Singapore Journal of Legal Studies
[2020] 526–563

# THE FAILED HOPES OF DISINTERMEDIATION: CRYPTO-CUSTODIAN INSOLVENCY, LEGAL RISKS AND HOW TO AVOID THEM

MATTHIAS **HAENTJENS*** TYCHO **DE GRAAF**** and ILYA **KOKORIN*****

This article explores the legal risks involved in depositing cryptocurrency with crypto-custodians such as crypto-exchanges. These risks materialise most acutely in case these crypto-custodians fall insolvent, which has happened over the last decade in several instances. Recent years have witnessed the demise of crypto-exchanges such as Cryptopia (New Zealand), QuadrigaCX (Canada), BitGrail (Italy) and a host of other crypto-exchanges around the world. These cases reveal that the qualification of the contractual and property law rights of crypto-investors is problematic. This is why this article discusses which rights crypto-investors can and should be able to assert in case a crypto-custodian falls insolvent. To answer this question, the (legal) qualification of bitcoin is analysed (can it be owned and if so, how can such ownership be created and transferred?) and the status of deposited bitcoins is discussed (do stored crypto-assets form a part of the crypto-custodian's insolvency estate or can they be revendicated by customers?). Private international law aspects form the starting point of the legal analysis (which court has jurisdiction to open insolvency proceedings and hear crypto-investors' claims, and what law applies to such claims?) and the analysis is based on the current terms and conditions of major crypto-custodians.

## I. INTRODUCTION

The market for crypto-assets is highly unstable. The price of bitcoin, for instance, reached USD19,800 in December 2017, fell to USD3,200 in December 2018, rose to USD12,500 in July 2019 and dropped to USD6,500 in December 2019.[1] Nevertheless, the holdings of crypto-assets remain substantial and in the words of the

* This paper was written in the context of the Oxford project on Digital Assets, led by Professors Louise Gullifer (now at Cambridge) and Jennifer Payne, and co-run by Guy Morton. The authors presented their initial findings at a Digital Assets conference held at Harris Manchester College on 26 June 2019. The present paper benefitted greatly from the comments there received, and was subsequently revised for a conference organised by the Centre for Banking & Finance Law at the National University of Singapore, entitled "The Future of Banking and Finance in the Digital Era". Unfortunately, that conference did not take place in March 2020 as scheduled, due to measures related to Covid-19. The authors also thank Professor Joost Visser of the Leiden Institute of Advanced Computer Science (LIACS) for his comments on an earlier version of this paper.

* Professor of Law, Leiden University (The Netherlands).
** Associate Professor of Civil Law, Leiden University (The Netherlands).
*** PhD candidate, Department of Financial Law, Leiden University (The Netherlands).

1 According to Coindesk, see online: Coindesk <https://www.coindesk.com/price/bitcoin>.

Executive Vice-President of the European Commission, Valdis Dombrovskis, cryptocurrencies "are here to stay".[2] The proliferation of various types of crypto-assets may create risks for crypto-investors. The first group of risks, technology-driven risks, relates to the nature of crypto-assets as assets arising from distributed ledger technology (blockchain) and cryptography. The second group is economic and stems from the (price) volatility of crypto-assets. The third group follows from the legal uncertainty regarding the status of crypto-assets and the rights of crypto-investors (legal risks).[3] This paper addresses the third group of risks, *viz* legal risks. In this category, the risks that may materialise in the insolvency of crypto-custodians belong to the most acute ones.

As to terminology, in this paper, we understand crypto-investors to be persons having acquired crypto-assets for the purchase of other crypto-assets, services/products in the real world or as a storage of value (investment). Sometimes we refer to crypto-investors as customers to highlight their relationship with crypto-custodians, whose services they use.

Crypto-assets, and cryptocurrencies such as bitcoin, in particular, are currently mainly deposited (stored or held in custody) with intermediaries. Two types of intermediaries can be distinguished: cryptocurrency exchanges (crypto-exchanges) and specialised entities providing storage services. Cryptocurrency exchanges allow for the exchange of fiat currency for cryptocurrency (and vice versa) and the exchange of one cryptocurrency for another. Specialised storage providers offer services of safekeeping customers' cryptocurrencies or their private cryptographic keys without offering an exchange function. In this article we refer to both types of intermediaries as crypto-custodians, since crypto-exchanges usually also engage in safekeeping customers' crypto-assets, regardless of whether this is their main function. Nonetheless, crypto-exchanges store enormous amounts of customers' crypto-assets and this is why our primary focus is on crypto-exchanges acting as crypto-custodians.[4]

As most crypto-assets are currently held through intermediaries, crypto-investors may risk losing substantial amounts if these intermediaries become insolvent. This so-called intermediary risk has materialised over the last decade in several instances. Recent years have witnessed the demise of crypto-exchanges such as Cryptopia (New Zealand), QuadrigaCX (Canada), BitGrail (Italy), Cointed GmbH (Austria) and a host of other crypto-exchanges around the world. These cases reveal that the qualification of the contractual and property law rights of crypto-investors is problematic. This is why this article explores *which rights crypto-investors can and should be able to assert in case a crypto-custodian falls insolvent*. To answer this question, the (legal) qualification of bitcoin is analysed (can it be owned and if so,

---

2 Wolfie Zhao, " 'Crypto assets are here to stay,' says EU Commission Vice President" *Coindesk* (10 September 2018), online: Coindesk <https://www.coindesk.com/crypto-assets-are-here-to-stay-says-eu-commission-vice-president>.

3 European Banking Authority, *Report with advice for the European Commission on crypto-assets* (9 January 2019), online: European Banking Authority <https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1> [EBA Report].

4 J Cant, "Nearly $10 Billion in BTC Is Held in Wallets of 8 Crypto Exchanges" *Cointelegraph* (8 October 2019), online: Cointelegraph <https://cointelegraph.com/news/nearly-10-billion-in-btc-is-held-in-wallets-of-8-crypto-exchanges>.

how can such ownership be created and transferred?) and the status of deposited bitcoins is discussed (do stored crypto-assets form a part of the crypto-custodian's insolvency estate or can they be revendicated by customers?). Private international law aspects are also paid attention to (which court has jurisdiction to open insolvency proceedings and hear crypto-investors' claims, and what law applies to such claims?).

The scope of this article is limited in several ways. First, our analysis primarily concentrates on Bitcoin, as one of the oldest and most prevalent cryptocurrencies.[5] Nevertheless, most of our conclusions and recommendations may be extrapolated to other cryptocurrencies, taking into account their specificities such as the mechanics of cryptocurrency transfer. Second, we focus on European Union ("EU") law and Dutch law as an example of a civil law jurisdiction, but we will also occasionally refer to other jurisdictions such as Japan, Russia, England and the United States of America ("USA"). Third, in order to legally categorise current practices of bitcoins custody, we rely on the provisions of relevant terms and conditions/user agreements available on the websites of some of the most popular crypto-custodians. As a result, we offer a typology of custody arrangements, which, however, does not claim to be complete. Fourth, we take a private law perspective, as we believe that the legal risks that may materialise in the context of crypto-investments are most acute there. At the same time, this perspective does not limit our recommendations where we believe that public or administrative solutions may be more appropriate to protect the rights of crypto-investors than private law.

The article starts with a short introduction to cryptocurrencies and their underlying technology (Section II). In Section III, we discuss some of the reasons why customers may choose to store their cryptocurrency with crypto-custodians. On the basis of the analysis of current terms and conditions of some major crypto-custodians, including Coinbase,[6] Gemini,[7] OKEx,[8] Wirex,[9] and Xapo,[10] Section II provides a typology of crypto-custodians and the different ways in which they hold and manage crypto-assets through segregated and omnibus blockchain addresses. This is followed by an overview of problems arising from the insolvency of crypto-custodians, based on two case studies: the insolvencies of MtGox and BitGrail (Section IV). Section V explores some pertinent private international law aspects related to crypto-investments and insolvency of crypto-custodians. This is followed by considerations of the legal qualification of bitcoins from a property law perspective (Section VI), which is then used to determine the rights a crypto-investor may assert if a crypto-custodian goes insolvent (Section VII). Section VIII suggests several legislative recommendations to improve legal certainty and enhance the protection of crypto-investors' rights.

---

5 The share of Bitcoin in the cryptocurrency market is approximately 70%. See O Godbole, "Bitcoin's Total Share of Crypto Market Now Highest since March 2017" *Coindesk* (3 September 2019), online: Coindesk <https://www.coindesk.com/bitcoin-price-bounces-to-10-5k-as-dominance-rate-passes-70>. For more information on market capitalisation of leading crypto-assets, see CoinMarketCap, online: <https://coinmarketcap.com/>.

6 Coinbase, online: <https://www.coinbase.com/>.

7 Gemini, online: <https://gemini.com/>.

8 OKEx, online: <https://www.okex.com/en>.

9 Wirex, online: <https://wirexapp.com/en>.

10 Xapo, online: <https://xapo.com/en>.

## II. Crypto-Assets: Major Features

### A. *Characteristics and Functioning of Blockchain*

Prior to any legal analysis of bitcoin, its nature must be explained with the reference to its technological foundation, *ie* the technology of blockchain. According to De Filippi and Wright, blockchain is a "highly resilient and tamper-resistant database where people can store data in a transparent and non-repudiable manner and engage in a variety of economic transactions pseudonymously".[11] The (perceived) resilience of blockchain comes from three technological features, namely peer-to-peer networks, public-private key cryptography and consensus mechanisms. All these features were invented and used long before the appearance and popularity of blockchain.[12] It was the combination of these technologies that caused a sudden increase of interest in distributed ledger technology (DLT).

Blockchain is essentially a database of transactions, *ie* a ledger, saved (recorded) in a distributed manner. The distributed manner means that the ledger is not centrally controlled and stored by a trusted intermediary such as a bank. Instead it is distributed through a peer-to-peer network of computers (nodes),[13] multiplied across the network, openly accessible and freely verifiable by anyone with internet access. It was the control by (and occasional failure of) banks and high transaction costs arising from their involvement, as well as the general distrust of central governments[14] that created the environment in which blockchain and Bitcoin originated.[15]

While the exclusion of trusted intermediaries that use centralised ledgers may help decrease transaction costs, it leads to several problems. One such problem is double-spending, *ie* the problem that the same digital asset may be spent twice under two different transactions. This is particularly imaginable in case of cryptocurrencies, as transactions on the blockchain involve non-physical assets that are not registered in a centralised ledger. Therefore, such assets can be easily multiplied and transferred to various recipients, whilst there is no central authority to control or prevent this from happening. Blockchain solves this problem by means of an approval mechanism for new transactions relying on public-private key cryptography and an algorithm-based consensus mechanism.

Imagine Alice, who wants to transfer a number of bitcoins to Bob. First, both Alice and Bob need to have bitcoin addresses on the blockchain. These are created

---

[11] P De Filippi & A Wright, *Blockchain and the Law: The Rule of Code* (US: Harvard University Press, 2018) at 2.

[12] Coindesk, "What is Blockchain Technology?" *Coindesk* (March 2017), online: Coindesk <https://www.coindesk.com/information/what-is-blockchain-technology>.

[13] Nodes store, spread and preserve the blockchain data. Full nodes store the whole history of blockchain transactions and are involved in the work of recording (putting in blocks) new transactions. For more see Bitcoin Wiki, *Full node*, online: Bitcoin Wiki <https://en.bitcoin.it/wiki/Full_node>.

[14] Before the invention of Bitcoin, the movement of Cypherpunks (a derivation of "cipher" and "cyber-punk"), was developed. Cypherpunks shared a distrust of central governments and their encroachment on personal privacy. See E Hughes, "A Cypherpunk's Manifesto" *Bitcoin News* (2 May 2020), online: Bitcoin News <https://news.bitcoin.com/eric-hughes-a-cypherpunks-manifesto/>, stating that "privacy in an open society requires anonymous transaction systems".

[15] S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", online: Bitcoin <https://bitcoin.org/bitcoin.pdf> [Nakamoto].

by means of a private key from which a public key is derived by way of an algorithm. The addresses are used for sending and receiving bitcoins and are usually shown as the shorter version of a public key.[16] Alice initiates a transaction by specifying how many bitcoins she wishes to transfer from her address to Bob's address and signing that transaction with her private key. This transaction (along with other transactions in a so-called block) needs to be validated in order to prevent double-spending. This validation process is called "mining" and requires computational power and energy and therefore needs to be incentivised. In the case of bitcoins, this is done by means of transaction fees (paid by the sender) and newly created bitcoins awarded to the winning miners (*ie* a block reward, which is automatically created by the blockchain system like printing extra money, until a pre-set maximum is reached).[17] Once more than 50% of the nodes, measured in computational power, verify and confirm that the winning miner has performed his work correctly, the transactions in that block are added to the record of all previous transactions (to ensure that everyone uses the same ledger) and the winning miners get paid. Once added, the transactions in that block are very difficult to erase or alter. This is why blockchain is considered resilient and tamper resistant.[18]

The registration of transactions on blockchain is publicly visible. As a matter of principle, anyone can check how many bitcoins were transferred from one address to another. For this purpose, a variety of blockchain explorers, *ie* interfaces allowing for the exploration of blockchain information, have been created.[19] Through the use of these interfaces, one can check the progress of a transaction (*eg* number of confirmations received), the "balance" of a particular address, the incoming and outgoing transactions (inputs and outputs) and the transaction history of the addresses involved. The identities of the sender and the recipient are, however, not revealed in the database—only the address can be known. Nevertheless, true anonymity requires "unlinkability" —the impossibility of linking an address to a particular person. This is not necessarily the case in blockchain,[20] where various ways exist to discover the identity of address holders, particularly when the same address is used multiple times.[21] In addition, the identity of a crypto-investor is usually

---

16 European Securities and Markets Authority ("ESMA"), *Advice: Initial Coin Offerings and Crypto-Assets*, at para 22, online: ESMA <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> [ESMA Advice].

17 The process of adding transaction records to the blockchain is called "mining" and parties involved in this process are referred to as "miners". For more see Bitcoin Wiki, *Mining*, online: Bitcoin Wiki <https://en.bitcoin.it/wiki/Mining>.

18 This comes from the fact that the change of information on blockchain requires the agreement of the majority of nodes, measured in computational power, to agree on such a change. Besides, this would require the change of all subsequently made blocks, which is theoretically possible, but rather unlikely. See Nakamoto, *supra* note 15.

19 Among the most well-known blockchain explorers are Blockchain.info, online: <https://www.blockchain.com/explorer>, BlockCypher, online: <https://live.blockcypher.com/> and BTC.com, online: <https://btc.com/>.

20 Bitcoin is in fact pseudonymous, as its transactions are vulnerable to being traced and linked to particular individuals using Bitcoin accounts. See S Chandler, "Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It" *Cointelegraph* (7 October 2018), online: Cointelegraph <https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it>.

