ESSAYS ON ISSUES
THE FEDERAL RESERVE BANK OF CHICAGO
DECEMBER 2013
NUMBER 317

Chicago Fed Letter

Bitcoin: A primer

by François R. Velde, senior economist

Bitcoin is a digital currency that was launched in 2009, and it has attracted much attention recently. This article reviews the mechanics of the currency and offers some thoughts on its characteristics.

Bitcoin is an elegant implementation of a digital currency, but can it truly rival or replace existing currencies?

In this *Chicago Fed Letter*, I explain the digital currency called bitcoin. The current number of bitcoin units is around 11.8 million; and, unlike physical coins, they are divisible to the eighth decimal place. Bitcoins are traded on various online exchanges for other currencies. At the time of this writing, the average worth of a bitcoin over the previous six months had been a little over $100. Thus, the total balances held in the form of bitcoins stood at around $1 billion, compared with $1,200 billion circulating in U.S. currency. There are on average about 30 bitcoin transactions per minute (Visa transactions average 200,000 per minute). The average bitcoin transaction size is about 16, i.e., on the order of $2,000 (the average Visa transaction is about $80). Bitcoin is thus a relatively small phenomenon, but it has been growing; the value of a bitcoin has increased tenfold since early 2013.[1]

What precisely is digital money?

Money is a medium of exchange—something that is accepted in exchange for a valuable good or service, not for itself but to be exchanged later for another good or service. For thousands of years that medium has taken the form of a physical object whose supply is scarce, either naturally (precious metals) or artificially (a token issued by a monopolist). But it has taken more disembodied forms as well, such as enforceable claims on some individual or entity transferred between buyer and seller. Nowadays in the United States, base money takes the physical form of coins (tokens issued by the United States Mint under authority of Congress) and notes (which used to be circulating claims on the Federal Reserve but are now in the nature of paper tokens), as well as the electronic form of reserves, which are claims held on the books of the Federal Reserve by depository institutions (claims to notes and coins).

Bitcoin is not a claim to a physical object or to a currency; it aims to be itself a currency and replace the physical object with a computer file. When a physical object is exchanged, there is little doubt that the giver owns it and the recipient receives it (whether the object is what it seems to be—and not a counterfeit—has always been a problem for money, but one that is mitigated in a variety of ways). A digital file is easily created and duplicated, so how do we avoid doubts about its authenticity as currency? The solution is basically recursive. Assume that my ownership of the file is ascertained. The bitcoin protocol ensures that the transaction by which I cede ownership of the bitcoin is validated by adding it to a record of all transactions. The recipient's ownership is now validated.

A simple method of validating the transaction would be to entrust a central

record of the transactions to an authority—as medieval merchants did when they paid each other by transferring sums on a bank's books or as modern banks do when they settle their transactions on the books of the Fed. Bitcoin, however, does not rely on a single recordkeeper. It solves the two challenges of controlling the creation of a unit of digital currency and avoiding its duplication at once. Validation is difficult to do, and those who do it are rewarded for doing so by being allowed to create new bitcoins in a controlled way.

Bitcoin solves two challenges of digital money—controlling its creation and avoiding its duplication—at once.

Creation/validation details

Now, to further explain how this process works, I have to be more technical and more precise. Consider the following scenario: Ann is the owner of a bitcoin—i.e., a string of zeros and ones whose precise nature will become clear—stored in a "wallet" (essentially, an encrypted computer file), managed by an application that she has installed on a computing device. She wants to cede the bitcoin to Bob, who also has a wallet, managed by an application. The two applications carry out the transaction (ensuring its safety through the use of public and private keys—essentially, a way to send someone a padlock with which to lock the item before it's sent while keeping the key to unlock the padlock). At this point, the application broadcasts a message to a large network of nodes on the Internet, announcing the proposed transaction between Ann and Bob (more precisely, between Ann's wallet and Bob's wallet, each identified by its public key). Every ten minutes, the nodes, called "miners," gather up the proposed transactions that were recently broadcast and attempt to add them to the "block chain," or the universal ledger of bitcoin transactions.

The key to preventing falsification of the block chain is to make the additions costly. Think of Ann and Bob exchanging a gold coin; the coin's gold content, which is costly to extract from the earth, "proves" that Ann did not counterfeit the coin, but this will work only if it is reasonably easy for Bob to check the gold content. Bitcoin requires a similar "proof of work" from the miners, in the following way: A valid addition to the block chain must include the solution to a difficult mathematical problem, which is costly to find (in terms of computer hardware required, electricity consumed, and time expended). The problem is difficult to solve, but the solution is easy to verify, as it is difficult to factorize[2] a very large number but easy to verify that a proposed factorization is correct. Moreover, the problem is not arbitrary or irrelevant, but tied to the verification of transactions.

