Cryptocurrency: Collateral for Secured Transactions?

Xavier Foccroulle Ménard[*]

This article aims to summarize the present situation with regards to the use of cryptocurrency as collateral in secured transactions in the United States, Canada, the United Kingdom and France, and offer solutions to issues related to the use of cryptocurrency for this purpose. These proposed solutions are arranged as a framework that could be enacted in Canada, and elsewhere. The article first reviews the concept of a cryptocurrency, with special emphasis on bitcoin, and the concept of secured lending. Then, it discusses the categorization of bitcoin in the United States, Canada (with Ontario and Québec as examples), United Kingdom and France. At this time, only the United States and Ontario have doctrinal and regulatory guidance when using cryptocurrency specifically for secured lending. Finally, this article proposes a legislative framework to take security interests in cryptocurrency in Canada, including drafts of specific statutory amendments for both Ontario and Québec legislation. The article concludes by noting how this framework can be replicated elsewhere, notably in the United States, the United Kingdom and France.

L'auteur de cet article dresse un tableau de l'utilisation actuelle de la cryptomonnaie comme objet de sûreté aux États-Unis, au Canada, au Royaume-Uni et en France. Il préconise la mise en place d'un cadre réglementaire pour solutionner les problèmes rencontrés en ce domaine, au Canada et ailleurs. L'auteur examine d'abord la notion de cryptomonnaie (en insistant sur le bitcoin), puis celle de prêt garanti. Il traite de l'analyse juridique du bitcoin aux États-Unis, au Canada (en prenant pour exemple l'Ontario et le Québec), au Royaume-Uni et en France. Selon l'auteur, ce n'est actuellement qu'aux États-Unis et en Ontario qu'on peut s'appuyer sur la doctrine ou la réglementation existantes pour encadrer l'utilisation de la cryptomonnaie aux fins de prêts garantis. L'auteur propose la mise en place d'un cadre législatif pour la prise de garantie sur la cryptomonnaie au Canada et trace les grandes lignes de ce que ce cadre pourrait être en Ontario et au Québec. En conclusion, il fait valoir que ce cadre pourrait être reproduit ailleurs, notamment aux États-Unis, au Royaume-Uni et en France.

---

[*] Xavier Foccroulle Ménard holds a B.C.L./L.L.B. from the McGill Faculty of Law and is a LL.M. candidate at the University of Toronto Faculty of Law. He clerked at the Québec Superior Court for the Honorable Gregory Moore and works at Norton Rose Fulbright's office in Montréal. The author wishes to thank Professor Catherine Walsh for her supervision, help and thoughtful comments.

Electronic copy available at: https://ssrn.com/abstract=3548126

''Bitcoin is the most important invention in the history of the world since the Internet."

— Roger Ver, aka Bitcoin Jesus

1. INTRODUCTION: ANSWERING THE ''WHATS" AND THE ''WHYS"

This article intends to provide two things. One, its goal is to summarize the present situation with regards to using cryptocurrency as collateral in secured transactions in North America, with eyes on the United Kingdom and France as well. Two, it aims at providing realistic solutions to arising issues when using cryptocurrency for such purposes and incorporating them into a framework that could be enacted in Canada, and elsewhere as well.

First, it will superficially go over the concepts of cryptocurrency with special emphasis on bitcoin and of secured lending. The aim of this article is not to go into details with regards to these two concepts, but rather brushing over them to justify the importance of having this discussion and coming up with a solution to incumbent problems. Second, the article will have a discussion on the categorization of bitcoin in various western jurisdictions including the United States, Canada (with Ontario and Québec as examples), the United Kingdom and France. As the development of cryptocurrency makes for new regulations, new policy and general legal expansion adapted to the latest considerations, focus will be put on regulations and categorization that relate specifically to secured lending.

Third, we will dive into the applicable rules and the arising issues following the categorization of cryptocurrency specifically for secured lending in the United States and in Ontario, the only two jurisdictions within which there is a trace of doctrinal and regulatory guidance. Hence, after reviewing how cryptocurrency is categorized under certain set of laws related to secured lending, we will look at which rules apply. We will also analyze the issues and limitations that exist to taking a security interest in cryptocurrency under the present rules. Fourth, this article will address these issues and find possible solutions to consider when building a legal framework allowing the use of cryptocurrency as collateral in secured transactions. These solutions, which will be based on present information and practice at the time of writing, aim to be sufficient in facilitating the transactions as much as possible, helping the cryptocurrency market to solidify and fully take ground. Sixth, this article includes a proposition of legislative framework to take security interests in cryptocurrency in Canada, thus including a draft proposition for both Ontario and Québec. This proposed legislative framework could also serve as a basis for similar frameworks in cousin jurisdictions such as the United States, the United Kingdom or France.

Electronic copy available at: https://ssrn.com/abstract=3548126

(a) What is Bitcoin? Why Bitcoin?

Bitcoin hit an all-time-high of roughly US $19,900 on December 17, 2017,[1] followed by other major cryptocurrencies like Ethereum, Ripple, Bitcoin Cash, Litecoin and Cardano the next days and weeks. All have since retracted to lower levels, but not without leaving many early adopters and miners of such cryptocurrencies with sizeable assets value. So what is Bitcoin really, and why is it at all interesting?

Before engaging in this discussion, it is important to clarify two things. First, Bitcoin is only one type of virtual currency, as there are several virtual currencies on the market, many of which are used, held, transferred and created in a very different manner than Bitcoin.[2] Second, Bitcoin is also a system network. When referring to the system itself, the term Bitcoin with capitalization is used. The term bitcoin without capitalization is used to describe bitcoins as units of account.[3] Throughout this article, because bitcoins are the most prevalent cryptocurrency to date, the term bitcoin without capitalization refers to the general concept of cryptocurrency, so that the two words "bitcoin" and "cryptocurrency" can be used interchangeably. In this respect, the term bitcoin here encompasses all the possible cryptocurrencies that can be used as collateral to secure lending.[4]

The excitement surrounding bitcoin and its underlying blockchain technology is not to be minimized. It comes from both the bitcoin community[5] and key players in technology markets. Bill Gates, co-founder of Microsoft, considers bitcoin as "a technological tour de force."[6] Eric Schmidt, the executive chairman of Google, had this to say on the cryptocurrency: "Bitcoin is a remarkable cryptographic achievement . . . The ability to create something which is not duplicable in the digital world has enormous value . . . The bitcoin architecture, literally the ability to have these ledgers which can't be replicated, is an amazing advancement. Lots of people will build businesses on top of that."[7] In addition to generating a general enthusiasm toward the technology,

---

1 "Cryptocurrency Market Capitalizations", *Bitcoin (BTC) Chart* (2017), retrieved February 2018, online: < https://coinmarketcap.com/currencies/bitcoin/ >.

2 See FMLC, "Issue of Legal Uncertainty Arising in the Context of Virtual Currencies", *Financ Mark Law Comm* (July 2016) at 1-4. See also Louise Gullifer, ed, *Goode and Gullifer on Legal Problems of Credit and Security*, 6th ed. (London, UK: Sweet & Maxwell, 2017) at 41, paras. 1-59.

3 "Vocabulary - Bitcoin", *Bitcoin,* online: < https://bitcoin.org/en/vocabulary#bitcoin >.

4 For e.g. Bitcoin here encompasses, among all the other cryptocurrencies, the ten biggest in capitalization at the time of writing this article: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Cardano, NEO, Stellar, EOS, IOTA.

5 See e.g. Andreas M. Antonopoulos, *The Internet of Money* (Merkle Bloom LLC, 2016).

6 See Fox Business, *Munger/Buffett Disagree on Corporate Tax Rates* (2013) at 0:00:45 min.

7 See Eric Schmidt, *Bitcoin, consequences of the Edward Snowden revelations, the global Internet revolution, regulation and other highlights* (Computer History Museum, 2014).

Electronic copy available at: https://ssrn.com/abstract=3548126

cryptocurrency is also quite a promising collateral medium for secured transactions as more and more merchants, Internet retailers and service providers accept bitcoin as payment.[8] Martinson and Masterson are of the opinion that "[a]s both market size and transaction volume have been growing rapidly, Bitcoin may seem like an increasingly attractive source of collateral."[9] Cryptocurrency provides additional benefits compared to other type of assets such as the ability to increase in value, or "gain interest," while the coins are being held by either the debtor or the lender.[10] Also, it is taxed as property rather than currency, which would prove advantageous to some lenders, and its volatility allows for investment opportunities to lenders willing to accept the accompanying risks.[11] Lenders cannot afford to ignore Bitcoin any longer.

The revolution of cryptocurrency like bitcoin, and blockchain technology more generally, is that it provides a brilliant solution to what is commonly known as the "double-spending problem" that comes with digital assets.[12] Indeed, physical cash can only be spent once, as once you hand it over in a transaction, you no longer possess it; on the contrary, digital files can be duplicated and falsified. Until the apparition of bitcoin, central trusted third parties like banks would verify whether the digital money, which constitutes most of the money circulating in the economy, has been spent twice.[13] Commercial parties could trust each other because of the intervention of this trusted intermediary. With bitcoins, the intermediary is not needed for the establishment of trust between parties. Because the research has been done elsewhere and in a better fashion than it could ever be summed up in this article on secured transactions, and because it largely goes beyond the ambit of this article, the technical descriptions of bitcoin will be kept to the minimum required for a proper understanding of our discussion.[14]

---

8 See Jaime Hage & Thomas Wertman, "Drugs, Charity and Patio Furniture? How Digital Currencies Are Changing the Way We Look at Money" (2014) 20:1 Westlaw J. Secur. Litig. Regul. 1.

9 Pamela J Martinson & Christopher P Masterson, "Bitcoin and the Secured Lender" (2014) 33:6 Bank. Financ. Serv. Policy Rep. 13.

10 See Timothy Bierer, "Hashing it Out: Problems and Solutions Concerning Cryptocurrency Used as Article 9 Collateral" (2016) 7 J. Law Technol. Internet 79 at 83.

11 *Ibid.*

12 See Melanie Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. (Beijing: Sebastopol, CA: O'Reilly Media, 2015) at 2-3.

13 See Adam S. Armstrong & Marko Trivun, "Blockchain Technology Part 1: 'Blockchain Assets' as Collateral" (2017) Summer 2017:Q3 Torys Quaterly. See also Henning Diedrich, *Ethereum: blockchains, digital assets, smart contracts, decentralized autonomous organizations* (Wildfire Publishing, 2016) at 63 on the necessity of trust between financial institutions like banks.

14 For an introduction to the topic, see Jerry Brito & Andrea Castillo, "Bitcoin: A Primer for Policymakers" (2013) Mercatus Center George Mason University. For a more in-depth and comprehensive immersion on Bitcoin, cryptocurrency and blockchain

Electronic copy available at: https://ssrn.com/abstract=3548126

At its simplest expression, bitcoin is digital money or virtual currency, also called cryptocurrency.[15] It operates in a peer-to-peer payment network through an open source software, independent of any central authority, banking intermediary or government.[16] Anyone can be a user. There is no need to trust anyone since no person can abuse the system.[17] Indeed, cryptography ensures that only the owner of the bitcoin has the authority to spend them.[18] The system is secured through the use of the blockchain.[19] A blockchain is a decentralized peer-to-peer network of computers, where each computer is known as a node, which collectively process, maintain and distribute a single authoritative record of confirmed transactions.[20]

The blockchain is like a "central registry" of bitcoin transactions. All transactions specify the sender and recipient of bitcoins by their respective public addresses, which correspond to a set of digital keys where there is one public key and at least one private key.[21] A mathematical procedure called elliptic curve multiplication is used to derive the public key from the private key, and then from the public key is derived the bitcoin address with a cryptographic "hash" function.[22] To conduct a transaction, the sender must digitally sign the proposed transaction to the public address of the recipient with his private key.[23] The address corresponding to the set of keys is often named a "wallet", which effectively is the means for a user to hold bitcoins or other cryptocurrency.[24]

The blockchain creates a single master registry of the already cryptologically-secured bitcoin transactions, verifying them and locking them down in a highly competitive market called mining.[25] The process of mining, also called proof-of-work, starts with a transaction in bitcoins.[26] Then, nodes race to confirm transactions by solving mathematical puzzles, and once a node is successful, it

---

technology, see Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1st ed. (Sebastopol CA: O'Reilly Media, 2014); Swan, *supra* note 12.

15 Swan, *supra* note 12 at 3.

16 See Don Tapscott & Alex Tapscott, *Blockchain Revolution* (New York: Penguin Random House, 2016) at 17-18, 60 on how it could improve financial services.

