CHAPTER 16

The Law Governing Secured Transactions in Digital Assets

Matthias Haentjens and Matthias Lehmann

1 Introduction: Practical Relevance and Legal Problems of Secured Transactions in Digital Assets*

Despite their relatively recent emergence, and despite the fact that many of them do not represent any "real world" asset, digital assets – such as cryptocurrencies or tokens – are becoming both increasingly valuable and increasingly common. This makes them interesting also as an object for secured transactions, which could raise (additional) value for the holder of such assets. After all, why leave your bitcoin sitting idly on a USB key, when it could be used as collateral for a loan or other financial transactions?

The use of digital assets as collateral is especially relevant in light of the current scarcity of other assets that can be used as collateral, whether financial or non-financial. This scarcity is due to a number of different causes. Foremost among them are the COVID-19 pandemic and more recently the war in Ukraine, which have caused an economic slowdown; have limited the circulation of money, securities as well as commodities; and, have destroyed valuable assets. Central banks upped the ante by throwing cash into the financial markets – partly in a reaction to the pandemic – , with the consequential spiralling of asset prices. In addition, regulatory developments have contributed to the 'collateral crunch', such as the stricter capital requirements for banks under the latest Basel regime and the mandatory central clearing requirement for important categories of derivatives, which all require additional collateral.

Digital assets may at least partly cover this shortfall as it may be argued that they are particularly well suited to serve as collateral in secured transactions. This has to do with some of their properties: first, the technological infrastructure for digital assets, *i.e.* Distributed Ledger Technology (DLT) or blockchain has been specifically designed to minimise the risk of fraud, as DLT aims to avoid double spending by making transactions irreversible through the combined use of a network validation mechanism and cryptographic methods,

* Many thanks to Emeric Prévost for his help and useful comments on the manuscript.

which create an immutable record.[1] Second, the transfer of digital assets is relatively straightforward; as a matter of fact, Bitcoin – the first fully decentralised blockchain – was conceived as a global peer-to-peer transfer mechanism on which value was supposed to be transferred from one party to another without the need for any intermediary. Third, the value of most digital assets can be easily determined as the current price is published regularly, similarly to share or bond prices, in various media and can be gleaned from offers by crypto exchanges. Since the euphoria of the first years, all three properties just discussed must be nuanced: first, over the last years, several digital assets, networks, and crypto-exchanges have been the victims of serious hacks which cost investors a fortune; second, a transfer of bitcoins nowadays takes a long time to settle because validation on the blockchain has become increasingly difficult and expensive, which is one of the reasons why most investors now use intermediaries such as crypto-exchanges and wallet providers to transfer their digital assets; and third, the value of most digital assets has proven to be extremely volatile. Nonetheless, digital assets are still considered to be well suited to serve as collateral in secured transactions, especially because of their spectacular growth.

Consequently, it is anything but surprising that the interest in transactions secured by digital assets has soared. A striking example is provided by the first Bitcoin-backed loan, which was recently offered for the first time in history.[2] Goldman Sachs granted opened a lending facility in fiat currency for the borrower, who secured it with Bitcoin as collateral. The bank stated that it was particularly attracted by the opportunity for 24-7-365 day risk management.[3] The same possibility was also raised in the debate about crypto derivatives clearing and settlement, which was ignited by FTX-owner and billionaire Sam Bankman-Fried.[4] One of the main arguments for such a revolutionary approach to derivatives clearing and settlement is the possibility of managing collateral in real time.[5]

[1] See Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 26 May 2022.

[2] Shashank Bhardwaj, "Goldman Sachs rolls out first bitcoin-backed loan" (*Forbes*) <https://www.forbesindia.com/article/crypto-made-easy/goldman-sachs-rolls-out-first-bitcoin backed-loan/75833/1> accessed 31 May 2022.

[3] *Id.*

[4] Javier Paz, "FTX CEO Sam Bankman-Fried To Defend His Disruptive Plan For Crypto Derivatives In Front Of Congress" (*Forbes*, 12 May 2022) <https://www.forbes.com/sites/javierpaz/2022/05/12/ftx-ceo-sam-bankman-fried-to-defend-his-disruptive-plan-for-crypto-derivatives-in-front-of-congress/?sh=78b88e9c42a6>.

[5] *Id.*

A further illustration is a complex project dubbed "Security Tokens Refinancing" carried out by the company *Forges*, a subsidiary of the French bank *Société Générale*.[6] According to media reports, the company plans to issue "security tokens" backed by mortgages to the tune of US$ 40 million, which will be used as collateral for a loan of the stablecoin DAI worth US$ 20 million. The lender here will not be a traditional financial intermediary, but MakerDAO, the decentralised finance (defi) protocol. Importantly for present purposes, the "security tokens" will be deposited with a security agent. The structure of the operation is quite complex and involves in total no less than six entities.

There are also very simple forms of collateral arrangements. A most basic version is described in Satoshi Nakamoto's initial white paper itself: when discussing sales transactions, he contends that "routine escrow mechanisms could easily be implemented to protect buyers," after having hailed the virtues of bitcoin transfers for sellers.[7] This would mean holding back or reserving title in the bitcoins sold until the seller's performance. The fact that Nakamoto uses a legal term ("escrow") is quite revealing because it demonstrates the continuing importance of the law even in the highly technological context of Bitcoin, which is normally a no-go for crypto aficionados. Although legally to be distinguished from the creation of a security rights in certain assets, reservation of title and escrow accounts are time-honoured methods of securing the performance of a debtor.

Since Nakamoto's white paper, secured transactions have taken on a wholly different function in the context of new and innovative operations on the blockchain. A first example of this is "staking." Staking plays an important role in "proof of stake" mechanisms, which increasingly replace "proof of work" mechanisms. Both serve to shield the verification of blocks, or mining, against the risk of manipulations by a malevolent node, *i.e.* an ill-intentioned participant in the blockchain. As is well-known, "proof of work" mechanisms means that mining nodes compete against each other until one miner or mining pool comes out as the first to solve the "hashing" algorithmic riddle[8] that allows for the addition of a new block of transactions to the chain; since this requires considerable computing power and energy, it would be too cumbersome to do this effort for a malevolent node on a large scale. The proof of work mechanism

[6] See Florent D, "La Société Générale fait une proposition à MakerDAO" (*Cryptoast*, 2 October 2021) <https://cryptoast.fr/societe-generale-collaboration-historique-defi-makerdao/>.