21 See Bitcoin Wiki, *Address reuse*, online Bitcoin Wiki <https://en.bitcoin.it/wiki/Address_reuse>.

revealed to crypto-custodians, whenever such crypto-investor opens an account with them.[22]

### B. *Transfer of Bitcoins: Coin Analogy*

Some sources compare a Bitcoin address to a bank account.[23] Although easy to understand, this analogy is misleading in several respects. First, unlike money on a bank account, bitcoins (bitcoin transactions, to be precise) do not commingle.[24] Thus, even if there are several transfers of bitcoins made to the same bitcoin address, it is possible to trace each individual transaction on the blockchain. We will return to this unique feature below. Second, bitcoins resemble physical coins (rather than money in a bank account) in the way they are spent. We will now shortly analyse these features of bitcoin in more detail, as they may play a crucial role in qualifying and determining the rights of crypto-investors in case of insolvency of a crypto-custodian.

A bitcoin wallet is used to store public and private keys and interact with the blockchain and is usually represented by an app on a smartphone containing key pairs (public and private keys) for all bitcoin addresses linked to that wallet. Each bitcoin address, as noted above, is a possible destination of bitcoins.[25] There are usually several addresses linked to the same wallet. Let's assume that Alice has only one, newly created bitcoin address linked to her wallet and that no transaction fees are due for transferring bitcoins. Alice receives, as a result of two separate transactions to her bitcoin address, 0.5 bitcoin and 0.3 bitcoin. Her wallet now contains one 0.5-bitcoin-coin and one 0.3-bitcoin-coin, just like a physical wallet holds coins (*eg* a 1 euro coin and a 2 euro coin). In other words, no single coin of 0.8-coin is created, even though the aggregate amount may be shown as such.

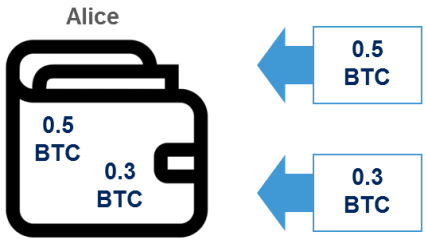


**Fig. 1.** Bitcoin Address and Transaction Record.

---

22 For more on identity verification procedures of major crypto-exchanges, see "Top 5 Crypto Exchanges — Identity Verification Procedures" (29 March 2018), online: Cointelegraph <https://www.trulioo.com/blog/top-5-crypto-exchanges/>. Recent years have seen the introduction and proliferation of mandatory know-your-customer (KYC) and anti-money laundering (AML) requirements. See C Adeyanju, "What Crypto Exchanges Do to Comply With KYC, AML and CFT Regulations" *Cointelegraph* (17 May 2019), online: Cointelegraph <https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations>.

23 See Crypto Currency Simplified, *Address: What is a Bitcoin or Cryptocurrency address?*, online: Crypto Currency Simplified <https://cryptocurrencysimplified.com/dictionary/address/>.

24 See on this point also covered extensively below, Section VI.C.

25 See Bitcoin Wiki, *Address*, online: Bitcoin Wiki <https://en.bitcoin.it/wiki/Address>.

If Alice decides to transfer bitcoins to Bob, she needs to use the coins available in her wallet. So, if she wants to transfer 0.2 bitcoin to Bob, she cannot simply transfer 0.2 bitcoin and keep 0.6 bitcoin, as she would when transferring cash from one bank account to another. Instead, she needs to use the coins available in her wallet and pay Bob with either the 0.5-bitcoin-coin or 0.3-bitcoin-coin. The exact coin to be spent is randomly chosen by an algorithm.[26] Imagine the 0.5-bitcoin-coin is chosen, what happens with the remaining 0.3 bitcoin (0.5 bitcoin – 0.2 bitcoin)? This constitutes the change from the transaction. Somewhat counterintuitively, Bob does not give back 0.3 bitcoin in change to Alice, but Alice from the outset specifies another address in which the change should be placed so that the change comes out of her own pocket instead of Bob's. In essence, what happens is that Alice melts down the 0.5-bitcoin-coin and re-mints it into 0.3 and 0.2-bitcoin-coins, the latter of which she transfers to Bob and the former she puts in another address of hers, *ie* a so-called change address.

Although the coin analogy is very helpful in explaining how a bitcoin transfer works at a basic level, the terminology used in the bitcoin network is somewhat different and, upon closer inspection, more insightful. Instead of coins, the bitcoin system calls them inputs and outputs. When Alice transfers bitcoins to Bob, she actually takes a number of unspent transaction outputs ("UTXOs") of prior incoming transactions with a total combined value equal to or exceeding the value of bitcoins to be transferred to Bob. However, when Alice spends bitcoins, she must use the entire value of any unspent transaction outputs as input for her outgoing transaction with Bob. So, in the example above, Alice's bitcoin address lists two UTXOs of previous transactions: one output of 0.3 bitcoin and one output of 0.5 bitcoin. If Alice wishes to transfer 0.2 bitcoin to Bob, the input for that transaction will be the entire value of the unspent transaction output of 0.5 bitcoin to be transferred to Bob's bitcoin address (again assuming that the algorithm chooses the 0.5 and not the 0.3 UTXO for such transfer). The address to which the change of 0.3 bitcoin is transferred is the automatically created change address and can be either the same address from which Alice transfers the bitcoins to Bob or (more likely) a new one.

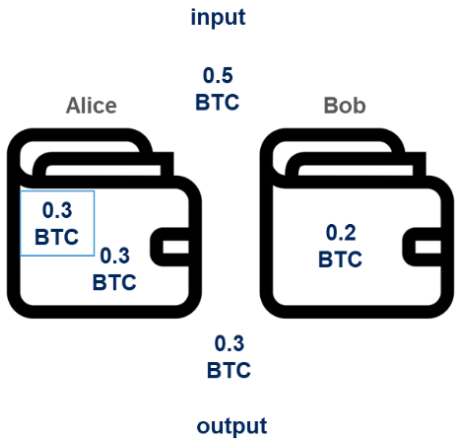


**Fig. 2.** Bitcoin UTXO, Outputs and Inputs.

[26] See Bitcoin Wiki, *Coin analogy*, online: Bitcoin Wiki <https://en.bitcoin.it/wiki/Coin_analogy>.

Transaction outputs can only be created and destroyed in their entirety, not changed. Why, one may wonder, was the bitcoin system not designed to allow for changing transaction outputs so that they are more akin to bank account transfers, in which case we need not worry about the extra complexity of spending entire coins/transactions outputs and subsequently having to deal with the change? For instance, Ethereum records balances directly in the ledger, which proves that an account and balance based blockchain system is possible.[27] There does not seem to be a clear answer to this question. Most answers start by explaining that in order to verify that bitcoins/transactions outputs have not been spent previously, *ie* to avoid a double spending problem, the bitcoin system only needs to check whether the transaction outputs (of previous transactions) used as inputs (for new transactions) exist and what their value is, but further explanation is not given.[28]

## III. Custody of Crypto-Assets in Practice

### A. *Reasons for Custody of Crypto-Assets*

Historically and conceptually, bitcoin was introduced as a tool to avoid control by intermediaries such as governments, banks and brokers. However, whenever a crypto-investor deposits his or her bitcoins or private keys with a third party, an intermediary or a crypto-custodian, this is precisely what happens. There are several reasons why customers may nonetheless decide to do so.

The first reason relates to the services offered by a crypto-exchange. To store, withdraw, exchange or trade cryptocurrencies at a crypto-exchange, the exchange usually requires that an account be opened with that exchange. By opening the account and sending bitcoins to an address associated with that account, one effectively gives up access and control over bitcoins deposited in that account because the associated addresses are held and controlled by the exchange rather than by the customer. On the other hand, this model makes the execution of transactions with cryptocurrencies[29] easier and quicker to perform.

The second reason comes from the need to protect private keys. If a private key is not backed up and is forgotten, stolen or lost, a crypto-investor irrevocably loses his

---

27 F Sun, "UTXO vs Account/Balance Model" *Medium* (15 April 2018), online: Medium <https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf>.

28 Bitcoin Stack Exchange Network, *Why does Bitcoin store all transaction inputs and outputs, instead of just an "account/balance" ledger?*, online: Bitcoin Stack Exchange Network <https://bitcoin.stackexchange.com/questions/29780/why-does-bitcoin-store-all-transaction-inputs-and-outputs-instead-of-just-an-a>.

29 Many crypto-exchanges allow the transfer of fiat currency to their accounts. For example, Coinbase provides the so called "e-money services". According to the Coinbase User Agreement 2019, funds (fiat currency) can be uploaded into the E-Money Wallet. When funds are loaded into the E-Money Wallet, E-Money is issued. The funds themselves are credited to accounts opened for Coinbase by a regulated financial institution. See Coinbase User Agreement 2019, at Section 4 ("Payment Services"), online: Coinbase <https://static-assets.coinbase.com/user_agreements/cb_uk_user_agreement_29_March_2019.pdf> [Coinbase User Agreement 2019].

ability to transfer the bitcoins linked to the associated address. By some estimates, around four million bitcoins have been lost forever this way.[30] Opening a wallet with a crypto-custodian relieves the stress of holding and protecting the keys as these tasks are outsourced to a crypto-custodian. Unlike the private key, a wallet with a crypto-custodian can usually be accessed even if the password to it is forgotten or lost. If the customer loses his credentials, a crypto-custodian undertakes to provide new credentials if it is able to authenticate the customer in a different manner, just as in the case of a password reset.[31]

Thus, through crypto-custody, a crypto-investor gives up his direct rights to the blockchain, but gains the comfort of being able to (indirectly) dispose of those rights even when he loses his private key. From the crypto-investor's perspective, the user agreement or crypto-custody contract with his crypto-custodian has therefore become the gateway to his rights relating to 'his' bitcoin. The situation may be graphically rendered as follows:

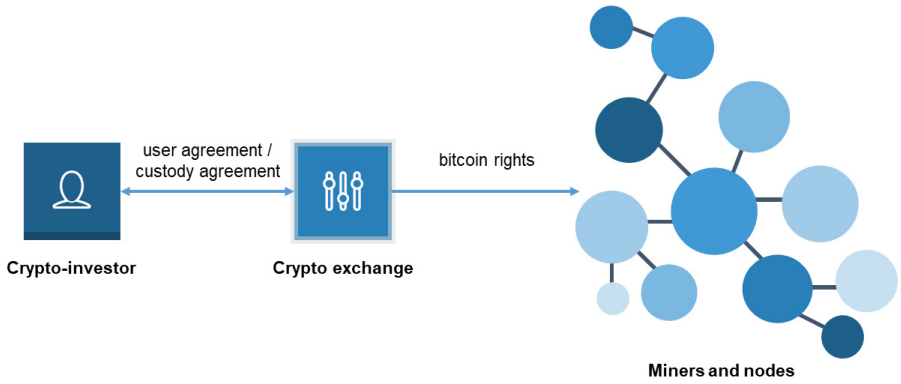


**Fig. 3.** Crypto-Custody.

Our analysis of crypto-custody below is based on the terms and conditions published on the websites of crypto-custodians, and mainly concentrates on the mechanics of storing bitcoins by crypto-exchanges. There appear to be vastly different approaches to the custody of deposited bitcoins. On the basis of our investigation, we have distinguished two main approaches, namely: (1) custody with a single omnibus blockchain address (*eg* Coinbase) and (2) custody with separate blockchain addresses (*eg* Gemini).

---

[30] J Roberts & N Rapp, "Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says" *Fortune* (25 November 2017), online: Fortune <http://fortune.com/2017/11/25/lost-bitcoins/>. There are famous stories of people losing their private keys. For instance, a British man unintentionally dumped a hard drive containing the private key to 7,500 bitcoins in mid-2013. Since then he has tried (unsuccessfully) to get access to a local landfill. Read further A Sulleyman, "Man who 'threw away' bitcoin haul now worth over $80M wants to dig up landfill site" *Independent* (4 December 2017), online: Independent <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html>.

[31] See *eg* Coinbase Help Center, *I can't remember my password*, online: Coinbase Help Center <https://support.coinbase.com/customer/en/portal/articles/1403849-i-can-t-remember-my-password>.

### B. *Coinbase and Storage in an Omnibus Address*

Coinbase is a cryptocurrency exchange headquartered in San Francisco, California.[32] It hosts cryptocurrency wallets enabling customers to store, track, transfer, and manage the balances of several cryptocurrencies, such as Bitcoin and Ethereum.[33] It also offers cryptocurrency exchange services, allowing for the exchange (purchase and sale) of various cryptocurrencies, *inter alia*, via funds deposited into so-called E-Wallets. Importantly, Coinbase stores cryptocurrencies' private keys that are needed to approve transactions on the blockchain. The Coinbase User Agreement of 2018 states: "We [Coinbase] securely store private keys in our control in a combination of online and offline storage."[34] In a separate clarification, Coinbase explained that it offered a hosted wallet, and did not "provide the keys to individual wallet addresses"[35] but instead managed the private keys for its clients.[36]

In March 2019, Coinbase amended its User Agreement. The previous version of the Coinbase User Agreement from 2018 did not contain rules concerning property rights over crypto-assets deposited with the exchange. This has changed in the new agreement. According to the new agreement, "[a]ll Digital Currencies held in your Digital Currency Wallet are custodial assets held by the Coinbase Group for your benefit. Title to Digital Currency shall at all times remain with you and shall not transfer to any company in the Coinbase Group."[37] It is evident that this provision was introduced specifically to address the possible ambiguity when it comes to the title over crypto-assets transferred to the exchange. Despite the fact that Coinbase holds private keys and is therefore practically in a position to dispose of stored cryptocurrencies, the above provision confirms that at least the intention of the parties is not to transfer title over bitcoins to Coinbase.

The User Agreement 2019 also stipulates that the Coinbase Group "may use shared blockchain addresses, controlled by a member of the Coinbase Group, to hold Digital Currencies held on behalf of customers and/or held on behalf of Coinbase UK."[38] It continues, "[a]lthough we maintain separate ledger accounting entries for customer and Coinbase Group accounts, no member of the Coinbase Group shall have any obligation to segregate by blockchain address Digital Currencies owned

---

[32] However, customers based outside the USA conclude the agreement with Coinbase UK, Ltd, a private limited company incorporated in England and Wales. See Coinbase User Agreement 2019, *supra* note 29.

[33] Coinbase User Agreement 2018, at para 1.3, online: Coinbase <https://static-assets.coinbase.com/user_agreements/cb_uk_user_agreement_14_March_2018.pdf> [Coinbase User Agreement 2018].

[34] *Ibid* at para 4.4.

[35] Coinbase Help Center, *Where can I find the private key for my wallet?*, online: Coinbase Help Center <https://support.coinbase.com/customer/portal/articles/1526452-where-can-i-find-the-private-keys-for-my-wallet->.

