WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Can I Secure A Loan with Bitcoin? Part II

Written By **Lance P. Martin** (lpm@wardandsmith.com)
April 6, 2018

In my previous article, I discussed the challenges of using Article 9 of the Uniform Commercial Code ('UCC') to create and perfect a security interest in virtual currency like Bitcoin, Ethereum, or Litecoin.

(I use "bitcoin" as a generic term for all virtual currencies.) Because bitcoin is likely a general intangible under Article 9, lenders cannot be certain that bitcoin is not encumbered with other security interests before being pledged by the holder. And the nature of bitcoin means it is nearly impossible for a lender to exercise "control" over bitcoin for default and repossession purposes.

Article 8 of the UCC, which governs the ownership and transfer of securities, may provide a better regime to create and perfect a security interest in bitcoin—if the owner is willing to hold bitcoin indirectly through a third party. This would be ironic since a hallmark of virtual currency is the absence of third-party intermediaries. Irony aside, Article 8 seems to be a better option than Article 9 for lenders seeking "cash collateral" from virtual currency.

Bitcoin and Blockchain

Virtual currencies are electronic representations of value that may not have an equivalent value in a real government-backed currency. They can be used as a payment system, or digital currency, without an intermediary like a bank or credit card company. While virtual currencies can function like real currencies in certain transactions, and certain virtual currencies can be exchanged into real currencies, a virtual currency itself does not have legal tender status. Virtual currency is virtual—there is no bitcoin equivalent to a quarter or dollar bill.

Bitcoin operates on a protocol that uses distributed-ledger technology. This technology is called the blockchain. The blockchain eliminates the need for intermediaries such as banks. Unlike a dollar, which is interchangeable, each bitcoin is unique. The blockchain records all bitcoin transactions to prevent someone from re-spending the same bitcoin over and over.

Suppose you want to transfer cash to a friend. You could transfer funds from your bank account to her bank account. The banks act as intermediaries. Suppose you wanted to transfer cash to that same friend without a middleman. The only way to do that is meet her and hand over the cash. This exchange may not be practical for many reasons. You might live far from each other. Even if you're near each other, you might not want to travel around town with a briefcase full of cash. Bitcoin and blockchain technology allow the transfer of cash directly and digitally without a middleman.

The blockchain is both transparent and opaque. It is transparent as to the ownership chain of every bitcoin. In this way, it is easier to "trace" a bitcoin than to trace cash. But the blockchain presently does not show liens on bitcoin. So a secured party

can confirm if a borrower owns bitcoin, but not if the borrower or a previous owner encumbered the bitcoin.

Article 8 Basics

Article 8 of the UCC deals with investment property. It is a familiar regime that lenders use routinely for securities. It involves "financial assets" held by a third-party "securities intermediary" that maintains securities accounts for others in the ordinary course of business. To qualify as a securities intermediary, the intermediary—typically a clearing corporation, bank, or brokerage—agrees to treat the assets it holds as financial assets under Article 8.

Applying Article 8 to Bitcoin

If a bank wants to make a loan secured by bitcoin, the borrower could open a securities account with a securities intermediary and transfer the bitcoin to the securities intermediary. The bank could act as the securities intermediary, or the parties could use a third party. The borrower, lender, and securities intermediary would agree to treat the bitcoin held in the securities account as a "financial asset" under Article 8. At this point, the borrower would no longer hold the bitcoin directly. Under the parlance of Article 8, the borrower would hold a securities entitlement in the financial asset in the securities account.

If the parties use a third-party securities intermediary, the next step would be granting the lender a perfected security interest in the bitcoin through a control agreement. Lenders will be familiar with control agreements, which are used for cash, investment, and other accounts to prevent a borrower from transferring collateral to a third party. Short of maintaining the securities account itself, a three-party control agreement provides a lender with the best possible security. The written control agreement would govern the terms under which the borrower could transfer the bitcoin in the account through instructions to the securities intermediary. The borrower would have relinquished the ability to engage in peer-to-peer transfers on the blockchain.

Recall from Part I of this article that if bitcoin is a general intangible under Article 9, then a security interest in bitcoin continues even after disposition or transfer. But if bitcoin is treated as a financial asset under Article 8, then the parties to the transaction can take advantage of certain "super-negotiation" rules not available in Article 9. The upshot is that the parties to the transaction could direct the securities intermediary to transfer the bitcoin and the transferee (in almost all cases) would take the bitcoin free and clear of liens. The securities intermediary would have to comply with all the safeguards in Article 8 to protect the borrower and lender.

Creating a Secured Bitcoin Account

Even if Article 8 provides a method to use bitcoin as collateral, there are security issues for the securities intermediary and the bitcoin owner.

A virtual currency account or wallet is used to buy, sell, and store funds, but it differs from a traditional securities account. Virtual currency exists only as computer code—verified addresses on the blockchain. The cryptography that undergirds virtual currency and blockchain relies on public keys and private keys. The public key is like a sophisticated account number and ensures that you are the owner of an address that can receive funds. It is related to, but technically not the same thing as, a bitcoin account or wallet address.

A private key is like a password. It is a randomly-generated 80-digit code that is, in theory, impossible to guess, fake, or reverse-engineer. The private key allows the owner to verify and undertake transactions. Each virtual coin or coin fragment has its own private key. A digital wallet contains the account holder's public and private keys and a log of all transactions.

A digital wallet should be encrypted with a password or two-factor authentication to protect it from hackers. If someone accesses a digital wallet, they acquire the private keys and can steal the virtual currency associated with them. In other words, although the cryptography associated with bitcoin makes it impossible for someone to figure out the private keys, digital wallets can be the targets of hacking, phishing, and other scams that bedevil traditional bank accounts.

To mitigate the risk of unintended access to private keys and potential loss of bitcoin securing the loan, lenders could require an offline wallet that stores the private keys on a computer not connected to the Internet. Some companies promote this service in tandem with an online “watching-only” wallet. The idea is to allow the buying and selling of virtual currency without exposing the private keys to hackers.

Whether the digital wallet is maintained on the web, the lender’s desktop computer, a third-party intermediary’s computer, or an air-gapped computer (a computer with a network security measure to ensure that it is physically isolated from unsecured networks), the bitcoin owner must relinquish the private keys to the lender or the third-party intermediary.

Conclusion

Article 8 is one possible solution for borrowers and lenders who want to use bitcoin in secured transactions. A major issue, however, is that doing so requires a third-party securities intermediary. But is it possible to use blockchain technology to accomplish the same result without a third-party intermediary? Part III of this article will discuss how smart contracts may provide lenders with a comparable level of security while eliminating the need for a middleman.

--