[7] Nakamoto (n 1), 1.

[8] Simply put, "hashing" refers to the algorithmic process of randomly converting an arbitrary amount of data bytes input into a fixed amount of encrypted data output (generally represented on a hexadecimal (hex) base). For instance, Bitcoin uses the SHA-256 hash algorithm.

has fallen out of favour, though, because of its high-energy consumption. In proof of stake mechanisms, it is no longer necessary to solve a mathematical riddle in the validation/mining process, but nodes evidence their serious intentions by the stake they have in the network, in particular through the digital assets they own. To acquire more of these assets, and to be able to do more mining, some nodes simply offer other users a participation in the profits they make from using their digital assets. Staking thus means the use of one's assets for this purpose. In this process, the relevant assets will be blocked, frozen, or locked up, depending on the particular network. It does not seem far-fetched to compare the operation of staking with placing assets in escrow to secure the performance of an obligation, and therefore with a secured transaction, the conditions of which vary with the network in question.

Another example of an innovative blockchain operation in which secured transactions may play a role is "yield farming." This operation is relevant in the context of Decentralised Finance, or "DeFi." It consists in the lending of digital assets to a DeFi platform, *e.g.*, a decentralised exchange (Dex), which will use it as liquidity for its pool. The lender receives in return a portion of the platform's fees and return. Yield farming may involve an outright transfer, with a later right of return, similar to a repurchase (repo) transaction. But where the digital assets are merely locked up or "bonded," it may as well be assimilated to a secured transaction: the platform acquires a secured right in customer's asset(s).

Because of the operations just explained, but also because of the current scarcity of other categories of assets that can be used as financial collateral as discussed earlier, it is to be expected that the use of digital assets as collateral is going to rise in the years to come. This raises a number of legal questions. Among the most salient is that of the applicable law: which legal system governs a secured transaction in digital assets? And, more precisely: which law determines the requirements for the validity and the effects of security rights in digital assets?

The need to answer those questions cannot be negated by the slogan "code is law." This slogan was originally coined by Lawrence Lessig to demonstrate the need to regulate the internet,[9] but is often abused for precisely the opposite purpose, *viz.* for denying the need for law and legal regulation of the internet in general and of the blockchain in particular. Notwithstanding the claims

[9] Lawrence Lessig, "Code Is Law" (*Harvard Magazine*, 1 January 2000) <https://www.harvardmagazine.com/2000/01/code-is-law-html> accessed 20 March 2022; see also Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (2nd edn, Basic Books 2006).

of some radical believers in the autonomy of the blockchain, digital assets are and will always be subject to the law and legal rules. Moreover, digital assets need law.

First, there are legal constructs and mechanisms that even the most autonomous DLT cannot code around. For instance, when the world's then leading bitcoin exchange Mount Gox was declared bankrupt in 2014, no code could have prevented the Tokyo District Court to assert jurisdiction and decide how the digital assets and their proceeds connected with the exchange should be distributed amongst creditors.

Moreover, even the staunchest believers in DLT and blockchain claim that investors in digital assets have "ownership" of those assets. Nakamoto, in his 9-page white paper, for instance, uses "own" and "ownership" of bitcoin and its keys 25 times. Ownership is a legal term deeply rooted in history which is, has been, and will be used to protect those who claim entitlement to assets. Therefore, digital assets also need (the application of) this doctrine. More generally, and as a matter of principle, digital assets need the application of proprietary rights, which are generally believed to provide certainty and predictability because they have effects against everybody, or *erga omnes*.

Law and legal rules more or less rigidly regulate proprietary rights, precisely because of their *erga omnes* effects. One of the first questions that the court had to decide when Mount Gox was declared insolvent, for instance, was whether the investors had proprietary rights in the digital assets under Japanese law, a question that was ultimately denied by the Tokyo District Court.[10]

The need for law and legal rules is even stronger with regard to security rights as a sub-set of proprietary rights. The *raison d'être* of security rights is to secure the position of the creditor and minimise its counterparty risk; a security right that would not provide certainty and predictability of protection against the debtor and its other creditors would be futile. While it is true that technology can factually provide the creditor with the possibility to dispose of an asset or block transfers that would endanger his rights, this is not always sufficient to safeguard his position. For instance, the need for legal help arises where the blockchain is hacked and the assets that serve as collateral have been stolen. Similarly, other creditors, with equally or stronger technological capabilities,

[10] Tokyo District Court, Reference number 25541521, Case claiming the bitcoin transfer, etc., Heisei 26 (Year of 2014), (Wa) 33320, Judgment of Civil Division 28 of 5th August 2015; English translation by Megumi Hara, Charles Mooney and Louise Gullifer, available at <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf> accessed 26 May 2022.

may compete for the same asset. Thus, (also) digital assets need law to prevent the technologically strongest from prevailing.

In the following, we will first examine whether the law governing the requirements for the validity and effects of security rights in digital assets deserves a specific rule, or whether the same rule can be used as that which determines the law governing the relevant network (2). As a matter of principle, we believe the first assertion is correct, save for exceptional cases, such as a permissioned blockchain operated and/or supervised in a specific country only. Therefore, we will argue which law should govern security rights in digital assets independently. To do so, we draw a distinction between digital assets that are "held" by a (crypto-) custodian and those that are not. We first analyse which law should apply to digital assets that are "held" by a (crypto-) custodian (3). For digital assets that are not so "held," we determine whether security rights in digital assets can be subject to a choice of law, *i.e.* to the principle party autonomy (4.1). After that, we argue which law should apply to these digital assets in the absence of a choice (4.2). Because of the universal nature and world-wide accessibility of digital assets recorded on a blockchain, the issue of "control" plays a special role. This raises the question as to whether such control should be defined in a globally uniform way, independently of the governing law (5). Finally, we deal with the law governing remaining legal issues, such as capacity, error, fraud, succession or insolvency, which will be summarised under the catchphrase "other laws" (6).