17 See Swan, *supra* note 12 at x.

18 See Diedrich, *supra* note 13 at 102-111.

19 This is true for all cryptocurrency at the moment, except IOTA. See Serguei Popov, *The Tangle* (IOTA Whitepaper, 2017). To simplify, in this article, when blockchain technology is discussed, it also includes IOTA.

20 See Diedrich, *supra* note 13 at 91-101.

21 Antonopoulos, *supra* note 14 at 2448. See also J Dax Hansen & Joshua L Boehm, "Treatment of Bitcoin Under U.S. Property Law" (2017) Perkins Coie LLP at 5.

22 Antonopoulos, *supra* note 14 at 1494, 1513.

23 *Ibid*. at 1479.

24 See Isaac Pflaum & Emmeline Hately, "A Bit of a Problem: Nation and Extraterritorial Regulation of Virtual Currency in the Age of Financial Disintermediation" (2014) 45 Georget J. Int. Law 1169 at 1176-77. See also, Swan *supra* note 12 at 3.

25 Swan, *supra* note 12 at x.

Electronic copy available at: https://ssrn.com/abstract=3548126

broadcasts the results to all the other nodes on the network. They then independently verify the solution, reach a majority consensus and the information, the block, is placed next in the chain, thus permanently recorded on the network and time-stamped.[27] The miners are incentivized to solve these puzzles and verify the transactions by being rewarded with a small amount of the cryptocurrency being mined when they are successful.[28] The number of miners who monitor the transactions ensures that the transactions cannot be changed or reversed. So, no bitcoin holder may sell their bitcoin or percentage thereof more than one time.

Blockchain technology, and especially cryptocurrency, provides many advantages that make it valuable. Among other things, it is secure. The blockchain is not a conventional computer network where all the nodes constituting the network connect to a single and central database. Rather, it is decentralized and distributed on each node of the network, so that the nodes each host their own copy of the master record of all transactions.[29] This way, the inherent risks of single point of failures and data breaches are eliminated, which are growing concerns for financial institutions and large corporations, thereby creating value by enhancing security.[30] In addition, it is decentralized and disintermediated in the sense that it cuts out the intermediary, also called the middle man, since the blockchain theoretically allows users to transact among themselves on a peer-to-peer basis, without the need for intermediaries. This technology could potentially lead to immense savings on costs from escrow agents and other financial intermediaries that historically were needed to establish trust between the parties. This article does not go into details about securities held through a blockchain system with or without intermediation, also called "crypto-securities", and strictly concerns itself with bitcoin.[31]

(b) What are Secured Transactions? Why Secured Transactions?

As explained above, blockchain technologies and cryptocurrency are very important innovations and have the potential to drastically change the way we exchange, transact and generally do business. To unlock their full potential value as significant tools in commercial transactions, it is important that they can be used in credit transactions, and particularly secured transactions. As Sandra Appel puts it: "For the use of bitcoin to continue to increase and be accepted as a currency, or legitimized, it will be necessary eventually, for persons to be able to borrow bitcoin and borrowing in bitcoin."[32]

---

[26] See Diedrich, *supra* note 13 at 144-51, 157.

[27] *Ibid.*

[28] Antonopoulos, *supra* note 14 at 1479.

[29] See Swan, *supra* note 12.

[30] Antonopoulos, *supra* note 14 at 1479.

[31] For a greater discussion on the topic, see Eva Micheler, "Custody chains and asset values: why crypto-securities are worth contemplating" (2015) 74 Camb. Law J. 505.

Electronic copy available at: https://ssrn.com/abstract=3548126

A secured transaction enables a lender to take a security interest in property which provides means of obtaining repayment if the borrower defaults. In other words, if the borrower does not make good on his loan payments, the lender can look to the value of the assets, also called collateral, to satisfy the debt.[33] As Cuming, Walsh and Wood summarize it, the security interest usually provides the secured party three basic rights: (1) the right to seize and sell, or realize the value of the encumbered asset, (2) the right to apply the proceeds realized from seized asset in satisfaction of the obligation, and (3) the right to enforce the security interest against third parties who acquire proprietary rights in the assets.[34] This is important because the global economy runs on credit, or in other words "debt moves the world,"[35] and secured transactions laws provide certainty to lending, which greatly helps the economy.

One secured lending platform with collateral backed by blockchain assets stated on their website that "[b]lockchain assets are an ideal form of collateral because they are inexpensive to transfer, store, and liquidate when compared to traditional forms of collateral like real estate or stocks."[36] While that may be true, we will see that the current legal regime with regards to secured transactions is ill-equipped to provide a proper framework where cryptocurrency is used as collateral to secure loans. The actual secured transactions laws give rise to many uncertainties regarding the categorization of bitcoin, which in turn lead to uncertainties about the applicable rules. Further, the rules that apply to bitcoin are extremely limited and exhibit important shortcomings. As some authors have expressed, "it is unlikely that lenders would accept such assets as collateral without having certainty that lenders could legally enforce their rights against such collateral."[37] This lack of security affects the lenders' ability to ascertain whether they will receive the value bargained for in credit transactions, and consequently greatly diminishes the ability of bitcoin owners to finance investments and projects levering their assets.

---

[32] Sandra Appel, "Can you take a security interest in Bitcoin?", *DLA Piper* (7 May 2014), online: < https://www.dlapiper.com/en/canada/insights/publications/2014/05/can-you-take-a-security-interest-in-bitcoin > .

[33] See Ronald C. C. Cuming, Catherine Walsh & Roderick J. Wood, *Personal Property Security Law*, 2nd ed. (Toronto: Irwin Law, 2012) at 1.

[34] *Ibid.*

[35] Buttonwood, "Debt moves the world", *The Economist* (9 October 2013), online: < https://www.economist.com/blogs/buttonwood/2013/10/money-and-credit > .

[36] "Why are blockchain assets ideal collateral?", online: *SALT Lend* < https://salt-lending.zendesk.com/hc/en-us/articles/115009274748-Why-are-blockchain-assets-ideal-collateral- > .

[37] See Armstrong & Trivun, *supra* note 13.

Electronic copy available at: https://ssrn.com/abstract=3548126

2. CATEGORIZATION OF BITCOIN

Cryptocurrency raises difficult questions for many fields of the law. In June 2014, the Report of the Financial Task Force (FATF), an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction, provided a comprehensive definition of virtual currency that seems highly inspired from Martinson and Masterson. The definition is set out in these terms:

> Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.[38]

Although bitcoin users describe it as a "virtual currency," it is hardly seen as such by the regulators. As Martinson and Masterson note, economists consider three traits when determining if something serves as currency: (1) whether it is a medium of exchange, (2) whether it is a unit of account, or (3) whether it is a store of value. Unfortunately, bitcoin may be too volatile to serve as a unit of account or store of value and may not be used by enough people to be considered a medium of exchange.[39]

In Singapore, the authorities classified bitcoin as a good rather than currency and have imposed a tax whenever it is used for trading or as a payment for services.[40] In China, the People's Bank of China, the country's central bank, enacted strict regulations banning financial institutions from handling bitcoin transactions and published a notice stating that Bitcoin was "not a currency in the real meaning of the word" but rather a "virtual commodity that does not share the same legal status of a currency. Nor can, or should, it be circulated or used in the marketplace as a currency."[41] These strict approaches may change, however. For example, the Russian Prosecutor's General office initially declared in 2014 all bitcoin transactions illegal since the rouble is the sole official currency of the country,[42] but then in 2018 the Finance Ministry announced that they would be looking into a way to regulate cryptocurrencies, instead of a ban.[43]

---

[38] Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (FATF Report, 2014) at 4.

[39] See Martinson & Masterson, *supra* note 9 at 13.

[40] *Ibid.* at 16.

[41] Gerry Mullany, "China Restricts Banks' Use of Bitcoin", *NY Times* (5 December 2013), online: < https://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html > .

[42] Gabriela Baczynska, "Russian authorities say Bitcoin illegal", *Reuters* (9 February 2014), online: < https://www.reuters.com/article/us-russia-bitcoin/russian-authorities-say-bitcoin-illegal-idUSBREA1806620140209 > .

Electronic copy available at: https://ssrn.com/abstract=3548126

(a) The United States and the UCC

In the United States, secured transactions are governed by Article 9 of the Uniform Commercial Code (UCC). First published in 1952, the UCC is the longest and most elaborate of the uniform acts, which have been put into law to harmonize the law of sales and other commercial transactions across the country. That is, every single state has adopted the rules contained in Article 9 UCC, some of them with very slight variations, which govern transactions where security interests are taken in personal property. Article 9 lists various categories of property because the rules for attachment and perfection differ based on the category of asset over which the security interest is created.[44]

While bitcoin is definitely property, thus can be subject to ownership rights under United States law,[45] it is not quite clear how it is categorized under the UCC. In our opinion, by way of elimination, bitcoin would be categorized under "general intangibles," the residual property category found in UCC Article 9. The UCC does not seem to categorize bitcoins as "money," since money is defined as a "medium of exchange currently authorized or adopted by a domestic or foreign government."[46] Maybe one day bitcoin will be authorized or adopted by a domestic or foreign government, and we will have to reconsider its categorization, but to this date this has yet to happen.

Nevertheless, a Texas federal district court has ruled that when considered in an investment context, despite the statutory definitions, bitcoin is a currency or a form of money. In *Sec. & Exch. Comm'n v. Shavers*,[47] Trendon T. Shavers and his company, Bitcoin Savings and Trust (BTSCT), were accused by the Securities & Exchange Commission (SEC) of the United States of operating a Bitcoin-based Ponzi scheme in which the investors would use bitcoin to invest. The investors were defrauded of more than 700,000 bitcoins. The defendants asked for a dismissal, arguing that the defendants' investors used bitcoins to make their investments, and since bitcoins were not currency, there could be no investment of money in the transaction. The federal district court analyzed the use of bitcoins in an investment context. The court held that bitcoin is a currency or a form of money and wrote the following:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses.

---

[43] Andrey Ostroukh & Jack Stubbs, "Russia ready to regulate, not ban cryptocurrencies", *Reuters* (25 January 2018), online: < https://www.reuters.com/article/us-russia-crypto-currencies-bill/russias-finance-ministry-ready-to-regulate-not-ban-crypto-fx-idUSKBN1FE0Y0 >.

[44] Jeanne L. Schroeder, "Bitcoin and the Uniform Commercial Code" (2016) 24:1 Univ Miami Bus Law Rev 1 at 10.

[45] See Hansen & Boehm, *supra* note 21.

[46] UCC § 1-201(b)(24).

[47] *Sec. & Exch. Comm'n v. Shavers*, Doc. 4:13-CV-416 (E.D. Tex., August 6, 2013) [*Shavers*].

Electronic copy available at: https://ssrn.com/abstract=3548126

> The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Bitcoin is a currency or form of money . . .

If this ruling were to be applied to the UCC, it could have significant consequence on the creditors' perfection methods with regards to security interests in assets such as virtual currencies. Nevertheless, chances are almost nonexistent that *Shavers* will be applied for secured lending purposes, and in the meantime, most legal commentators in the United States share the opinion that cryptocurrency cannot be considered as "money" under UCC Article 9.[48]

The UCC also distinguishes "money" from "deposits accounts," which for Schroeder confirms that money in the UCC intended to cover physical, or hand-to-hand money, and not virtual currency like bitcoin.[49] As a matter of fact, UCC § 9-102(a)(2) defines a deposit as such: "'Deposit Account' means a demand, time, savings, passbook, or similar account maintained with a bank. The term does not include investment property or accounts evidenced by an instrument."[50] In other words, to make a deposit in fact signifies making an unsecured loan to a bank or another financial institution, which means that "a deposit account is a ledger that records the amount of this unsecured loan."[51] This is quite different from bitcoin, since cryptocurrency works with wallets, which are essentially keys, and does not involve any type of bank or regular financial institution. As previously mentioned, the Bitcoin system gets rid of such intermediaries.

Bitcoin is disruptive and does not fit into either category of "money" or "deposit account" under the UCC not because it is digital, but because it can be held and transferred directly by registration on a decentralized ledger, the blockchain. Consequently, bitcoin can only fall under the catchall category of "general intangibles" provided at UCC § 9-102(a)(42). Indeed, this provision states that general intangible "means any personal property" that is not listed in the article. As expected, cryptocurrency is not listed, ergo the category applies.[52]

(b) The Canadian Common Law Provinces, the *Personal Property Security Act* and the *Securities Transfer Act*

From 1990 onward, in every Canadian province except Québec, Personal Property Security Acts were enacted to govern the rules for taking security

---

48 See gen. Schroeder, *supra* note 44 at 10, 14, 16-22.

49 *Ibid*. at 21.