[36] Coinbase Help Center, *Is a wallet address safe to display publicly?*, online: Coinbase Help Center <https://support.coinbase.com/customer/en/portal/articles/2275614-is-a-wallet-address-safe-to-display-publicly>.

[37] Coinbase User Agreement 2019, *supra* note 29, at para 5.16.

[38] *Ibid* at para 5.16. This pooled storage of crypto-assets seems to be a common practice also among other cryptocurrency exchange and storage service providers. For example, Wirex Cryptoassets Terms clarify that "[w]hen you ask us to buy cryptoassets on your behalf through the Wirex Service, we will store the cryptoassets in pooled crypto wallets created and maintained by our third-party wallet custodian or by us." The Terms also highlight that Wirex may convert cryptoassets held in pooled accounts into fiat and other cryptoassets to ensure day-to-day liquidity (*ie* to pay other customers upon their request). See Wirex Cryptoassets Terms, online: Wirex <https://wirexapp.com/en/cryptoasset-terms> [Wirex Terms].

by you from Digital Currencies owned by other customers or by any member of the Coinbase Group." The fact that Coinbase stores all bitcoins in one (or several) omnibus addresses could create a problem of segregation and identification of crypto-assets deposited with the exchange by its customers.[39]

In the case of Coinbase, transaction settlement happens in the books of the exchange itself by ledger accounting entries, which are not necessarily recorded on the blockchain (off-chain settlement).

In sum, Coinbase has full control over the private keys to deposited bitcoins. It can effectively access crypto-wallets and their content. This may not only increase the risks of hacks or mismanagement,[40] but also lead to disputes about the ownership over crypto-assets deposited with Coinbase, since control over the private key (and therefore the possibility to dispose of bitcoins) may indicate that Coinbase is the owner of such bitcoins or that ownership has been transferred to it.[41] In the absence of proper segregation, allocation of cryptocurrencies to individual customers may become problematic. This risk is analysed in more detail in the following Sections of this article. It is remarkable that according to the User Agreement 2019, crypto-assets may be held on blockchain addresses controlled by any member of the Coinbase Group. Coinbase does not disclose to customers the identity of the specific legal entity (or legal entities) involved in the storage or control over the deposited bitcoins (i*e* private keys) stored with it (or them).[42] As a result, it might be impossible for a crypto-investor to determine which legal entity within the Coinbase Group is actually holding the deposited bitcoins (*ie* private keys) at any particular moment in time.

### C. *Gemini and Storage in a Segregated Address*

In the previous sub-Section, we introduced the Coinbase User Agreements. It is worth noting that these agreements are not specialised custody agreements. In fact,

---

[39] The fact that the pooling of crypto-assets may lead to individual customer's entitlements not being identifiable and a customer not being able to receive the full entitlement, is explicitly recognised in the Terms of Service of OKEx. As a result, in the event of insolvency, customers may have to share pro rata. See OKEx Terms of Service, online: OKEx <https://www.okex.com/support/hc/en-us/articles/360021813691-Terms-of-Service> [OKEx Terms].

[40] South Korean cryptocurrency exchange Coinbin has declared bankruptcy citing corporate executive moral hazard as one of the reasons for its bankruptcy. It explained that the executive of its subsidiary exchange Youbit allegedly lost paper wallets containing hundreds of cryptocurrency private keys. For more see Y Khatri, "South Korean Crypto Exchange Declares Bankruptcy Citing Embezzlement" *Coindesk* (25 February 2019), online: Coindesk <https://www.coindesk.com/south-korean-crypto-exchange-declares-bankruptcy-citing-embezzlement>. In yet another more recent case of QuadrigaCX, once the largest crypto-exchange in Canada, the death of a CEO forced the crypto-exchange to file for creditor protection under the Canadian Companies' Creditors Arrangement Act. The major reason for this was that the CEO of QuadrigaCX was the sole keeper of the keys to some of the company's wallets, which could not be easily accessed upon his death. For more on QuadrigaCX's insolvency see T Copeland, "QuadrigaCX report: $400,000 in assets found, bankruptcy recommended for troubled exchange" *Decrypt* (2 April 2019), online: Decrypt <https://decryptmedia.com/6273/quadriga-report-canada-crypto-exchange>.

[41] EBA Report, *supra* note 3 at 8, noting that "[t]he private keys are used to control the ownership of their respective Bitcoins."

[42] The same concern may be raised with regard to Wirex's Terms, *supra* note 38, which state that cryptocurrency is not held in Wirex's custody and that the custody remains with the relevant cryptocurrency custodian. The identities of cryptocurrency custodians used by Wirex are not disclosed in its Terms.

the word "custody" is used only twice in the User Agreement 2019, whilst the User Agreement 2018 did not mention custody at all. These references relate to the digital currency wallets necessary to trade cryptocurrencies on the exchange. In other words, custody is considered here as a by-product of crypto-trading. In contrast to Coinbase, other crypto-exchanges offer separate custody agreements. Gemini, for example, is a digital currency exchange founded in 2014 by the Winklevoss brothers that operates on the basis of a User Agreement[43] and a Custody Agreement.[44] These two documents apply simultaneously and by opening an account with Gemini, customers enter into these two separate agreements.

According to the Gemini User Agreement, each Gemini user account has the following sub-accounts: (1) one or more associated User accounts; (2) a fiat currency account that reflects its fiat currency balance; and (3) a Digital Asset account that reflects a digital asset balance. Each Digital Asset account is, in turn, subdivided into a depository account and a custody account. The relation between these two sub-accounts is not entirely clear and we will only deal with the latter, which is governed by the special Gemini Custody Agreement. Similar to Coinbase, Gemini clarifies that digital assets placed into custody on customers' behalf in the Digital Assets account "are not treated as general assets of Gemini."[45] A custody account is characterised by Gemini as a bailment relationship between the customer and the exchange. Thus, in principle, a customer does not express his will to transfer title over crypto-assets to the crypto-exchange by opening an account and depositing crypto-assets with it.[46]

Gemini guarantees that the custody account has one or more "associated unique blockchain addresses" and that crypto-assets "will be (i) segregated from any and all other assets held by [Gemini] and (ii) directly verifiable via the applicable blockchain."[47] Of particular interest in this context is the following provision:

> "The ownership of your Assets will be clearly recorded in our books as belonging to you. Our records will at all times provide for the separate identification of your Assets. We will not loan, hypothecate, pledge, or otherwise encumber any Assets in your Custody Account, absent General Instructions from you. You agree and understand that nothing herein prevents us from using our Cold Storage System to custody our own property and/or the property of third parties; provided, however, that, at a minimum, separate Blockchain Addresses are utilized to segregate your Assets from such other property."[48]

---

43 Gemini User Agreement, online: Gemini <https://gemini.com/legal/user-agreement#welcome> [Gemini User Agreement].

44 Gemini Custody Agreement, online: Gemini <https://gemini.com/custody-agreement/> [Gemini Custody Agreement].

45 Gemini User Agreement, *supra* note 43.

46 In the judgment of the Tokyo District Court in August 2015 in relation to the insolvency of MtGox, the court decided that there was no contract of deposit based on the presupposition of ownership of the deposited goods. As a result, the plaintiff could not exercise a right of segregation on the basis of ownership of bitcoins. This argument is given in addition to finding that bitcoins cannot be the object of ownership. See Issue 2, District Court, Tokyo, 5 August 2015, (2014 (Wa) 33320) (Japan), Reference number 25541521 (English translation commissioned by the Digital Assets Project Harris Manchester College, Oxford), online: <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf> [Tokyo District Court Judgment].

47 Gemini Custody Agreement, *supra* note 44.

48 *Ibid.*

This segregation contrasts with the Coinbase contract, which does not promise to segregate customers' crypto-assets with separate blockchain addresses, but instead allows shared blockchain addresses. The Gemini Custody Agreement guarantees segregation of customers' assets (at a minimum) by way of separate blockchain addresses. Due to the traceability and immutability of blockchain entries, proper asset segregation seems to be ensured.[49]

## IV. Crypto-Custodian Insolvencies: Case Observations

### A. *MtGox and Ownership of Bitcoin*

Recent cases involving the insolvency of crypto-custodians highlight the risks associated with the custody of crypto-assets. This Section will discuss two of these cases, namely MtGox (Japan) and BitGrail (Italy). The main purpose of our discussion is to describe how special technical features of bitcoin and the methods for its storage, as introduced above, have multiplied the risks for crypto-investors, who in both cases ultimately lost their (property) rights over deposited crypto-assets.

MtGox Co Ltd ("MtGox") was once the largest bitcoin trading exchange. Based in Japan, it handled around 70% of the world's bitcoin trades in 2013. It allowed its users to buy, sell, convert and keep their bitcoins and fiat currencies with the exchange. Following a massive hack, which led to the loss of around 850,000 Bitcoins worth USD473 million at that time, MtGox stopped all withdrawals and shut down its website in early February 2014. On 28 February 2014, MtGox filed for insolvency protection in Tokyo under a procedure called civil rehabilitation (*minji saisei*), claiming that rebuilding MtGox in a legally organised manner "will not be for the sole benefit of the company but for that of the whole bitcoin community."[50] The latter turned out to be problematic as the rehabilitation procedure soon grew into a full scale insolvency liquidation.[51] Mr Nobuaki Kobayashi, a Japanese attorney, was appointed as the bankruptcy trustee. On 22 June 2018, the District Court of Tokyo issued an order commencing civil rehabilitation proceedings against MtGox.[52] The previously ongoing insolvency liquidation proceedings were therefore stayed.[53]

---

[49] This type of asset segregation has also been recently proposed by the Swiss Federal Council, which advised that crypto-assets are individually attributed to the relevant third party (*ie* crypto-investor) in the distributed ledger, so that it is always clear which coins belong to which crypto-investor. Provided this is the case and the insolvent crypto-custodian has the power to dispose of the relevant crypto-assets (which most often is the case), a customer is given an explicit right to request segregation of its assets from the insolvency estate. See Eidgenössisches Finanzdepartement ("EFD"), "Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register: Erläuternder Bericht zur Vernehmlassungsvorlage" *Newsd* (22 March 2019) at 39, online: Newsd <https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf>.

[50] MtGox Co Ltd, *Announcement Regarding an Application for Commencement of a Procedure of Civil Rehabilitation* (28 February 2014), online: MtGox Co Ltd <https://www.mtgox.com/img/pdf/20140228-announcement_eng.pdf>.

[51] MtGox Co Ltd, *Announcement of Commencement of Bankruptcy Proceedings* (24 April 2014), online: MtGox Co Ltd <https://www.mtgox.com/img/pdf/20140424_announce_qa_en.pdf>.

[52] MtGox Co Ltd, *Announcement of Commencement of Civil Rehabilitation Proceedings* (22 June 2018), online: MtGox Co Ltd <https://www.mtgox.com/img/pdf/20180622_announcement_en.pdf>.

[53] For more on insolvency of MtGox, see I Kokorin, ""Hacked" insolvencies of crypto exchanges" *Leiden Law Blog* (5 July 2018), online: Leiden Law Blog <https://leidenlawblog.nl/articles/hacked-insolvencies-of-crypto-exchanges/>.

In the insolvency proceedings, the District Court of Tokyo was requested to decide on a claim filed by one of the customers of MtGox.[54] The customer requested the return of crypto-assets deposited with the exchange. The claim was based on Article 62 of the *Japanese Bankruptcy Act*.[55] The court held that its decision on this claim depended on whether bitcoin can be the object of ownership. Japanese law only recognises property interests in tangible things, unless specifically provided otherwise.[56] The plaintiff argued that the possibility of exclusive control over bitcoin (*ie* through a private key) was sufficient to make it a tangible thing, even if it was incorporeal. The court analysed the nature of bitcoin and concluded that as cryptocurrency it did not have the necessary corporeality. Moreover, and somewhat unexpectedly, the court reasoned that due to the involvement of other participants of the network (*ie* nodes) in the process of transferring bitcoins, the person who manages the private key of a bitcoin address does not have exclusive control over a remaining bitcoin balance on this address. As a result, the court found that bitcoin cannot be the object of ownership. This conclusion prevented any further consideration of the plaintiff's claims for asset segregation and revendication.

In the wake of MtGox's insolvency, Japan introduced amendments to its *Payment Services Act* specifically addressing the issue of cryptocurrencies. These amendments define cryptocurrency as "proprietary value" and introduce regulation for "virtual currency exchange service providers" that are involved in the purchase and sale of cryptocurrencies or cryptocurrency exchange.[57] On the basis of these recent legislative changes, which explicitly recognise property rights over cryptocurrency, the outcome of the MtGox case just discussed might have been different now.

### B. *BitGrail and Revendication Claims*

The issues of crypto-asset segregation, crypto-ownership and control over private keys have also been recently addressed by the Court of Florence in the case involving BitGrail, the Italian cryptocurrency exchange, which was declared insolvent in January 2019.

BitGrail was an online exchange platform through which different types of cryptocurrencies could be purchased, exchanged and deposited against the payment of a fee. In February 2018, BitGrail released a statement, announcing the loss of 17 million Nanos (altcoins traded on the exchange) worth approximately USD170 million and cessation of platform services.[58] Later the Italian court

---

54 Tokyo District Court Judgment, *supra* note 46.

55 *Bankruptcy Act*, 2004 (Japan), (Act No 75 of June 2, 2004). Article 62 reads as follows, "The commencement of bankruptcy proceedings shall not affect a right to segregate, from the bankruptcy estate, property that does not belong to the bankrupt (referred to as a "right of segregation" in Article 64 and Article 78(2)(xiii))." See editorial notes by Editors M Hara, C Mooney & L Gullifer to the translation of the Tokyo District Court Judgment, *ibid*.

56 For instance, Japanese law recognises ownership over certain rights, including claims (receivables) and IP rights (*eg* copyright, patents). See Tokyo District Court Judgment, *ibid*.

57 Mai Ishikawa, "Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case" (2017) 3:1 Journal of Financial Regulation 125 at 126.

