The qualification of bitcoins as documentary intangibles

Tycho DE GRAAF*
Published in European Review of Private Law (ERPL) 5 (2019), p. 1051-1073

Abstract
It is unclear how bitcoins should be qualified from a legal perspective. This qualification is, among other things, relevant to determine how bitcoins should be transferred, pledged, attached and executed. In this article, bitcoins and bitcoin transfers are explained from a technical perspective and subsequently qualified from a contract and property law perspective. Given the borderless nature of bitcoins and its underlying bitcoin technology, these subjects are dealt with in an international manner, often drawing upon legal concepts which form the backbone of most if not all legal systems, especially those in the EU. In this article, the following conclusions are reached. First of all, from a contract law perspective, the bitcoin network qualifies as a multi-party contract to which the various participants (users, miners and nodes) accede by participating in the network for the first time and, in doing so, accept the third-party rights clause stipulated in that agreement in their favour. Secondly, from a property law perspective, the rights with respect to the bitcoins credited to a bitcoin address are put to bearer at the same moment these bitcoins are so credited. They are put to the bearer of the holder of the value bearer on which the private key associated with that bitcoin address is stored. That value bearer embodies the right of that bearer to perform the work necessary to transfer the bitcoins on that bitcoin address, more specifically vis-à-vis the miners to validate that transaction and vis-à-vis the nodes to verify the work of the winning miner. Those bitcoin rights can be transferred, pledged, attached and executed by possession of the value bearer.

1. Introduction

1. It is unclear how bitcoins should be qualified from a legal perspective. The answer is, among other things, relevant to determine how bitcoins should be transferred, pledged, attached and executed. In this article I will try to qualify bitcoins from a contract and property law perspective. To that end I will first explain from a technical perspective what bitcoins are and how they are transferred. Then I will discuss how the bitcoin network can be qualified from a contract law perspective in order to be able to take the leap to a more extensive qualification from a property law perspective. For the purposes of this contribution, I assume that bitcoin is not money,[1] and investigate in particular whether bitcoins can be seen as documentary intangibles.[2] In the process, I will identify and overcome requirements and

* mr. dr. Tycho de Graaf is an assistant professor civil law at Leiden University. This article is an extensively remastered version of my Dutch language article 'De kwalificatie van bitcoins', *NJB* 2019-1, p. 6-18, from which a large number of Dutch law specific elements were removed and to which many more comparative law elements were added.

[1] In the Netherlands, bitcoins is not considered money, see W.A.K. RANK, 'Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten' in R.A. WOLF e.a., *Bitcoins. Civiele en fiscale aspecten in beeld* (Deventer: Kluwer 2015), p. 26-39; and B. BIERENS, 'Veranderend betaalgedrag vanuit een juridisch perspectief. Kan het contant geld al worden afgeschaft?', *NJB* 2018-19, p. 1348, who argues that bitcoin is similar to an electronic equivalent of cash and that the transfer of a bitcoin is similar to a bank transfer. See for Belgian law J.-L. VERHELST, 'Zijn cryptomunten munten? Een analyse van Bitcoin' in M.E. STORME & F. HELSEN (eds), *Innovatie en disruptie in het economische recht* (Antwerpen: Intersentia 2017), p. 23-78.

[2] In furtherance of E. MCKENDRICK, *Goode on Commercial Law* (LexisNexis UK and Penguin Books, 2016), paragraph 2.56-2.58, I will use the term documentary intangibles as a generic term comprising both documents obliging the debtor to pay a sum of money (usually referred to as negotiable instruments, such as bills and

assumptions with respect to signatures, the written form and the concept of giving and taking documentary intangibles; as well as discuss objections that can be raised against my arguments.

Given the borderless nature of bitcoins and its underlying bitcoin technology, I will deal with the subjects at hand in an international manner, often drawing upon legal concepts which form the backbone of most if not all legal systems, especially those in the EU. By doing so, the reader will hopefully recognize that the concepts and arguments presented may also be applied in his or her own legal systems, if need be with some modifications. Nonetheless, I will sometimes discuss local law if a specific topic so requires, especially in those cases where it helps substantiate the argument presented and make it more concrete.

2. What are bitcoins, how are they transferred and where are they?

2. Bitcoin is a cryptocurrency and bitcoin transactions are:
   1. stored in a decentralized manner on various computers called nodes, which are connected to each other in a network without a central intermediary by using the internet and which belong to different people (so it works in a disintermediated way);
   2. stored in a ledger, which is publicly accessible, to which transactions can, at the end of the day, only be added if at least 51% of the nodes agree that the transaction is correct (which is called reaching consensus) and which can otherwise not be changed (so it is a secure, tamper-resistant public ledger with a single source of truth);
   3. that is constantly being synchronized without an intermediary using a peer-to-peer protocol (think bittorrent) so that everyone possesses the same ledger.[3]

3. In order to better understand bitcoins and bitcoin transactions, it is useful to explain how bitcoin transactions work, for example if A has one bitcoin and wants to transfer his bitcoin to B. This is done in three basic steps: (1) B generates three sets of keys with which he opens a bitcoin account and the private key of which B safely stores, (2) A transfers a bitcoin to the bitcoin account of B, after which B receives one bitcoin in a yet unverified manner and (3) the transaction is verified by other participants in the bitcoin network and, if they deem the transaction to be correct, added to the decentralized ledger. The reality is more complex, as will now be demonstrated.

2.1 *Creation of keys, address and wallet*

4. The transfer starts with B needing to have a bitcoin address (think of a bank account number) to which A can transfer his bitcoin. B creates such a bitcoin address as follows. Using wallet software (running on B's own computer or smartphone, or on a third party's server), B generates three sets of key strings:
   1. a private key, which is necessary to transfer the bitcoins that are on the corresponding bitcoin address (see below) (more or less comparable to a long, complicated and difficult to remember password for internet banking);
   2. a public key derived from the private key, a (still) long string of characters; and
   3. a bitcoin address, which is a shortened (58 characters long) version of the public key that is needed in order to receive bitcoins (think about a bank account number), and

notes) and documents to perform an obligation (such as a bill of lading requiring the carrier to provide possession of the cargo to the holder of the bill of lading pertaining to that cargo).

[3] See for a simple explanation of bitcoin https://medium.freecodecamp.org/explain-bitcoin-like-im-five-73b4257ac833 and for a more complex one https://en.wikipedia.org/wiki/Bitcoin. See for a comprehensive treatment of smart contracts on the blockchain the special issue of ERPL 2018/6.

often also appears as a QR code that can be scanned (in order to avoid having to copy/paste or retype the bitcoin address).[4]

5. After generating those key strings, B stores his private key in a so-called wallet. There are two different forms of wallets: hot/live wallets and cold wallets.[5] A hot wallet is software that runs on hardware that is connected to the internet. That hardware belongs either to the user (B's own computer or smartphone) or to a third party (e.g. B's supplier). If the hardware is owned by B's supplier, the private key stored should be encrypted by that supplier. B can retrieve the key from that supplier, for example, by logging in to the supplier's environment using his username and password (or more).[6] Such a wallet is also called a web/online wallet. If the hardware belongs to the user, the private key is stored in encrypted form by means of software on his computer (a desktop wallet[7]) or an app on his smartphone (a mobile wallet[8]). In most cases, this is the same software/app as the software/app with which the aforementioned key strings (private key, public key and bitcoin address) were generated.