Though our study is quite extensive, we do not strive to be comprehensive. Therefore, we will not cover all issues connected with secured transactions on the blockchain. Specifically, we will not deal with the question of which court may or should have jurisdiction with regard to disputes that may arise out of such transactions. We also do not address specific insolvency law issues, such as fraudulent transfers (of digital assets). This does not exclude that our analysis will be most helpful in the case of insolvency proceedings when the law applicable to a secured transaction needs to be determined, because such analysis has to be made independently of the law governing the insolvency, or *lex fori concursus*.[11]

Finally, whilst we do cover proprietary rights in digital assets, we do not intend to do so exhaustively. This chapter is limited to the extent that, first, we will focus on Private International Law (PIL) rather than substantive law (although matters of substantive law will be covered in section 5), and, second, we will specifically investigate the law that should apply to security rights in

[11] See, *e.g.*, Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings, [2015] OJ L 141/19 ("EU Insolvency Regulation").

digital assets. Therefore, we will not extensively discuss the law applicable to ownership. On the other hand, we do understand "secured transactions" in a broad sense, such that we intend to cover both transactions in which security rights *stricto sensu* (such as pledges, liens, hypothecs, *etc.*) are created in digital assets for the benefit of a creditor, and transactions in which (full) ownership in digital assets is transferred to a creditor for the purpose of securing a debtor's obligation(s). These latter transactions are sometimes referred to as "title transfer collateral arrangements,"[12] and are within the remit of our investigation.

2 The Independence of the Law Governing the Secured Transaction from the Law Governing the Blockchain

It is well known that the law applicable to the blockchain, as such, or to assets recorded on the blockchain, poses difficult questions of conflict of laws.[13] The blockchain is a decentralised network with nodes dispersed all over the planet. This makes it nearly impossible to localise it or otherwise find a closest or most significant connection with a single state or jurisdiction. It also seems undesirable that the law of one state, say New York law or England, should govern the entire blockchain and all the operations happening in connection with it. In sum, it does not promise much success to try to connect an inherently global and virtual phenomenon to a specific, physical, and geographically localised asset.

At this point, it is unnecessary to restate the discussion of this conundrum and the solutions that have been suggested to resolve it. Fortunately, our task is somewhat easier: we do not need to localise the blockchain as such or determine the specific asset recorded on it. Instead, we must "only" determine the law that applies to a secured transaction and to security rights vested in digital assets. This law could be the same as that governing the network and the assets recorded thereon. However, we would argue that as a matter of principle, the law governing a secured transaction and security rights vested in digital assets may be different from that governing the blockchain and the assets as such.

[12] See, *e.g.*, Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements [2002] OJ L 168/43, Art. 2(1)(b) ("Financial Collateral Directive").

[13] See the other contributions in this volume.

Such an "independence" is not new or unheard of. In reality, it has long been recognised for other assets. One case in point is that of claims or receivables: Under the UNCITRAL Convention on this topic, their assignment may be governed by a law different than that governing the original contract by which the receivable was created.[14] The UNCITRAL Model Law on Secured Transactions suggests more generally for the security right in *any* intangible asset that the law applicable is the law of the place of residence of the provider of such security.[15] Both of these international texts thus assume that the law governing a security right is independent from the law governing the asset as such.

This "principle of independence" is not absolute and does not need to apply to blockchains that are exclusively governed by the law of a specific country. The paradigm case here is a network the nodes of which are all located in the same country: in this case, it is obvious that the only connection is with this country. An example that is more likely to occur in practice is a permissioned network where a central operator is located in a specific country.[16] Networks regulated and supervised by the financial authorities of only one state are another illustration[17] wherein the closest connection of the whole network will obviously be with that state. It thus stands to reason to consider

[14] United Nations, *United Nations Convention on the Assignment of Receivables in International Trade* (New York: United Nations Publications, 2004), Art. 30 (submitting the priority of the right of an assignee to the law of the state in which the assignor is located). On this provision, see also *infra* section IV(2).

[15] UNCITRAL, "Model Law on Secured Transactions" (*United Nations*, 16 February 2017), Art. 86 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-08779_e_ebook.pdf> (submitting the creation, effectiveness against third parties and priority of a security right in an intangible asset to the law of the State in which the grantor is located). On this provision, see also *infra* section IV(2).

[16] For instance, one could think of a blockchain between multiple banks and other financial service providers that is run by one of them.

[17] See the "crypto securities register" (*Kryptowertpapierregister*) in German law, which are supervised by the German BaFin, BaFin "Kryptowertpapierliste nach eWpG" (*BaFin*, updated 24 May 2022) <https://www.bafin.de/DE/PublikationenDaten/Datenbanken/Kryptowertpapiere/kryptowertpapiere_artikel.html?nn=7845918>; see Das Gesetz zur Einführung von elektronischen Wertpapieren vom 3. Juni 2021 (BGBI. I S. 1423), sec. 11. See also the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of 19 June 2015, RS 958.1, Art 73a et seq. (requiring the operators of "DLT trading systems" (*DLT Handelssysteme*) to be registered with the Swiss FINMA).

the law of this state as governing any secured transaction with regard to assets recorded on that network.[18]

The independence of the law governing the blockchain from the secured transaction is however of vital interest in the case of permissionless blockchains, where the law applicable to the blockchain itself is notoriously difficult to determine. In fact, such an independence may more often than not be the *only* chance to determine the applicable law in a legally certain way *at all*. An example is the Bitcoin blockchain, where a law governing the whole blockchain is not identifiable.