58 G Rocco, "BitGrail cryptocurrency exchange hacked, $170 million in Nano allegedly stolen" *Bitcoinist* (11 February 2018), online: Bitcoinist <https://bitcoinist.com/bitgrail-cryptocurrency-exchange-hacked-170-million-nano-allegedly-stolen/>.

ordered the founder of BitGrail, Mr Francesco Firano, to repay losses suffered by crypto-investors in a 2018 hack.[59]

With the help of a court-appointed expert, the court noted that deposited cryptocurrencies were directed towards the main address of the exchange (one single omnibus address), controlled by its founder. Therefore, the court noted, in case of a shortfall it was impossible to establish which customer the disappeared crypto-assets belonged to. Because of the interchangeability within the omnibus address, the court held: "once the users' cryptocurrencies were directed toward BitGrail's main address, the currencies . . . no longer bore the distinctive elements associated with ownership by a single user, thereby giving rise to a relationship of irregular deposit."[60] Article 1782 of the *Italian Civil Code* defines irregular deposit (*deposito irregolare*) as "the deposit . . . of an amount of money or other fungible things, which the depository is authorised to make use." Irregular deposit is characterised by an obligation of the custodian to return items of the same type, quantity and quality (*tantundem eiusdem generis*), rather than individualised items, back to the customer. Most importantly, in cases of irregular deposits, the deposited items become property of the custodian.[61]

Special attention was given by the court to the fact that customers did not have any private keys and could not engage in trading activities or withdraw funds without support from the exchange. The crypto-exchange could at any time prohibit or restrict the access to its services, and hence controlled all access to the customers' bitcoins. According to the court, crypto-assets deposited with BitGrail became the property of the exchange. As a result, the position of customers was weak, as they could only exercise personal claims against the crypto-exchange.

## V. Private International Law

### A. *Introduction*

In the above, we described the main technical features of blockchain and of bitcoin in particular. We zoomed in on the custody of crypto-assets and analysed the terms and conditions of various crypto-custodians. On this basis, we established that in practice, bitcoin can be either held in an omnibus address (Coinbase) or in segregated addresses (Gemini). Then, we discussed two cases of crypto-custodian insolvencies (MtGox in Japan and BitGrail in Italy), which both brought to light the legal risks inherent in the custody of crypto-assets. Thus, in the above we approached the custody of crypto-assets from a mainly practical perspective, as we analysed the terms and conditions of crypto-custodians and real-life cases. In the following Sections, we will take a more legal perspective, in that we will analyse which rules of law can and should

---

[59] BitGrailVictimsGroup, "The BitGrail Exchange Ruling: a Win for Cryptocurrency Exchange Users" *Medium* (28 January 2019), online: Medium <https://medium.com/@bitgrailvictims/the-bitgrail-exchange-ruling-a-win-for-cryptocurrency-exchange-users-50df6c383571?fbclid=IwAR2QaNYhrF-sxsrU7b4ZYGpwR_rDcHt1Ei-OsRXQIlJwv6dqHCvJ-bs3354>.

[60] Court of Florence, 21 January 2019, *Bankruptcy Docket Nos 178/2018 and 205/2018*, Decision No 17/2019 (Italy), English translation online: Medium <https://medium.com/@bitgrailvictims/court-decision-by-the-court-in-florence-jan-21-20-c6d0c3e4247c>.

[61] Guido Alpa & Vincenzo Zeno-Zencovich, *Italian Private Law* (UK: Routledge-Cavendish, 2007) at 219.

apply to the custody of cryptocurrencies. We will take private international law as a starting point and then proceed to discuss rules of substantive law.

In the previous Sections, we have seen that as a matter of principle, the Bitcoin network is decentralised and concerns digitalised items. Bitcoin therefore does not seem to have a link to any specific jurisdiction. Yet crypto-custodians are usually operated by legal entities which do have a geographical location. For customers based outside the USA, for instance, Coinbase performs its services through the United Kingdom ("UK")-registered Coinbase UK Ltd and CB Payments Ltd.[62] This link to a specific jurisdiction is crucial for the determination of a court's jurisdiction for the opening of insolvency proceedings against a crypto-custodian. The following legal analysis is given on the assumption that a crypto-custodian in the EU falls insolvent and that its customers, *ie* crypto-investors, demand retrieval of 'their' cryptocurrency. We thus assume that an EU court is addressed and the following analysis is therefore based on EU conflict of laws rules. However, the legal principles discussed are widely accepted so our analysis is likely to be relevant for other jurisdictions as well.

Also, we assume that the crypto-custodian does not qualify as a credit institution, an investment firm or insurance undertaking. This assumption is in line with reality, as most crypto-custodians are not licensed as such. For a private international law analysis this is important, since for financial institutions, different jurisdiction and conflict of laws rules apply.[63] Where the insolvent entity does not qualify as a financial institution, EU courts determine international insolvency jurisdiction under the *European Insolvency Regulation* ("*EIR Recast*"),[64] which is directly applicable in all EU Member States except Denmark.

### B. *Jurisdiction and Insolvency Law*

As its main jurisdictional rule, Article 3(1) of the *EIR Recast* provides that the courts of the Member State where the centre of the debtor's main interests ("COMI") is situated have jurisdiction to open insolvency proceedings. COMI is the place "where the debtor conducts the administration of its interests on a regular basis and which is ascertainable by third parties." This place is presumed to coincide with the place of the debtor's registered office. This presumption is strong and can be rebutted only in exceptional circumstances, for instance in the case of a "letterbox" company not carrying out any business in the territory of the country in which its registered

---

62 Coinbase User Agreement 2019, *supra* note 29. As another example, Huobi operates through the US-registered HBUS Holdco Inc. See HBUS Terms of Service, online: HBUS <https://www.hbus.com/terms-of-service/>.

63 If the insolvent entity qualifies as an investment firm or a credit institution, the court's jurisdiction is to be determined under (national law implementing) the EC, *Directive 2001/24/EC of the European Parliament and of the Council on the reorganisation and winding up of credit institutions,* [2001] OJ, L 125/15 [*Winding-up Directive*], online: EUR-Lex <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0024&from=EN>. Insolvency of insurance undertakings is covered by (national law implementing) the EC, *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II),* [2009] OJ, L 335/1, online: EUR-Lex <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0138&from=en>.

64 EC, *Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (recast)*, [2015] OJ, L 141/19 [*EIR Recast*].

office is situated.[65] Thus, the place of the registered office usually indicates the international jurisdiction of the court to open (main) insolvency proceedings. The court proceedings in the insolvencies of MtGox (Japan), BitGrail (Italy), Quadriga (Canada), Cryptopia (New Zealand) and Blockport B V (Netherlands) all confirm this analysis.

Insolvency jurisdiction is closely tied to the applicable substantive insolvency law. For example, under Article 7(1) of the *EIR Recast*, "the law applicable to insolvency proceedings and their effects shall be that of the Member State within the territory of which such proceedings are opened." Thus, if the court of Amsterdam would open insolvency proceedings, this court must apply (substantive) Dutch insolvency law. This law (referred to as *lex concursus*) defines, *inter alia*, the powers of the trustee in insolvency, the effects of insolvency proceedings on current contracts and the ranking of creditors' claims in insolvency, etc.

Importantly, the *lex concursus* determines which assets form part of the insolvency estate and the treatment of such assets in insolvency (Article 7(2)(b) of the *EIR Recast*). This rule is also applied in other jurisdictions. For example, in the bankruptcy of Mr Tsarkov, Russian courts were requested to decide whether the contents of a crypto-wallet opened with a crypto-custodian and amounting to around 0.2 bitcoin (allegedly owned by Mr Tsarkov) were part of the insolvency estate. The insolvency practitioner asked the court to oblige Mr Tsarkov to transfer the password to the wallet. The court of first instance refused to recognise bitcoin as an asset for the purposes of insolvency law, citing the unclear nature of cryptocurrencies under Russian law.[66] This decision was subsequently reversed by the appellate court, which found that any property of the debtor having economic value, including cryptocurrency, must not be arbitrarily excluded from the insolvency estate.[67] Ultimately, the court demanded that Mr Tsarkov grant the insolvency practitioner access (password) to the debtor's crypto-wallet.

As a matter of EU conflict of laws rules, the determination of the insolvency estate, *ie* which assets form part of the insolvency estate, must be distinguished from the determination of ownership, *ie* which assets are owned by the debtor or by any third party. These two issues are to be decided under different conflict of laws rules. The determination of the insolvency estate is considered an insolvency law matter and thus governed by the *EIR Recast*, whereas the determination of ownership is governed by the law that applies to the property law aspects of the asset in question. We will return to this distinction in the following Section.

---

65 Judgment of the Court (Grand Chamber), 2 May 2006, *Eurofood IFSC Ltd*, Case C-341/04, ECLI:EU:C:2006:281 (Ireland) at para 35; Judgment of the Court (First Chamber), 20 October 2011, *Interedil Srl v Fallimento Interedil Srl and Intesa Gestione Crediti SpA*, Case C-396/09, ECLI:EU:C:2011:671 (Italy) at para 50, holding the presumption irrebuttable "where the bodies responsible for the management and supervision of a company are in the same place as its registered office and the management decisions of the company are taken, in a manner that is ascertainable by third parties, in that place."

66 Decision of the Commercial Court of Moscow (Moscow Arbitrazh Court), 5 March 2018, Case No A40-124668/17-71-160 Ф (Russia).

67 Decision of the 9th Arbitrazh Appellate Court, 15 May 2018, Case No A40-124668/2017 (Russia). For comments, see I Kokorin, "When Bitcoin meets insolvency: Is Bitcoin property? Dutch and Russian responses" *LexisNexis* (8 June 2018), online: LexisNexis <https://www.lexisnexis.co.uk/blog/restructuring-and-insolvency/when-bitcoin-meets-insolvency-is-bitcoin-property-dutch-and-russian-responses>.

Once a court has assumed jurisdiction to open insolvency proceedings (*forum concursus*) and the law applicable to the effects of such opening (*lex concursus*) is determined, the jurisdiction for adjudication of claims filed by crypto-investors against the insolvent crypto-custodian and the law applicable to such claims should be established. Assuming that the *EIR Recast* applies, its Article 6(1) now becomes relevant. Article 6(1) of the *EIR Recast* stipulates that the courts of the Member State within the territory of which insolvency proceedings have been opened "shall have jurisdiction for any action which derives directly from the insolvency proceedings and is closely linked with them."[68] This principle is called '*vis attractiva concursus'*, *ie* the principle that ancillary actions are "attracted" by the insolvency forum and must therefore be resolved by that same forum. For example, the Court of Justice of the European Union ("CJEU") has determined that a transaction avoidance claim (*actio pauliana*) filed by a liquidator[69] and an insolvency-related director liability claim[70] are closely linked to insolvency proceedings and must therefore be subject to the jurisdiction of the *forum concursus*.

In contrast, actions for the performance of obligations under a contract concluded by the debtor prior to the opening of insolvency proceedings are not considered to derive directly from these proceedings.[71] In the same vein, a contractual choice for a dispute resolution forum (*forum contractus*), including a choice for arbitration, generally remains valid in insolvency.[72] However, this does not necessarily mean that contract-based claims will always escape the "attraction" of the insolvency forum, as courts may consider attraction to be a matter that is ultimately governed by the applicable national insolvency law if that national insolvency law says that only the insolvency court has the competence to decide on all claims against the insolvent debtor. In several recent cases, courts in Member States ruled on this matter, *ie* determined whether choice of forum clauses that granted jurisdiction to courts other than the courts of the opening of insolvency proceedings could trump the insolvency court's jurisdiction when the relevant national insolvency law said that only the insolvency court had the competence to decide on claims against the insolvent debtor.[73]

---

68 *EIR Recast*, *supra* note 64, art 6(1).

69 Judgment of the Court (First Chamber), 12 February 2009, *Christopher Seagon v Deko Marty Belgium NV*, Case C-339/07, ECLI:EU:C:2009:83 (Germany).

70 Judgment of the Court (Sixth Chamber), 10 December 2015, *Simona Kornhaas v Thomas Dithmar als Insolvenzverwalter über das Vermögen der Kornhaas Montage und Dienstleistung Ltd*, Case C-594/14, ECLI:EU:C:2015:806 (Germany).

71 *EIR Recast*, *supra* note 64, Recital 35.

72 The majority of terms and conditions of crypto-exchanges provide for arbitration as the chosen dispute resolution method. See Coinbase User Agreement 2019, *supra* note 29, at para 10.3 (arbitration in London Court of International Arbitration); Gemini User Agreement, *supra* note 43, on Dispute Resolution (arbitration held in New York, New York, administered by Judicial Arbitration and Mediation Services, Inc ("JAMS")); Kraken Terms of Service, at para 23, online: Kraken <https://www.kraken.com/legal> (arbitration held in San Francisco, California, in accordance with the rules of JAMS) [Kraken Terms]; Binance Terms of Use, at Section X, online: Binance <https://www.binance.com/en/terms> [Binance Terms].

73 Z Fabok, "Vis Attractiva Concursus Throughout the EU? New Ruling of the Hungarian Curia on the Jurisdiction for Post-opening Actions Against an Insolvent Debtor" *Oxford Business Law Blog* (31 October 2017), online: Oxford Business Law Blog <https://www.law.ox.ac.uk/business-law-blog/blog/2017/10/vis-attractiva-concursus-throughout-eu-new-ruling-hungarian-curia>.

In a recent case, for instance, proceedings were initiated before an English court against the insolvent Icelandic bank Kaupthing. Kaupthing's creditor addressed the English court on the basis of a valid choice of forum. Kaupthing challenged the English court's jurisdiction on the ground that Icelandic bankruptcy law establishes that only the Icelandic insolvency court has the competence to rule on monetary claims against an insolvent debtor. Both the court in first instance and the court of appeal sided with the defendant, and held that in this case, the insolvency court's jurisdiction (*forum concursus*) should prevail over (valid) contractual arrangements with respect to jurisdiction, including a dispute resolution clause.[74] This conclusion was based on Article 10(2)(e) of the *Winding-up Directive*, which prescribes the application of *lex concursus* to the effects of winding-up proceedings on proceedings brought by individual creditors, and is identical to Article 7(2)(f) of the *EIR Recast*. This led the Court of Appeal to decide that if the *lex concursus* (*ie* Icelandic bankruptcy law) establishes that only the (Icelandic) insolvency court has the competence to rule on monetary claims against the insolvent debtor, parties' choice for an alternative court or arbitration is trumped by the authoritative force of *vis attractiva concursus*. However, the CJEU—as the ultimate authority to interpret the *Winding-up Directive* and the *EIR Recast*—has not yet ruled on this issue, and it is not certain whether it would come to the same conclusion as the English Court of Appeal. It could also be argued—and in fact, the appellant in the case just discussed seems to have done so—that Article 10(2)(e) of the *Winding-up Directive* must not be interpreted so as to refer to foreign jurisdiction rules, but more narrowly, *ie* along the lines of other CJEU case law saying that proceedings of individual creditors are only attracted to the *forum concursus* if these proceedings concern 'typical' insolvency-related issues such as whether a liquidator may void a contract on *actio pauliana* grounds. Proceedings on issues such as whether the relevant contract was concluded in error, would thus be governed by the contract's forum clause (if present and valid, see below), any insolvency jurisdiction rule of the *forum concursus* notwithstanding. In this line of reasoning, (a strict interpretation of) the *Winding-up Directive* and the *EIR Recast* would take precedence over national insolvency law rules such as the Icelandic one saying that only the national insolvency court has the competence to rule on monetary claims against the insolvent debtor.