A cold wallet is not connected to the internet and therefore safer than a hot wallet, albeit less user-friendly. To transfer bitcoins from one bitcoin address to another, the private key must first be 'removed' from the wallet and 'inserted' in software running on hardware which is connected to the internet. The simplest form of a cold wallet is a paper wallet.[9] This is a piece of paper on which the public key and the bitcoin address are visible and, usually hidden beneath a scratch layer or sticker, the private key. A hardware wallet is more complicated.[10] This is a physical device that looks like a USB stick and is intended exclusively for storing private keys. This device encrypts the private keys and secures access to them by means of a code.

2.2 *Unverified transfer from A to B*

6. The transfer can begin as soon as B has generated the three key strings (private key, the public key and bitcoin address) and stored the private key in a wallet.[11] B then provides A with the bitcoin address on which he wants to receive the bitcoin. B can do this by opening his bitcoin wallet app on his smartphone and showing the QR code of the bitcoin address to A. A then scans that QR code with his bitcoin wallet app and the camera on his smartphone. In doing so, A makes clear to his app to which bitcoin address he wants to transfer bitcoins, namely B's bitcoin address. A then selects in his app the bitcoin address from which he wants to transfer bitcoins (his own account), the amount of bitcoins he wants to transfer (in this case one), and the transaction fees (in bitcoin) he is prepared to pay for such transfer. The higher the transaction costs proposed are, the faster the transaction will be processed. A then confirms the transaction by signing it with his private key stored in his

---

[4] A.M. ANTONOPOULOS, *Mastering Bitcoin. Programming the Open Blockchain* (Sebastopol, CA, USA: O'Reilly 2017), p. 55-70.
[5] https://www.coindesk.com/information/how-to-store-your-bitcoins/ and https://www.buybitcoinworldwide.com/wallets/#types-of-wallets.
[6] Considering that there is a risk that bitcoins get stolen if the supplier is hacked, suppliers often take extra measures, such as storing private keys on servers which are not connected to the internet and from which these keys are retrieved as soon as the customer so requests, see for example https://www.coinbase.com/security.
[7] For example: Electrum, https://electrum.org/.
[8] For example: Edge, https://edge.app, of BRD, https://brd.com.
[9] Made by using, for example: Wallet Generator, https://walletgenerator.net, or Bitcoin Paper Waller, https://bitcoinpaperwallet.com.
[10] For example a Trezor, https://trezor.io, or Ledger, https://www.ledger.com/products/ledger-nano-s?r=2c06&path=/products/ledger-nano-s&tracker=walletsintro.
[11] For a more extensive description of how bitcoins are transferred see A.M. ANTONOPOULOS, *Mastering Bitcoin*, p. 8-14.

app. By means of such signature, it can later be determined (in the manner discussed below) whether A was permitted to transfer the bitcoins on the bitcoin address to which that private key is related and whether that address contains at least one bitcoin. This check is performed to prevent bitcoins from being spent twice.

Within a few seconds after A signs the transaction, that transaction is spread peer-to-peer over the nodes in the bitcoin network and these nodes will see, for the first time, the bitcoin address generated by B as well as the relevant transaction. In the meantime, B's app constantly listens to transactions on the network that match the bitcoin address stored in that app. Once B's app has found a match, that app indicates that B has received one unconfirmed bitcoin.

2.3 *Validation of transactions by miners and verification by nodes*

7. The next step is that the unverified transaction is approved and added as a block to the blockchain and thereby to the decentralized general ledger.[12] This is done in two steps by two different types of parties: miners and nodes, who have each installed software on their computers to participate in the bitcoin network and fulfil their respective tasks.[13]

As a first step, a *speed competition* takes place. That is a contest in which computers (so-called *miners*) fully automatically perform three tasks: they collect different transactions in a *block* (a *candidate block*), validate whether the transactions included therein are correct (comparable to clearing when transferring money from one bank account to another) and solve (in order to prevent abuse) a complicated and unique cryptographic puzzle relating to that block (the so-called *proof of work*).[14] The person who first solves the puzzle wins the right to add the block thus created to the blockchain.[15] He is therefore called a *proposer*.

As a second step, a *quality competition* takes place. That is a contest in which nodes verify whether the proposer has done his job properly, so whether he has correctly established which transactions included in the candidate block are correct and whether the solution of the cryptographic puzzle is correct. Checking this is fairly simple. If at least 51% of the nodes agree that the proposer has done his job well, so-called *consensus* is reached, the verified transaction is confirmed and the candidate block is added to the blockchain as a new block. In exchange for all his work, the proposer receives a reward that is transferred to the bitcoin address he specified. This remuneration consists of a block reward and transaction costs. The *block reward* consists of new bitcoins created by the bitcoin network and is currently 12.5 bitcoins.[16] Such block reward is the only way new bitcoins can be mined or, in other words, come into existence. The transaction costs consist of the bitcoins specified up front by the transferor and are paid by him.

8. However, if at least 51% of the nodes conclude that the proposer did not do his job properly, the candidate block is rejected, the transaction is not confirmed, no new block is added to the blockchain and a new speed competition starts. In that case, the proposer will

---

[12] For a more precise description of how verification works and what transaction costs must be paid for such verification see A.M. ANTONOPOULOS, *Mastering Bitcoin*, p. 212-267.

[13] See D. DRESCHER, *Blockchain Basics. A Non-Technical Introduction in 25 Steps* (Apress: New York 2017), Step 18 Verifying and Adding Transactions, p. 153-164. A miner downloads mining software such as CGMiner https://en.bitcoin.it/wiki/CGMiner or BFGMiner http://bfgminer.org, a node BitcoinCore https://bitcoincore.org.

[14] See https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ and A.M. ANTONOPOULOS, *Mastering Bitcoin*, p. 28-29 (general description) and p. 213-240 (detailed description).

[15] In reality, miners work together in so-called *mining pools* and share the profits they receive (the *block reward*, see below) if their pool wins. See for an overview of mining pools and their 'market share' https://www.blockchain.com/pools.

[16] The block reward is halved every four years. See for the next moment http://bitcoinclock.com.

not only receive no remuneration (no block reward and no transaction costs), but he will also be 'punished' because he has unsuccessfully put all that effort into solving that cryptographic puzzle. So that puzzle is so complicated to discourage abuse.

Back to A and B. If the transaction is confirmed, A's app shows that one bitcoin is transferred to the bitcoin address of B and B's app shows that one confirmed bitcoin has been received. That can take a while.[17] B can then use the one bitcoin received using the private key associated with his bitcoin address.