On the other hand, the independence principle is also not without issues. First, it may result in a different law applying to the security right and the encumbered digital asset, which may be problematic *per se*. For instance, the law applying to the creation of the security right may require that for a valid creation of a security right such as a pledge, the pledgee must be the owner of the (digital) asset. Typically, however, ownership is to be determined by the law that applies to the asset itself, which may thus be a different law. Also, the law applying to the security right may not be easily foreseeable to third parties, which can be considered as problematic because security rights, as a sub-set of proprietary rights, apply *erga omnes*. Finally, the independent determination of the law governing security rights in digital assets may lead to conflicting laws following from various secured transactions related to the same digital asset, without a 'meta'-law that determines the priority between those laws. These problems are not without solutions, but they depend on the specific conflict-of-laws rule chosen to govern security rights in digital assets, and will therefore be discussed in their context below.

In sum, where it is clear that a network is governed by the law of a particular state, this law should also apply to secured transactions and the security rights vested in digital assets recorded on that network. By contrast, the following analysis will focus on situations in which a law governing the whole network is *not* clearly submitted to one law exclusively. It is only then that the law governing the secured transaction and the security rights vested in digital assets must separately be determined.

[18] Explicitly in this sense; see the German Act on the Introduction of Electronic Securities of 3 June 2021 (*Gesetz zur Einführung von elektronischen Wertpapieren*) (Federal Law Gazette I p. 1423), sec. 32.

3 Digital Assets "Held" by a Custodian

As already stated above, the blockchain was originally conceived as a mechanism for the direct, or "peer-to-peer," transfer of digital assets, but most of these assets are today held through a service provider, such as a crypto-exchange or a wallet provider. For our present purposes, we call both types of service provider, perhaps somewhat counterintuitively, a "custodian." In our view, where digital assets are "held" by a custodian, this custodian forms an indispensable link between the investor and their assets because the investor cannot dispose of its assets without the custodian's cooperation. For the purposes of determining the law that applies to the investor's proprietary rights in his digital assets, the custodian therefore forms the closest connecting factor.[19] In other words, the investor-custodian relationship must determine the law that governs the investor's proprietary rights in the digital assets in custody, because the custodian exercises factual control over those assets. Control corresponds to possession in the real world. In other words, in more than a merely metaphorical way it could be said that rights in digital assets are "located" with the custodian. Connecting the law governing an investor's proprietary rights in his digital assets to the custodian also has another advantage: it allows the investor to dispose of its entire portfolio of digital assets held with the same custodian under the same law. Otherwise, the investor and custodian may have to comply with the rules of multiple laws to transfer, or create security rights in the same digital assets portfolio. To have one law govern the entire portfolio would therefore considerably facilitate the lives of both the investor and its custodian, as the experience with intermediated securities has also demonstrated.[20]

The law of the investor-custodian relationship should thus determine the validity and effects of security rights in digital assets held through a custodian. This is true both for the situation in which the custodian itself is the security taker, and for the situation in which the security taker is a third party, such as the investor's creditor or a DeFi-Platform. In both cases, the validity and effects of security rights in digital assets should be subject to the "custody law."

Which law is this custody law that should apply to secured transactions? In this regard, the 2006 Hague Convention on Intermediated Securities

[19] Matthias Haentjens, Tycho de Graaf and Ilya Kokorin, "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them" (2020) 2 Singapore Journal of Legal Studies 526, 526–563.

[20] See, on the law applicable to intermediated securities, *e.g.*, Matthias Haentjens, *Harmonisation of Securities Law: Custody and Transfer of Securities in European Private Law Private Law* (Alphen aan den Rijn: Kluwer Law International 2007), 36–40 and the references there given.

(hereinafter, the "Hague Securities Convention")[21] is instructive. The Convention deals with securities that are held by an intermediary for a client. In practice, the vast majority of securities is uncertificated and exists only as a book-entry into a securities account, *i.e.* an electronic record. The custody of intermediated or book-entry securities is thus not entirely dissimilar to the custody of digital assets.

The Hague Securities Convention says how to determine the law of custody for intermediated securities. In its Article 4, the principle of party autonomy takes centre stage, which means that client and custodian are free to choose the law governing the proprietary rights in the securities held by the intermediary. If they have not specifically chosen a law to govern proprietary rights, these rights are governed by the law they have chosen to govern the agreement between the custodian and the client.[22] Given the similarity of the custody of book-entry securities and of digital assets, it makes sense to follow the same principle in the blockchain context. A choice for the custody agreement between investor and crypto-custodian should therefore determine the law that applies to security interests in digital assets under the control of the custodian.

However, the Hague Securities Convention restricts the choice to the law of states in which the custodian has an office that is either engaged in a business or regular activity or that is clearly identified in the securities account agreement. This restriction does not make much sense in the blockchain context, in which custodians do not have a network of offices around the world that are visited by customers, but exercise their business exclusively virtually. This is not to deny that there may be physical offices. The crypto exchange Coinbase, for instance, has a number of offices around the world. But it is unlikely that the administration of clients' accounts is done there. Rather, it is done virtually, *i.e.* on the blockchain. We believe restricting a choice of law by trying to attach it to a certain physical presence will unnecessarily complicate matters, give rise to legal arguments and thus increase legal uncertainty. As a matter of principle, the existence of an office should therefore not limit the possibility of choice of law and parties should be free to choose any law.

If no law has been chosen, the Hague Securities Convention refers to the office of the intermediary that has been specified in the account agreement.[23] Because crypto-custodians do not typically have widespread brick-and-mortar

[21] The Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary of 5 July 2006 ("Hague Securities Convention").

[22] *Id.* at Art. 4(1).

[23] *Id.* at Art. 5(1).

presence, such an office will only rarely exercise specific tasks on the blockchain. Even where they have offices, it is unlikely that these offices will perform any administrative tasks regarding the digital assets held for investors, because this is commonly done virtually, *i.e.* on the blockchain. Yet there are exceptions. For instance, the website blockchain.com separates customers according to their country of residence and the services provided, and assigns them to different country offices.[24] This may well indicate an implicit choice of law.