If the claim for retrieval of their cryptocurrency is not to be decided by the *forum concursus* but by another EU court, the *Brussels I Regulation (recast)* ("*Brussels Ibis*")[75] comes into play, provided the matter is 'international'.[76] The threshold for internationality is not high, but purely domestic matters are excluded from the formal scope of the *Brussels Ibis*. The material scope of the *Brussels Ibis* covers "civil and commercial matters" according to Article 1 of the *Brussels Ibis*.[77] The delineation

---

74 *Tchenguiz v Grant Thornton UK LLP* [2017] EWCA (Civ) 83.

75 EC, *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*, [2012] OJ, L 351 [*Brussels Ibis*].

76 For a matter to qualify as international, parties need not necessarily be resident in different Member States. It suffices if, for instance, the transaction needs to be performed in another Member State. See M Bogdan & M Sender, *Concise Introduction to EU Private International Law*, 4th ed (The Netherlands: Europa Law Publishing, 2019) at 38 [Bogdan & Sender].

77 *Brussels Ibis, supra* note 75, art 1.

of insolvency law matters has already been just discussed. What is important to note is that the terms "civil and commercial matters" which define the material scope of the regulation need to be interpreted autonomously, *ie* without reference to national law.[78]

A claim for retrieval of cryptocurrency would probably qualify as a matter that falls under the formal and material scope of the *Brussels Ibis*, so that Article 4 of the *Brussels Ibis* applies. This provision says that persons domiciled in a Member State are, whatever their nationality, to be sued in the courts of that Member State. Legal persons or associations are domiciled at the place where they have their statutory seat, central administration or principle place of business.[79] In any event, the courts of the place where the defendant is domiciled cannot refuse jurisdiction, whilst courts of other Member States must refuse jurisdiction if their jurisdiction cannot be based on one of the grounds provided for in the *Brussels Ibis*. This means that absent an explicit choice for another court than the *forum concursus*, it is likely that the courts of the same jurisdiction as the *forum concursus* will have jurisdiction when crypto-investors sue their insolvent crypto-custodian.

Article 25(1) of the *Brussels Ibis* allows prorogation of jurisdiction through choice-of-court agreements and in most commercial contracts, such a choice of forum is indeed made.[80] Pursuant to Article 25 of the *Brussels Ibis*, parties can agree on a court or the courts in a Member State that has jurisdiction to settle their disputes arising in connection with a certain legal relationship.[81] This choice of forum may apply to both contractual claims regarding the transaction in question (*ie* a user agreement or crypto-custody contract as discussed above), and property law disputes, such as a claim for retrieval of assets. Such jurisdiction is in any event exclusive, unless agreed otherwise by the parties. Choice-of-court clauses are thus presumed to be exclusive, depriving all courts other than the agreed ones of jurisdiction. The agreed court(s) have exclusive jurisdiction also in regard to the validity of the choice-of-court clause itself.[82]

Article 25(1) of the *Brussels Ibis* does not require that any of the parties concluding a choice-of-court agreement are domiciled in a Member State.[83] It is important to note, however, that Article 25(1) only covers those choice-of-court agreements that choose the courts of a Member State. *Fora* outside the EU may be chosen, but the validity and effect of such a clause is not governed by Article 25(1) of the *Brussels Ibis*, but as a matter of principle by the application of national private international law rules.

To the general analysis just rendered, two nuances should be made which may lead to a different outcome in a specific case of a crypto-investor claiming retrieval of his cryptocurrency from an insolvent crypto-custodian. First, under Article 18(2) of the *Brussels Ibis*, a consumer "may bring proceedings against the other party to

---

78 Bogdan & Sender, *supra* note 76 at 36-37 and the references there given.

79 *Brussels Ibis, supra* note 75, art 63(1).

80 *Ibid*, art 25(1).

81 *Ibid*, art 25.

82 Judgment of the Court (Sixth Chamber), 3 July 1997, *Francesco Benincasa v Dentalkit Srl*, Case C-269/95, [1997] ECR I-3767 (Germany).

83 *Brussels Ibis, supra* note 75, art 25(1).

a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled".[84] This means that if a crypto-investor qualifies as a 'consumer' as defined in the *Brussels Ibis* and if, in short, the crypto-custodian directs his activities to the Member State where the consumer is domiciled,[85] this consumer may also sue in his own jurisdiction, a possible choice-of-court clause in the relevant user agreement or crypto-custody contract for a court of another Member State notwithstanding. Second, several user agreements we analysed do not contain a choice-of-court clause but refer to arbitration.[86] Under the laws of the contracting States to that Convention (and many States have indeed ratified the Convention), arbitration clauses are governed (not by the *Brussels Ibis*, but) by the *New York Convention*.[87] However, for consumers, again, mandatory rules of law may impact the enforceability of an arbitration clause.[88]

Bitfinex

### C. *Applicable Contract or Property Law*

After having established jurisdiction, the court or arbitral tribunal must determine the applicable law. For this determination, the court or arbitral tribunal must first qualify the matter, *ie* the crypto-investor's claim for retrieval of his cryptocurrency, as either contractual or proprietary in nature. Considering the nature of this specific asset, this qualification is not straightforward. Nonetheless, the decision is of great relevance, because contractual claims are governed by other conflict of laws rules than proprietary claims. The qualification of a claim for the return of deposited bitcoins by a crypto-investor against an insolvent crypto-custodian probably depends on the qualification of the asset the retrieval of which is requested, *ie* the object of the claim (bitcoin). This was also the court's analysis in the MtGox insolvency.[89] If bitcoin is to be considered as purely contractual in nature (*ie* similar to cash credited to an account), the claim for retrieval would also qualify as such. In contrast, should bitcoin be considered proprietary (*ie* similar to financial instruments), the crypto-investor's claim would also qualify as such. We will return to the issue of bitcoin qualification extensively below, in Section VI. For now, we will proceed to investigate both qualifications.

Should the court qualify a crypto-investor's claim for retrieval as contractual (for instance because the claim is formulated as a claim for performance of the user agreement or because the nature of bitcoin is qualified as contractual in nature), the governing law of that claim is probably to be determined under the *Rome I Regulation*

---

84 *Ibid*, art 18(2).

85 *Brussels Ibis*, *supra* note 75, art 17(1)(c).

86 See Kraken Terms, *supra* note 72; Binance Terms, *supra* note 72; Bitfinex Terms of Service, online: Bitfinex <https://www.bitfinex.com/legal/terms>; Gemini User Agreement, *supra* note 43.

87 *Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958*, 330 UNTS 3, online: UNCITRAL <https://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/New-York-Convention-E.pdf>.

88 See *eg*, *Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts*, [1993], OJ, L95, art 3(3) and Annex, art 1(q).

89 See Section IV.A.

("*Rome I*").[90] This position assumes the extensive interpretation of the English courts as discussed above is not followed and that the matter to be decided falls under *Rome I*'s material scope. In this respect, Article 12(1) of *Rome I* contains a non-exhaustive list of matters that are governed by the law to be applied under *Rome I*.[91] Among these issues are the interpretation of the contract, the performance of the contract, as well as consequences of breaches and termination of the contract.

As its principal substantive rule for the determination of the applicable law, *Rome I* gives primacy to party autonomy in that it stipulates that a contract is governed by the law that the parties have chosen.[92] All user agreements or crypto-custody contracts that we have seen contain a choice of law clause, so that pursuant to Article 3 of *Rome I*, this chosen law applies.[93] *Rome I* does require that the choice of law be made expressly, or be clearly demonstrated by the circumstances of the case or the contractual terms. The chosen law does not have to be related to any elements of the contract. Nonetheless, there are certain restrictions to this general rule, including several weak-party protection rules (such as consumers) and overriding mandatory rules. Should a party qualify as a consumer as defined in *Rome I*, a choice of law may not "have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable" (Article 6(2) of *Rome I*).[94] Otherwise, as a matter of principle, *Rome I* does not subject a choice-of-law clause to stringent requirements.

Even if the choice for another law than the *lex concursus* is made and recognised by the insolvency court, the applicable *lex concursus* often permits the insolvency practitioner to refuse to satisfy a claim for specific performance, so that this claim is converted into a claim for damages. Under most insolvency laws, a claim for damages ranks *pari passu* with all other creditors and it is often unlikely that these claims are satisfied in full. Alternatively, if the object of the claim, *ie* bitcoin, has been qualified as contractual in nature, it will most likely be considered a monetary claim that will also rank *pari passu*, with a low chance of satisfaction for the crypto-custodian's customers.

Should the court qualify the crypto-investor's claim for retrieval of his cryptocurrency as proprietary, Article 8(1) of the *EIR Recast* is of relevance. This Article provides that creditors' property rights (rights *in rem*) in assets located in EU Member States other than the debtor's COMI-jurisdiction are not to be affected by the *lex concursus*.[95] These rights include, amongst others, "the right to demand assets

---

90 EC, *Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations* (*Rome I)*, [2008] OJ, L177/6 [*Rome I*].

91 *Ibid*, art 12(1).

92 *Ibid*, art 3(1).

93 *Rome I, supra* note 90, art 3. See *eg* Coinbase User Agreement 2019, *supra* note 29, at para 13.19 (English law), OKEx Terms, *supra* note 39, at para 13 (laws of Seychelles), Kraken Terms, *supra* note 72, at para 23 (laws of the State of California and applicable United States law), Upbit Terms of Use, at art 2, online: Upbit <https://sg.upbit.com/terms_of_service> (Singapore law).

94 Assuming that the consumer's interests in bitcoin do not qualify as a 'financial instrument' as defined in *Rome I*, *supra* note 90.

95 Article 8(1) of the *EIR Recast*, *supra* note 64.

from, and/or to require restitution by, anyone having possession or use of them contrary to the wishes of the party so entitled".[96] The CJEU has ruled that an action based on a reservation of title clause (*ie* repossession/revendication) "constitutes an independent claim, as it is not based on the law of the insolvency proceedings and requires neither the opening of such proceedings nor the involvement of a liquidator".[97] If the object of a crypto-investor's claim for retrieval, *ie* his deposited bitcoin, is considered proprietary in nature, this claim surely qualifies as a claim for "assets from, and/or ... restitution by, anyone having possession or use of them contrary to the wishes of the party so entitled".[98] Thus, a crypto-investor's revendication claim against an insolvent crypto-custodian does not arise from or depend on the insolvency proceedings, so that this claim is not affected by the *lex concursus*.

However, it is far from evident under which conflict of laws rule the law governing a proprietary claim for the retrieval of cryptocurrencies must be determined.

First, there is a conceptual difficulty in establishing precisely which asset is the object of the claim for retrieval where it regards cryptocurrency. From our analysis of the practice of crypto-custody in Section III above, it follows that the relationship with a crypto-custodian is the source of a crypto-investor's interests in 'his' bitcoin. The object of a crypto-investor's claim for retrieval against a crypto-custodian, *ie* his indirect interest in cryptocurrency, therefore needs to be distinguished from the cryptocurrency itself (*ie* the bitcoin rights between the network participants).[99] Just as a securities account holder's rights against his custodian bank must not be confused with (interests in) the underlying shares and bonds, a customer's rights against his crypto-custodian are to be distinguished from any (interests in) bitcoin.

Second, also if the crypto-investor/crypto-custodian relationship is to be taken as the source of a claim for retrieval, the connecting factor is not self-evident. It could be argued, for instance, that the physical embodiment of the credentials (*ie* the paper or the carrier (paper/smartphone/PC) containing the username and password by means of which the crypto-investor can access his account on the crypto-custodian's website), must be considered to be the decisive connecting factor, as bitcoin can only be accessed and disposed of through these credentials. However, connecting to a physical carrier would only be appropriate when having to decide on the law applicable to (property interests in) the physical carrier itself, but not necessarily to the underlying rights of the crypto-investor regarding 'his' cryptocurrency against the crypto-custodian. Moreover, the content of a physical carrier can be multiplied, sent electronically and subsequently stored in or on another physical carrier in a different jurisdiction (*eg* in an app on a smartphone or another piece of paper), or physically transferred from one jurisdiction to another. To use a physical carrier as connecting factor would therefore be both theoretically and practically unsound. Alternatively, the relevant blockchain address administered by the crypto-custodian could be considered as the connecting factor. As was explained in Section III above, this can be either an omnibus or segregated bitcoin address. It is doubtful, however, whether a crypto-custodian's blockchain address would solve the objections just

---

96 *Ibid*, art 8(2)(c).

97 Judgment of the Court (First Chamber), 10 September 2009, *German Graphics Graphische Maschinen GmbH v Alice van der Schee*, Case C-292/08, [2009] ECR I-08421(Netherlands).

98 Article 8(2)(c) of the *EIR Recast*, *supra* note 64.

99 See Figure 3 above and more extensively Section V below.

raised against using the relevant physical carrier as connecting factor, because a bitcoin address is stored decentrally on all the (servers of the) nodes keeping a copy of the public blockchain and each and any of those could then be considered the connecting factor. Moreover, because of the intangible nature of bitcoin addresses, the *lex rei sitae* rule traditionally used for proprietary claims proves to be of little use.[100]

The problem of having to localise the unlocalisable is not new and has also been addressed where it regards financial instruments that are credited to accounts. It therefore seems appropriate to investigate the conflict of laws rules that have been developed for proprietary claims in financial instruments as inspiration for property claims in cryptocurrency.

The *EIR Recast*, for instance, offers specific conflict of laws rules for rights *in rem* in financial instruments, registered shares, cash held with credit institutions and claims against third parties.[101] Even more specifically, Article 2(9)(ii) of the *EIR Recast* concerns financial instruments and refers to the Member State in which the register or account in which the relevant account entries are made is maintained. A similar rule can be found in the *Collateral Directive*,[102] the *Settlement Finality Directive*[103] and the *Winding-up Directive*.[104] These instruments all express a version of the so-called Place of the Relevant Intermediary Approach ("PRIMA") rule, which connects the applicable law to the place of the "relevant intermediary account", *ie* the place where the relevant securities account is held by the custody bank.[105] However, it is not always clear where the relevant account must be located, particularly in cases involving multinational banking groups having branches, subsidiaries and IT systems in multiple jurisdictions,[106] so that this version of PRIMA also

---

100 F Guillaume, "Aspects of private international law related to blockchain transactions", in D Kraus, T Obrist & O Hari, eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (UK: Edward Elgar, 2019) at 64; M Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2019) EBI Working Paper Series, No 42 at 16, noting that "bitcoin has no geographical home and is impossible to locate."

101 *EIR Recast*, *supra* note 64, art 2(9).

102 EC, *Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements*, [2002] OJ, L 168, art 9.

103 EC, *Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems*, [1998] OJ, L 166, art 9(2).

104 *Winding-up Directive*, *supra* note 63, art 24.

