.[63] Others consider the place of conduct as more

[59] It is generally agreed that the law applicable to a contract also governs the consequences of its invalidity, see sec. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 221 (1971) and HAY ET AL., *supra* note 37; Rome I, art. 12(1)(e).

[60] See references *supra* note *.

[61] See e.g. Rome I, art. 4(2); Hō no tekiyō ni kansuru tsūsokuhō [Act on the General Rules of Application of Laws], Law No. 78 of 2006, art. 8(2) (Japan); Swiss PILA art. 117(1); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1211(2) (Russ).; Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和合国外围民俗法轮关西石永发) [Laws Applicable to 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).

[62] See e.g. Commission Regulation No 864/2007 (Rome II), on the law applicable to non-contractual obligations, 2008, art. 4(1), O.J. (L199) 6 [hereafter Rome II]; Hō no tekiyō ni kansuru tsūsokuhō [Act on the General Rules of Application of Laws], Law No. 78 of 2006, art. 17 (Japan); Swiss PILA, art. 133(2); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1219(1)2 (Russ).; Zhonghua Renmin Gongheheguo Shewai Minshi Falvguanxi Shiyongfa (中华人民共和合国外围民俗法轮关西石永发) [Laws Applicable to Foreign-related Civil Relations] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2010, effective April 1, 2001) Chap. 6, art. 44 (China).;

[63] See e.g. Rome II, art. 4(1); Hō no tekiyō ni kansuru tsūsokuhō [Act on the General Rules of Application of Laws], Law No. 78 of 2006, art. 17 (Japan).

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.[64] 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 US because arguably the country of residence of the victim has the strongest interest in regulating this tort.[65] 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: 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 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 ones. The proposal made here is no exception in this regard. 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.

[64] See Swiss PILA, art. 133(2); GRAZHDANSKII KODESK ROSSIISKOI FEDERASTII [GK RF] [Civil Code] art. 1219(1)2 (Russ).

[65] See HAY ET AL., *supra* note 37 at 808-22 (discussing governmental interest analysis and torts).

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.[66] Others have qualified Bitcoin as a "new class of private property".[67] An expert in criminal law has stressed the societal expectation that "cryptotheft" must not go unpunished.[68] Uniting all of these statements is the conviction that the law must protect the holders of bitcoins 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 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 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 it calls 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, despite the fact that they do not relate to physical objects and that they can be infinitely multiplied.

[66] Fairfield, *supra* note 1, at 849-54.
[67] Bayern, *supra* note 15, at 29.
[68] Henry Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 N.C. L. REV. 395, 401 (2019).

There is consensus that they merit protection independently of their precise legal categorization and their invisibility in the real world. 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" to only 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

The thesis here is 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 to this concept: 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 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 done a transfer to himself.[69]

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 (see below D 3). 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 she would have no guarantee of getting her assets back even if she can prove the wrongdoing. The other creditors in the insolvency proceedings should however not 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

[69] In case that the hacker has merely obtained the information of 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 he 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.

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.[70] 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 analysis. Beyond the case in which the private key was hacked, obtained by fraud or by blackmail from the defendant, there should therefore not be any analysis of the property situation before the suit. Where a person has willfully typed the private key into a computer, it should not be able to attack the position of the recipient. In case it made a mistake or has not be received a counter performance, it must rely on the reverse transfer to vindicate its rights. 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 counterperformance. 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.[71] Consider the example of succession: Upon death, legal systems typically vest the ownership of the decedent in his representative or heir.[72] This legal transfer comprises all of the decedent's assets, thus it should also include her crypto assets. The transfer happens by mere operation of the law without

[70] See above C 3.
[71] See supra part A 2.
[72] See references above fn. *.

regard to whether the representative or heir has knowledge of the private key or access to it. 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 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.[73] 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. 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.[74] In the case of crypto assets, this

[73] See 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 persons [heirs]"). 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.

[74] 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. in German law Bürgerliches Gesetzbuch [BGB] [German Civil Code], Jan. 2, 2002, BGBL. I at 42. § 2048, no. 2 (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.] art. 724(1) (Fr.) cited *supra* note 73. In both cases, the heir has a cause of action against any person that possesses an object belonging to the estate.

entails the duty to provide the private key. 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 NewCo in a merger transaction or the bankruptcy administrator after the opening of a bankruptcy proceeding. In all 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 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.[75] Where problems under a contract occur, the obligation to perform a reverse transaction will result from the applicable contract law.[76] In the case of hacking, blackmailing or fraud the transfer has no legal effect.[77] Nevertheless, the victim may claim the restoration of the private key under tort law. The applicable national law can be determined according to the ordinary conflict-of-laws rules, which point to the place of the tort.[78] 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 or business secrets. 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

[75] See e.g. Art 10 Rome I Regulation. In the US, see HAY ET AL., *supra* note 37, at 1218-19; Restatement (Second) of Conflict of Laws § 221(2)(b) (1971).
[76] See *supra* note *.
[77] See *supra* C 2 at the end.
[78] See *supra* B 3.

in question will be in danger of losing their crypto assets due to hacking, fraud or coercion.

The consequences of a succession, merger or bankruptcy proceeding are determined by the applicable national law. This law can be determined using the normal conflict rules. For instance, the law applicable to succession is usually determined based on the nationality or habitual residence of the deceased, the law applicable to mergers by the law of the entities in question, and the law applicable to bankruptcies by the law of the country in which the bankruptcy proceedings are opened. 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.

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. A good way to provide more certainty would be an international text that endows a blockchain record with some legal protection. It could also provide for the exceptions in case 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.

E. Conclusion

The 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 as being 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. 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 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.

EBI European Banking Institute

Address

European Banking Institute eV.

Mainzer Landstrasse 251

60326 Frankfurt am Main

Germany

For further information please visit our website www,ebi-europa.eu or contact us at info@ebi-europa.eu

www.ebi-europa.eu

The European academic joint venture for research in banking regulation

Universiteit van Amsterdam

University of Piraeus

universität bonn
Rheinische Friedrich-Wilhelms-Universität Bonn

Universidad Complutense Madrid

CUNEF

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Goethe Universität Frankfurt am Main

Universiteit Gent

University of Helsinki

Universiteit Leiden

EBI
European
Banking
Institute

University *of Ljubljana*

Queen Mary
University of London

uni.lu
Université du Luxembourg

JG|U
Johannes Gutenberg Universität Mainz

University of Malta
L-Università ta' Malta

Università Cattolica del Sacro Cuore

University of Cyprus

Radboud Universiteit

Universiteit Antwerpen

– Panthéon - Sorbonne –
Université Paris 1

Université Paris II
Panthéon-Assas

Stockholm University

University of Tartu

Católica Faculdade de Direito

Católica Global School of Law

U Lisboa
Universidade de Lisboa

UAM
Universidad Autónoma de Madrid

www.ebi-europa.eu