Failing a choice of law or a specified office, the Hague Securities Convention refers to the law under which the intermediary is incorporated or organised or has its principal place of business.[25] Even though a crypto-custodian may not have an office, it must have a state of incorporation, so that this connection factor may also work in the context of digital assets. In particular, a crypto-custodian such as a wallet provider or crypto-exchange will virtually always be incorporated under the law of some jurisdiction, and may also have a principal place of business. For instance, Coinbase Global Inc. is incorporated under the law of Delaware, notwithstanding the fact that the company hails itself as having become a "remote-first company."[26]

What if these connecting factors fail, *i.e.* if no choice has been made and the crypto-custodian's place of incorporation or principal business cannot be determined? In this case, it seems impossible to identify the governing law by reference to the custody agreement or the custodian, and other connecting factors must be sought. These will most likely be the same as those used for digital assets that are not controlled by a custodian, which is the topic of the next section.

4 Custody-Free Digital Assets

Where assets are not controlled by a custodian, one must use other connecting factors. This applies to digital assets directly held on the blockchain, and the private key of which is stored on a computer, on an external hard disk or flash

[24] See "Blockchain.com User Agreement" <https://www.blockchain.com/legal/terms> accessed 8 April 2022.

[25] See the Hague Securities Convention (n 21), Art. 5(2) (submitting intermediated securities to the law under which the intermediary is incorporated or otherwise organised, or, failing such incorporation or organisation, to the law of its principal place of business).

[26] See Coinbase Global Inc., "Registration Statement under the Securities Act 1933 with the SEC" (*SEC*, 25 February 2021) <https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm>.

drive. The same is true when the custody law cannot be identified, because no law has been chosen and the place of incorporation or principal place of business of the custodian cannot be determined.

4.1 *Choice of the Applicable Law?*

Secured transactions are often embodied in a formalised agreement. Such an agreement may contain a choice of the applicable law and the competent court. This is also true for the many "staking agreements," as discussed above. An example is the "Nomination Agreement" by Pure Stake, which provides under the title "Governing Law; Dispute Resolution" the following *inter alia*:

> This Agreement shall be interpreted, construed and enforced in accordance with the internal laws of the Commonwealth of Massachusetts, without regard to its conflict of laws principles.[27]

As already implied above (see *supra* section III), most PIL regimes will honour party autonomy here, *i.e.* the choice that parties have made to govern their secured transaction. More specifically, it seems virtually uncontested that party autonomy is to be allowed when it comes to contractual aspects, *i.e.* the *inter partes* aspects, of such secured transaction. These *inter partes* aspects include the interpretation of the contract, what constitutes default, *etc.*[28] Party autonomy is even allowed where the contract forms the basis for the creation of security rights. Thus, the fact that property law in most jurisdictions is largely mandatory law and applies notwithstanding any contractual arrangements, does not exclude the application of the principle of party autonomy to the contractual aspects of secured transactions, except in situations that are exclusively connected to one country.[29] The contractual rights and obligations

[27] See PureStake, "Nomination Agreement" (*PureStake* 22 October 2019), No 21 <https://www.purestake.com/staking-agreement/>.

[28] But see, *e.g.*, Katharina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton: Princeton University Press 2019) who is highly critical of party autonomy where it concerns PIL, especially in the context of corporate and property law.

[29] See sec. 187(2) Restatement (Second) Conflict of Laws (allowing the parties, safe for some exceptions, to choose the law to govern their contractual rights and duties "even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue"), 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 L 177/6, Art. 3(3) ("Rome I Regulation") (providing that a choice of the parties shall not prejudice the application of mandatory rules where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen). See also United Nations, *United*

under a secured transaction, *i.e.* the *inter partes* aspects, are thus to be determined by the chosen law.[30]

A trickier question is whether party autonomy is also to be allowed when it comes to the proprietary aspects of the transaction, *i.e.* the *erga omnes* aspects. These *erga omnes* aspects include the creation and perfection of security rights, and the priority between proprietary rights. Serious objections seem to militate against this possibility. It could violate, first, the principle of *privity of contract*, according to which an agreement between two parties cannot have effects against third parties who were not taking part in the agreement.[31] Second, the choice made is not always easily identifiable for third parties, who would have to rely on the allegations of the parties to the contract.[32] Third, the possibility of choice could open up avenues for fraudulent manipulation. For instance, the parties to a secured transaction could choose a law that backdates the finality of the transferor in order to disenfranchise a transferee of an earlier transaction.

Against all these objections, equally valid counter arguments could be formulated: first, privity of contract is not absolute, and even in contract law, it is generally acknowledged that contracts may have legal consequences for third parties, who may thus either rely on those contracts or (unjustifiably) suffer from them. Second, in several instances, contractual agreements with third party effects are also not considered problematic in other situations, provided it is not impossible that they become identifiable, for instance by court order or attachment. An example would be the situation described above, *i.e.* when third parties try to acquire or seize specific digital assets, and have to learn

Nations Convention on the Assignment of Receivables in International Trade (New York: United Nations Publications 2001), Art. 30(2) (clarifying that mandatory of the law of the forum or another state may not prevent the application of the law of the state in which the assignor is located).

[30] See UNCITRAL (n 15), Art. 84 (allowing a choice of law for "the mutual rights and obligations of the grantor and the secured creditor arising from their security agreement"). See also Swiss Federal Act on Private International Law (PILA) of 18 December 1987, SR 291, AS 1988 1776, Art. 105 (subjecting the pledging of claims, securities and other rights to the law chosen by the parties, with the explicit proviso that the choice cannot be asserted against third parties).

[31] On privity of contract, see *e.g.*, Ewan McKendrick, *Contract Law* (10th edn, Oxford University Press 2022); Chris Turner, *Contract Law* (2nd edn, Hodder Education Group 2007), 48 et seq.