105 However, the Place of the Relevant Intermediary Approach ("PRIMA") rules contained in the directives cited differ in their precise formulation. In its Communication, COM(2018) 89, "on the applicable law to the proprietary effects of transactions in securities" (12 March 2018), the European Commission addressed the different wordings. The Commission is of the view that all directives must be interpreted similarly, viz to refer to the law of the jurisdiction where the relevant securities account is maintained. For a critical analysis of the directives, see *eg*, M Haentjens, *The Law Applicable to Indirectly Held Securities: The Plumbing of International Securities Transactions* (The Netherlands: SDU Uitgevers, 2006) at 29-38 [*Haentjens, The Law Applicable to Indirectly Held Securities*] and of the Commission's position paper, see M Haentjens, *Financial Collateral* (UK: Oxford University Press, forthcoming 2020) at ch 4.

106 *Haentjens, The Law Applicable to Indirectly Held Securities, ibid* at 87-98, M Haentjens, *Harmonisation of Securities Law*: *Custody and Transfer of Securities in European Private Law* (The Netherlands: Kluwer Law International, 2007) at 287-290 and P Paech, "Conflict of Laws and Relational Rights", in L Gullifer & J Payne, eds, *Intermediation and Beyond* (UK: Hart Publishing, 2019) at 293 [Paech].

seems to offer little legal certainty for blockchain addresses maintained by crypto-custodians.

The *Hague Securities Convention* (effective since 1 April 2017)[107] solves the practical problems of the EU instruments just cited and contains another version of the PRIMA rule. The *Hague Securities Convention* gives effect, also with respect to property law aspects, to the express agreement on the governing law between an account holder and its intermediary, provided that the relevant intermediary has, at the time of the agreement, an office in the jurisdiction whose law has been selected.[108] Thus, this approach enables party autonomy to govern the property law regime of indirectly held securities, in effect adopting a *lex contractus* rule albeit within certain limits. This solution adequately addresses the difficulty of and uncertainty around determining the location of the securities account or the location of the office where the securities account is maintained or managed.[109] If the applicable law has not been chosen by the parties, the *Hague Securities Convention* suggests several fall-back rules, which refer to the law of the state under whose law the relevant intermediary is incorporated.[110]

Whilst we realise that the *Hague Securities Convention* is currently ratified only by Mauritius, Switzerland and the USA,[111] and cryptocurrencies do not fall under its material scope,[112] we advocate that the *Hague Securities Convention* approach is the most appropriate approach for proprietary claims of customers against their crypto-custodians. Under this approach, the law chosen by the parties to the user agreement or crypto-custody contract, *ie* by the customer and his crypto-custodian, would govern the customer's claim for retrieval of cryptocurrency. In the unlikely event that the user agreement or custody contract would not contain a choice of law clause (as we have already seen, all user agreements we analysed do contain such choice of law clause), the law of the place where the relevant crypto-custodian is incorporated applies. The advantages of this approach are multiple. First, it abandons the ill-fitted *lex rei sitae* rule. Second, it addresses the deficiencies of the EU versions of PRIMA that require the determination of a physical location for a securities account that has no location. Third, it honours the parties' legitimate expectations, as both the chosen law and the registered office of the crypto-custodian are easily ascertainable for the relevant parties, *ie* crypto-investor and his custodian.

---

107 Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, 5 July 2006 (entered into force 1 April 2017), online: Hague Conference on Private International Law <https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf> [*Hague Securities Convention*].

108 *Ibid*, art 4.

109 R Goode, H Kanda & K Kreuzer, *Hague Securities Convention Explanatory Report*, 2d ed (2017) at 20. For the discussion on factual versus contractual approaches to determining law applicable to intermediated securities, see Paech, *supra* note 106 at 291-294.

110 *Hague Securities Convention*, *supra* note 107, art 5.

111 Hague Conference on Private International Law, *Status table*, online: Hague Conference on Private International Law <https://www.hcch.net/en/instruments/conventions/status-table/?cid=72>.

112 Pursuant to the *Hague Securities Convention*, *supra* note 107, art 1(1)(a), it applies to "securities" which are defined as "any shares, bonds or other financial instruments or financial assets (other than cash), or any interest therein". Cryptocurrencies would probably not qualify as such.

## VI. Property law qualifications

### A. *Two Qualifications of Bitcoin*

In the preceding Section, we analysed which court would have jurisdiction and which law should apply to a crypto-investor's claim for the return of crypto-assets from his crypto-custodian in the latter's insolvency. This analysis proved to be highly complex. A question we did not answer was whether the crypto-investor's claim should be qualified as contractual or as proprietary. Which of the two qualifications would be more desirable from the investor's perspective is ultimately a matter of substantive (insolvency and private) law, but from the above it might already be inferred that a qualification as a property law claim would probably be more protective, as a contractual claim is likely to rank *pari passu* with the crypto-custodian's other unsecured debt. It would therefore seem appropriate to investigate how a concrete legal system could assess a customer's claim for retrieval of his assets against the insolvent crypto-custodian as proprietary. It will be seen that central to this assessment will be a qualification of the object the claim for retrieval, *ie* his indirect interest in cryptocurrency.

Applying property law to bitcoins is challenging.[113] Some argue that under Dutch law, bitcoin is more akin to a tangible asset than a (property) right *stricto sensu*, but that it should be considered an (absolute) property right from a property law perspective.[114] Some subsequently dismiss this notion because the Dutch *numerus clausus* rule (the closed system of property rights) does not allow for the creation of new property rights.[115] Others argue under German law that the transfer of bitcoins is exclusively a contract law matter, is a "Realakt" and irrelevant from a property law perspective.[116]

In light of this legal uncertainty, Russia, for instance, has recently adopted legislation that defines "digital rights" as property.[117] In the wake of the MtGox collapse, and as already mentioned above, Japan has also amended its law, so that it now

---

[113] See, with respect to Dutch law, WAK Rank, "Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten" in R A Wolf, ed, *Bitcoins: Civiele en fiscale aspecten in beeld* (The Netherlands: Wolters Kluwer, 2015) at 36-37.

[114] See, with respect to Dutch law, V Tweehuysen, "Goederenrechtelijk puzzelen met bitcoins," (2018) *Ars Aequi* July/August, at 602-610, online: <https://core.ac.uk/download/pdf/159142331.pdf>; J LSnijders & Y C Tonino, "Goederenrechtelijke status van bitcoin (kapitaalkracht)" (2018) *Tijdschrift Financiering, Zekerheden en Insolventierechtpraktijk*, Nummer 6, September 2018/ SDU at 46-55; Central Netherlands Court, Rechtbank Midden-Nederland (vzr), 7 December 2017, ECLI:NL:RBMNE:2017:6646 with respect to Ether, another cryptocurrency; and Rechtbank Amsterdam, 14 February 2018, *Koinz Trading*, ECLI:NL:RBAMS:2018:869, JOR 2018/154, where the court considered 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.

[115] See, with respect to Dutch law, F H J Mijnssen, *Verbintenissen tot betaling van een geldsom (Mon BW nr B39)* (The Netherlands: Wolters Kluwer, 2017) at para 1.6 whilst referring to the *Dutch Civil Code*, 1992 (The Netherlands), art 3:83 at para 3 [*DCC*].

[116] See, with respect to German law, C Engelhardt & S Klein, "Bitcoins—Geschäfte mit Geld, das keines ist. Technische Grundlagen und zivilrechtliche Betrachtung" MultiMed Recht 2014, 355.

[117] According to the new Art 141.1 of the Russian Civil Code, 1994, following the Federal Law of 18 March 2019 No 34-FZ, "Regarding amending parts of the first, second and third part 1124 of the Civil Code of the Russian Federation" (in force since 1 October 2019), "digital rights" are "obligations and other rights, the content and conditions of which are determined in accordance with the rules of the information system that meets the criteria established by law." The exercise, disposal and pledge of digital rights are only possible within an information system and without the engagement of a third

recognises that virtual currency has property value (limited to that which is recorded on an electronic device) which can be used for the purchase of goods or services or mutually exchanged, and which can be transferred by means of an electronic data processing system.[118] In the USA, property law is traditionally a state law rather than a federal law matter.[119] Recently, the State of Wyoming enacted an Act that expressly recognises digital assets as "a representation of economic, proprietary or access rights that is stored in a computer readable format, and includes digital consumer assets, digital securities and virtual currency."[120] Virtual currency is classified as "intangible personal property". In *B2C2 Ltd v Quoine Pte Ltd*, the Singapore International Commercial Court, while accepting that cryptocurrencies are not legal tender in the sense of being a regulated currency issued by a government, has found that they nevertheless have the fundamental characteristic of intangible property as being an "identifiable thing of value".[121]

One of us has argued elsewhere that rights to bitcoins are embodied in the physical carrier of the wallet in which the public and private keypair to those bitcoins are stored and that that carrier can be considered a documentary intangible.[122] He came to that conclusion on the basis of the following argument.

The bitcoin system can be considered a multi-party contract[123] to which the bitcoin owners, miners and nodes (collectively: participants) become a party by using the bitcoin network and therefore accepting implicit third-party rights clauses made for their benefit.[124] The content of this multi-party contract is determined by the way the bitcoin software (*ie* the underlying algorithm) operates and by its documentation and open source code that is available to everyone.[125] By becoming a party to this multi-party contract, every miner undertakes to provide validation services against payment of transaction fees and newly created bitcoins if he becomes the winning miner. Each node, in turn, commits to verify and confirm the miners' work. For that verification, a node is not paid in bitcoins. However, he benefits indirectly because: (1) if he wishes to transfer bitcoins, his transactions will be validated, verified and

---

party. The holder of a digital right should be the person who, under the rules of the information system has the opportunity to dispose of this right.

118 *Payment Services Act 2009* (Japan) (Act No 59 of 2009, as amended by Act No 62 of 2016, the amendments taking effect on 1 April 2017), art 2(5), translation online: Japanese Law Translation <http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02>.

119 *Logan v Zimmerman Brush Co*, (1982) 455 US 422, 430.

120 US, SB 125, *Digital assets-existing law*, 2019-65, Gen Sess, Wyo, 2019 (effective as of 1 July 2019), online: Wyoleg <https://www.wyoleg.gov/Legislation/2019/SF0125>.

121 *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03 at para 142. For an overview of approaches to crypto-assets in property law of selected jurisdictions see Baker McKenzie Client Alert, *Bite-size Briefings: The approach to cryptoassets in property law and regulation* (November 2019), online: Baker McKenzie <https://www.bakermckenzie.com/en/insight/publications/2019/11/bite-size-briefings-autumn>.

122 TJ de Graaf, "The qualification of bitcoins as documentary intangibles" (2019) 27:5 European Review of Private Law 1051. For further detail reference is made to that article [Graaf].

123 See also with respect to Belgian law, S Geiregat, "Cryptocurrencies are (smart) contracts" (2018) 34:5 Computer Law & Security Review 1144, online: <https://www.sciencedirect.com/science/article/pii/S0267364918302279?via%3Dihub>.

124 For third party rights clauses and their acceptance under Dutch law, see Arts 6:253, 6:254 and 3:37 of the *DCC*, *supra* note 115; for English law, see *Contracts (Rights of Third Parties) Act 1999* (UK), c 31, s 1.

125 See GitHub, online: <https://github.com/bitcoin/bitcoin>; Bitcoin, online: <https://bitcoin.org/en/developer-documentation>.

confirmed by other miners and nodes; and (2) if he also mines and establishes that the winning miner has not performed the work correctly, he gets another chance to become the winning miner and be paid accordingly.

The rights of users of bitcoin network (*eg* transferors and transferees of bitcoins) against miners and nodes to perform their validation and verification activities are what we refer to as *bitcoin rights*. These bitcoin rights are made to bearer when a bitcoin is first mined, *ie* put to the bearer (*ie* possessor) of the physical carrier of the wallet in which the public and private keypair (associated with the bitcoin address to which the block reward is credited) are stored. In doing so, a documentary intangible put to bearer is created. The same applies, *mutatis mutandis*, at the moment that mined bitcoins are transferred to another bitcoin address, as well as to each subsequent transfer. The simplest way to imagine this is by considering a paper wallet: a piece of paper containing the public key and a (usually hidden) private key.[126] That private key is presented to the miners and nodes to effectuate the bitcoin rights embodied therein, *ie* to have bitcoins transferred, in the same way that a bill of lading can be presented to a carrier to effectuate the rights embodied in the bill of lading, *ie* to have the cargo delivered in the port of destination.[127] In case a paper wallet is used, the owner of the paper containing the private key is considered also to be the 'owner' of the bitcoin rights embodied in the paper and therefore, in essence, the bitcoins to which the private key provides access.

Whether a certain legal system allows for bitcoin rights to be made to bearer, depends on the law applicable to such rights. The Netherlands, for instance, has an open system of documentary intangibles which allows parties to put their rights to the bearer of a documentary intangible. Whether they agree to do so is a matter of contractual interpretation and general documentary intangible law may apply even if specific formal requirements for a specific documentary intangible are not met.[128] Also, under Dutch law, a documentary intangible does not need to be signed in order to be considered as such.[129] Also, English law seems to allow sufficient flexibility

---

[126] Made by using, for example: Wallet Generator, online: <https://walletgenerator.net/>; or Bitcoin Paper Wallet, online: <https://bitcoinpaperwallet.com/>.

[127] See TFE Tjong Tjin Tai, "De blockchain als alternatief voor de notariële praktijk" in FWJM Schols & BCM Waaijer, eds, *Financiële zorgplicht van de notaris (preadviezen KNB)* (The Netherlands: Sdu, 2018) at 123, who writes: "Maybe it is possible to regard the verification possibilities or potential claim with respect to a bitcoin balance as a right, which can be attached at that party by means of a third party attachment." (our translation). See, however, M Schellekens, E Tjong Tjin Tai *et al.*, "*Blockchain en het recht. Een verkenning van de reguleringsbehoefte"*, Wetenschappelijk Onderzoek- en Documentatiecentrum Report (June 2019), annex to Kamerstukken 2019, nr 26 643, at 30-34, who argue that in a permissionless blockchain (such as bitcoin) nodes have no legal obligation to do anything, but only a de facto incentive to process transactions.