2.4 *Anonymity*

9. For the creation of a bitcoin address and the transfer of bitcoins, A and B do not have to enter personal or other identifying data. They can remain anonymous if they leave no information about any computer or smartphone from which they perform their actions.[18] For transferring bitcoins, only the following is required: the transferor's bitcoin address and associated private key as well as the transferee's bitcoin address. Unlike when transferring money from one bank account to another, it is irrelevant who actually 'owns' a bitcoin address. The signing of the transaction with the private key only serves to establish in a technical sense that the signatory (not as a person, but as the presenter of the private key) is entitled to transfer the bitcoins on that bitcoin address. Signing of the transaction does not (also) purport to authenticate the signatory as a person, i.e. establish that the signatory is the person he claims to be.

The downside is that the person who loses his private key can no longer use the bitcoins on the corresponding bitcoin address. In contrast, the person who loses his password for internet banking can regain access to the money in his bank account. He can do this, for example, by visiting a bank branch, identifying himself with his passport, showing his face and signing a piece of paper.

2.5 *Technical summary*

10. From a technical point of view, the foregoing can be summarized as follows:
    1. a wallet contains a private key that can be used to transfer bitcoins (and the wallet as such does not contain the bitcoins);
    2. transactions in bitcoins are stored on the blockchain (and not in wallets);
    3. transactions are validated by miners who all want to be the first to validate transactions and solve a cryptographic puzzle in order to receive a remuneration;
    4. the work of the winning miner (proposer) is verified by nodes (computers participating in the network that have each downloaded and distribute the decentralized ledger);
    5. transactions approved by the proposer are added to the blockchain as a block if at least 51% of the nodes have reached consensus that the proposer has done his job correctly;
    6. in that case the proposer receives a remuneration comprised of bitcoins (new bitcoins from the system (=block reward) and existing bitcoins from the transferor (= transaction costs));

[17] See for an explanation of how long a bitcoin transaction takes https://coincentral.com/how-long-do-bitcoin-transfers-take/.

[18] They can prevent leaving identifying data by, amongst other things, using a Virtual Private Network (VPN) service, such as NordVPN https://nordvpn.com, TorGuard https://torguard.net or privateinternetaccess https://www.privateinternetaccess.com/. Miners and nodes can remain anonymous the same way. Of course, the weakness in the system is when bitcoins are exchanged for money and identification often occurs.

7. participants can remain anonymous; and
8. there is no central authority that verifies or supervises.

3. Contract law analysis: the bitcoin multi-party contract

11. How should this system be qualified from a contract law perspective? In my opinion, the bitcoin system is to be regarded as a multi-party contract.[19] The first-ever participation of a user, miner or node (collectively: participants) in the bitcoin network can be considered as accepting an implicit third-party rights clause.[20] This third-party rights clause is included in that multi-party contract and is stipulated in favour of each user, miner and node that wants to participate in the bitcoin network. By accepting the third-party rights clause addressed to him, the relevant user, miner or node becomes a party to the multi-party contract. This acceptance takes place by participating in the network and is addressed to another participant who is already a party to the contract, i.e. the first participant with whom the new entrant has peer-to-peer contact for the first time. The multi-party contract to which the new entrant has become a party is a framework contract that not only encompasses the general rights and obligations of the parties, but also the rights and obligations with respect to each individual transaction. The content of these rights and obligations depends on the capacity of the participant in question and is therefore best explained by means of an example, which I will do below.[21]

12. Before I do that, it is important to emphasize that the bitcoin multi-party contract is not a classic, written contract with all kinds of contractual provisions. This multi-party contract is a contract the content of which is determined by the technology described above, more specifically, the operation of the bitcoin software. That software and the related documentation is open-source and available to everyone.[22] By analyzing the source code of the software and reading the documentation of that software, every participant in the bitcoin network knows, depending on the capacity in which he participates in the bitcoin network, what to do or, in other words, what obligations he has vis-à-vis his fellow participants. Since these obligations are not explicitly included in the multi-party contract, but inferred by technology, many stipulations which I will describe below are stipulations that have been tacitly agreed upon.

Furthermore, it is worthwhile considering the moment the multi-party contract terminates. That is the moment in time when the participant no longer participates in the bitcoin network. At that moment in time, only the part of the multi-party contract that applies to him ends and the remainder of the multi-party contract remains in existence. The participant that no longer participates, leaves the contract (as opposed to accedes to the contract). Therefore, the multi-party contract is a contract by which third parties can accede to or leave at any time and in respect of which creditor and debtor replacement continuously takes place (and which I will discuss in more detail below).

---

[19] See also S. GEIREGAT, 'Cryptocurrencies are (smart) contracts', *Computer Law & Security Review*, 2018, Volume 34, Issue 5, p. 1-6, https://doi.org/10.1016/j.clsr.2018.05.030, who argues that according to Belgian law, the bitcoin network should be regarded as a multi-party contract and the rights ensuing therefrom as an expectation of whoever has a bitcoin wallet that the other participants accept bitcoin as a means of payment if that person wishes to fulfil a payment obligation vis-à-vis one of the other participants.

[20] See for third party rights clauses and their acceptance under Dutch law: articles 6:253, 6:254 and 3:37 of the Dutch Civil Code, under Belgian law: art. 1121 Belgian Civil Code and for English law section 1 of the Contracts (Rights of Third Parties) Act 1999.

[21] Participants can participate in the bitcoin network in various different capacities. Miners are, for example, often also nodes.

[22] See https://github.com/bitcoin/bitcoin and https://bitcoin.org/en/developer-documentation respectively.

13. Let us now, as mentioned, illustrate the content of rights and obligations by means of an example. Take again user A who wishes to transfer one bitcoin to B. A enters the required transaction information in his application, signs the transaction with his private key and sends it to the bitcoin network. Through the first contact with the bitcoin network, he accepts the third-party rights clause addressed to him and thereby becomes party to the multi-party contract. Every miner who already participates in the bitcoin network has already become a party through his first contact with that network, just like every node has by means of his first contact.

By becoming a party to the multi-party contract, every miner has undertaken to participate in any speed competition initiated by a transferor wishing to transfer bitcoins to a transferee. In that respect, the miners are obliged to provide services (namely: collect transactions in a block, validate those transactions and solve cryptographic puzzles), against remuneration (of a block reward and transaction fees) to the winning proposer whose candidate block is added to the blockchain, so on a no cure no pay basis.

By becoming a party to the multi-party contract, each node in turn has committed himself to verify the work done by each proposer, and thus determine whether that proposer has correctly established whether the user transactions included in the candidate block as well as the presented solution to the associated cryptographic puzzle are correct. A node is discharged from that obligation as soon as more than 51% of the nodes reach the same conclusion about the verification of the proposer's work. For that verification, the nodes are not paid directly. A form of indirect payment can, however, be construed.[23] After all, nodes that wish to conduct transactions themselves benefit from having their transactions verified. And nodes that mine themselves benefit from verifying proposers because if it is established that a proposer has not performed his work correctly, the speed competition starts again and each miner has another chance to become a proposer. If is established that that proposer has performed his work correctly, he receives the block reward and transaction costs.