50 See UCC § 9-102(a)(2).

51 Schroeder, *supra* note 44 at 22.

52 See UCC § 9-102(a)(42): "'General intangible' means any personal property, including things in action, other than accounts, chattel paper, commercial tort claims, deposit accounts, documents, goods, instruments, investment property, letter-of-credit rights, letters of credit, money, and oil, gas, or other minerals before extraction. The term includes payment intangibles and software."

Electronic copy available at: https://ssrn.com/abstract=3548126

interests in personal property. They establish a comprehensive statutory framework to govern their creation, perfection, priority and enforcement.[53] In fact, these acts are remarkably similar to the unified framework found in Article 9 UCC. The rules have since been completed by the Securities Transfer Acts. In this article, we will use Ontario as the model province, meaning that the relevant legislation is the *Personal Property Security Act*[54] (PPSA) and the *Securities Transfer Act*[55] (STA), but the other provinces have almost exactly similar regimes.

Since the PPSA is largely influenced by Article 9 UCC, bitcoin would also be characterized as an "intangible," by measure of elimination.[56] Bitcoins cannot be considered as "goods" under the PPSA because goods are defined as tangible personal property.[57] It cannot be considered as "money" either since money is considered to be "a medium of exchange authorized or adopted by the Parliament of Canada as part of the currency or by a foreign government as part of its currency."[58] Similarly, the definitions of "chattel paper", "documents of title" and "instruments" have very specific meanings and do not encompass bitcoin. What is left is the "intangible" category where intangible is defined as "all personal property that is not goods, chattel paper, documents of title, instruments money or investment property, including choses in action."[59] Like "general intangibles" in the UCC, the PPSA category of "intangible" intends to encompass all property, which includes bitcoin.

Furthermore, bitcoin is likely not considered "investment property" under the provisions of the STA because it is neither a certificated or an uncertificated security, nor a futures contract or a futures account.[60] Trading bitcoins does not require an intermediary and the activity is not currently regulated by an exchange. There is a possibility that bitcoin be categorized as a "financial asset" and consequently be included in the concepts of securities account or securities entitlement. Yet, since the current provisions of the STA and the interests in these types of collateral are directed to securities as well as rights and property interests in securities, it would be unlikely. In other words, "bitcoin does not fall within the purview of the STA, as presently construed."[61]

Some government agencies have already started to define bitcoin for the purposes of their enabling legislation. For example, the Canadian Revenue Agency (CRA) views virtual currencies as a commodity.[62] Similarly, the

---

53 See Cuming, Walsh & Wood, *supra* note 33 at 5-6.

54 R.S.O. 1990, c. P.10.

55 2006, S.O. 2006, c. 8.

56 For a similar conclusion, see Appel, *supra* note 32.

57 See PPSA, *supra* note 54, s. 1(1).

58 *Ibid.*

59 *Ibid.*

60 Sandra Appel, *supra* note 32.

61 *Ibid.*

Electronic copy available at: https://ssrn.com/abstract=3548126

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) does not consider bitcoins as "funds" as defined by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[63] Instead, bitcoins are viewed as goods and a cryptocurrency-only transaction is considered a barter transaction.[64] But, looking at these government agencies to define bitcoin is unwarranted because it is unhelpful in the context of the PPSA. More and more, efficient categorizations are developed for the purpose of specific acts, rather than generally created and applied to all situations.[65] This should be the same for bitcoin.

(c) The United Kingdom, France and Québec

The three other jurisdictions that are of interest to us, the United Kingdom, France and Québec, offer very scarce literature and little guidance with regards to cryptocurrency and its use as collateral in secured transactions.

(i) The United Kingdom

In his article "Transacting in a Vacuum of Property Law",[66] Noel McGrath considers the law of money in the United Kingdom and examines whether, and to what extent, bitcoin fits with contemporary understandings of money's legal nature. To do so, he first investigates the society theory of money which posits that "an item attains the status of money when it becomes acceptable as a means exchange among members of a community."[67] In *Miller v. Race*, Lord Mansfield in considering whether Bank of England notes constitute money wrote:

> Now [the bank notes] are not goods, not securities, nor documents for debts, nor are so esteemed: but are treated as money, as cash, in the ordinary course and transaction of business, by the general consent of mankind; which gives them the credit and currency of money, to all intents and purposes. They are as much money, as guineas themselves are; or any other current coin, that is used in common payments, as money or cash.[68]

---

62 See Jerry Brito et al, *The Law of Bitcoin*, Stuart Hoegner, ed. (Bloomington, IN: iUniverse, 2015) at 38.

63 S.C. 2000, c. 17.

64 See Brito, *supra* note 62 at 24.

65 See e.g. *Saulnier (Receiver of) v. Saulnier*, 2008 SCC 58, 2008 CarswellNS 569, 2008 CarswellNS 570, EYB 2008-149205, (*sub nom.* Saulnier v. Royal Bank of Canada) [2008] 3 S.C.R. 166, (*sub nom. Saulnier (Bankrupt), Re*) 271 N.S.R. (2d) 1, 50 B.L.R. (4th) 1, 48 C.B.R. (5th) 159, (*sub nom.* Royal Bank of Canada v. Saulnier) 298 D.L.R. (4th) 193, 867 A.P.R. 1, 381 N.R. 1, 13 P.P.S.A.C. (3d) 117, [2008] S.C.J. No. 60 (S.C.C.). where it was ruled that commercial fishing licences constitute "property" under the *Bankruptcy and Insolvency Act* and *Personal Property Security Act*.

66 Noel McGrath, "Transacting in a Vacuum of Property Law" (2016) Paper 22/2016 TLI Think.

67 *Ibid.* at 8.

68 Miller v. Race, 1 Burr 452, 97 ER 398 (K.B., 1758).

Electronic copy available at: https://ssrn.com/abstract=3548126

But, it is unlikely that a court would be convinced to consider bitcoin as a societally constructed form of money because the current volume of bitcoin transactions is too small.[69] McGrath also investigates the state theory of money in which bitcoin clearly does not fit.[70] In support of McGrath's conclusion, the Bank of England is of the view that the use of bitcoins as a digital currency is not prevalent enough to serve as money.[71]

Hence, bitcoin cannot be regarded as money in English law.[72] It also cannot presently be considered as cash under the *Financial Collateral Arrangements Regulations* (FCARs) definition since cash must be held in an account,[73] and bitcoins are not.[74] On a theoretical level however, bitcoin is certainly capable of being the subject of property rights. In short, McGrath arrives at this conclusion using Penner's theory of common law property, combining "separability" and "exclusivity" to determine which things can be the subject of property rights.[75] For McGrath, this recognition is highly significant for enterprise financing as it will have consequences on whether taking security interests in bitcoin is at all possible, and how.[76] After reviewing recent developments in English case law, McGrath concludes that the law will protect as property that which is transferable and which has value.[77] Because bitcoin has both qualities, it is possible to recognize it as a form of "chose in action". In her article published in 2016 on cryptocurrency, Lucy Chambers arrives at the same conclusion.[78] It has also been argued that cryptocurrency could be considered a "chose in possession" instead, since it is transferred through control. As a matter of fact, transferring bitcoin consists of giving the transferee exclusive access to the means of control, that is to the private key.[79] Ultimately, even if bitcoin does not fit into the category of a "chose in action," scholar Louise Gullifer reminds us that it could simply be considered as "other intangible property", over which security interests can be taken.[80]

---

69 McGrath, *supra* note 66 at 11.

70 *Ibid*. at 14-15.

71 See Brito, *supra* note 62 at 159.

72 *Ibid*. at 16.

73 See FCARs, reg. 3(1). See also Geoffrey Yeowart et al, *Yeowart and Parsons on the Law of Financial Collateral* (Cheltenham: Edward Elgar Publishing, 2016) at 51, para. 3.05.

74 See Gullifer, *supra* note 2 at 237, para. 6-05.

75 See J.E. Penner, *The Idea of Property Law* (Oxford, UK: Oxford University Press, 1997) at 71, 111.

76 McGrath, *supra* note 66 at 17.

77 *Ibid*. at 25.

78 See Lucy Chambers, "Misappropriation of cryptocurrency: propelling. English private law into the digital age?" (2016) 5 J. Int. Bank Financ. Law 263.

79 See David Quest QC, "Taking security over bitcoins and other virtual currency" (2015) 7 J Int Bank Financ Law 401. See also Gullifer, *supra* note 2 at 42, 1-59.

80 See *ibid*. at 42, paras. 1-59.

Electronic copy available at: https://ssrn.com/abstract=3548126

(ii) Civil law jurisdictions: France and Québec

There is no literature on using cryptocurrency as collateral for security interests in France or Québec. In reality, even finding general work dealing with civil law's approach to regulating blockchain technology proved to be difficult comparatively to common law jurisdictions. This is rather surprising because France adopted what Stéphane Blemus calls "the most advanced far-reaching legislative projects in the EU member states" when it introduced two legal bills, one in 2016 and the other in 2017, to recognize blockchain technology.[81] Indeed, the first bill (Macron II Law) defined blockchain technology as a "shared electronic registration technology,"[82] which could be used to register the issuance and transfer of "minibonds."[83] Also, a registration of a "mini-bond" transfer in the shared electronic registration technology now constitutes a written legal contract under French law.[84] The second bill (Sapin II Law) pushed things further by giving the French government the mandate to adopt by ordinance a regulation that would aim at the registration of some financial instruments on a shared electronic registration technology.[85] Such an ordinance was published in December 2017,[86] yet its implementation and enforcement was subject to a decree due by July 2018, which was never published.[87]

At the G20 Meeting of Finance Ministers which took place in Argentina in March 2018, French Finance Minister Bruno Le Maire seriously planned to make joint proposals with Germany to regulate cryptocurrency.[88] This initiative has gathered support among the finance ministers of the group,[89] and in December 2018, leaders from the G20 reiterated their pledge to regulate "crypto-

---

81 See Stéphane Blemus, "Law and Blockchain: a legal perspective on current regulatory trends worldwide" (2017) N°4-2017 Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) at 11-12.

82 *Ibid*. at 12.

83 See *Code monétaire et financier*, 13 January 2018 [CMF], Article L. 223-12: "Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État."

84 See *ibid*., Article L. 223-13: "Le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du code civil."

85 See Blemus, *supra* note 81 at 12.

86 *Ordinance n° 2017-1674 of 8 December, 2017*, France [*Ordinance n° 2017-1674 of 8 December, 2017*].

87 *Ibid*., article 8.

88 See Reuters Staff, "France, Germany to make joint bitcoin regulation proposal at G20 summit", *Reuters* (18 January 2018), online: <https://www.reuters.com/article/us-global-bitcoin-france-germany/france-germany-to-make-joint-bitcoin-regulation-proposal-at-g20-summit-idUSKBN1F728X>.

89 See Francesco Canepa, "G20 agrees to 'monitor' cryptocurrencies but no action yet", *Reuters* (20 March 2018), online: <https://www.reuters.com/article/us-g20-argentina-

Electronic copy available at: https://ssrn.com/abstract=3548126

assets" as one of the measures to help grow the global economy.[90] Minister Le Maire also created an internal working group to develop cryptocurrency regulations which will be lead by Jean-Pierre Landau, a Sciences Po economic professor and former Bank of France deputy governor.[91] Yet, the focus of this working group is not the use of cryptocurrency as collateral in secured transactions. In Minister Le Maire's words:

> We want a stable economy. We reject the risks of speculation and the possible financial diversions linked to bitcoin. [. . .] Jean-Pierre Landau's mission will be responsible for proposing guidelines on the evolution of regulations and to better control development and prevent their use for the purpose of tax evasion, money laundering or for financing criminal activities and terrorism. [. . .] There is evidently a risk of speculation. We need to consider and examine this and see how . . . with all the other G20 members we can regulate bitcoin.[92]

In the meantime, bitcoin users and market players in France and in Québec are in the same boat. They have very little guidance as to what the rules are and how they should behave if they want to use their bitcoin assets to secure loans. In this article, we want to start remedy this situation by proposing, at the end, a legal framework allowing for cryptocurrency subjection to civil law hypothecs.[93]

3. THE APPLICABLE RULES UNDER THE PRESENT LEGAL REGIME

(a) Under the UCC in the United States

Following the guidance of UCC Article 9, state laws require creditors wishing to take collateral as security for their loans to perfect their interests. The rules for perfection depend on the category of the collateral over which the security interest is created.[94] For example, creditors can perfect a security interest in a deposit account or in investment property by having "control" over the collateral,[95] while a security interest over money can be perfected by the creditor

---

bitcoin/g20-agrees-to-monitor-cryptocurrencies-but-no-action-yet-idUSKBN1GW2R9>.