[32] Eva-Maria Kieninger, "Freedom of Choice of Law in the Law of Property?" (2018) 7 European Property Law Journal 221 (arguing against choice of law in property law in general); Harry C. Sigman and Eva-Maria Kieninger, "The Law of Assignment of Receivables: In Flux, Still Uncertain, Still Non-Uniform," in Harry C. Sigman and Eva-Maria Kieninger (eds.)*, Cross-border Security Over Receivables* (Sellier European Law Publishers 2009).

through attachment order with which custodian these assets are held. Third, possibilities of fraud are always present, and should not determine our preference of one rule over another. For instance, fraud is equally possible – and sometimes to much greater negative effects – where it regards the contractual aspects of transactions. Moreover, manipulations of the applicable law can, as always, be countered with the exception of fraud, which also applies in conflicts of laws (see in that sense the concept of *fraude à la loi*).[33]

Be this as it may, many PIL regimes are reluctant to allow party autonomy for proprietary aspects, although prominent exceptions exist.[34] However, the blockchain environment, because of its technical nature, may require a solution that derogates from the traditional views just summarised. For instance, the residence of the transferor at the time of the transfer may be even more difficult to identify than the law to which the parties have subjected their agreement. To exclude the uncertainty connected to the location of the transferor, the transferee in a secured transaction may want to choose the applicable law or fix the location by agreement. This seems legitimate from the perspectives of legal certainty and predictability, which, as already stated above, should be the leading principles in the context of proprietary rights. The same considerations informed the drafters of the Hague Intermediated Securities Convention, as it allows, with certain limits, to choose both the applicable law to proprietary rights and the location of the intermediary (see *supra* section 3). The interests of third parties can then be protected by requiring sufficient evidence about such a choice, *e.g.* that it must be made in writing or in electronic form. They may further be safeguarded by a universal requirement that the transferor must lose "control" over the digital assets as a result of the secured transaction (see in more detail *infra* section 5).

In sum, we argue that the choice of law of the parties should govern not only the contractual aspects of the secured transaction (*i.e.* the *inter partes* aspects), but also the proprietary aspects (*i.e.* the *erga omnes* aspects). According to many, the law that applies to a blockchain as a whole can also be chosen,

[33] On this, see *e.g.*, Bernard Audit and Louis d'Avout, *Droit International Privé* (8th edn, L.G.D.J. 2018), 269 et seq.

[34] See Kieninger (n 32). See also European Law Institute, "EU Principles on the Use of Digital Assets as Security" (*ELI*, February 2022), footnote 44 <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> (arguing that "allowing the parties to a security agreement to choose the law applicable to third-party relations … would be inconsistent with some of the basic tenets of property "aw"). See Uniform Commercial Code (UCC) Article 8 and the Hague Securities Convention (n 21), as well as the Dutch Civil Code Art. 10:135 (Debt-claim to name) which regards the property law aspects of assignment of claims.

for instance in terms and conditions downloaded with the blockchain software and accepted by the user (node).[35] How do these types of choices relate to each other? According to the principle of independence discussed above (see *supra* section 2), the law applicable to the chain and to the secured transaction must not necessarily be the same. Nevertheless, where a law governing the blockchain has been explicitly chosen, such choice will usually have been intended to cover all operations on this chain. It seems difficult to imagine, or at least highly impractical if such a choice would leave the parties the freedom to agree to another law for an individual transfer or creation of security interests. In other words, we would argue that by accepting the terms of the blockchain, the parties also accept the predominance of the choice of law clause in it, including where it regards the requirements for validity and effects of security rights in digital assets recorded on that same blockchain.

A choice of law of the blockchain as a whole will thus most of the time exclude a different choice for an individual secured transaction. However, this predominance of the choice of law for the blockchain over the choice of law for the secured transaction is not absolute. Should coders of the blockchain or drafters of its terms and conditions wish to leave the choice of the law applicable to secured transactions to the parties of such transactions, there is no reasonable ground to deny this possibility. In the end, determining whether a separate choice of law is possible for secured transactions is thus a matter of interpretation of the choice-of-law clause for the blockchain as a whole.

4.2 *Law Applicable in the Absence of a Choice*

When digital assets are not "held" in custody and the parties have not chosen the law applicable to a secured transaction, there is no significant connection of the transaction as such to the law of a country. Instead, the governing law can only be found via the location of the parties involved, unless international principles of substantive law can be relied on. Absent such principles, and for want of a better connecting factor, one must necessarily refer to the location of one of the parties, if the digital assets are held on a permissionless blockchain and no choice of law has been made for the blockchain as a whole or the secured transaction specifically. The same is true where the law applicable to custody cannot be determined (see *supra* section 3).

The relevant parties in a secured transaction are: (1) the security provider; and (2) the security taker. Should we have to choose between the location of

[35] See Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019).

either one of those parties, the location of the security provider seems to be preferable. A first reason is that the security provider is necessarily only one person, whereas it is not to be excluded that different persons in different jurisdictions may allege to be security takers and that a single law is needed to decide between those competing claims (see *supra* section 2). When there is a dispute over who acquired the better (security) right, the security provider is thus a more appropriate criterion than the security taker. Moreover, in a blockchain context, the identity or location of the security taker is often not known. For example, assets that are staked to a DeFi platform: it may be very difficult if not impossible to identify the place of incorporation or business of such a platform, its operator or coder. In contrast, it will be much easier to identify the customer of such a platform. In fulfilling the Know-Your-Customer duties, the platform or the crypto service provider that acts as its agent would need to inquire not only about the identity but also about the place of residence of the customer/security provider.

Additional arguments for the security provider's location as a connecting factor can be found in several texts of uniform law. For instance, the UN Convention on the Assignment on Receivables refers to the location of the assignor to determine the law governing priority rights.[36] The same connecting factor can be found in the Proposal for an EU Regulation on the law applicable to third-party effects of assignment.[37] If the assignment is done in the context of a secured transaction, the assignor is in effect the security provider. The UNCITRAL Model Law on Secured Transactions refers more generally to the law of the state in which the grantor is located to determine the creation, effectiveness against third parties, and the priority of a security right in an intangible asset.[38]

Certainly, there are also undeniable problems with the application of the law of the security provider's location. First, the location of the security provider may be not be readily identifiable for third parties. But so is the location

[36] United Nations (n 29), Art. 30(1). *Cf.* also the proposal of 12 March 2018 of the EU Commission: Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, COM/2018/096 final - 2018/044 (COD).