A final technical concept is needed. A hash function maps text or numbers of arbitrary length into a number of fixed length. For instance, taking the first letter of a word (or summing the digits of a number and summing the digits of the result until a single digit is obtained) maps any word (or number) to a hash of length one. The problem that miners solve is roughly the following: Let block chain be x, let the proposed added block be y, and let an additional number be n. The goal is to find n such that the resulting hash function, $f(x, y, n)$, is less than a set value α. The hash function is deterministic but so complex that the output seems random. It is therefore nearly impossible to guess n, and the only reliable method is to try out many different values of n (using much computing power) until the condition is satisfied. Moreover, the lower the value of α, the harder it is to satisfy the condition. A proposed solution (x, y, n), however, can easily be verified. Part of finding n involves verifying that no bitcoin transacted in the block y has already been spent in the block chain x.

The code allows each miner to include in the block y a particular type of transaction, one which creates N new bitcoins and attributes them to the miner. The first miner to find a solution broadcasts it to the other miners, who verify it. Once verified (i.e., accepted by the majority of other nodes), the new block is added to the chain. The fortunate miner now possesses N new bitcoins as a reward for the effort expended.

Part of the bitcoin protocol regulates the values of N and α over time. The difficulty α is adjusted every two weeks so as to keep the rate at which blocks are added to six times per hour. Thus, if more miners join the network or if computing power improves, the difficulty increases. The size of the reward N was initially 50, and it is halved every 210,000 blocks (i.e., every four years at the rate of six blocks per hour). This implies that the total number of bitcoins in existence will approach but never exceed $2 \times 50 \times 210{,}000 = 21$ million; moreover, this time path will be independent of the size or computing power of the bitcoin network. With time, mining becomes unprofitable, but an additional incentive is provided to miners: Users can offer to pay a transaction fee to ensure inclusion of the transaction in the next block successfully added to the block chain; this fee will be allocated to the miner who adds that block.

So, the bitcoin protocol provides an elegant solution to the problem of creating a digital currency—i.e., how to regulate its issue, defeat counterfeiting and double-spending, and ensure that it can be conveyed safely—without relying on a single authority. What, in the end, is this new currency? It is a list of authorized transactions, beginning with the creation of the unit by a miner and ending with the current owner. The currency can be exchanged because all potential recipients have the means to verify past transactions and validate new ones, and one's ownership rests on the consensus of the nodes.[3]

Bitcoin is a fiduciary currency

Fiduciary currencies—in contrast with commodity-based currencies (such as gold coins or bank notes redeemable in gold)—have no intrinsic value, and derive their value in exchange either from government fiat or from the belief that

they may be accepted by someone else. They are inherently fragile; government orders can be ignored or doubted, and a currency that has value only because of the belief that it will have value may have no value at all (for instance, if I believe that no one will accept it, I will not accept it either).

The term "mining" may lead one to think that bitcoin is not fiduciary. It is true that real resources (computing hardware and energy) are expended in creating bitcoins. Since entry to mining is free, the value of these resources will be the market value of bitcoins produced (whose number per day does not depend on the size of the network). But once created, the bitcoin has no value other than in exchange, contrary to a gold coin.

Bitcoin's viability as currency

Can bitcoin truly rival or even replace existing currencies—particularly in the form of cash? A dollar bill in my hand cannot be anywhere else at the same time, my ownership of it is undoubted, and it can be exchanged immediately and finally. The many ingenious features of bitcoin try to emulate these properties of cash, but do so at some costs. One prominent cost is the loss of anonymity. Possession of the virtual currency must be linked to the unique identifier of the wallet. Admittedly, there is no limit on the number of wallets one can own and there are ways to make the wallet hard to trace back to its owner, but these require additional efforts. Another cost of using bitcoin is in the speed of the transaction. At a minimum, one must wait ten minutes for the proposed transaction to be included in the block chain, and for large amounts it is customary to wait for six blocks, or one hour. These times are much slower than those to complete electronic retail transactions in most other currencies (e.g., a few seconds to charge a credit card either online or at a physical retail location), not to mention the times to make large financial transactions on standard networks.

Why this delay to complete bitcoin transactions? It is rooted in the decentralized nature of the bitcoin network (and its reliance on a sort of majority voting), which is both its most ambitious feature and its main vulnerability. The confirmation that the bitcoin is not being spent twice must await validation by the network, requiring at least ten minutes (although confirmation might be skipped for small transactions). Moreover, there have been a few instances of "forks," moments when part of the network accepted one new block as valid while another part rejected it and accepted a different block. These incidents happened for accidental reasons, but a fork could someday be the result of malicious action. It is generally thought that it would be too expensive for a single malicious user (or group of malicious users) to take over more than half of the network; but if bitcoin were to grow significantly in value, this calculation could change.