90 See G20 Leaders' declaration, "Building consensus for fair and sustainable development", G20 Argentina 2018 (1 December 2018), online: < http://www.g20.utoronto.ca/2018/2018-leaders-declaration.html>.

91 See David Meyer, "France's Newly-Appointed 'Monsieur Bitcoin' Is a Notable Cryptocurrency Skeptic", *Forbes* (16 January 2018), online: <http://fortune.com/2018/01/16/bitcoin-cryptocurrency-france-regulation-jean-pierre-landau/>.

92 See Sujha Sundararajan, "France Creates Working Group for Cryptocurrency Regulation", *CoinDesk* (16 January 2018), online: <https://www.coindesk.com/france-creates-working-group-for-cryptocurrency-regulation/>.

93 See section "Proposition: the PPSA and the CCQ".

94 See Schroeder, *supra* note 44 at 10.

95 See UCC, § 9-312(b)(1), § 9-314(a).

Electronic copy available at: https://ssrn.com/abstract=3548126

taking physical possession of the collateral.[96] Effectively, control is accomplished when the debtor, the debtor's bank, and the creditor sign a deposit account control agreement setting out their respective rights in the account:

> A secured party has control of a deposit account if:
>
> > (1) the secured party is the bank with which the deposit account is maintained;
> > (2) the debtor, secured party, and bank have agreed in an authenticated record that the bank will comply with instructions originated by the secured party directing disposition of the funds in the deposit account without further consent by the debtor; or
> > (3) the secured party becomes the bank's customer with respect to the deposit account.[97]

We have determined however that bitcoin does not involve any bank accounts, and wallets can hardly be considered "banks" by regulators. As a matter of fact, we have established that the most likely categorization of bitcoin under the UCC is "general intangibles", for which the perfection rules are different. Under this category, perfecting a security interest in bitcoin requires that the creditor files a UCC-1 financing statement with the appropriate state authority, sufficiently describing the collateral. This is called registration. If the bitcoin categorization in *Shavers* as a "currency or a form of money" is applied to the UCC Article 9,[98] perfecting a security interest is not done by the creditors filing a UCC-1 financing statement as they would for general intangibles, but instead by securing "possession" of the virtual currency.[99] As mentioned above, this is an issue because taking possession of a cryptocurrency wallet or other non-deposit accounts in which the security interest has been granted may prove to be a very difficult task. In fact, it has been argued that perfection by possession of general intangibles is impossible given the lack of physical item.[100] At the moment, the UCC does not allow for security interests in bitcoins to be perfected through control agreements.

This means that the creditor cannot rely on the self-help provisions that allow to quickly sweep funds of a bank account whose depositary has agreed to cooperate with that process. It becomes much more time consuming and expensive for a creditor to recover bitcoin funds compared to a regular deposit account. Instead you have to go to court and get a judgment.[101] And even if you do, one major concern is that the borrower could easily transfer the collateral to another wallet whose owner may be unknown, putting the bitcoins out of reach

---

96 See UCC, § 9-312(b)(3).

97 UCC § 9-104(a).

98 See *Shavers*, *supra* note 47.

99 See UCC, § 9-312(b)(3) and § 9-313.

100 Martinson & Masterson, *supra* note 9 at 18.

101 *Ibid.*

Electronic copy available at: https://ssrn.com/abstract=3548126

from the creditor seeking to collect. In these situations, it is very likely that the "recovery of Bitcoin collateral will be impossible."[102]

(b) Under the PPSA in Canada

Under the PPSA, the first step for a security interest to be enforceable against third parties is that it must have attached to the collateral.[103] Attachment happens "when value is given, the debtor has rights in the collateral or the power to transfer rights in the collateral to a secured party" and the debtor has signed an agreement containing a description of the collateral sufficient to enable it to be identified.[104] To use bitcoin as collateral, the holder has to enter into a security agreement describing the bitcoins with the secured party. For such a task to be completed accurately, the secured party will have to rely on the bitcoin holder's good faith and accuracy in describing the bitcoin by reference to its encoded cryptological information so that the bitcoin as collateral may be distinguished from other bitcoins.

The second step for a security interest in the collateral to be enforceable against third parties is that it must be perfected. Section 19 of the PPSA provides that: "A security interest is perfected when, (a) it has attached; and (b) all steps required for perfection under any provision of this Act have been completed, regardless of the order of occurrence."[105] Under the PPSA and the STA, an intangible cannot be perfected by control unless the intangible is an investment property.[106] This includes certificated and uncertificated security, security entitlement, futures contract and a securities account.[107] For all other intangibles, the secured party must register his security interest to perfect it. Since we have established in this article that bitcoin does not presently fit within the definition of "investment property", perfecting a security interest in bitcoin assets requires registration. Of course, the debtor could allow the creditor to have access to the cryptocurrency wallet by making the private key available to him as part of the agreement, as to provide the means for the secured creditor to know if the coins have been removed.[108] But the debtor would still remain in possession, or in control, of the assets: this type of arrangement would not be sufficient to establish control over the cryptocurrency, nor can it be recognized as establishing control at all under the PPSA.

---

[102] *Ibid.*

[103] See PPSA, *supra* note 54, s. 11(1).

[104] *Ibid.*, s. 11(2).

[105] *Ibid.*, s. 19.

[106] *Ibid.*, s. 1(2).

[107] *Ibid.*

[108] See Pflaum & Hately, *supra* note 24 at 1177-78.

Electronic copy available at: https://ssrn.com/abstract=3548126

4. BROAD LIMITATIONS (OR ISSUES) ARISING FROM THE RULES

(a) Enforceability

Do the rules under the UCC and the PPSA allow for adequate enforcement of security interests in bitcoin? And is the present legal framework for secured transactions well adapted to using cryptocurrency as collateral? Martinson and Masterson answer these two questions in the negative: "[C]reditors may find it prudent to restrict borrowers' Bitcoin use at this time due to the high degree of regulatory uncertainty, irreversible payments, volatile exchange rates, and system anonymity."[109] We will address these issues.

(i) Describing the collateral

Registration of security interests in bitcoin appears to present some practical problems. When the lender registers his security interest in bitcoin under the PPSA, he has a choice to make. Either the bitcoin registration description is generic, that is describing all of the wallet or just a percentage interest, either it is more specific, including a description of the encoded cryptology.[110] Both display shortcomings. On the one hand, the generic description could prohibit the borrower from dealing with other bitcoin interests that are not part of the collateral. Moreover, it does not provide mechanisms to prevent the borrower from transferring the bitcoin interest if he so choses.[111] This issue will be addressed later in the article. On the other hand, the specific description, which includes the encoded cryptology, is not a proper alternative because third parties could have access to the information and transfer the borrower's bitcoin interest.[112] Indeed, under s. 18(d) of the PPSA, a debtor, a judgment creditor or a third party who has an interest in the collateral may require, by written notice, the secured party to provide him with a copy of the security agreement.

(ii) The lack of central authority

As explained previously, cryptocurrencies like bitcoin are decentralized, which means that there is no central authority governing or regulating their supply. Because of this decentralization, "[t]here is an inability to execute deposit account control agreements (or their analogs), thus precluding lenders from easily exercising 'control,' as defined for UCC purposes over debtor Bitcoin assets. This, in turn, means lenders cannot easily sweep funds from a debtor's Bitcoin accounts, or 'wallets'."[113] The secured lender could require that the debtor provides its private key pertaining to his cryptocurrencies addresses, which is the equivalent of providing access information for a bank account. But

---

[109] Martinson & Masterson, *supra* note 9 at 13.

[110] Sandra Appel, *supra* note 32.

[111] *Ibid.*

[112] *Ibid.*

[113] Martinson & Masterson, *supra* note 9 at 14.

Electronic copy available at: https://ssrn.com/abstract=3548126

because there is no central authority or neutral third party to ensure the truthfulness, debtors could provide fake private keys. A possible solution would be for lenders to establish their own cryptocurrency accounts and requiring the debtor to make a nominal transfer from the collateral account to the lender's account. If the transfer is successful, the lender would at least know that the debtor's address is real and controlled by the borrower. But, this will not guarantee availability or accessibility of funds at a future date.[114]

(iii) Irreversibility & traceability

One other problem is that "the blockchain merely logs the addresses of each party involved in the transaction, not the identity of the parties holding each such address."[115] It is possible to discover a party's identity when looking at the transactions made from the address, but this could prove a difficult task: cryptocurrency users have multiple wallets, they transfer funds through chains of wallets and they use software like Tor to keep their identity private. "This difficulty of tracing funds through the Bitcoin network means that recovering Bitcoin collateral after it has been transferred in the network is likely to be prohibitively expensive or even impossible for a lender."[116]

On top of that, transfers are not necessarily unitary and often involve multiple input/output accounts.[117] Sometimes, transactions will be recorded as the following: A uses as inputs five bitcoins from B and five bitcoins from C, with the outputs being eight bitcoins to D and two bitcoins back to A. Only inputs and outputs are listed, hence it is not possible to determine which bitcoins were transferred to who. This process makes tracing bitcoins incredibly difficult. Business will likely transfer the received bitcoins in different accounts for consolidation purposes or reducing transaction fees. Users receiving bitcoins will likely divide them between various parties whenever they make a transaction. Additionally, "mixers" exist to provide the service of making the tracing impossible by masking bitcoin transactions through intermediate transactions.[118]

Another thing is that transactions conducted with cryptocurrencies are irreversible by the nature of the system.[119] In fact, the cryptography and the software protocols make it mathematically impossible to reverse payments. This means that any collateral a debtor holds in cryptocurrency can be transferred at any moment, placing it permanently out of the lender's grasp. In effect, "there is no guaranty that the collateral will be there when the lender comes to collect."[120]

---

[114] Martinson & Masterson, *supra* note 9 at 14.

[115] *Ibid.*

[116] *Ibid.* at 15.

[117] Stephen McJohn & Ian McJohn, "The Commercial Law of Bitcoin and Blockchain Transactions" (2016) Legal Studies Research Paper Series: Research Paper 16-13 Suffolk Univ. Law Sch. 1 at 11.

[118] McJohn & McJohn, *ibid.* at 12.

[119] See Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency" (2012) 4 Hastings Sci. Technol. Law J. 159 at 165.

Electronic copy available at: https://ssrn.com/abstract=3548126

The current framework for taking security interests in bitcoins is not well adapted to the technology: the only way for a creditor to perfect the security interest is through registration, which in a default setting would leave the debtor in control of the collateral. Even if the debtor gives the creditor access to the wallet holding the bitcoins, allowing him to verify if the cryptocurrency has been removed or not, the structure provides no protection whatsoever from an irreversible and almost impossible to track transfer of the assets.[121]

One interesting solution that has been discussed in the cryptocurrency community is the use of multisignature wallets, M-of-N protocols, where more than one key is required to authorize a bitcoin transaction. This approach is analogous to a tri-party escrow arrangement. A neutral third party is added to the equation, and his assent is mandatory for the funds to be transferred, effectively protecting the creditor. This solution is not perfect, however. First, alike other payment systems, this setup does not protect creditors from untrustworthy third parties. Second, it creates problems regarding erroneous transfers. For instance, if a claim for funds from the debtor's wallet has been made to the escrow agent, and the agent by mistake authorizes the transfer of funds to an unentitled party, the transaction cannot be cancelled, and the funds will be almost impossible to recover since bitcoin transactions are irreversible.[122]

This type of arrangement also clashes with the ethos of bitcoin, because at its core lies the goal of democratizing the financial system and getting rid of the intermediary. Evan Rose, the CEO of Bitcoin ATM maker Genesis had this to say: "When you introduce a third-party holding on to people's funds, it's absolutely antiethical to the idea of Bitcoin. You're giving someone cash over the Internet that you'll never be able to get back."[123]

(b) Volatility

The history of bitcoin is filled with extreme fluctuations in value as cryptocurrencies are highly volatile.[124] For that reason, practising lawyers at Dentons' office in London expressed hesitation with regards to the viability of bitcoin to be used as a security asset because it does not have a stable value. In their words, "Bitcoin's peak unit value hit US $1,217 in November 2013. At the time of writing, the value of Bitcoin is US $246. This volatility in itself makes Bitcoin an unattractive form of collateral at present."[125] This skepticism is

---

[120] Martinson & Masterson, *supra* note 9 at 15.

