



07 May 2014

By: M. Sandra Appel

Bitcoin is constantly in the news. Whether you believe it is the currency of the future or just a fad, a great investment or just an easy and cheap way to effect transactions, what is not yet clear is whether bitcoin will be a financing tool and if so, whether a security interest can be taken in bitcoin.¹

As will be discussed in this bulletin, until the legislation is changed, using bitcoin as collateral will be a challenge. Currently a security interest in bitcoin may not be taken by "control" and perfecting a security interest by registration does not seem to be viable. This does not take into consideration the current security issues for holders of bitcoin at exchanges or bitcoin banks.

What is Bitcoin?

The buzz surrounding any new technological phenomenon often leads to speculation and even confusion. Fortunately, Bitcoin's official website includes a detailed FAQ section that quite clearly addresses recurring questions. For the purposes of this bulletin, a brief summary of key points is provided below.

Bitcoin is, in essence, digital money. Operating through open-source software, it is a peer-to-peer payment network that is independent of any central authority, banking intermediary or government. As a result, while it is a digital currency being used by people around the world with a "market capitalization worth nearly \$10 billion," Bitcoin is not a monetary system.²

Anyone can be a Bitcoin user. Canada has ATMs that issue bitcoin. More businesses are accepting, or planning to accept, bitcoin as payment. As Bitcoin starts to enter the mainstream, questions of security are of critical concern. Overall media coverage suggests that one of the significant attributes of Bitcoin is that trading in bitcoin is extremely secure. There is no need to "trust" anyone; there is no one person who can abuse the system. Cryptography ensures that only the owner of the bitcoin has the authority to spend them. However, while trading in bitcoin may be secure, storage of bitcoin may not. The recent demise of bitcoin exchange Mt. Gox as a result of the "loss" of over 740,000 stored bitcoin is just one example.

The way to secure the system is by the use of the blockchain. This is described as a single authoritative record of confirmed transactions which is stored on the peer-to-peer bitcoin network. This is like a "central registry" of bitcoin transactions. The blockchain apparently creates a single master registry of the already cryptologically-secured bitcoin transfers, verifying them and locking them down in a highly competitive market called mining. Briefly, the Bitcoin community monitors and records the transactions as they occur in exchange for compensation. The numbers of miners who monitor the transactions ensure that the transactions cannot be changed or reversed. So, no bitcoin holder may sell their bitcoin or percentage thereof more than one time.

Is it Possible to Borrow in Bitcoin?

(a) Bitcoin in our Current Legal System

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 borrow in bitcoin. Therefore, can bitcoin be provided as security for borrowing? If so, how does a borrower provide a lender with a security interest in the borrower's bitcoin, recognizing that bitcoin is not tangible personal property, per se.

In order to address how bitcoin can be used as collateral, it is necessary to determine what Bitcoin is in the context of our existing legal system. Currently there is no legislation or case law that specifies the regulation of Bitcoin. Canada Revenue Agency has advised that the buying and selling of bitcoin could result in capital gains (and possible capital losses) and that transactions involving bitcoin should be reported as in any other barter transaction.

It has been suggested that either securities regulations should be amended or that the Financial Transaction and Reports Analysis Centre of Canada, known as FINTRAC, the financial regulator, should weigh in and require business licences in order to trade in bitcoin, if a bitcoin exchange functions as a money services business. In the 2014 budget, the Government of Canada indicated it would be introducing anti-money laundering and anti-terrorist financing regulations that would encompass virtual currencies such as bitcoin, since banks and other governments are concerned that bitcoin may be used for suspicious transactions and may allow a person to bypass proceeds of crime legislation if not regulated.

One of the innovations and challenges of bitcoin is its fluctuating value, which has been reported as being about ten times the volatility of typical currencies.³ This fluctuation makes borrowing using bitcoin more of a concern. But is using bitcoin as collateral for borrowing any different than using securities, as both rise and fall based upon the market? From a lender's perspective, the lender has to ensure that the lender is prepared for the value of the bitcoin to diminish while it is being used as collateral for a loan, not unlike securities or the common "margin loans" offered by investment dealers. The borrower needs to be cognisant that the lender may want additional security. But borrowing with bitcoin as security is possible.

(b) The Relevant Legislation: *The Personal Property Security Act* and the *Securities Transfer Act, 2006*

To take a security interest in bitcoin, it is necessary to determine how to categorize it from this perspective. As noted, bitcoin is a digital currency. It may be similar to a security or a financial asset. Based upon our current legislation, bitcoin would be an "intangible."