One well-known fork that emerged in March 2013 was due to nodes using two different versions of the bitcoin protocol.[4] This incident reminds us that the bitcoin protocol is based on open-source software. Bitcoin is what bitcoin users use. The general principles of bitcoin and its early versions are attributed to an otherwise unknown Satoshi Nakamoto;[5] improvements, bug fixes, and repairs have since been carried out by the community of bitcoin users, dominated by a small set of programmers. Although some of the enthusiasm for bitcoin is driven by a distrust of state-issued currency, it is hard to imagine a world where the main currency is based on an extremely complex code understood by only a few and controlled by even fewer, without accountability, arbitration, or recourse.

The role of the state

A fiduciary currency like bitcoin is useful only insofar as others accept it broadly. As a matter of theory, this broad acceptance need not rely on the state, and history certainly offers several examples of currencies used without state support, oftentimes because the state-sponsored currency was proving deficient. But throughout most of Western history, the state has involved itself in money. At a minimum, the state has used money as a coordinating device, usually supporting its value by accepting it in the payment of taxes. The state has also concerned itself with money because one main function of money is to free a debtor from his or her obligations, tying money to an essential state function, the administration of justice. That is why the U.S. Constitution gives Congress the power "to coin Money, regulate the Value thereof, and of foreign Coin, and fix the Standard of Weights and Measures." Bitcoin is free of the power of the state, but it is also outside the protection of the state. How likely is bitcoin to remain so if it gains wide acceptance and the incentives to hijack it grow accordingly?

Fraud concerns

To the extent that the motivations of bitcoin's founder, Satoshi Nakamoto, can be discerned from his original paper, they revolved around transaction costs, which he argued would arise mostly from the need to preclude fraud. His proposal was for a low-cost secure payment system that did not involve a central authority or "trusted third party." The resulting invention of a state-independent unit of value is remarkable but perhaps coincidental. Much of the interest in bitcoin is inspired by the ideas of Friedrich Hayek,[6] that money should cease to be

ISSN 0895-0164

a state monopoly and its production should be left to the competitive private sector. The linkage is misguided. Bitcoin is indeed free from government (so far) but has turned out unlike anything Hayek imagined. It is not issued by a private enterprise operating in a competitive environment, disciplined by the market to maintain the stable value of its currency. The bitcoin network is an automaton, issuing currency at a predictable rate, perfectly incapable of providing "good money" in Hayek's sense, i.e., a currency of stable value. It has, moreover, a status of quasi-monopoly in the realm of digital currencies by virtue of its first-mover advantage, and Hayek did not address whether currency is a natural monopoly.

Conclusion

So far, the uses of bitcoin as a medium of exchange appear limited, particularly if one excludes illegal activities. It has been used as a means to transfer funds outside of traditional and regulated channels and, presumably, as a speculative investment opportunity. People bet on bitcoin because it may develop into a full-fledged currency. Some of bitcoin's features make it less convenient than existing currencies and payment systems, particularly for those who have no strong desire to avoid them in the first place. Nor does it truly embody what Hayek and others in the "Austrian School of Economics" proposed. Should bitcoin become widely accepted, it is unlikely that it will remain free of government intervention, if only because the governance of the bitcoin code and network is opaque and vulnerable. That said, it represents a remarkable conceptual and technical achievement, which may well be used by existing financial institutions (which could issue their own bitcoins) or even by governments themselves.

[1] Author's calculations based data from the Board of Governors of the Federal Reserve System, H.4.1 statistical release; Visa fact sheet (http://corporate.visa.com/_media/visa-fact-sheet.pdf); and Bitcoincharts (www.bitcoincharts.com).

[2] To factorize a number means to express it as a product of prime numbers.

[3] Note the difference with the concept of "money is memory" of Minneapolis Fed President Narayana Kocherlakota; in his model, money embodies information about the content of past transactions—not only the identity of the parties, but also what was exchanged. See www.minneapolisfed.org/research/sr/sr218.pdf.

[4] For details, see http://bitcoin.org/en/alert/2013-03-11-chain-fork.

[5] Nakamoto's original paper providing bitcoin's specifications is available at http://bitcoin.org/bitcoin.pdf.

[6] See F. Hayek, 1976, *Denationalisation of Money*, London: Institute of Economic Affairs.