[121] See Grinberg, *supra* note 119 at 165. See also Bierer, *supra* note 10 at 87.

[122] Martinson & Masterson, *supra* note 9 at 19.

[123] *Ibid*. at 19 citing Jose Pagliery, "Silk Road heist could doom Bitcoin black markets", *CNNMoney* (19 February 2014), online: *CNNMoney* < http://money.cnn.com/2014/02/19/technology/security/bitcoin-black-market/index.html >.

[124] See Martinson & Masterson, *supra* note 9 at 15.

[125] Martin Fanning, Adam Pierce & James Marsden, "Bitcoin: is it a viable security asset?", *Dentons LLP* (31 March 2015), online: < https://www.dentons.com/en/insights/news-

Electronic copy available at: https://ssrn.com/abstract=3548126

shared among many other legal commentators. For example, Lew Koflowitz writes that "[t]here are a number of reasons why lenders need to be cautious when considering taking bitcoin as collateral. For example, bitcoin volatility means that their value can drop sharply, and this is a real risk for lenders seeking to ensure the stability of their collateral."[126]

However, this volatility is a risk that all lenders must deal with when they are taking property as collateral. We have seen during the housing bubble crisis of 2007-2008 that even low volatility assets such as houses are not protected from a drastic plunge in their market value.[127] In reality, this issue flowing from volatility risk can easily be counterbalanced by the lender providing a lower amount of liquidity compared to the value of the collateral. Here is how Olga Kharif explains the way lenders adapt to the reality of cryptocurrency:

> One problem is that bitcoin's price swings violently, which can make it dangerous for lenders to hold. That means the terms can be steep. Someone looking to tap $100,000 in cash would probably need to put up $200,000 of bitcoin as collateral, and pay 12 per cent to 20 per cent in interest a year, according to David Lechner, the chief financial officer at Salt, which has arranged dozens of loans.[128]

Ergo, it is not so much that bitcoins are unattractive as collateral because of their volatility like some lawyers argue, but that the borrowers will need more of their bitcoins to secure a loan. Moreover, to some lenders willing to accept the risks, the volatility in a cryptocurrency's value produces investment opportunities that prove advantageous compared to traditional currencies.[129]

(c) The Blanket Lien and the Non-Negotiability of General Intangibles

Some authors have argued that Article 9 of the UCC could "kill the use" of bitcoins because of the way blanket liens work when general intangibles are

---

letters/2015/march/31/bank-notes/bank-notes-spring-2015/bkn5-bitcoin-is-it-a-viable-security-asset > .

[126] Lew Koflowitz, "Lenders Face Serious Issues in Taking Bitcoin as Collateral", *BPlans*, online: < https://articles.bplans.com/lenders-face-serious-issues-taking-bitcoins-collateral/ > .

[127] See e.g. David Streitfield, "A Town Drowns in Debt as Home Values Plunge", *NY Times* (10 November 2008), online: < http://www.nytimes.com/2008/11/11/business/11home.html > .; Les Christie, "Home prices in record plunge", *CNN Money* (12 February 2009), online: < http://money.cnn.com/2009/02/12/real_estate/Latest_median_prices/ > .

[128] Olga Kharif, "Lenders are offering loans with bitcoin and digital currency as collateral", *The Independent* (14 December 2017), online: < http://www.independent.co.uk/news/business/news/bitocin-loans-digital-currency-collateral-ethlend-coinloan-nebeus-a8109991.html > .

[129] See Bierer, *supra* note 10 at 83. See also Jason M. Weinstein, "What Businesses Really Need To Know About Bitcoin", (2014) *Law 360*, online: < https://www.law360.com/articles/515708/what-businesses-really-need-to-know-about-bitcoin > .

Electronic copy available at: https://ssrn.com/abstract=3548126

involved.[130] They brought forth the idea of a bakery accepting bitcoins that also has a loan from a bank, which is secured by its "inventory, goods, equipment, accounts, and general intangibles whether now existing of hereafter acquired." In other words, the bank has a security interest in all of the bakery's property that is not real estate; this type of arrangement is referred to as a "blanket lien": "A lien is an interest in a borrower's property that serves as collateral to be used to pay off a lender, should the borrower default. If there are liens in bitcoins, the blockchain wouldn't provide that information."[131] When a customer pays the baked goods in bitcoins, those bitcoins become part of the bakery's collateral and the bank's security interest attaches to them. Why is that? Because it is provided under UCC § 9-315(a) that "a security interest attaches to any identifiable proceeds of collateral,"[132] and proceeds are defined as "whatever is acquired upon the sale, lease, license, exchange, or other disposition of collateral."[133] And while the bitcoin transactions are listed on a public ledger providing information on ownership of each bitcoin, for now the ledger provides no information on liens or similar security interests that may attach.[134]

The problem is that the security interest never detaches from the bitcoins because it "continues in collateral"[135] and will remain with the collateral through subsequent transfers as well.[136] Thus, "when the bakery uses the same bitcoin to buy flour from a supplier, the bank's security interest will continue to encumber them."[137] The supplier who receives the bitcoins will not be protected by the "buyer in ordinary course" provision since the provision only gets rid of security interests in "goods."[138] The bakery is merely an example to illustrate that each time a person whose property is subject to a security interest in general intangibles becomes the owner of a bitcoin, the said bitcoin becomes burdened with the security interest.[139] Jeanne Schroeder rightly points out that "general

---

[130] See e.g. Schroeder, *supra* note 44 at 30; Yves Smith, "Is UCC Article 9 Going to Kill the Use of Bitcoin by US Businesses?", *Naked Capital* (13 March 2014), online: <https://www.nakedcapitalism.com/2014/03/ucc-article-9-going-kill-us-bitcoin-us-businesses.html>; Bob Lawless, "Is UCC Article 9 the Achilles Heel of Bitcoin?", *Credit Slips* (10 March 2014), online: <http://www.creditslips.org/creditslips/2014/03/is-ucc-article-9-the-achilles-heel-of-bitcoin.html>.

[131] See Perkins Coie LLP, "Perkins Coie: The UCC and Bitcoins — Solution to Existing Fatal Flaw", *CoinDesk* (29 January 2015), online: <https://www.coindesk.com/perkins-coie-bitcoin-can-learn-real-estate-law/>.

[132] See UCC § 9-315(a)(2).

[133] See UCC §9-102(a)(64)(A).

[134] See Perkins Coie LLP, *supra* note 131.

[135] See UCC § 9-315(a)(1).

[136] See UCC § 9-325.

[137] Lawless, *supra* note 130.

[138] See UCC, § 9-332(a). Same thing goes for buyers in the ordinary course of business, see UCC § 9-320(a).

[139] See See Perkins Coie LLP, *supra* note 131.

Electronic copy available at: https://ssrn.com/abstract=3548126

intangibles are non-negotiable," meaning that unlike most personal property, "once a general intangible becomes encumbered by a security interest, it can never become unencumbered even by a transfer to a bona fide purchaser for value."[140] Negotiation exceptions allow certain parties under certain conditions to take the assets free of security interests.[141] Only certain transferees of general intangibles do take assets free of unperfected security interests,[142] but this does not apply to bitcoins. Moreover, this exemption rule only applies when security interests are not perfected, yet chances are that lenders granting a general line of credit or other commercial loan always perfect their security interest through registration.

Security interests in general intangibles are very prevalent among businesses benefiting from a bank secured line of credit. In these situations, using non-negotiable bitcoins is much more disadvantageous compared to money since transferees of money take it free of a pre-existing security interest.[143] Indeed, UCC § 9-332(a) provides that: "A transferee of money takes the money free of a security interest unless the transferee acts in collusion with the debtor in violating the rights of the secured party."[144] This is what legal scholar Jeanne Schroeder calls the "super-negotiability" of money.[145] Commercial parties never have to worry that the United States currency used in a transaction is encumbered by a security interest. Contrary to money, bitcoins are are not super-negotiable under the present state of the law. Coming back to our bakery example where bitcoins are used to buy bread, we should assume in this scenario that the bank took the necessary steps to perfect its blanket lien security interest. This gives the bank a superior property interest in the cryptocurrency, meaning that it can seize it in whoever's hands it is found. In theory, this decreases drastically the practicality of using bitcoins as a medium of exchange.

In practice however, the theoretical concern might be overstated for two reasons. First, the perfection rules as to when collateral is transferred to a new debtor provide that the perfection lapses after a time when there is a change in jurisdiction for the debtor or the collateral.[146] Indeed, UCC § 9-316(a) states that:

> a security interest perfected [. . .] remains perfected until the earliest of:
>
> (1) the time perfection would have ceased under the law of that jurisdiction;

---

[140] See Schroeder, *supra* note 44 at 8, 34.

[141] *Ibid*. at 34.

[142] See UCC, § 9-317.

[143] UCC § 9-332.

[144] *Ibid*.

[145] Schroeder, *supra* note 44 at 14.

[146] But see *ibid*. at 40-41 on the idea that if bitcoin truly becomes a payment system, it will be subject to the rolling continuous perfection because of how the rules under UCC § 9-316(a) are set out.

Electronic copy available at: https://ssrn.com/abstract=3548126

> (2) the expiration of four months after a change of the debtor's location to another jurisdiction; or
> (3) the expiration of one year after a transfer of collateral to a person that thereby becomes a debtor and is located in another jurisdiction.[147] (Emphasis added)

Second, it is quite unlikely that the bank to which the security interest belong will go after the bitcoins once they are transferred to different parties and circulating on the market. Chances are that by the time any action is taken to retrieve the bitcoins, they will have exchanged many hands. By then, the bitcoins will be so spread apart and the security interests' portion attached to each bitcoin unit will be so minimal that the costs to recover them will far outweigh the returns. But, if by misfortune, a big payment has been made to a single commercial party with bitcoins burdened by a security interest, the bank might want to follow through with the procedure to get them back.

The current legal regime creates some risks for bitcoin users. This greatly affects bitcoin's liquidity and decreases its utility as a payment system, consequently diminishing the overall value of transacting with cryptocurrency.[148] To unleash bitcoin's full potential, Schroeder suggests adding a super-negotiation rule for cryptocurrency that would be similar to the super-negotiable regimes for money, deposits accounts and investment property.[149]

(d) Relevance of Due Diligence

The secured party will usually conduct due diligence before signing any agreement providing a loan against collateral. With bitcoin, there are practical questions at the due diligence stage which may be impossible to answer, hence circumventing the relevance of such verifications. Is the borrower's bitcoin already encumbered by a security interest? Does another party already have an interest in the asset that could rank ahead? Is it possible for the secured party, by reviewing the blockchain, to know that there have not been any prior borrowings against the bitcoin? While bitcoin users can monitor and record transactions, the blockchain does not currently allow them to monitor and record borrowings or security interests.[150] To remedy this, it has been proposed that the private key related to the bitcoins used as collateral could notify the prospective lender when a security interest in it had been provided by the bitcoin owner. Nonetheless concerns were raised since this notice may entirely foreclose the borrower's ability to transfer his interest, plus this type of notice is not customary yet.[151]

---

[147] UCC § 9-316(a).

[148] See Schroeder, *supra* note 44 at 8.

[149] *Ibid*. at 43.

[150] Sandra Appel, *supra* note 32.

[151] Sandra Appel, *supra* note 32.

Electronic copy available at: https://ssrn.com/abstract=3548126

5. FINDING SOLUTIONS AND BUILDING A FRAMEWORK

(a) Due Diligence and Paperwork

Before extending credit to a borrower, creditors should go through the necessary due diligence and take steps to ensure that all bitcoin wallets are disclosed. Martinson and Masterson adequately pointed out that the current due diligence questionnaires used by creditors for vetting potential borrowers contain inadequate language to capture such accounts: "These forms typically solicit information regarding any bank accounts or similar holdings. Because Bitcoin accounts are not provided by a bank and Bitcoin wallets may not be thought of as deposits, potential borrowers might exclude them from their disclosure and believe their responses to be correct."[152] For that specific reason, it would be wise for creditors and their counsel to incorporate diligence questions specifically targeting bitcoin assets, for example by asking the potential borrower if he maintains a bitcoin wallet, holds on to any bitcoin assets, or conducts business using bitcoin. As some practising lawyers point out, the lenders may need to do significant diligence on the wallet provider, as many of them are based in "offshore jurisdictions" and are likely to be uncooperative when dealing with traditional financial institutions.[153]

And if borrowers build up funds in their bitcoin wallets in the conduct of their business activities, creditors would be wise to draft credit agreements incorporating: (1) covenants governing the amount held in such wallets; (2) definitions indicating whether the amounts will be treated as cash equivalents for financial covenant calculations, and (3) representations and warranties that the wallets are to be used for legitimate transactions in the ordinary course of business only.[154]

Ultimately, because of the risks — extreme volatility, relative anonymity, inaccessibility through normal enforcement process, complete irreversibility of payment — some creditors may prefer to limit or prohibit the use of bitcoin by the borrower. In this case, the lending documents should include explicit clauses to this effect: the credit agreement could contain covenants prohibiting the borrower from using or accepting bitcoin, or operating bitcoin wallets altogether.[155]

(b) Creating a New Category for Cryptocurrency

Within our existing legal system, bitcoin could easily be used as collateral for loans if the security interest was simple to establish and enforcement possible when needed. In their seminal article "Bitcoin: A Primer for Policymakers," Jerry

---

[152] Martinson & Masterson, *supra* note 9 at 17.