In Ontario, the most relevant legislation for taking a security interest in bitcoin is the *Personal Property Security Act*⁴ (the "PPSA") and the *Securities Transfer Act, 2006*⁵ (the "STA"). It is necessary to consider the definitions under the PPSA and STA to ascertain how bitcoin may be categorized. This will assist in the determination of the collateral classification and suggest the subsequent manner of perfection of the security interest.

"Goods" is defined under the PPSA as tangible personal property.⁶ Since bitcoin, per se, is not "tangible" personal property, it does not fall within the definition of "goods". An "intangible" is defined in much the same way, as all personal property, including choses in action, that is not goods, chattel paper, documents of title, instruments, money or investment property.⁷ The definitions of "chattel paper", "documents of title" and "instruments" are more specific and bitcoin does not fall within any of their parameters. Bitcoin also does not currently fall within the definition of "money" as that definition in the PPSA specifies "a medium of exchange authorized or adopted by the Parliament of Canada as part of the currency of Canada or by a foreign government as part of its currency."⁸

Under the provisions of the STA, bitcoin is likely not "investment property", as it is not a security, whether certificated or uncertificated, nor a futures contract or futures account. Trading in bitcoin is not currently regulated by an exchange, nor is an intermediary required. It is possible that bitcoin could be subsumed under the concepts of a securities account or securities entitlement as these are defined under the STA with reference to a financial asset. While it could be argued that bitcoin is a financial asset, from other provisions of the STA dealing with securities accounts and entitlements, currently the provisions of the STA and the interest in these types of collateral are directed to securities and rights and property interests in securities. Bitcoin does not fall within the purview of the STA, as presently construed.

Having excluded all of the specified sub-categories of collateral in the definition of intangible, bitcoin would seem to be classified pursuant to the current provisions of the PPSA simply as an "intangible".

(c) Taking a Security Interest in an Intangible

The PPSA provides that for a security interest to be enforceable against third parties, it must have "attached".⁹ In order to have attachment, value must have been given, the debtor must have rights in the collateral or the power to transfer rights in the collateral to a third party, and the debtor must have signed an agreement that contains a description of the collateral sufficient to enable it to be identified.¹⁰ As a result, in order for a holder of bitcoin or an interest in bitcoin to use it as collateral, the holder will have to enter into a security agreement with the secured party and in that security agreement provide the secured party with a description of the bitcoin. The secured party would have to rely upon the bitcoin holder to describe the bitcoin accurately and presumably by reference to the encoded cryptological description, so that it may be distinguished from other bitcoin or bitcoin interests.

The PPSA further provides that a security interest is perfected when it has attached and all steps required for

perfection under any provision of the PPSA have been completed, regardless of the order.¹¹ To perfect a security interest in an intangible, a registration has to be made. There is no current provision in either the PPSA or the STA which contemplates perfection of an intangible by control, unless the intangible is an investment property. The PPSA defines “control” and possession is required. This is similar to perfecting a security interest in money. If a lender cannot take control of the bitcoin or interest in the manner prescribed, the only way, at present, to take a security interest under the PPSA is to register.

Taking a Security Interest in Bitcoin

(a) The Relevance of Due Diligence?

When a lender is considering providing a loan against collateral, the lender or secured party usually conducts due diligence (in addition to entering into a security agreement with the borrower which describes the collateral and sets out the rights of the secured party in the event that the borrower defaults).

Undertaking this due diligence raises a number of questions with respect to Bitcoin and the blockchain:

- Does the borrower own the asset or collateral and does any other party have an interest already in that collateral that could rank ahead of the lender's?
- Can a lender be certain by reviewing the blockchain that there has not been any prior borrowings against the bitcoin or percentage interest?

The Bitcoin community can monitor and record transactions, also known as transfers. But the blockchain does not currently seem to monitor and record borrowings and security interests. Although it is possible that the public account or key of the bitcoin may have a notation that a security interest in that public key has been provided by the bitcoin owner to a lender, this type of notice is not yet customary and may not foreclose the ability of the borrower to transfer that interest.

(b) A Security Agreement for Bitcoin: Is it Possible?

If the lender is comfortable with the due diligence the lender can perform, or doing without, can the lender's agreement with the borrower adequately and accurately describe the bitcoin to enable the agreement to be a security agreement? Perhaps more importantly, do the remedies under the PPSA allow for adequate enforcement of the security interest in the bitcoin, if necessary?