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

[129] The Dutch law articles dealing with transfer of the rights embodied in a documentary intangible (Arts 3:93 and 3:90 of the *DCC*, *supra* note 115) only require that paper is used for a documentary intangible. Signing that documentary intangible is not a requirement for a transfer of the rights embodied therein, see FG Scheltema, *Mr M Polak's Handboek voor het Nederlandse Handels- en faillissementsrecht, Derde deel, Wissel- en Chequerecht, by, reworked by W R Meijer* (The Netherlands: Samson H D Tjeenk Willink,1993) at 25 as well as Zwitser, *supra* note 128, 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 & JB Huizink, *Betaling, waardepapier en documentair krediet* (The Netherlands: Kluwer, 2002), nr 24, who acknowledge that nowhere in the Dutch statute requires a signature for putting rights to bearer, but that bearer instruments are usually signed. In contrast: A van Oven, *Handelsrecht* (The Netherlands: WEJ

for the creation of new documentary intangibles: whether a right is considered to be embodied in a documentary intangible depends on mercantile usage.[130]

It is true that not all private keys are stored on paper wallets, yet all private keys are ultimately stored in physical carriers (hardware wallets in the form of USB-sticks, mobile wallets as apps on a smartphone or desktop wallets as software on a computer). Therefore, bitcoin rights exercised in order to effectuate a transfer of bitcoins can also ultimately be considered to be embodied in a physical carrier, the contents of which (*ie* the public and private keypair) are presented to those needed to effectuate such transfer, just like the contents of a bill of lading (*ie* the description of the goods to be delivered and other information) are presented to the carrier in order to demand delivery. This is easiest to imagine in case of a paper wallet and more difficult in case of non-paper wallets, because in most legal systems, two important objections may be raised against the qualification of non-paper wallets as documentary intangibles: (1) they are not made of paper; and (2) they cannot be given in such a way that nothing remains with the transferor. Both objections can be refuted.

The first objection (that non-paper wallets are not documentary intangibles because they are not made of paper) can be countered with reference to Article 9(1) of the *E-Commerce Directive 2000/31*[131] or similar rules found in other countries outside of the EU.[132] This Directive requires EU Member States to 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".[133] In Dutch law, for example, many contracts do not need to be concluded in a specific form and therefore may also be concluded electronically, and for those contracts which may only be concluded in writing, Article 6:227a(1) of the *Dutch Civil Code* ("*DCC*") provides: "If a statutory provision implies that an agreement can only be formed validly and inviolably (unchallengeable) in writing, then this formal requirement will also be met if the agreement is entered into by electronic means and: (a) the agreement is and remains accessible for the parties; (b) the authenticity of the agreement is sufficiently guaranteed; (c) the moment on which the agreement was formed, can be determined with sufficient certainty, and (d) the identity of the parties can be assessed with sufficient certainty."[134] In line with previous work,[135] we conclude that the bitcoin contract embodied in the non-paper wallet meets these

---

Tjeenk Willink, 1981) at 206, who argues that a documentary intangible needs to be a deed and therefore needs to be signed.

130 McKendrick, *Goode on Commercial Law*, 5th ed (UK: Penguin, 2017) at para 2.58. See also JS Roger, *The Early History of the Laws of Bills and Notes* (UK: Cambridge University Press, 1995), who argues that English judges composed commercial law regarding bills by incorporating commercial practice.

131 EC, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),* [2000], OJ, L 178 [*E-Commerce Directive*].

132 See *Uniform Electronic Transactions Act* ("UETA") §7 (1999), the Australian *Electronic Transactions Act 1999* (Cth) ss 8 and 15C, and the 2005 *United Nations Convention on the Use of Electronic Communications in International Contracts*, 23 November 2005, 2898 UNTS 3, art 8 at para 1, art 9 at para 2 (entered into force 1 March 2013).

133 Art 9(1) of the *E-Commerce Directive*, *supra* note 131.

134 See a translation of Book 6 of the *DCC*, *supra* note 115, online: Dutch Civil Law <http://www.dutchcivillaw.com/civilcodebook066.htm>.

135 See for an analysis of whether these requirements are met (and the conclusion that they are indeed met): Graaf, *supra* note 122.

requirements of Dutch and similar laws, so that bitcoin wallets need not always be made of paper.

The second objection (that non-paper wallets are not documentary intangibles because they cannot be given in such a way that nothing remains with the transferor) can be refuted as follows. Transferring the rights embodied in a documentary intangible by transferring possession of such documentary intangible presupposes (if not requires), those objecting may reason, that the documentary intangible is given by the transferor to the transferee in such a way that nothing remains with the transferor. However, paper and hardware wallets can be given in such a way. On the one hand, if something is stored on a wallet device, a smartphone, computer or server (a non-dedicated device), that device is rarely given to the transferee. Instead, the public and private keypair are, for example, copied and e-mailed to the transferee as a result of which the physical carrier can be said to dematerialise and materialise again when the transferee stores the keys received in his wallet on another physical carrier, his own. On the other hand, the transferor may be required to subsequently delete his copy of the private key, just as the transferor of a paper documentary intangible may not photocopy it before giving the original to the transferee.

Also, it is mercantile practice that documentary intangibles can be issued by means of several paper copies.[136] In such a situation, a holder of a documentary intangible put to bearer cannot be certain that another holder will not present his copy to the carrier earlier than he does, and by doing so exercise the rights embodied therein and render any other copies worthless. In the same vein, it can be argued that parties to the bitcoin multi-party contract upon conclusion of or accession to such contract implicitly agreed that the winning miner receives bitcoins on a bitcoin address, the public and private keypair of which he stores in a wallet. This wallet is ultimately kept on a physical carrier which we qualify as a documentary intangible put to bearer in the form of this physical carrier. Upon receipt of the bitcoins, he also receives the right to issue multiple documentary intangibles put to bearer. When that miner subsequently wishes to transfer access to his bitcoins by e-mailing his public and private keypair to a transferee and thereby provides access to the bitcoins stored in the address to which that private key gives access, the miner/transferor in effect exercises his right to have the transferee create another documentary intangible by storing those public and private keypair in his own wallet on a new physical carrier.

By agreeing to a transfer of the public and private keypair instead of a transfer of the bitcoins themselves, the transferee risks that the transferor retains a copy of those keys and uses them to transfer the bitcoins stored in the associated address to a third party before the transferee does so. From a practical point of view, the transferee would therefore be well advised to have the bitcoins transferred to his *own* address instead of receiving the keys to an address of the *transferor*.

In essence, there are therefore two ways in which a transferee can obtain bitcoins from a transferor. First, the transferor provides a copy of the public and private keypair to *his* address to the transferee. In that case, the transferor and transferee can both access the bitcoins in that address. Whoever presents his public and private keypair to that address to the miners and nodes first, is the one whose transfer will be accepted, even though the person presenting those keys might not be the real

[136] Bills of lading are, for example, commonly issued in sets, see for English law, Günther, Treitel & FMB Reynolds, *Carver on Bills of Lading* (UK: Sweet & Maxwell 2017) and for Dutch law, see *DCC*, *supra* note 115, art 8:413 and Zwitser, *supra* note 128, nr 16.

owner of the bitcoins in question. Second, the transferor may use the bitcoin system to send bitcoins to another address, *ie* a public address of the transferee. In that case, the transferor presents the public and private keypair to his address in order to send bitcoins to the transferee. The transfer results in an additional entry to the transferee's address. This address with the bitcoins received can then only be accessed with the use of the transferee's public and private keypair. And in each case, presenting the public and private keypair (in the wallet ultimately stored on a physical carrier) results in exercising the bitcoin rights and thereby requiring the miners and nodes to perform their validation and verification activities required to effectuate the transfer of the bitcoins.

### B. *Transfer of Bitcoin*

Now that we have discussed the possible property law qualifications of bitcoins, we will address the question which rights a crypto-investor can assert against an insolvent crypto-custodian. The answer to this question not only depends on the applicable law, but also on the type of custody arrangement. As seen above, the two types of custody arrangement applied in practice are through omnibus or pooled, and through segregated blockchain addresses. We will therefore now proceed to apply the property law qualifications discussed above to these two types of crypto-custody. For this purpose, we must first take a closer look to the transfer of bitcoin. Again, the following analysis is based on Dutch law, but our findings may be extrapolated to other jurisdictions.

As shown above, from a property law perspective rights to bitcoins can be qualified either as absolute rights or rights embodied in a documentary intangible, *ie* the physical carrier (paper, smartphone or computer) containing the wallet in/or which the public and private keypair of the blockchain address is stored. In light of these qualifications, an important question to analyse is whether commingling occurs with bitcoin, *ie* whether crypto-investors may not assert their proprietary interests in bitcoin because these are fungible and have commingled when held by a crypto-custodian. The legal consequences of commingling have been decided by the Dutch Supreme Court in the *Mulder cs/Teixeira de Mattos* ("*Teixeira de Mattos*").[137] In that case, investors deposited numbered paper bearer shares in the company Nillmij in a so-called open deposit, *ie* in one vault, with the bank Teixeira de Mattos. The bank was declared insolvent and failed to register which specific shares the investors deposited in an open deposit.

Translated into the terms of the current version of the *DCC* enacted in 1992, the Dutch Supreme Court held that bearer shares are tangible goods to which the rules regarding possession apply. This means that the bank holding the bearer shares is deemed to hold the shares for itself[138] and is presumed to be the possessor of those shares in good faith.[139] Such possessor is presumed to be the owner of those

---

[137] Dutch Supreme Court, 12 January 1968, *Mulder cs/Teixeira de Mattos*, ECLI:NL:PHR:1968:AC2286, NJ 1968/274. See also M Haentjens, *Harmonisation of securities law: custody and transfer of securities in European private law* (PhD thesis submitted to the University of Amsterdam, 2007) at 147-151, para 7.3.2.

[138] *DCC*, *supra* note 115, art 3:109.

[139] *DCC*, *ibid*, arts 3:107(1) and 3:118(3).

shares,[140] subject to counterproof. In *Teixeira de Mattos*, the bank was presumed to own the shares deposited by two clients, whilst the investors were unable to provide the required counterproof showing specific shares of the deposited shares belonged to them. So even though *de jure* the investors remained owners of those shares, *de facto* they could not assert their ownership rights in the absence of the proof required by law. Ultimately, the bank could acquire ownership after the relevant statutory period of limitation had expired.

Let us now apply the *Teixeira de Mattos* reasoning to bitcoin transactions (see Section II above) and investigate whether or not the required counterproof can be provided in a blockchain situation. The crypto-investor who transfers bitcoins into an omnibus (pooled) address held by his crypto-custodian (possibly under the impression that the transfer is made to a segregated account) can most probably show the bitcoin address which the crypto-custodian indicated, as well as the transaction details. The crypto-custodian's bitcoin address will list thousands of transactions by means of which crypto-investors transferred their bitcoins to the crypto-custodian. That information is publicly available on the blockchain, so that the crypto-investor can do a simple search and see that his transaction is included in the crypto-custodian's (blockchain) list of transactions. Theoretically, this transaction could be individualised and could remain untouched (unspent) by the crypto-custodian. In that case the crypto-investor may provide the required counterproof to the presumption of the crypto-custodian's ownership.

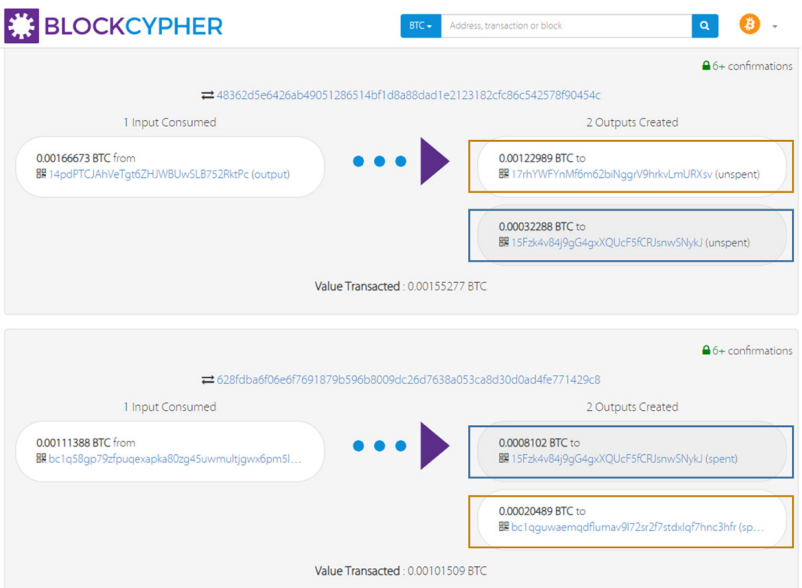


**Fig. 4.** Two Transaction Outputs to the Same Blockchain Address.

In the figure above one can see the record showing two outputs (incoming transactions) made to one bitcoin address, 15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ

[140] *DCC*, *ibid*, art 3:119(1).

(indicated in the blue box). On the right-hand side two recordings are shown for each transaction, one linked to this address—the actual value of bitcoin received under two transactions (0.00032288 bitcoin and 0.0008102 bitcoin), and another one—change (0.00122989 bitcoin and 0.00020489 bitcoin). Change (indicated in the yellow box) is deposited in the newly algorithmically created change address associated with the same bitcoin wallet. Value Transacted indicates the total transaction amount, *ie* transferred bitcoins plus change. Transaction fees for each bitcoin transaction are also typically shown.

Imagine the owner of the receiving address decides to transfer (spend) some bitcoins to a third address.

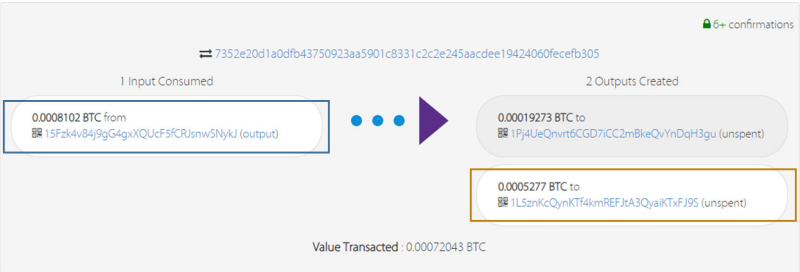


**Fig. 5.** Outgoing (Input) Transaction to a Third Address.

In the above figure one can see the outgoing (input) transaction, indicating the transfer of bitcoins from one address, 15Fzk4v84j9gG4gxXQUcF5fCRJsnwSNykJ (again indicated in the blue box), to another address, 1Pj4UeQnvrt6CGD7iCC2mBkeQvYnDqH3gu. The second recording on the right-hand side (in the yellow box) indicates change. From the input transaction we can see that bitcoin is taken from the previous output transaction of 0.0008102. This output is spent and marked as such in the blue box of the first figure, while the second output (0.00032288 bitcoin) remains untouched.

### C. *Custody of Bitcoin in a Pooled Address*

Our example above shows that it is possible to: (1) prove that bitcoins do not commingle; (2) individualise each on-chain transaction and value assigned to it; and (3) show proof that the deposited bitcoins have not been spent and remain on the blockchain address of the crypto-custodian, provided this is indeed the case. However, most crypto-custodians do not commit not to spend any specific unspent transaction output received from its customers. Instead, the crypto-custodian only commits to maintain the total value of all coins or unspent transaction outputs received from its customers and, once the customer in question requests a transfer of bitcoins, the crypto-custodian has contracted to be at liberty to use transactions outputs resulting from one or more other customers as input for that transfer.