[153] Fanning, Pierce & Marsden, *supra* note 125.

[154] Martinson & Masterson, *supra* note 9 at 17.

[155] *Ibid*. at 17.

Electronic copy available at: https://ssrn.com/abstract=3548126

Brito and Andrea Castillo conclude by specifically advocating in favour of making legal change "that takes into account the technology's unique nature."[156] This includes creating a new category of assets for bitcoin in the PPSA and the UCC when developing policy and implementing new regulations on secured lending. Some authors have proposed to cover "digital currency,"[157] but it would be more careful to keep the category as narrow as possible for now to prevent that any type of digital currency is swept in. What is most important at this stage is only the broad concept of integrating bitcoin into the secured lending framework. Indeed, the exact definition should be up for debate and amended as the use and the technology develops.

As discussed earlier,[158] the rules at UCC § 9-314 do not at the moment allow a lender to perfect his security interest in cryptocurrency through control, as this is only permitted for "investment property, deposit accounts, letter-of-credit rights, or electronic chattel paper." The Ontario PPSA has similar limitations for perfection by control because it is limited to investment property, and as mentioned earlier, bitcoin does not fit into the category.[159] One way to remedy this situation and facilitate the use of cryptocurrency as collateral would be to add it as a new category of assets altogether, which entails:

1. A definition of cryptocurrency would need to be added at the beginning of the act. This definition could be up for debate and refined through the use and the technological development. The fact is that blockchain technology was originally created to solve the double-spending problem of digital currency, and its potential uses are almost limitless. Therefore, the definition must be flexible enough to encompass future evolutions of cryptocurrency but remain narrow enough to not sweep in other uses of blockchain.[160]
2. Cryptocurrency would need to be added to the list of assets over which a security interest can be perfected through control.[161]
3. Rules defining and explaining what constitute control over a cryptocurrency asset would have to be enacted as well. In Ontario, such rules are set out in the STA,[162] but since bitcoin is not a security, the rules for control could be included in the PPSA.
4. If needed, remedies specific to bitcoin in case of default could also be set out in the legislation. This would provide guidance to the market players as to what their rights are and what level of risk they are looking at when lending against a borrower's cryptocurrency. Again, this should be up for

---

[156] Brito, *supra* note 14 at 36.

[157] Sandra Appel, *supra* note 32.

[158] See section "Under the UCC".

[159] See PPSA, s. 1(2). See also STA, *supra* note 55 ss. 23-26.

[160] See Schroeder, *supra* note 44 at 44.

[161] Bierer supports such an amendment to Article 9 UCC, see *supra* note 10 at 88.

[162] STA, *supra* note 55 ss. 23-26.

Electronic copy available at: https://ssrn.com/abstract=3548126

debate and thought through the use and technological development of the blockchain technology.

5. Finally, since cryptocurrency would be a new type of asset over which security interests can be created in various ways and structures, new rules with regards to priority between secured lenders would also need to be set out.[163]

By recognizing the lender's control over the collateral as sufficient "publication", the law allows market players to safely engage in various commercial relationships that benefit them, but that would not otherwise. For example, if a debtor were to transfer its bitcoins to the creditor, thereby giving him control over them, the creditor could simply hold them, as this would be the default setting. But, he also could actively trade them if the security agreement permits it, as the debtor and the creditor may want to engage in such a structure where the risks of loss and the potential profits are allocated amongst them.[164]

(c) Perfection of the Security Interest Through Control

Allowing perfection of a security interest in bitcoin by possession, or control, would be a great addition to the PPSA and UCC. The parties could decide conventionally what constitutes proper "possession or control of bitcoin" and include it in the security agreement. But the fact is that treating a security interest in bitcoin the same way the law does when money or other investment property are involved by allowing perfection by control would greatly benefit the market of secured lending using cryptocurrency as collateral.

(i) Taking physical control of cryptocurrency

The bitcoin that is used as collateral could be placed by the borrower on a flash drive and then the physical drive could be delivered to the lender as a security. This method has the effect of materializing the bitcoin into the drive, so that the drive with the bitcoin on it becomes the asset used as collateral. As a flash drive qualifies under "goods", delivering it to the lender would be the equivalent to provide the lender with perfection by possession.[165] Presumably, the borrower would choose to protect the flash drive with a password to ensure that the lender does not transfer the bitcoin to a third party, and that he has no incentive to transfer the physical flash drive either. The same way, the lender will almost certainly want assurance that he will be able to access the bitcoin on the drive if the borrower defaults. To do so, a third party or an escrow agent could

---

[163] Schroeder, *supra* note 44 is also of the opinion that priority rules would be needed. It is necessary because perfection both by registration, which is not ideal, and by control will be permitted, and because there will be different type of structure and various security agreements, e.g. blanket liens, specific biparty agreements, agreement involving an intermediary, etc.

[164] See Bierer, *supra* note 10 at 86.

[165] Sandra Appel, *supra* note 32.

Electronic copy available at: https://ssrn.com/abstract=3548126

be involved by holding the password and releasing it only when certain conditions are met.

We have touched on the subject earlier, but this type of transactional arrangement may not be well received by adherents to the cryptocurrency and blockchain technology community. Some of them argue that the value of bitcoin transactions comes from the absence of a third-party intermediary.[166] By putting bitcoin on a flash drive, perfection can be accomplished, but the protection of the parties' security interest will most likely necessitate the involvement of an escrow agent, which defeats the "interaction without intermediary" idea. Nonetheless, under the current secured transactions legal regime, transferring bitcoin on a flash drive is by far preferable to registration, provided that the lender does not lose the flash drive and that the escrow agent has the private key and password.

(ii) Transferring the bitcoin

Lenders can ask the borrowers to transfer the bitcoin or the bitcoin interest to them until repayment has been made, which would be similar to endorsing a stock certificate.[167] This transfer would give the creditor control over the cryptocurrency assets. In this situation, the borrowers must be comfortable that the bitcoin will be returned to them once the loan has been repaid. Practically, both parties to the secured transaction have to ensure that their agreement addresses the transfer, as well as other situations such as the transfer back upon payment and any fluctuation in the value of the asset used as collateral. As Sandra Appel writes, "[t]his type of agreement may obviate the need for any security agreement or PPSA registration as the transaction would be an outright transfer."[168]

While this is true, it does not mean that the PPSA becomes irrelevant altogether for such situations. In fact, the PPSA specifically covers secured transactions that, while not security interests per se, are deemed as such by law.[169] Since the PPSA applies to "every transaction without regard to its form and without regard to the person who has title to the collateral that in substance creates a security interest,"[170] one could argue that it already covers these transfers of bitcoin or of bitcoin interests. To make it clear however, Canadian provinces would need to amend their respective PPSAs and add this type of transactional arrangement to the lists of transactions to which the PPSA applies.

Similar to the physical transfer of bitcoins on a flash drive, the virtual transfer of bitcoins could be made to an escrow agent, who will hold the cryptocurrency in security for the creditor, and the borrower.[171] Even if

---

[166] *Ibid.*

[167] *Ibid.*

[168] Sandra Appel, *supra* note 32.

[169] See PPSA, ss. 2(b)-(c).

[170] See PPSA, s. 2(a).

[171] See Martinson & Masterson, *supra* note 9 at 18-19.

Electronic copy available at: https://ssrn.com/abstract=3548126

importing an intermediary into the transaction is contrary to the very idea of cryptocurrency, the power of the intermediary may be significantly diminished by the use of smart contracts,[172] and may prove a necessary addition for complex financing structures or when the lender lacks the ability to securely store the cryptocurrency assets.[173] While an escrow agent may provide for additional certainty and security, "the benefits such as potential trading, profit sharing, or grants of interest earned may not be present," as they may be eaten up by the escrow service fee.[174]

The idea behind laws specifically governing security interests taken in property, rather than letting the parties set their own rules entirely through contract law, is to provide lenders more certainty and safety. Thus, these types of bitcoin transfer, whether an escrow agent is involved or not, cannot merely be considered as "outright transfers". Instead, legislative bodies should deem such transfers as effectively creating a security interest and taking possession, or control, over the collateral. With time, use, market norms and technological development will most likely demand that precise rules be added to govern such transfers.

(d) Solving Traceability Issues

The gravity of traceability issues when it comes to bitcoin transactions is most likely overstated. As a matter of fact, some legal commentators believe that lenders will be able to trace the transferred bitcoins. For example, Jeanne Schroeder qualifies the bitcoins transfers as "pseudonymous," which means that the bitcoins can be traced from one address to the other. This means that the moment the bitcoin come into the hands of an identifiable transferee, the secured party will be able, and have the right to, repossess it.[175] Others like Böhme and Tsukerman also agree that bitcoins can be traced back through the various transactions, as they are all recorded on the public ledger.[176] Koji Takahashi wrote that "[w]hen we consider whether it is possible in law to obtain the recovery of stolen cryptocurrency units, what matters is normative, rather than technical, traceability of the stolen units."[177]

---

[172] See what the cryptocurrency community is already doing and how third-parties are acting in the market in section "The Cryptocurrency Community's Technical Solution".

[173] See Bierer, *supra* note 10 at 86.

[174] *Ibid.*

[175] See Schroeder, *supra* note 44 at 42. See also Diedrich, *supra* note 13 at 53, 127-129 for a discussion on the non-anonymity of Ethereum.

[176] See respectively Rainer Böhme et al, "Bitcoin: Economics, Technology, and Governance" (2015) 29:2 J Econ. Perspect 213; Misha Tsukerman, "The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future" (2015) 30 Berkeley Technol. Law J. 1127 at 1128.

[177] Koji Takahashi, "Technical traceability and normative traceability", *Blockchain Cryptocurrency Law* (10 November 2015), online: <http://cryptocurrencylaw.blogspot.ca/2015/11/technical-traceability-and-normative.html>.

Electronic copy available at: https://ssrn.com/abstract=3548126

In reality, courts have developed tracing doctrines like the first-in-first-out or the lowest intermediate balance to determine from a legal point of view whether the property can be traced to a certain source. These doctrines could apply to bitcoin transactions.[178] Consider for example the following situation: A receives five bitcoins from B and then five bitcoins from C, then sends seven bitcoins to D while keeping three bitcoins, which are sent back to his account as output. The first-in-first-out analysis would allow the court to deem that B's five bitcoins and two of C's bitcoins are now in possession of D, the rest of C's three bitcoins still in possession of A. The court could also decide to go with a pro rata approach and apply a 50% (5/10) split to each output on the basis that the bitcoins from B and C were proportionately divided in the output. And if D has been colluding with A, then the court might decide that all C's bitcoins went to D.[179]

Furthermore, the law can account for facts outside of the blockchain, like when parties to a fraudulent transaction work together to hide a trail, or when a party converts the bitcoin into dollars, which may require identifying information.[180] If A wants to send C five bitcoins without leaving a trail, he could send them to B and have B sending them from one of his other account to C afterwards, since the blockchain only records transactions from separate accounts. Yet, upon evidence of collusion between A and B, the court could easily deem traceable to A the five bitcoins sent to C.[181] Also, legal tracing does not require an exact trail to achieve fair results. Suppose a substantial number of bitcoins would be fraudulently transferred, and a known partner of the defrauder would subsequently acquire a new house or a new car without explanation. This trail could be sufficient to trace the assets back to the lender or the borrower, depending on how the fraudulent party is.[182] We could even look at the rules of Article 8 UCC to determine whether and when a security can be traced after transfers through an intermediary.[183]

Many options exist, and the law is flexible enough to practically solve a situation where a technical analysis would fail to be any help. We also need to remember that there are legal mechanisms which can be deployed preventively, that is before the transfer is made. For instance, it is possible in the United States per UCC § 4A-503 to ask the court to grant an injunction or a restraining order with respect to funds transfers. In Canada, similar temporary injunctions that

---

[178] Richard L. Barnes, "Tracing Commingled Proceeds: The Metamorphosis of Equity Principles into U.C.C. Doctrine" (1990) 51 Univ Pittsburgh Law Rev 281. at 296.