As noted, to describe the bitcoin, the agreement would have to set out the digital currency or public key of that bitcoin, in a manner sufficient to enable it to be identified. This, however, may not be enough. To enable enforcement, the secured party will need to be able to access the holder's bitcoin private key or wallet. How can the lender be certain that the borrower will not deal with the collateral while it has been provided as security to the lender? Even if the lender did effect a registration under the PPSA, to perfect the lender's security interest in the bitcoin, and the registration described the bitcoin or interest, the registration would likely be generic, and describe all of the account or just a percentage interest. This may prohibit the borrower from dealing with other bitcoin interests that are not part of the collateral. Again, this type of registration may not prevent the borrower from transferring the bitcoin interest. A more specific registration with a description of the encoded cryptology would not appear to be prudent as a third party could perhaps use this information to transfer the borrower's bitcoin interest. The PPSA does contemplate that a secured party may be contacted and be requested to provide a copy of the security agreement to a judgment creditor of the debtor or to a third party who has an interest in the collateral.¹² Would that be prudent practice? Enforcing would require that the lender be able to transfer the bitcoin interest and, therefore, access to the account or wallet.

Although it is possible that a lender could simply ask the borrower to transfer the bitcoin or bitcoin interest to the lender until repayment has been made, in a manner similar to endorsing a stock certificate, the transfer would be an outright assignment of ownership and would be reflected in the blockchain. The borrower would have to be comfortable that the bitcoin would be returned once the loan had been repaid. The borrower and lender would have to ensure that their agreement addressed this transfer, transfer back and any fluctuation in the value of the asset. This type of agreement may obviate the need for any security agreement or PPSA registration as the transaction would be an outright transfer.

While entering into a security agreement and effecting a registration under the PPSA in respect of this intangible is possible, it does not seem to adequately protect either party nor does it currently seem practical. Registration in

respect of a security interest in bitcoin does not appear viable at this time.

(c) Transfer of a Bitcoin to a Flash Drive

Another option would be to have the borrower place the bitcoin or interest that is to be used as collateral on a flash drive and deliver the flash drive to the lender, as security. This would be similar to providing the lender with “perfection by possession”, and since a flash drive is “goods”, perfection by possession is possible. The borrower would need to be comfortable that the lender would not transfer the flash drive or bitcoin to a third party, so the borrower would have to ensure that the flash drive is password protected. Conversely the lender would want to have some assurance that if the borrower defaulted, the lender could access the bitcoin on the flash drive. This would suggest that a third party or escrow agent would have to be engaged to have the password and release it only on certain conditions being met.

If the value of bitcoin transactions is to occur without a third party intermediary, then although transferring bitcoin to a flash drive could accomplish “perfection”, it may defeat the no intermediary interaction, if the security interest requires an escrow agent to protect both parties. However, transferring the bitcoin to a flash drive is clearly preferable to registration and also should protect against the bitcoin interest being taken by an unauthorized third party, like with Mt. Gox, provided the lender does not lose the flash drive and the escrow agent has the private key or password.

Bitcoin as Collateral: Not Impossible but Not Easy

It does not seem that this digital currency, within our existing legal system, may be easily used as collateral to borrow monies, if a security interest is deemed necessary and if enforcement is subsequently required. However, adding a definition of “digital currency” to the PPSA and allowing “perfection” by possession would seem to be one possible partial solution. The parties to that security agreement would still have to determine what is necessary for “possession of the bitcoin interest, but treating a security interest in bitcoin similar to “money” or other “investment property” seems reasonable. Adding a new definition avoids the issue of whether a government needs to recognize digital currency.

While the idea is not an impossible one, currently using bitcoin as collateral means the lender must be open to a high level of risk.

¹ When referring to the system itself, the term “Bitcoin” is used; however when discussing the currency, “bitcoin” is referred to in the lower case. See bitcoin.org/en/vocabulary.

² “Bitcoin is Not a Monetary System” *Bitcoin Magazine*, Jeffery Tucker, January 3, 2014.

³ “Like an Emerging Currency, Bitcoin is ‘Vastly Inferior’ to Fiat Money”, *Barron’s* Brendan Conway, February 11, 2014.

⁴ R.S.O. 1990 c.P.19, as amended.

⁵ S.O. 2006 c.8.

⁶ *Supra* section 1(1).

⁷ *Ibid.*

⁸ *Ibid.*

⁹ *Supra*, section 11(1).

¹⁰ *Ibid.*, section 11(2).

¹¹ *Ibid.*, section 19.

¹² *Ibid.*, section 18.

AUTHORS



M. Sandra Appel

Partner

Toronto | T: +1 416 365 3500

sandra.appel@dlapiper.com