Chances are high that when a customer clicks on his transaction as listed in the crypto-custodian's bitcoin address, he will see that the crypto-custodian's wallet has already transferred that customer's bitcoins to someone else's bitcoin address.

This may be a result of another customer requesting the crypto-custodian to transfer bitcoins and happens for two reasons. First, the wallet used by the crypto-custodian chooses randomly or arbitrarily which unspent transaction outputs are used as inputs for new transactions (see Section II.B. above). Second, the crypto-custodian could have programmed the wallet so that when a customer requests that his bitcoins are transferred, the wallet selects which unspent transaction outputs are used for this transfer in such a way that transaction costs are minimised. In any of these two cases, it is highly likely that the unspent transaction output originally allocated to one customer will be used for the benefit of another customer.

As a result, the customer will see on the public blockchain that his unspent transaction output was used as input for another transaction involving a third party, but if that third party address, like many addresses, cannot be linked to a specific person, the customer cannot assert any property claim against that third party from a practical point of view. Even if this would practically be possible, the third party would probably have acquired bitcoins in good faith. Under various (if not all) systems of private law,[141] the third party would therefore be protected against competing claims and the bitcoins in question would be deemed part of that third party's estate (rather than that of the concerned customer). As another consequence of the transfer(s) just discussed, the customer may request retrieval of his bitcoin from the crypto-custodian, but the crypto-custodian can only deliver other bitcoins of equal value as those deposited. Because the claim for retrieval does not concern the very same specific assets as those deposited, most jurisdictions qualify such a claim as a contractual one. Consequently, it will probably rank *pari passu* with the other unsecured claims of other creditors of the crypto-custodian.

In the unlikely situation, however, that a customer can prove that his bitcoins have remained unspent, he may successfully assert a revendication claim against his crypto-custodian. Where (physical) securities are held in custody such as in the Teixeira de Mattos case, investors cannot successfully revendicate, because their certificates commingle in the bank's vault. Where cryptocurrency such as bitcoin are held in crypto-custody, the cryptocurrency does not so commingle. With bitcoin, a crypto-investor does not provide his public and private keypair to *his* account to the crypto-custodian so that the crypto-custodian can access or control the bitcoins in that account. Instead, bitcoins are transferred from the customer's account (to which the customer's private and public keypair provides access) to the crypto-custodian's address (to which the crypto-custodian's public and private keypair provides access). Moreover, not even the same bitcoins are acquired by the crypto-custodian as were disposed by the customer. As shown in Section II.B. above, the customer's bitcoins used in the transfer are re-minted as new bitcoins (as bitcoins are destroyed and new bitcoins are created) or, put differently, the transaction output sent by the customer differs from that received by the crypto-custodian. Thus, in essence, the crypto-custodian does not hold in custody the same bitcoins sent by the customer, but different ones. This means that the Teixeira de Mattos case does not apply to bitcoin, for two reasons. First, the bitcoins (or transaction output) that the crypto-custodian

---

[141] *Eg DCC*, *supra* note 115, art 3:88; *Civil Code of the Russian Federation 1994,* art 302; *Uniform Commercial Code* ("UCC") § 2-403 (1952); *Bürgerliches Gesetzbuch 1896*, § 933. A Schwartz & R Scott, "Rethinking the Laws of Good Faith Purchase" (2011) 111 Colum L Rev 1332.

holds in custody are not the same ones as the ones provided by the customer. Second, both customer and crypto-custodian intended that the customer's bitcoins be held in custody for the customer, and although the bitcoins have changed "in transit" (been reminted), these bitcoins remain distinguishable as originating from the customer because of the blockchain. This is due to inherent traceability of blockchain transaction records.

Let us now apply the two property law qualifications of bitcoins discussed above, in Section VI.A. First, we consider crypto-custody if (rights to) bitcoins are qualified as absolute rights and the bitcoins received by a crypto-custodian are deemed to be held in custody by the crypto-custodian for the customer. The *DCC* articles regarding possession apply both to tangible goods and to absolute and relative rights.[142] As long as bitcoins originating from the customer remain unspent, the crypto-custodian will therefore be assumed to be the owner of (the rights to) these bitcoins, but the customer should be able to provide the required counterproof that the bitcoins are in his indirect possession and that the crypto-custodian holds them on his behalf. By providing such counterproof, the customer can successfully exercise property rights (*ie* absolute rights) against the crypto-custodian with respect to the bitcoins held in custody for him. Again, this assumes those bitcoins are unspent.

If rights to bitcoins are considered to be embodied in a documentary intangible consisting of the physical carrier of the wallet containing the public and private keypair, the following applies. As explained above, when the customer transfers bitcoins to the crypto-custodian, he does not provide to the crypto-custodian his documentary intangible, *ie* the physical carrier (paper, smartphone or computer) containing the wallet in which the public and private keypair of the blockchain address is stored. Instead, he transfers his bitcoins to the crypto-custodian's bitcoin address by exercising his bitcoin rights (see Figure 3 above) against the miners and nodes as a consequence of which they provide their validation and verification activities in order to effectuate the transfer in the manner described above. Here, the documentary intangible qualification becomes problematic. The customer's documentary intangible embodying the customer's bitcoin rights will be very different from the crypto-custodian's documentary intangible embodying the crypto-custodian's bitcoin rights, if only because the crypto-custodian holds a public and private keypair to his omnibus account containing a lot of bitcoins that originate not only from this transfer, but also many other customers. A solution could be to consider the crypto-custodian's documentary intangible as something similar to a Delivery Order ("D/O"). A D/O has been created in international transport to allow for bills of lading with respect to a large shipment of bulk goods to be split into various documentary intangibles each embodying rights with respect to parts of that large shipment.[143] Following this line of reasoning, the crypto-custodian's documentary intangible may be considered to issue a D/O-type document to each customer (evidenced by his username/password combination) each time a customer transfers bitcoins to the crypto-custodian's omnibus account. The relationship between the customer and the crypto-custodian would thus be governed by a D/O-type arrangement, whereas

---

[142] SE Bartels & AIM van Mierlo (m m v H D Ploeger), *Mr C Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht 3 Vermogensrecht algemeen Deel IV Algemeen goederenrecht* (Deventer: Kluwer, 2013) at 105.

[143] Zwitser, *supra* note 128 at 53.

the relationship between the crypto-custodian on the one hand and the miners and nodes on the other be governed by a documentary intangible type of arrangement.

In all, the qualification of (rights in) bitcoin as documentary intangible has its advantages when having to explain how the miners and nodes effectuate a transfer when presented with the correct public and private keypair, regardless of whether they are presented by the rightful owner. However, the documentary intangible qualification is difficult to fit crypto-custody relationships and accords badly with the private international law analysis of Section V.C, where it was argued that physical carriers embodying credentials would make an unsuitable connecting factor. Nonetheless, when applied as explained above, *ie* on the basis of a D/O-type arrangement, the qualification as documentary intangible leads to the same results under property law as the absolute right qualification, *viz* the bitcoins are presumed to be owned by the crypto-custodian (as he holds the public and private keypair), but the customer will be successful in providing counterproof by showing which exact bitcoins or unspent transactions outputs are held in custody for him. Perhaps surprisingly, similar results are therefore achieved when applying either type of property law qualification.

### D. *Custody of Bitcoin in a Segregated Address*

From the previous Section, it follows that transferring bitcoins to a crypto-custodian's pooled account exposes the crypto-investor to legal risk, as the crypto-custodian may (and probably will) spend those bitcoins. It is therefore in the crypto-investor's interest to agree with a crypto-custodian that he keeps his customers' bitcoins in separate, segregated blockchain addresses and does not spend them but at the request of the customer. This means that the crypto-custodian uses separate blockchain addresses for each crypto-investor and keeps the associated public and private keys separate on their behalf.

From a legal point of view, custody of bitcoin in a segregated address is not different from custody in a pooled or omnibus address as discussed in the previous paragraph. In both cases, as soon as the crypto-investor transfers his bitcoins to the crypto-custodian's bitcoin address, the crypto-investor's ability to directly access and dispose of those bitcoins is replaced with the crypto-investor's ability to indirectly access and dispose of those bitcoins (by using credentials provided by the crypto-custodian to log onto the crypto-custodian's website in order to have the crypto-custodian dispose of the bitcoins now held by him). With segregated address custody, however, chances are lower that the crypto-custodian spends customer's bitcoins as a result of which the customer is left with a contractual (rather than not a property law) claim against the crypto-custodian, should the latter be unable to transfer bitcoins with a value equal to those deposited.

## VII. Conclusions and Recommendations

The founding fathers of cryptocurrencies wished to free value transfers from the interference of governments, banks, brokers and other intermediaries. It was the control by, and frequent failure of such intermediaries, as well as the high transaction costs arising from their involvement that created a fertile environment for Bitcoin's

origins. In reality, however, disintermediation has not occurred. A large number of bitcoins and other cryptocurrencies are stored with crypto-exchanges. While such custody may be attractive because it is (usually) free of charge and user-friendly, it creates significant risks related to the possible insolvency of crypto-custodians.

In this article we have shown that clear and generally accepted rules to deal with legal risks arising from the insolvency of crypto-custodians are currently absent. Rights of customers in insolvency proceedings ultimately depend on the applicable insolvency and property laws. Determination of the applicable law is, however, complicated by a lack of harmonised private international law rules that are appropriate for the specific nature of cryptocurrencies and the relations between crypto-investors and crypto-custodians. On the one hand, existing rules of private international law can, with some modifications, be applied to a crypto-investor's claim for retrieval of 'his' bitcoin against an insolvent crypto-custodian. As shown in Section IV above, however, this exercise is highly complex and riddled with uncertainties. One of the most critical uncertainties in this regard is whether a crypto-investor's claim for retrieval is qualified as contractual or proprietary in nature. Yet as the cases of MtGox and BitGrail have shown, this qualification has significant legal consequences. Moreover, if a crypto-investor's claim for retrieval would be qualified as proprietary in nature, no appropriate conflict of laws rule is currently available. We therefore advocated an amended version of the *Hague Securities Convention*.

From a substantive law perspective, a proprietary claim for retrieval of bitcoin from an insolvent crypto-custodian means a claim for revendication of the stored (deposited) bitcoins based on an ownership title. A contractual claim would boil down to the return of the monetary value equal to the value of the deposited cryptocurrency. However, the property and insolvency laws of many jurisdictions will treat such a contractual claim *pari passu* with other unsecured claims, as the MtGox and BitGrail cases illustrate. In both cases, the courts refused revendication claims, whether on the basis that bitcoin cannot be the object of ownership (MtGox) or due to the commingling of deposited crypto-assets (BitGrail). Under Dutch law, the result may have been different, provided that the customer would have succeeded in proving that the individualised bitcoins deposited with a crypto-custodian were not spent or re-used, *ie* transferred to third parties. From a practical point of view, the risks that a crypto-custodian spends or re-uses clients' bitcoins are greater if a crypto-custodian keeps bitcoins in an omnibus or pooled blockchain address, rather than on separate blockchain addresses.

With this background, and taking into account the technical characteristics of bitcoin, several recommendations can be made. These recommendations may be addressed to crypto-investors, crypto-custodians and regulators. First, customers of crypto-custodians should be informed whether the crypto-custodian uses or may use the deposited bitcoins. This usually happens where the exchange operates through and stores customers' assets on its own omnibus blockchain address. Examples of this model are Coinbase, Wirex, OKEx. When deposited bitcoins are re-used, the possibility of revendication may be blocked and customers effectively lose their property rights, the terms of conditions of the crypto-custodian stating otherwise notwithstanding. This is especially problematic in a situation of crypto-custodian insolvency. This risk should be explicitly conveyed to customers via a user agreement. In this context, inspiration may be drawn from Article 15 of the *Securities*

*Financing Transactions Regulation*.[144] Under this regulation, the reuse of financial instruments is subject to at least two conditions: (1) appropriate information of the party providing financial instruments (providing counterparty); and (2) prior express consent in writing given by such a party. Regulation of reuse by crypto-custodians could be drafted along the same requirements.

Second, a customer's claim for retrieval of their bitcoin against an insolvent crypto-custodian can be qualified as either contractual or proprietary in nature. As the consequences of this qualification are critical from the customer's protection perspective, harmonisation of the nature of this claim is warranted. Also, clarification and harmonisation of private international law rules applicable to such claims are needed. Traditional connecting factors, such as *lex rei sitae* or the location of a physical carrier or an account are ill-suited for blockchain transactions and cryptocurrencies in general. To ensure predictability, the adoption of an approach similar to that of the *Hague Securities Convention* should be considered. This would give priority to the contractually agreed law, with the fall-back option of applying the law of the crypto-custodian's place of incorporation. Both of these connecting factors are easily verifiable by the relevant parties involved, and thus should guarantee legal certainty and predictability.

Third, in order to protect (retail) crypto-investors against the risk of crypto-custodian insolvency, it could be considered to prohibit or limit the re-use of the assets deposited. Inspiration for this type of regulation can be drawn from Article 16(8) of the *Markets in Financial Instruments Directive*,[145] which prescribes that when holding financial instruments belonging to clients,[146] an investment firm shall "make adequate arrangements so as to safeguard the ownership rights of clients, especially in the event of . . . insolvency, and to prevent the use of a client's financial instruments on own account except with the client's express consent." For this reason, it is advisable to prohibit a crypto-custodian to transfer, sell, pledge or otherwise dispose of, alienate or encumber customers' crypto-assets, unless upon explicit approval from a crypto-investor.[147] In practice, the risk that such prohibition is violated can be diminished if the deposited bitcoins are stored in segregated (separate) blockchain addresses rather than in omnibus or pooled addresses. It therefore makes sense to consider prescribing that crypto-custodians to store bitcoins in segregated accounts and perhaps in some cases prohibit them from storing them in omnibus addresses. However, customers should also be protected if the crypto-custodian fails to comply with these regulatory requirements. This means that customers should be granted a form of priority right by means of property and insolvency law with respect to their cryptocurrency.

---

144 EC, *Regulation (EU) 2015/2365 of the European Parliament and of the Council of 25 November 2015 on transparency of securities financing transactions and of reuse and amending Regulation (EU) No 648/2012*, [2015] OJ, L 337 [*Securities Financing Transactions Regulation*].

145 EC, *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast)*, [2014] OJ, L 173 [*MiFID II*].

146 It is likely that bitcoins and other pure payment-type crypto-assets do not qualify as financial instruments under *MiFID II*, *ibid*. See ESMA Advice, *supra* note 16, at para 80.

147 In a similar vein, the Securities Financial Transactions Regulation establishes that any right of counterparties to reuse financial instruments received as collateral shall be subject to proper informing obligations and prior express consent by the collateral provider. See *Securities Financing Transactions Regulation, supra* note 144, art 15.