[179] See McJohn & McJohn, *supra* note 117 at 12-13.

[180] See Kavid Singh, "The New Wild Est: Preventing Money Laundering in the Bitcoin Network" (2015) 13:1 Northwest J. Technol. Intellect Prop. 37 at 60.

[181] See McJohn & McJohn, *supra* note 117 at 13.

[182] See e.g. for a similar situation Yessi Bello Perez, "Czech Police Seize $345,000 Property Linked to Bitcoin Hack", *CoinDesk* (1 April 2015), online: < https://www.coindesk.-com/czech-police-seize-345000-property-linked-to-bitcoin-hack/ > .

[183] See Kenneth C Kettering, "Repledge Deconstructed" (1999) 61 Univ. Pittsburgh Law Rev. 45.

Electronic copy available at: https://ssrn.com/abstract=3548126

freeze the assets of a party exist under the name of Mareva injunctions,[184] and in the United Kingdom they have recently been renamed as ''freezing injunctions."[185] Would such a freeze be effective to prevent a debtor from transferring his bitcoins funds? Martinson and Masterson express some doubts on that aspect as cryptocurrency trading does not happen on traditional exchanges.[186] Nonetheless, it may only be a question of time before most of the cryptocurrency exchanges become registered businesses, with licences, and with a legitimate interest to conduct lawful activities, which include giving effect to court injunctions pronounced against their clients. This is pure speculation, but the future of legally protecting the secured lenders of a transaction involving cryptocurrency looks bright on both fronts: to prevent the illegal transfer and to retrieve the transferred funds.

(e) Looking at UCC Article 8

The UCC Article 8 structure provides a solution to the blanket lien problem and the non-negotiability of bitcoins described earlier and provides legal certainty for the parties involved. Instead of considering bitcoins as general intangibles, the said structure makes them financial assets as defined in UCC Article 8.[187] ''Financial assets" are defined as assets held by a ''securities intermediary"[188] that maintain ''securities accounts"[189] for others, commonly named account holders, in the ordinary course of business, provided the intermediary agrees to treat the assets as financial assets under UCC Article 8.[190] How does it work? Consider a future debtor who is the direct owner of bitcoins worth $100,000 and he wants to grant a security interest in them in exchange to secure a loan. He opens a securities account with a security intermediary, to which he transfers the bitcoins. The debtor and the securities intermediary must agree that the bitcoins constitute financials assets for the purpose of UCC Article 8, and because the debtor is no longer the direct owner of the bitcoins, he now

---

[184] See Aetna Financial Services Ltd. v. Feigelman, 1985 CarswellMan 19, 1985 CarswellMan 379, [1985] 1 S.C.R. 2, 29 B.L.R. 5, 55 C.B.R. (N.S.) 1, 4 C.P.R. (3d) 145, 15 D.L.R. (4th) 161, [1985] 2 W.W.R. 97, 32 Man. R. (2d) 241, 56 N.R. 241, [1985] S.C.J. No. 1 (S.C.C.).

[185] See James Farley, ''Mareva — more than a cigar!", *McCarthy Tétrault LLP* (26 March 2010), online: < http://www.mccarthy.ca/article_detail.aspx?id = 4915 > .

[186] Martinson & Masterson, *supra* note 9 at 18.

[187] See gen. Schroeder, *supra* note 44 at 47-66.

[188] See UCC § 8-102(a)(14): "'Securities intermediary' means: (i) a clearing corporation; or (ii) a person, including a bank or broker, that in the ordinary course of its business maintains securities accounts for others and is acting in that capacity."

[189] See UCC § 8-501(a): "'Securities account' means an account to which a financial asset is or may be credited in accordance with an agreement under which the person maintaining the account undertakes to treat the person for whom the account is maintained as entitled to exercise the rights that comprise the financial asset."

[190] See UCC § 8-102(a)(9). See also Schroeder, *supra* note 44 at 59.

Electronic copy available at: https://ssrn.com/abstract=3548126

holds a securities entitlement.[191] Now, the bitcoins are metamorphosed from general intangibles to investment property through a securities intermediary agreeing to treat it as a financial asset subject to UCC Article 8.[192]

This structure has many advantages. First, the security interests in the account of the creditor, or account holder, can be perfected by a control agreement, instead of a public filing, which maintains privacy.[193] Second, the bitcoins that are placed in the account become super-negotiable.[194] They would no longer be subject to liens granted in general intangibles, and the structure allows for bitcoin to be transferred free from security interests if the accountholder gives value for the bitcoins in the account without notice of existence of security interests.[195] Thus, existing but unknown security interests are not a problem anymore. Third, the bitcoins in the securities account are not property of the intermediary and would not be subject to claims of the intermediary's creditors.[196] In fact, transfers of bitcoins are made by the intermediary upon the instructions of the account holder, that is the true owner, which provides an additional layer of privacy for the account holder. It also means that the intermediary has the obligation to maintain bitcoins in quantity equivalent to the amount of bitcoins credited to the securities account.[197] Finally, the structure is well known in commercial transactions: perfection by control gives the secured creditor more control. This control creates legal certainty, and in turn should make access to credit both more available and less expensive. Suddenly, bitcoins held in a securities account become attractive assets to be used as collateral and leveraging them to secure debt financing is facilitated.

(f) The Cryptocurrency Community's Technical Solution

The technology is new, highly promising and its community is filled with innovators that are working day and night to improve its use through many variables, including security, anonymity, and control. Also, many members of this community are libertarian minded, meaning that they do not believe in government solutions, and much prefer voluntary or coercion-free answers to arising problems.[198] Thus, it is extremely probable that the blockchain

[191] See Schroeder, *supra* note 44 at 61.

[192] See Schroeder, *supra* note 44 at 47-66. See also Perkins Coie LLP, *supra* note 131.

[193] See UCC, § 9-314(1), § 9-312(a), § 9-102(a)(49), § 9-106(a), § 8-106(d).

[194] See Schroeder, *supra* note 44 at 56.

[195] See UCC § 8-502.

[196] See UCC § 8-503(a), § 8-507.

[197] See UCC § 8-504(a).

[198] See e.g. Malcolm Campbell-Verduyn, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, 1st ed. (Abingdon, UK: Routledge, 2017); Aaron Koenig, *A Beginners Guide to Bitcoin And Austrian Economics* (München, DE: FinanzBuch Verlag, 2015); Oliver Dale, "Bitcoin & Libertarianism — A Dream Combination?", (25 January 2018), online: *Blockonomi* <https://blockonomi.com/bitcoin-libertarianism/>; Wendy McElroy, "The Satoshi Revolution — Chapter 2: Was Satoshi a Libertarian

Electronic copy available at: https://ssrn.com/abstract=3548126

community will try to develop a technical solution that would entirely disrupt the methods by which lenders take the borrower's assets as collateral. An autonomous trust agent designed specifically to receive from the borrower a transfer of digital assets as collateral and to release the assets back either to the lender or to some other third party upon default, could be programmed through smart contracts on platforms like Ethereum by the secured transaction parties.

The terms and conditions of the underlying agreement between the parties to the transaction would be automatically executed by the smart contract. Because the code of the contract is transparent, unbiased and incorruptible, the creditor and the debtor would be confident in the transactional arrangement. Additionally, this structure can be setup at virtually no cost to the parties, except the nominal costs of operating and maintaining the nodes.[199] To some extent, this is already existing practice. For example, this is how ETHLend offers a fully decentralized peer-to-peer lending Smart Contract which runs on the Ethereum blockchain and uses digital tokens as collateral:[200]

> EthLend enables secured lending to Ethereum users. Borrower issues a loan request. The loan request creates a Smart Contract on the Ethereum Blockchain. Next, the borrower inserts data to the Smart Contract, such as the loan amount, the premium (interest rate) and time to borrow.
>
> The borrower then inserts the Digital Token address and the amount of tokens that are used as a collateral. After all the data is set, the borrower transfers the Digital Tokens to the Smart Contract. Now, lenders can fund the loan.
>
> In case the borrower does not repay on time, the Smart Contract transfers the Digital Tokens to the lender's Ethereum address. From this point, the lender can either hold or sell the Digital Tokens on Cryptocurrency Exchange to cover any losses.
>
> [. . .] What we actually created is a decentralized application that is running on the Ethereum Blockchain. This means that the data is not stored on centrally located serves. Therefore, even EthLend cannot move the tokens from the Smart Contract.[201]

Smart contracts can perform relatively simple tasks like monitoring the bank accounts of a borrower by relying on third-party data provided by "oracles"[202] to determine if certain financial covenants are fulfilled. Yet, it is questionable whether the machines will be able to read and execute more complex terms and conditions that are part of modern loan agreements.[203] Case in point, are smart

---

and Anarchist? (Part 4)" (11 November 2017), online: < https://news.bitcoin.com/satoshi-revolution-chapter-2-satoshi-libertarian-anarchist-part-4/ > .

[199] This technical solution had been proposed for e.g. by Armstrong & Trivun, *supra* note 13.

[200] See "ETHLend", online: < https://ethlend.io/en/ > .

[201] ETHLend & Stanislav Kulechov, *EthLend Introduces Secured Loans on Ethereum Blockchain* (Press Release, CoinTelegraph, 2017).

[202] Oracles are trusted sources.

Electronic copy available at: https://ssrn.com/abstract=3548126

contracts able to determine if a borrower has made reasonable best efforts to cure an event of default? Or if a lender has acted in bad faith? Without being restricted to, these are the kind of legal standards that are inherently subjective and require, for now, human intellect to be accurately interpreted. It will still take at least a few years, if not many, before the technology is advanced enough to perform these fundamental tasks.[204]

Also, there are additional risks with using smart contracts for secured loan agreements which are linked to the fact that cryptocurrency transactions are immutable, hence final. This means that there is limited recourse for the parties to recover their funds if the lender, the borrower or even a third party manages to exploit a bug in the code of the smart contract and misappropriates the collateral funds.[205] Maybe the security protocols have been improved and the risks associated with smart contracts have been drastically reduced, and maybe there are solutions,[206] but we cannot do away with the fact that the collective imagination is marked by the famous hack of the decentralized autonomous organization (DAO) in 2013.

What happened with the DAO in 2013? An unknown hacker took advantage of a bug in the Ethereum platform and stole $150 million worth of Ether, the cryptocurrency chosen to finance the project. In the aftermath of the DAO hack, the Ethereum community decided that the implications were severe enough to justify "forking" the blockchain, which means that every node of the networks agreed to undo the record of the hack from the transactions on the ledger. The polarizing decision led to the split between Ethereum, with the nodes in favour of the update, and Ethereum Classic, with a minority of the nodes that did not agree with record update.[207] In reality, as blockchains continue to scale and an ever-increasing number of cryptocurrency users are added to the market, undoing an illegal or contested transaction by updating every node's record of transaction history becomes unrealistic and impractical.

Another present practice from which we could inspire ourselves to find solutions is SALT Lending. Their platform allows holders of blockchain assets to leverage their holdings as collateral for cash loans without them having to sell their tokens.[208] First, the loan is created when the borrower sends the collateral to the SALT Oracle Wallet, a multi-signature blockchain wallet that stores collateral and automatically enforces lending terms, and receives the funds in his

---

[203] This issue has been raised by Armstrong & Trivun, *supra* note 13.

[204] *Ibid.*

[205] This issue has been raised by Armstrong & Trivun, *supra* note 13.

[206] See e.g. "Tezos", online: < https://www.tezos.com/ >. Voting rights are incorporated into the project's native token, theoretically allowing token holders to address any issue, including security issues, through the on-chain governance structure. This means that if a transaction had to be undone, or the protocol must be changed, it can be realized efficiently and democratically.

[207] See Armstrong & Trivun, *supra* note 13.

[208] "SALT Lending", online: < https://saltlending.com/ >.