[37] Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final, Art. 4(1).

[38] UNCITRAL (n 11). It is to be noted that, pursuant to Art. 90 of the Model Law, the "location" of the grantor refers in a subsequent and alternative order to the state of the place of business, the state where the central administration is exercised, or the state of habitual residence.

of the security taker, which is why we generally favour the application of the law chosen by the parties (see *supra* section IV(1)). Only where such an explicit choice is absent, the better arguments speak in favour of the security provider's location. It is also often criticised that the location of the security provider may change. While this is true, it is also true for the location of the security taker, which is yet an additional argument to allow the parties to determine the applicable law by choice.

In the end, it seems a necessary choice between two evils, and the security provider's location, while far from perfect, seems to be less bad than the security taker's location. This is also the choice that the European Law Institute has made in its recently adopted Principles on the Use of Digital Assets as Security.[39] A more attractive, third option, however, may be to rely on international principles of substantive law as *règles matérielles de droit international privé* (see on this solution also *infra* section 5).[40] This would avoid all arguments just discussed against either one of the parties' location, but unfortunately, no such international principles exist as of yet. This may change in future, when UNIDROIT will have adopted principles that are currently being drafted and negotiated in the context of their Digital Assets and Private Law Project.[41]

In sum, at present the law of the security provider's location should be used as the residual connecting factor to determine the law applicable to security rights in digital assets. However, it must be stressed that its importance is limited. It only applies provided that: (1) the digital assets are not recorded on a permissioned blockchain that is operated and/or supervised in one single state; (2) the digital assets are not held by a custodian; and (3) no express choice has been made for either the law governing the blockchain, or for the law governing the secured transaction. Only if all these conditions have been satisfied, one must necessarily refer to the location of the security provider, for want of a better criterion such as international principles of digital assets law. These latter principles may become available in the foreseeable future, and if they materialise, they should be preferred as a residual over the law of the security provider's location. The same is true where digital assets are held in custody and the custody law cannot be determined.

[39] See European Law Institute (n 34), Principle 3.

[40] Dominique Bureau and Horatia Muir Watt, *Droit international privé* (5th edn, Presses Universitaires de France 2021), 672–685, 540-1–551.

[41] See UNIDROIT, "Digital Asset and Private Law project" (*UNIDROIT*) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/> accessed 7 April 2022. (Full disclosure: both authors of the present chapter have been involved in this project).

5 Good Faith Acquisition and the Requirement of "Control"

Under most legal systems, a party that acquires an asset without knowing that it is encumbered with a security right will receive property unencumbered.[42] This is known as the principle of good faith acquisition. It must also apply with even more force to digital assets, because otherwise trading on blockchains would be subject to incalculable risks and would eventually stall. The law that governs good faith acquisition must be determined in the same way as that for any other acquisition. It will thus depend on the crypto-custodian, a choice of law, and the location of the transferor.

The specific problem here is that the content of the law governing the good faith acquisition is not necessarily known in advance. Although unlikely, it is possible that a law has little or no requirements for such acquisition. Consequently, it is theoretically possible that this law allows good faith acquisition of a digital asset encumbered with a security right without the transferor having given up any control over the asset. In this case, the creditor/security taker could assert its security right in the debtor's/security provider's insolvency, only to find that the relevant digital assets have been transferred to another party. Even worse, a creditor/security taker could claim to have obtained *bona fide* a security right that ranks higher than another security right in the same asset that the debtor has created before.

In the case of tangible assets, this problem is of minor importance because, according to the *lex rei sitae* principle, the law governing property rights, including security rights or rights *in rem*, is that of the state where the asset is located. The general public will usually know whether this law requires any condition for a secured transaction as to the publicity or transfer of control, and will take the necessary precautions. This is fundamentally different in a digital environment that has no location and where a multitude of different property laws may apply. In such environment, it is indispensable that a uniform indicator exists that signals to the general public the possible existence of a security right. Otherwise, the *erga omnes* effect of such rights could be hardly justified.

Such a signal can take various shapes and forms, depending on the technological specificities of the blockchain in question. One could imagine, for instance, some sort of colouring of coins and tokens that are encumbered, which would be visible to all users. The simplest way to indicate the existence of

[42] See on good faith acquisition from a comparative law perspective: Michele Graziadei and Lionel Smith, *Comparative Property Law: Global Perspectives* (Edward Elgar Publishing 2017).

a security right, however, is to require a loss of control by the security provider. This rough method avoids a second disposition by the security provider that would contradict the prior creation of the security right. The security provider could not effectuate such a second disposition because he would lack the necessary control.

Crucially, taking the loss of control as the relevant criterion is in line with the functioning of the blockchain. The technology that underpins the blockchain, the DLT, gives power to the party that is in control of a digital asset. Such control can be exercised, for instance, via a private key. The party having control has factual spending power, whereas others have not. It can transfer assets to others. Such transfers can also be made in the context of a secured transaction.

The law must not contradict the technology underpinning the blockchain and replace it with an entirely different legal analysis. Such an approach would put the functioning of the blockchain into danger and largely deprive it of its usefulness.[43] As a matter of principle, we believe, the law should not stand in the way of technology and commerce, but facilitate it.

Absent special techniques such as colouring of digital assets, which must be uniformly applied and be visible to all users, the creation of any security right on the blockchain must be accompanied by a transfer of control over the digital asset. At a minimum, the security provider should lose control over the digital asset so that he is prevented from transferring the relevant digital assets to another party or encumbering it again. There may be different technical means to achieve such a limitation of control, *e.g.* lock-up, blocking, bonding or freezing.