14. The aforementioned rights of the user vis-à-vis the miners and nodes to perform their validation and verification work respectively, I will call *bitcoin rights*.[24] Those rights must be effectuated to ensure that bitcoins are transferred from one to bitcoin address to another. I hereby conclude the technical explanation and contract law qualification, which I need in order to qualify bitcoins from a property law perspective.

[23] This is relevant for legal systems which, like English law, require consideration in order for a contract to be enforceable.

[24] See T.F.E. TJONG TJIN TAI, 'De blockchain als alternatief voor de notariële praktijk', in F.W.J.M. SCHOLS & B.C.M. WAAIJER (eds), *Financiële zorgplicht van de notaris (preadviezen KNB)* (Den Haag; Sdu 2018), p. 123, who writes: 'Maybe it is possible to regard the verification possibilities or potential claim with respect to a bitoin balance as a right, which can be attached at that party by means of a third party attachment.' (translated, TG).

4. Property law analysis

15. The qualification of bitcoins from a property law perspective is something which legal authors have struggled with. Some have taken a very physical approach, believing that by mining, the miner becomes owner of the newly created bitcoins on the basis of specification and that only paper wallets are documentary intangibles.[25] Others have argued a bitcoin is more like a tangible good than a property right, but can only be fitted into a property law system by considering it as an (absolute) property right.[26] Of those who qualify bitcoin as an (absolute) property right,[27] some subsequently run into trouble with the numerus clausus rule (i.e. the closed system of property rights) because a bitcoin (right) is not specifically mentioned in statute and is therefore not transferable.[28] As a consequence, some argue, the transfer of bitcoins takes place exclusively on the basis of contract law, is to be considered a 'Realakt' and does not result in a change to the property law positions.[29] Given this legal uncertainty, Russia is reportedly preparing legislation pursuant to which rights to cryptocurrencies are classified as property rights.[30]

Each of these approaches has its advantages and disadvantages. Given the length of this article I will, however, not discuss these further. Instead, starting from the earlier technological explanation and qualification from a contract law perspective, I will look for a property law qualification that best suits the way in which the bitcoin network functions from a technological perspective. Mirroring the technological reality with a legal qualification is necessary because in blockchain cases, code is (often) law.[31]

16. In view of the foregoing, a property right qualification must satisfy the following three requirements dictated by technology:

---

[25] See with respect to Belgian law: M. VANWYNSBERGHE, 'Bitcoin heeft het op de grenzen van het goederenrecht gemunt', *Rechtskundig Weekblad* 2014/15-37, p. 1442, but then concludes that bitcoin is an incorporeal right that cannot be qualified from a private law perspective.

[26] See with respect to Dutch law: W.A.K. RANK, 'Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten', p. 36-37, whilst at the same time recognising that that qualification is not a very good fit because rights to a bitcoin are thereby equated with the bitcoin itself, whilst they are essentially different things.

[27] See with respect to Dutch law: V. TWEEHUYSEN, 'Goederenrechtelijk puzzelen met bitcoins', *AA* 2018-juli/augustus, p. 602-610; J.L. SNIJDERS & Y.C. TONINO, 'Goederenrechtelijke status van bitcoin (kapitaalkracht)', *Tijdschrift Financiering, Zekerheden en Insolventierechtpraktijk* 2018-6, p. 46-55; Rechtbank Midden-Nederland (vzr.) 7 December 2017, ECLI:NL:RBMNE:2017:6646 with respect to Ether, another cryptocurrency; and Rechtbank Amsterdam 14 February 2018, ECLI:NL:RBAMS:2018:869, *JOR* 2018/154, *Koinz Trading*, which deems bitcoin to have 'characteristics of a property right', as a result of which a right to payment in bitcoin is considered as an asset within the meaning of bankruptcy law.

[28] See with respect to Dutch law: F.H.J. MIJNSSEN, *Verbintenissen tot betaling van een geldsom (Mon. BW nr. B39)* (Deventer: Kluwer 2017), paragraph 1.6 whilst referring to art. 3:83, paragraph 3 DCC.

[29] C. ENGELHARDT & S. KLEIN, 'Bitcoins – Geschäfte mit Geld, das keines ist. Technische Grundlagen und zivilrechtliche Betrachtung', *MMR* 2014-355.

[30] A. SEVELYEV, 'Some risks of tokenization and blockchainizaition of private law', *Computer Law & Security Review* 2018, Volume 34, p. 863-869 and A. ZHAROVA & I. LLOYD, 'An examination of the experience of cryptocurrency in Russia. In search of a better practice', *Computer Law & Security Review* 2018, Volume 34, p. 1300-1313.

[31] A. WRIGHT & P. DE FILIPPI, 'Decentralized blockchain technology and the rise of lex cryptographia', SSRN 2015-March 12, https://ssrn.com/abstract=2580664, p. 1-58 and P. FILIPPI & A. WRIGHT, *Blockchain and the Law. The Rule of Code* (Cambridge, Massachusetts: Harvard University Press 2018), who refer to lex cryptographica whilst referring to the 'code is law' concept introduced by L. LESSIG, Code and Other Laws of Cyberspace (New York: Basic Books 1999) and L. LESSIG, Code version 2.0 (New York: Basic Books 2006), http://codev2.cc. See also R.H. WEBER, 'Rose is a rose is a rose is a rose – what about code and law?', *Computer Law & Security Review* 2018, Volume 34, p. 701-706 and T.J. DE GRAAF, 'Van oud naar nieuw: van internet naar smart contracts en van mensen naar code (I) en (II, slot)', *WPNR* 7199 16 June 2018, p. 494-501 and *WPNR* 7200 23 June 2018, p. 525-530.

1. anonymity because the bitcoin network only deems important the fact *that* the transaction is signed with the private key associated with the bitcoin address from which the bitcoins are transferred, not *who* signs;
2. easy creditor replacement for the same reason; and
3. easy debtor replacement because miners and nodes can, at any given time, join or leave the bitcoin multi-party contract by joining or leaving the bitcoin network.

17. In qualifying, it should be borne in mind that it is a dead end to focus on the qualification of a bitcoin and bitcoin transactions. After all, this is stored decentrally in the bitcoin public ledger file on all nodes all over the world and there are currently around 10,000 nodes.[32] So there is no unique file and transferring, pledging, attaching and executing all (or even the majority) of these files is practically impossible. That impossibility is by design. The bitcoin network has been designed to ensure that an 'attack' on one or more nodes has no effect. Dead ends are also qualifications for which statute requires a signature to transfer, pledge, attach or execute bitcoins, e.g. by requiring a deed of transfer with a signature. After all, a signature within the meaning used in statute almost always serves to enable the signatory to identify himself (to make clear who he is) and to enable the one who receives the signed document to authenticate the signatory (to reliably prove that the signatory is the one he says or pretends to be).[33] This process of identification (by the user) and authentication (by miners and nodes) cannot take place in the bitcoin network because the bitcoin network has been built to transfer bitcoins anonymously.