Electronic copy available at: https://ssrn.com/abstract=3548126

bank account. Then, the loan is repaid by the borrower in timely and periodic payments to the lender. Finally, the loan is completed when, upon repayment of the loan, the collateral which was kept in a custodial relationship is returned to the borrower.[209] Thus, throughout the arrangement, the collateral remains the property of the borrower and any price appreciation or depreciation belongs to the borrower.[210]

Even if blockchain assets are provided by borrowers as collateral to secure their loans, loans made through the platform are both denominated in and repaid with traditional currencies like the United States dollar, the United Kingdom pound sterling or the Japanese yen. In fact, it is not required to have blockchain assets at all to become a lender on the platform. It is only required that lenders are accredited investors: in the United States, under *Regulation D*,[211] under the *Securities Act of 1933*[212] and the SEC. Moreover, they have to pass an internal suitability test. This process applies to existing lenders and regulated entities such as Broker Dealers, Private Equity funds, family offices, etc.[213] Other companies like Nebeus[214] from the United Kingdom and CoinLoan[215] from Estonia provide similar services.

6. PROPOSITION: THE PPSA AND THE CCQ

The goal of having a defined framework for secured lending is to create as much certainty as possible for market players. With this in mind, having a unified set of laws between jurisdictions is favorable.[216] Now, creating a new unified framework for using cryptocurrency as collateral in secured transactions will prove easier in Canada and in Québec than elsewhere. This is the reason why we chose to include an enactment proposition for these jurisdictions specifically. As a matter of fact, in the United States, the National Conference of Commissioners on Uniform State Laws could come up with a unifying framework that would enable a more widespread use of bitcoin as collateral in secured transactions, but it is unlikely in the short term.[217] The proposal for new uniform laws "is a slow

---

[209] See Hansen & Boehm, *supra* note 21 at 19 for conditions to ensure that the depositors are treated as owners of the bitcoin instead of the custodian.

[210] See Roger Aitken, "Disruptive Blockchain-Backed SALT Loans Platform In Launch To Leverage Bitcoin Assets", *Forbes* (19 May 2017), online: < https://www.forbes.com/sites/rogeraitken/2017/05/19/disruptive-blockchain-backed-salt-loans-platform-in-launch-to-leverage-bitcoin-assets/ > .

[211] *Regulation D*, 2012, 17 CFR § 230501 Ff [*Regulation D*].

[212] *Securities Act of 1933*, 1933, 48 Stat 74 PubL 73—22 15 USC § 77a Ff [*Securities Act of 1933*].

[213] See Aitken, *supra* note 210.

[214] See "Nebeus", online: < https://nebeus.com/ > .

[215] See "CoinLoan", online: < https://coinloan.io/ > .

[216] See Bierer, *supra* note 10 at 80.

[217] *Ibid*. at 85.

Electronic copy available at: https://ssrn.com/abstract=3548126

and deliberative process," and even if accepted, the uniform laws must subsequently be adopted by the individual states.[218]

(a) Amendments to the PPSA, the STA and the CCQ

A definition of cryptocurrency needs to be added to the PPSA, the STA and the *Civil Code of Québec*[219] (CCQ). In this article, a definition will be proposed, but it should be thoroughly debated and refined through use and technological development. Indeed, as expressed earlier, blockchain technology was originally created to solve the double-spending problem of digital currency, but we now realize that its potential uses are almost limitless.[220] Therefore, the definition must be flexible enough to encompass future evolutions of cryptocurrency while remaining narrow enough to not cover other uses of blockchain.[221] To achieve this, we would first add cryptocurrency to the list of s. 1(1) on definitions and interpretation in the PPSA, to the list of s. 1(1) on definitions in the STA, and to the CCQ by introducing a new article at 2714.10 respectively:

Definitions and interpretation
1 (1) In this Act,

> "cryptocurrency" means a digital or virtual currency that uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

Definitions
1 (1) In this Act,

> "cryptocurrency" means a digital or virtual currency that uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

> **2714.10**. For the application of this Act, cryptocurrency means a digital or virtual currency that uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions

Also, as mentioned previously in this article, we need to provide a mechanism by which secured parties can obtain and protect a security interest in bitcoins that would prevent illegitimate transfers. The best way to attain this is for the law to allow perfection by control of the cryptocurrency because it gives more security to the secured party.[222] Yet, it would also be a good idea to continue allowing the parties to perfect by registration if they so choose,[223] as

---

[218] *Ibid.*

[219] *Civil Code of Québec*, CQLR c. CCQ-1991 [CCQ].

[220] For a good introduction to the various uses of blockchain technology, see Swan, *supra* note 12; Tapscott & Tapscott, *supra* note 16.

[221] See Schroeder, *supra* note 44 at 44.

[222] See Schroeder, *supra* note 44 at 45.

Electronic copy available at: https://ssrn.com/abstract=3548126

there will most likely be various types of structure and various security agreements such as blanket liens, specific biparty agreements and agreements involving an intermediary. To do so, cryptocurrency needs to be added to the list of assets over which a security interest can be perfected through control in the PPSA and in the CCQ. Under the PPSA and the STA, certificated and uncertificated security, security entitlement, futures contract and a securities account can be perfected by control.[224] We need to add to this list cryptocurrency as ss. (f) to 1(2) of the PPSA in determination of control and a s. 28.1 to the STA setting out the ways in which control of cryptocurrency is achieved:

> **1**(2) For the purposes of this Act,
>
> (f) a secured party has control of cryptocurrency if the secured party has control in the manner provided under section 28.1 of the *Securities Transfer Act, 2006*;

And under the CCQ, s. 2934 provides that "[t]he publication of rights is effected by their registration in the register of personal and movable real rights or in the land register, unless some other mode is expressly permitted by law."[225] Another mode of publication effectively permitted for securities and security entitlements by the CCQ is through control.[226] We would add that cryptocurrency can be perfected the same way:

> § 6. — Movable hypothecs with delivery on cryptocurrency
>
> **2714.8**. In the case of cryptocurrency within the meaning of this Act, the requirement that the property be delivered to and held by the creditor in order for a movable hypothec with delivery to be constituted and set up against third persons may be met by the creditor obtaining control of the cryptocurrency in accordance with section 2417.9 of this Act.

Second, we must set out the ways in which control of cryptocurrency is achieved under both the PPSA/STA regime and the CCQ. We would add s. 28.1 to the STA:

> **Secured creditor's control of cryptocurrency**
>
> **28.1** (1) A secured creditor has control of cryptocurrency if,
>
> (a) the cryptocurrency is delivered to the secured party;
>
> (b) the cryptocurrency is delivered to an intermediary that has agreed that it will comply with orders that are originated by the secured creditor without the further consent of the cryptocurrency holder; or
>
> (c) another person has control of the cryptocurrency on behalf of the secured creditor or, having previously obtained control of the

---

[223] This is not an issue as PPSA, s. 23 provides that registration perfects a security interest in any type of collateral.

[224] See PPSA, s. 1(2).

[225] See CCQ, s. 2934.

[226] See CCQ, s. 2714.1 and ff.

Electronic copy available at: https://ssrn.com/abstract=3548126

> cryptocurrency, acknowledges that the person has control on behalf of the secured creditor.
>
> (2) Deliverance in s. 28.1 (1) means minimally,
>
> (a) the transfer of the private key from the debtor to either the secured creditor, the intermediary or another person having control of the cryptocurrency, and
>
> (b) a mechanism that prevents the debtor from unilaterally transferring the cryptocurrency.
>
> Consequently, deliverance includes, but is not limited to, the outright transfer of cryptocurrency from the debtor to either the secured creditor, the intermediary or another person having control of the cryptocurrency.

This proposed drafting of s. 28.1 is inspired by the rules set out in s. 25 STA for security entitlements, following Jeanne Schroeder's vision for the amendments to the UCC.[227] However, it is important be reminded that this is merely a proposition for blockchain technology and cryptocurrency as they can be currently understood. It may not be perfect for future expressions of cryptocurrency and might need from further amendments as markets uses become clearer. With regards to 28.1(2)b), an example of mechanism preventing the debtor from unilaterally transferring the cryptocurrency would be the use of multisignature wallets.[228] In the CCQ, the exact same section could be added as s. 2714.9, for the same reasons:

> **2714.9** (1) A secured creditor has control of cryptocurrency if,
>
> (a) the cryptocurrency is delivered to the secured party;
>
> (b) the cryptocurrency is delivered to an intermediary that has agreed that it will comply with orders that are originated by the secured creditor without the further consent of the cryptocurrency holder; or
>
> (c) another person has control of the cryptocurrency on behalf of the secured creditor or, having previously obtained control of the cryptocurrency, acknowledges that the person has control on behalf of the secured creditor.
>
> (2) Deliverance in s. 2714.9 (1) means minimally,
>
> (a) the transfer of the private key from the debtor to either the secured creditor, the intermediary or another person having control of the cryptocurrency, and
>
> (b) a mechanism that prevents the debtor from unilaterally transferring the cryptocurrency.
>
> Consequently, deliverance includes, but is not limited to, the outright transfer of cryptocurrency from the debtor to either the secured creditor, the intermediary or another person having control of the cryptocurrency.

For bitcoins transferred as part of lawful transactions, we need to be aware of Jeanne Schroeder's criticism of the present framework regarding the lack of negotiability rules with bitcoins.[229] Hence, we need to add a "super-

[227] See Schroeder, *supra* note 44 at 45.

[228] See discussion of multisignature wallets in this article under "Irreversibility & Traceability".

Electronic copy available at: https://ssrn.com/abstract=3548126

negotiability" rule to the PPSA and the CCQ.[230] A s. (11) to s. 28 PPSA on transactions in ordinary course of business[231] and the s. 1756.1 under CCQ § 7 on various modalities of sale in Title Two, Chapter One on sale:[232]

> **Transferee of cryptocurrency**
>
> (11) A transferee of cryptocurrency takes the cryptocurrency free of a security interest unless the transferee acts in collusion with the debtor in violating the rights of the secured party.

> III.a — *Sales Involving Cryptocurrency*
>
> **1756.1**. Where a sale involves cryptocurrency, the transferee of cryptocurrency takes the cryptocurrency free of a security interest unless the transferee acts in collusion with the debtor in violating the rights of the secured party.

As for priorities, we choose not to propose a framework, as this should be up for debate by the legislature, which will have access to more information such as the desires and needs of the market players. One way to deal with priority could simply be the application of the present framework for investment property where the secured party who obtains control has priority over all other secured parties who do not have control, and where two or more secured parties have obtained control, priority is accorded to the secured party who first obtained control.[233] Finally, similar to priorities, we thought best not to include a proposition for remedies in case of default since this should also be debated by elected members. Again, they will have access to more information than we do at this point, considering that the bitcoin market is quite new and in constant innovation. Further, the legislature is in better position to evaluate present uses, i.e. what the market placyers are already doing, as well as the desires and needs of cryptocurrency users.

7. CONCLUSION

To conclude, cryptocurrency is a decentralized digital asset that uses cryptography for security. It has value; hence it can serve as collateral for secured transactions. In all jurisdictions discussed in this article, the United States, Canada, the United Kingdom and France, bitcoin is not recognized as money for the purpose of secured lending acts. Consequently, bitcoin is relegated in a general category that encompasses assets not categorized, which leads to a few problems. Among others, it creates enforceability and negotiability issues that must be solved for bitcoin to preserve its value as a digital currency. Indeed, because transfers are irreversible and hard to trace, bitcoins seem risky assets to

---

[229] Even if her criticism applies to the UCC, it also applies to the PPSA and the CCQ.

[230] See Schroeder, *supra* note 44 at 44.

[231] See PPSA, s. 28.

[232] See CCQ, s. 1708 and ff.

[233] See PPSA, ss. 30.1(2)-(4). See also CCQ, ss. 2714.2-2714.4.

Electronic copy available at: https://ssrn.com/abstract=3548126

be used as collateral if debtor have the possibility of transferring them at any time. Moreover, there is a fear that security interests will continue to burden the cryptocurrency that has passed in the hands of a party whose property serves as security for a blanket lien.

Nonetheless, solutions exist. The main idea to facilitate the use of cryptocurrency as collateral in secured lending is to create a whole new category for it and amend the laws to create a more suitable framework. This entails that a definition of cryptocurrency must be added, as well as amendments to allow creditors to perfect their security interests in bitcoins through control. Also, it is neuralgic to add a super-negotiability so that blanket liens and other broad security interests do not unduly diminish the use of cryptocurrency. In this article, we have tried to include these solutions in a comprehensive framework for both the PPSA/STA regime in Ontario, and for the CCQ in Québec. Of course, while this article is a great step in the right direction, much remains to be discussed, debated and enacted. Even so, we ought to stay open to innovation: providing certainty and security to cryptocurrency users and market players should always be favored. The future is here, it would be unwise not to recognize it and to needlessly delay it.

Electronic copy available at: https://ssrn.com/abstract=3548126

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.

Electronic copy available at: https://ssrn.com/abstract=3548126