The question remains how the requirement of a loss of control can be imposed where the law governing the secured transaction does not require it. A traditional method under many conflict-of-laws regimes is to assume that a national law which allows for a secured transaction without any such loss is contrary to public policy (*ordre public*). Yet the threshold for violation of public policy is generally high. Thus, it would be difficult to argue that such a law “outrages its [the forum’s] sense of justice and decency”[44] or that it would “violate some fundamental principle of justice, some prevalent conceptions of

[43] Matthias Lehmann, “Who Owns Bitcoin? Private Law Facing the Blockchain” (2020) 21 Minnesota Journal of Law, Science & Technology 93, 116–120. Primavera De Filippi and Aaron Wright, *Blockchain and the Law: the Rule of Code* (Harvard University Press 2018), 193–204.

[44] *Re Fuld’s Estate* (*No 3*), [1968] P 675, at 678.

good morals, some deep-rooted tradition of the common weal."[45] In addition, public policy is not the right method here, because for this principle to apply, the result of the application of a foreign law must violate public policy, and as a matter of principle, a foreign law is not to be discarded for its abstract content.[46]

A technique to impose such universal substantive requirements has been developed in France. It is called the substantive rule of PIL (*règle matérielle de droit international privé*).[47] Such substantive rules are increasingly necessary due to the globalisation of exchanges, which calls for the surmounting of national idiosyncrasies and the application of uniform standards in various sectors.[48] This is particularly true for societal sub-systems that are completely devoid of any significant connection to a particular state. The blockchain is a prime example of such a societal sub-system. Its very nature as an a-national transfer mechanism calls for the establishment of a minimum of global rules.

As already indicated above, such global rules are currently elaborated by the UNIDROIT Working Group on Digital Assets.[49] The definition of control it uses could provide the basis for a world-wide substantive condition for the validity of secured transactions in particular. Such a requirement would greatly help the transparency of security rights to third parties. It would be an indispensable tool to justify the effect of such security rights against the whole world (*erga omnes*).

In sum, the validity of *any* secured transaction should be conditioned on a loss of control by the security provider. This condition is required independently of the content of the law that governs the transaction. The latter will thus merely determine other issues, in particular the existence of an agreement between the parties and the consequences of any defects of such agreement, *e.g.* in case of mistake, fraud or duress.

6 The Laws Applicable to Other Issues

We have so far identified two sources that govern a secured transaction and the validity and effects of security rights in digital assets: the national law applicable to the transaction as such, as well as a substantive rule of global

[45] *Loucks v Standard Oil of New York*, 224 N.Y. 99, at 111 (1918), per Justice Cardozo.

[46] Bureau and Watt (n 40), 457–458; Dicey, Morris and Collins, *Conflict of Laws* (15th edn, Sweet & Maxwell, 2018), 5-005–5-007.

[47] Bureau and Watt (n 40).

[48] See Gunther Teubner, "Global private regimes: neo-spontaneous law and dual constitution of autonomous sectors in world society?," in Karl-Heinz Ladeur (ed.), *Public Governance in the Age of Globalization* (Routledge 2017), 71–87.

[49] UNIDROIT Digital Asset and Private Law project (n. 41).

PIL regarding control. Besides these two sources, there are other laws that may have an effect on the validity of the transaction and thus, on the validity of the security rights created by that transaction.

One example of such laws relates to those governing the capacity of the parties. The security provider or the security taker can be under incapacity to enter into contracts under the national law applicable to them, for instance because one has not attained the legal age required or is suffering from mental disturbance. These issues are usually submitted to the "personal law" of the party in question, which is ordinarily the law of its nationality or domicile.[50] This law may deviate from that governing the secured transaction.

Another example is insolvency law. The rules on avoidance may affect the validity of transactions, especially those that are concluded in the "suspect period" or "twilight zone" in which the debtor is insolvent but insolvency proceedings are yet to be opened. These transactions may be void or voidable. The rules on avoidance are those of the country in which the insolvency proceedings have been opened, or *lex fori concursus*. This may be the country in which the debtor has its establishment, its principal place of business or its centre of main interest (COMI), but it is also sufficient that he has at least some assets there.[51] In each of these cases, this law may differ from the law governing the secured transaction, as well as from the law governing the capacity of the parties.

Although they considerably complicate the picture, these additional rules have to be respected as well. Otherwise, the interests of minors, adults in need or the other creditors would be disregarded. Even in a digital environment, these parties deserve protection. That the validity of a secured transaction will as a result be subject to a number of different laws is a price that must be paid.

7 Conclusion

The results of this study can be summarised in the following list. A secured transaction, and the validity and effects of security rights in digital assets must be governed:

1. if the transaction is done on a blockchain or a protocol that is governed exclusively by one law, for instance the law of the central operator or the law of an authority that supervises the network, by that law;

[50] Paul Torremans et al. (eds), *Cheshire, North and Fawcett: Private International Law* (15th edn, Oxford University Press 2017), 145 et seq; Bureau and Watt (n 36), 629 et seq.

[51] See UNCITRAL (in cooperation with UNIDROIT and HCCH), *Legislative Guide on Insolvency Law* (New York: United Nations Publications 2005), 41–43.

2. where 1 does not apply and the transaction concerns a digital asset that is held by a custodian
   a. by the law chosen in the custody agreement; or
   b. where (a) does not apply, by the law of the state in which the custodian is incorporated or has its principal place of business;
3. where 1 and 2 do not apply, by the law the parties to the secured transaction have chosen, subject to the globally uniform requirement that the security provider must have lost control over the digital asset (see *infra*);
4. where 1, 2 and 3 do not apply, by the law of the security provider, again subject to the globally uniform loss of control requirement (see *infra*), and provided no internationally accepted principles of digital assets law are available. Should the latter become available, those principles should govern.

In the latter two cases, the secured transaction and the creation of security rights are effective under the condition that the security provider has transferred or at least lost control over the relevant digital assets. This requirement does not apply in the two cases on the top of the list. In these cases, the law governing the secured transaction is sufficiently identifiable by third parties so that they can investigate its content. This does not mean that a loss-of-control requirement would not be useful also in these circumstances. Its precise form and shape or the choice of a potential alternative must however be left to the national legislator whose law applies.