Given this existing technological and legal reality, we must focus on the private key, the wallet in which the key is stored as well as the carrier on which the wallet is stored. From a technological point of view, the only way that bitcoins can be used is by using these keys, wallets and carriers. From a legal perspective, my first thought is to investigate whether that carrier can be qualified as a documentary intangible, namely a documentary intangible put to bearer. Documentary intangibles put to bearer are perfect for anonymity and simple creditor replacement. For this reason, I will investigate below whether bitcoins can qualify as documentary intangibles put to bearer in terms of property law and thus fulfil the aforementioned three requirements (anonymity, easy creditor replacement and easy debtor replacement).

4.1 *The physical appearance of the wallet as an embodiment of the bitcoin rights*

18. Bitcoins are, as mentioned, mined/created by a winning miner (proposer) as a block reward at the moment that (1) at least 51% of the nodes acknowledge that

[32] For an overview of participating nodes and the countries where they are located https://bitnodes.earn.com.
[33] This is almost always true for wet ink and electronic signatures. See for an overview of the various functions of signatures and paper documents, especially in relation to equating electronic with wet ink signatures under Dutch law: S.M. HUYDECOPER & R.E. VAN ESCH, *Geschriften en handtekeningen: een achterhaald concept?, ITeR-reeks nr. 7* (Alphen aan den Rijn/Diegem: Samsom BedrijfsInformatie 1997), p. 71-162 as well as T.J. DE GRAAF, 'De lappendeken van de gelijkstelling van elektronisch met schriftelijk in het licht van vormvereisten en bewijskracht', *MvV* 2018/7-8, p. 243-248. See for Belgian law P. VAN EECKE, *De handtekening in het recht: van pennentrek tot elektronische handtekening. diss. KU Leuven* (Larcier: Gent 2004). See for English law: E. MCKENDRICK, *Goode on Commercial Law*, paragraph 3.29, who notes that 'The function of a signature is to authenticate the document, that is, to demonstrate the signer's approval or apparent approval of its contents.' and S. MASON, 'Documents signed or executed with electronic signatures in English law', *Computer Law & Security Review* 2018, Volume 34, p. 933-945 as well as the sources mentioned therein. See for electronic signatures in the EU the eIDAS Regulation 910/2014 on electronic identification and trust services for electronic transactions.

the transactions included in the candidate block by that proposer have been correctly verified and the associated cryptographic puzzle has been correctly solved and (2) the block reward bitcoins are credited to the bitcoin address specified by that proposer. Assuming that the proposer has not, intentionally or unintentionally, left personal or otherwise identifying data when using the bitcoin network, this mining cannot be linked to a legal or natural person. From a technological point of view, those bitcoins are created anonymously.

19. The miner can subsequently only transfer those bitcoins on that bitcoin address by using the private key associated with said bitcoin address. In order to be able to transfer a bitcoin from that bitcoin address, that miner (as holder of the private key associated with that bitcoin address) exercises the aforementioned rights vis-à-vis the miners and nodes to have them perform their validation and verification work respectively. Whilst performing their work, the miners and nodes only check whether the private key is linked to the bitcoin address, and not who has created that bitcoin address or uses that private key to sign the transaction.[34] In other words, it does not matter to the miners and nodes whether the private key is presented by, in this case, the person who has mined the bitcoins, or someone to whom he has given his private key or even someone who has stolen that key. In order to reflect this technological reality from a legal perspective, these rights must be made to bearer as soon as possible. For the fully automatically acting miners and nodes, the person who first shows the private key, and nobody else, has the right to transfer the bitcoins to which the signed transaction pertains (to a bitcoin address of someone else or to another bitcoin address of himself).

20. Given the way the technology works, I believe that, from a legal point of view, the bitcoin rights[35] are made to bearer at the same time as a bitcoin has been mined, i.e. put to the bearer of the private key associated with the bitcoin address on which the bitcoin is first created. I understand that this may be hard to fathom at this moment because internationally, property law is even less harmonized than contract law. Nonetheless, I ask the reader to bear with me and consider to what extent his or legal system would allow for the application of the legal constructs proposed. So continuing: by the way in which transfer from one to the other bitcoin address technically works, it should in my view be assumed that the parties have agreed in the bitcoin multi-party contract (or it is considered mercantile usage) that at the same time bitcoins are mined, the bitcoin rights with respect to those bitcoins are immediately put to bearer, more specifically to the bearer of the (carrier of the) private key that is associated with the bitcoin address to which the block reward is credited. In doing so, a documentary intangible put to bearer is created. The same applies, mutatis mutandis, at the moment that mined bitcoins are transferred from the bitcoin address of the winning proposer to another bitcoin address, as well as for each subsequent transfer. Once transferred bitcoins are added to another bitcoin address and

[34] As Fairfield notes: 'Until recently, a party who wishes to pay for something online must reveal her personal information. This is because the nature of the transaction is contract-based, not property-based. An online payment is not a transfer of money from one person to another. It is, properly speaking, a chain of promises to pay. … Crypto-currency transactions, by contrast, permit consumers to buy items online without exposing their personal information. A consumer can transfer digital cash directly, instead of constructing a chain of identity supporting a promise of future payment. The vendor does not need to know who the buyer is, merely that the buyer can pay the amount of digital cash required.', JOSHUA A.T. FAIRFIELD, 'Smart Contracts, Bitcoin Bots, and Consumer Protection', 71 *Wash. & Lee L. Rev. Online* 36 (2014), https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3, p. 45-46.

[35] By way of reminder: bitcoin rights are rights of the participant vis-à-vis the miners and nodes to perform their validation and verification work respectively in order to transfer bitcoins from one bitcoin address to another.

confirmed, simultaneously bitcoin rights with respect to those bitcoins are put to bearer, more specifically to the bearer of the (carrier of the) private key belonging to that address.

That documentary intangible put to bearer is structured as follows. The private key with which the mined or otherwise credited bitcoins can be transferred is, as mentioned before, stored in a wallet. The wallet, in turn, is a physical carrier (paper wallet) or stored on a physical carrier (other wallets). If the wallet is stored on a physical carrier, it is in the form of a private key file that is stored on a disk, generally on the flash memory of a mobile device, or on a solid-state drive or hard disk of a computer. The disk, in turn, is part of a *dedicated device*, such as a hardware wallet (the USB stick like device), or a *non-dedicated device* that usually also has something else on it (such as a smartphone or computer). Because the bitcoin rights are put to the bearer of the private key that is associated with the relevant bitcoin address, that private key is stored in a wallet and that wallet (in the end) has a physical appearance, the bitcoin rights are (ultimately) embodied in a physical carrier. I will refer to this physical carrier with the neutral concept of *value bearer*.[36] Whether the fact that documentary intangibles are usually in the paper form and that documentary intangibles are usually transferred by one person giving and another taking (without leaving anything behind with the giver) poses problems, I will discuss below under the objections.

Anonymity and creditor replacement

21. First, I will finish the legal qualification of bitcoin rights as rights embodied in the value bearer. Once bitcoin rights are so qualified, it is relatively easy to meet the requirements of anonymity and easy creditor replacement. By its nature, the bitcoin network functions on an anonymous basis and putting the bitcoin rights to bearer is not undermining this anonymity.

Debtor replacement

22. Debtor replacement, however, poses more of a problem. A structure must be devised to make it possible, from a legal point of view, for the miners and nodes which leave the bitcoin multi-party contract to be replaced by miners and nodes which accede to that contract. That is quite a challenge. Putting rights to bearer is only a simple method of creditor replacement, but does not offer any possibility to easily replace the debtor(s). The most obvious possibility of having the obligations (or debts) be assumed by another debtor is to transfer these obligations to such debtor. Regardless of the legal formalities required for such transfer, this solution is not really a solution at all because it is not necessarily the obligation of that one miner or node leaving (to perform the validation and verification work respectively upon a user exercising his bitcoin rights) that is taken over one-by-one by another acceding miner or node.

23. It seems better to be of the opinion that in the multi-party contract, implicitly and already now for then, it has been agreed that every miner and node may leave the contract and that at that moment the users renounce their bitcoin rights in relation to that exiting miner or node. The 'new' miners and nodes which, by acceptance of the third party rights clauses stipulated in their favour, become a party to the multi-party contract will, the

[36] Comparisons can be made to the concept of ‘durable medium’ within the meaning of art. 2 under 10 Dir. 2011/83 of 25 October 2011 concerning consumer rights, with respect to which ECJ 5 July 2012, ECLI:EU:C:2012:419, *Content Services/Bundesarbeitskammer*; and ECJ 25 January 2017, ECLI:EU:C:2017:38, *BAWAG/Verein für Konsumenteninformation*.

argument goes on, each take on an independent debt vis-à-vis the users. That point of view is also not convincing. If miners and nodes are so easily able to evade their obligations by simply disconnecting from the bitcoin network and thereby immediately discharged from their obligations, then those obligations cannot (in retrospect) be considered as legally enforceable obligations whose flipside can be qualified as rights in respect of which creditor replacement can take place through providing possession of the value bearer.

24. One possibility of making the presented solution work, is by using company law. The bitcoin network can also be regarded as a multi-party contract to which users, a miner legal entity and a node legal entity are a party. Those two legal entities each take it upon them, as an independent obligation, to perform the work which the miners respectively nodes are required to perform. At the 'back-end' of these legal entities, different (legal) persons are at work, who start and stop working at will. This is done in the same way as with a legal entity whose personnel and subcontractors fluctuates because new employment/subcontract contracts are entered into or terminate. Which legal entity is most suitable for this and how the external and internal relationships of that legal entity work, is beyond the scope of this article.

25. What does fall within that scope, however, is a discussion of two important objections which can be raised against the proposed value bearer structure: firstly, that an electronic documentary intangible is not a documentary intangible because it is not made of paper, and secondly, that an electronic documentary intangible is not a documentary intangible because it cannot be given and taken. I will now discuss these objections.

Comparative notes

26. Whether the reader's legal system will allow for bitcoin rights to made to bearer, will of course depend on local law. In the Netherlands, for instance, this is possible: it has an open system of documentary intangibles law: parties are free to put their rights to the bearer of a documentary intangible. Whether parties want to, is a matter of contract interpretation and even if specific formal requirements for a specific documentary intangible are not met, general documentary intangible law will still apply[37] and a documentary intangible does not need to be signed in order to be a documentary intangible.[38] In England, it should also be possible: whether a right is considered to be embodied in a documentary intangible depends on mercantile usage,[39] and this too should provide sufficient leeway.

---

[37] R. ZWITSER, *Order- en toonderpapieren (Monografieën BW nr. A28*) (Deventer: Wolters Kluwer 2017), nrs. 4 and 5, with reference, insofar it concerns the open system, to HR 19 April 2002, ECLI:NL:HR:2002:AE1683, *NJ* 2002/456, *Zürich/Lebosch*.

[38] The Dutch law articles dealing with transfer of the rights embodied in a documentary intangible (articles 3:93 and 3:90 DCC) only presuppose that paper is used for a documentary intangible. Signing that documentary intangible it is not a requirement for transfer of the rights embodied therein, see F.G. SCHELTEMA, *Mr. M. Polak's Handboek voor het Nederlandse Handels- en faillissementsrecht, Derde deel, Wissel- en Chequerecht, by, reworked by W.R. Meijer* (Samson H.D. Tjeenk Willink: Alphen aan den Rijn 1993), p. 25 as well as R. ZWITSER, *Order- en toonderpapieren*, nr. 1, who both refer to the fact that a gift certificate for books is a bearer instrument and is also not signed. See also G. VAN EMPEL & J.B. HUIZINK, *Betaling, waardepapier en documentair krediet*, Deventer: Kluwer 2002, nr. 24, who acknowledge that Dutch statute nowhere requires a signature for putting rights to bearer, but that bearer instruments are usually signed. By contrast: A. VAN OVEN, *Handelsrecht*, Zwolle: W.E.J. Tjeenk Willink 1981, p. 206, who argues that a documentary intangible needs to be a deed and therefore needs to be signed.

[39] MCKENDRICK, *Goode on Commercial Law*, para 2.58. See also J.S. ROGER, *The Early History of the Laws of Bills and Notes* (Cambridge University Press: Cambridge 1995), who argues that English judges composed commercial law regarding bills by incorporating commercial practice.

4.2 *Objection 1: a documentary intangible is made of paper*

27. A documentary intangible presumes that paper is used. How is this requirement met in the proposed negotiable value bearer qualification? In general, after all, it is believed that documentary intangibles cannot exist electronically because transfer requirements with respect to documentary intangibles presume that there is paper, the possession of which is provided to the transferee. Art. 9, paragraph 1 of the EU E-Commerce Directive 2000/31, however, states that 'Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.'[40]

Many countries outside of the EU recognize similar principles. Section 7 of the US Uniform Electronic Transactions Act (UETA) states: '(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form. (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. (c) If a law requires a record to be in writing, an electronic record satisfies the law. (d) If a law requires a signature, an electronic signature satisfies the law.'[41] Sections 8 and 15C of the Australian Electronic Transactions Act 1999 (ETA) state: 'For the purposes of a law of the Commonwealth, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.' respectively 'A contract formed by: (a) the interaction of an automated message system and a natural person; or (b) the interaction of automated message systems; is not invalid, void or unenforceable on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.'[42] Last but not least, article 8, paragraph 1 of the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts states: 'A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.', whilst article 9, paragraphs 2 reads: 'Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.'[43]

28. Depending on the reader's legal system, the requirements which need to be abided by in order to equate an electronic contract with a written one may differ. However, a number of elements will often surface by way of common denominator: accessibility, determination of time of conclusion, integrity of the document and sometimes authentication of the parties.[44]

---

[40] Dir. 2000/31 of 8 June 2000 concerning electronic commerce.

[41] https://www.uniformlaws.org/viewdocument/final-act-with-comments-29?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments. For an analysis of the legal enforceability of smart contracts under the UETA and the E-Sign Act, see the Cardozo Blockchain Project, ''Smart contracts' & legal enforceability'. Research Project #2', 16 October 2018, https://cardozo.yu.edu/sites/default/files/Smart%20Contracts%20Paper%20-%20Final_0.pdf.

[42] https://www.legislation.gov.au/Details/C2011C00445.

[43] United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005), available at http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2005Convention.html.

[44] See for Dutch law: art. 6:227a, paragraph 1 DCC implementing art. 9, paragraph 1 Dir. 2000/31 of 8 June 2000 concerning electronic commerce. See for an answer to the similar question whether smart contracts on the blockchain can autonomously enter into legally enforceable contracts pursuant to English, US and French law M. GIANCASPRO, 'Is a 'smart contract' really a smart idea? Insights from a legal perspective', *Computer Law & Security Review*, 2017, Volume 33, Issue 6, p. 830-831, https://doi.org/10.1016/j.clsr.2017.05.007.

These elements are present in the value bearer system proposed, as will be demonstrated below.

29. The contract is accessible in that the contents of a bitcoin transaction and the rights and obligations pertaining thereto can be consulted by the parties. In the same way as someone can read a paper documentary intangible to determine the contents of the rights and obligations arising therefrom, so everyone (thereby including any contracting party) can consult the blockchain and determine how many bitcoins are on a specific bitcoin address.[45] The other, aforementioned rights and obligations of the users, miners and nodes - say the general terms and conditions – follow from the technology used, in particular the operation of the bitcoin software in the bitcoin network. As mentioned above, this software and the related documentation is open-source and available to everyone, and the rights and obligations of the parties are derived from them. Indeed, the rights and obligations of each participant are recorded much more precisely than in case of a paper documentary intangible. After all, the content of the rights and obligations in a paper documentary intangible is contained in text about the interpretation of which disputes can arise. The content of the rights and obligations with respect to bitcoins, on the other hand, is determined by code, the manner of execution of which can be determined in advance. As mentioned, in the blockchain code is (almost always) law.

30. The moment of conclusion of the contract can be determined with sufficient certainty. The moment in time a bitcoin is credited on a bitcoin address is, in fact, very precisely registered on the blockchain. With paper, the moment of creation is often much more uncertain.

31. The integrity of the contract is also sufficiently guaranteed. This element is often included in statute because paper protects parties from unnoticed manipulation of the data recorded thereon, whilst electronic files can more easily be manipulated unnoticed (at least if not protected against such manipulation). The bitcoin blockchain is, however, designed in such a way that once transactions are recorded in a block on the blockchain, they cannot be changed. The authenticity of the transactions included therein is therefore guaranteed. In fact, using modern scanning, photoshop and printing technology, manufacturing a manipulated copy of a piece of paper and subsequently destroying the original is much simpler than manipulating and destroying a transaction stored in the blockchain.

32. The final element present in some legal systems is that the identity of the parties can be recorded with sufficient certainty. This is a difficult element to be found in the bitcoin system because that system does not register the identity of parties. However, if statute at first sight seems to require this element to be present, closer inspection reveals that it may be negated. Dutch parliamentary history, for instance, allows a judge to equate an electronic document with a written one even if this element is not present.[46] This should not be a problem given that the bitcoin network satisfies the previous three requirements in a much better manner than a paper equivalent, the parties from the outset knowingly take part in a system that focuses on anonymity and therefore have no need to know each other's identity. Also, a written bearer instrument is not denied legal effect because it does not attach importance to the identity of the creditor, but only to his possession of the instrument. An electronic value bearer should not be denied legal effect for the same reason.

[45] For example by means of https://www.blockchain.com/explorer.
[46] Kamerstukken II 2001/02, 28197, 3, p. 53 (MvA).

4.3 *Objection 2: An electronic documentary intangible cannot be given and taken*

33. It becomes more difficult when looking at the act required to transfer the rights embodied in the documentary intangible. That act of transfer assumes, as explained, that the documentary intangible is given by the transferor to the transferee and nothing remains with the transferor. In my opinion, the giving and taking of the value bearer that embodies the bitcoin rights and that is needed for transfer works as follows. The giving and taking of the paper wallet is the easiest to imagine. That wallet consists of paper and so there is, for the purposes of giving and taking, no difference with other, more traditional paper documentary intangibles. In case of the hardware wallet, the value bearer can also easily be given and taken in such a way that the transferor retains nothing: in case of a USB key like device (a dedicated device), nothing remains at the transferor after he has given that device to the transferee.

34. However, if something different is also stored on the device, such as on a smartphone or a computer (a non-dedicated device), it will rarely be the case that the entire device is given to the transferee. In that case, the private key can, for example, be copied and e-mailed to the transferee. Once the transferor's private key is e-mailed to the transferee, the value bearer dematerializes. At the moment that the transferee stores the private key in his wallet on another value bearer, the value bearer materializes again. Of course, the private key in that case remains behind with the transferor, and strictly speaking, there is no longer a classic give and take as is the case when a paper documentary intangible is given and taken. The miners and nodes could not care less: they only look at whether the right private *key* is used to sign a transaction, not whether the *person* signing is the rightful holder of that key or not. By accepting an e-mail transfer of a private key, the transferee therefore risks that the transferor keeps a copy of that key and uses it to funnel away bitcoins from that bitcoin address to another bitcoin address before the transferee transfers those bitcoins to another bitcoin address. But is that really a problem? In order to answer that question, let me compare the electronic situation with a paper situation in which the transferee has a similar degree of uncertainty.

35. Take the situation that one bearer paper has been issued. In that case, the transferor can also have copied his bearer paper before he gives the original to the transferee. Because modern copying techniques are so good, the debtor to whom the rogue transferee presents the copied documentary intangible will not notice the difference between the original and copy and perform the obligations set out therein. Of course, that is not how the documentary intangible is supposed to function, but it also not what is supposed to happen if one person gives his private key to another person and retains a copy of his private key. It reminds me of the *Oracle/UsedSoft* case, in which the ECJ ruled that the first acquirer of a software license upon resale of it 'must, in order to avoid infringing the exclusive right of reproduction of a computer program which belongs to its author, … make his own copy unusable at the time of its resale.'[47] Although this is a different situation, the essence remains the same: if (the rights to) files are resold with the intention that the transferee should have exclusive access to them, the transferor is, of course, obliged to delete his copies of those files. It could, in other words, be argued that there is little difference between, on the one hand, the prohibition on making a copy *before* the transfer of a paper documentary intangible and, on the other hand, the obligation to delete copies of a private key stored on a non-dedicated device *after* the

[47] ECJ 3 July 2012, C-128/11, ECLI:EU:C:2012:407, *Oracle/UsedSoft*, point 70.

transfer. Because there is (too) little difference between those two situations, there is insufficient reason to let the documentary intangible character of bitcoin value bearers go up in flames and conclude that no legal transfer has taken place because the private key has moved from one wallet to another.

36. Those who consider such dematerializing and then materializing of the value bearer to be a bridge too far - and I do not find it hard to fathom - can hopefully be convinced by another argument that the transferee's value carrier is also a documentary intangible if the private key is moved without giving and taking the value bearer itself. That argument consists of the following building blocks. It is mercantile practice that certain documentary intangibles can be issued by means of several copies of paper.[48] In such a situation, a holder of such a documentary intangible put to bearer is also not certain that another holder will not present his copy earlier, and by doing so exercise his rights earlier and in effect render any other copies worthless. In a similar way, it can be argued that it has been implicitly agreed upon in the bitcoin multi-party contract that the transferee of a bitcoin right not only receives a documentary intangible put to bearer in the form of his value bearer, but also (at the same time) a power of attorney to issue multiple documentary intangibles put to bearer. At the moment that he then e-mails his private key to a subsequent transferee, and the latter stores that key in his wallet without obtaining the non-dedicated device from the transferor, this must be seen as the giving and taking of a new *copy* of the value bearer through the use of that power of attorney. That value bearer comes into existence at the moment in time the transferee stores the private key in his wallet on a value bearer. This way, an existing value bearer does not have to be dematerialized and then be materialized in another value carrier, and the transferee is aware from the outset of the risk that the transferor also has a copy of the private key with which he can also transfer the bitcoins linked to that bitcoin address, and perhaps even earlier than the transferee.

37. The above two lines of reasoning are even more persuasive if we realize that the transferee does not have to take the risk that the transferor outsmarts him. If he wants to make sure that the transferor does not hold back a copy of the private key with which he can outsmart him, he can agree with the transferor that he transfers the agreed quantity of bitcoins to a bitcoin address of the transferee. If the transaction is structured in that way, the transferee can be sure that the transferor can no longer transfer the bitcoins so transferred once that transaction is added to the blockchain in a block. By accepting the private key to the transferor's bitcoin address rather than having the bitcoins transferred to his bitcoin address, the transferee deliberately takes the risk that the transferor will outsmart him. Given this form of risk acceptance in the presence of a better alternative, it is less objectionable to maintain the legal status of a documentary intangible if the provision of the private key is not accompanied by the provision of the non-dedicated device. The opposite view, the deprivation of the rights attached to documentary intangibles and the conclusion that no legal transfer has taken place, would mainly (or even: only) benefit the transferor, whilst both parties desired a legitimate, albeit risky, delivery.

4.4 ***Effects***

38. What are the benefits from a property law perspective of this exercise of equating the value bearer (in which the bitcoin rights are embodied) with a paper documentary

[48] Dutch law, for instance, provides for the issuance of several copies of paper documentary intangibles in art. 163 and 226 Dutch Code of Commerce and art. 8:413 DCC. See also ZWITSER, *Order- en toonderpapieren*, nr. 16, who notes that, in practice, this usually occurs with bills of exchange and bills of lading.

intangible? The benefit is a legal qualification that is in line with the technical reality. The benefit is also relatively clean legal simplicity, which I can only show briefly because of the length of this contribution. Not only can these rights be easily transferred by providing the value bearer,[49] a pledge can oftentimes also easily be created by placing that value holder in the power of the pledgee.[50] No deed, signature, notary public or tax office is required for all of this. The attachment and execution are also relatively simple. The attachment of the rights embodied in the documentary intangible is usually effectuated simply by seizing the value bearer.[51]

5. Conclusion

39. I come to a conclusion. From a contract law perspective, the bitcoin network qualifies as a multi-party contract to which the various participants (users, miners and nodes) accede by participating in the network for the first time. They thereby accept, each in their own capacity, the third-party rights clause stipulated in that agreement in their favour. On the basis of that contract, each user who transfers a bitcoin actually exercises his rights vis-à-vis the miners to validate that transaction and vis-à-vis the nodes to verify the work of the winning miner. After that, the transaction (if confirmed) is added to the blockchain in a block. The bitcoin rights can only be effectuated by signing the transaction with the private key associated with the bitcoin address from which the bitcoins will be transferred.

40. For the purposes of executing the multi-party contract containing such arrangements, the bitcoins rights with respect to the bitcoins credited to a bitcoin address are put to bearer at the same moment these bitcoins are so credited. They are put to the bearer of the holder of the value bearer on which the private key associated with that bitcoin address is stored. That value bearer thereby embodies those bitcoin rights. Those bitcoin rights can be transferred, pledged, attached and executed by possession of the value bearer. The one who possesses the value beater can effectuate the bitcoin rights embodied therein by using the private key stored therein and thereby transfer the associated bitcoins to another bitcoin address.

41. Should the intended transferee of bitcoins want to prevent the transferor from holding back a copy of the private key and thus transfer those bitcoins earlier than the intended transferee can transfer them, he can agree with the transferor that the transferor does not provide the value holder to him, but instead transfers the bitcoins to a bitcoin address of

[49] See, for Dutch law: art. 3:93 DCC. See with respect to securities law and dematerialization with discussions regarding Belgian, French, Dutch and US law and global and European harmonization M. HAENTJES, *Harmonisation of Securities Law. Custody and Transfer of Securities in European Private Law. Private Law in European Context Series volume 11* (Kluwer Law International: Alphen aan den Rijn 2007); as well as art. 3 and 4 UCC; and J.S. ROGERS, *The end of Negotiable Instruments. Bringing Payment Systems Law Out of the Past* (Oxford University Press: New York 2012) who argues that art. 3 should be repealed, that art. 4 should undergo major revision and that a new statute regarding promissory notes and checks should view these instruments as assignable contracts rather than negotiable instruments.

[50] See for Dutch law: art. 3:236, paragraph 1 DCC.

[51] See for Dutch law: art. 474a, paragraph 1 Dutch Code of Civil Procedure (DCCP) for executory attachment and art. 702, paragraph 1 DCCP for prejudgment attachment which determine that the provisions with respect to the seizure of goods are in that case 'applicable mutatis mutandis, unless it follows otherwise from the relevant provision in light of the nature of the right'; and T.J. DE GRAAF & H.B. KRANS, 'Verhaal op bitcoins door gedwongen medewerking van de schuldenaar', *WPNR* 7217 1 December 2018, p. 940-945 for an overview of how a creditor can force his debtor (who has been ordered by a court to pay a sum of money) to provide his private key so that the creditor can execute the bitcoins of his debtor.

the transferee. After all, the transferor cannot transfer the bitcoins on the transferee's bitcoin address because the transferor does not possess the associated private key. The fact that the value bearer is usually not made of paper does not pose a problem. That private keys stored on some value bearer are provided without at the same time providing the value bearer itself, is also not a problem.