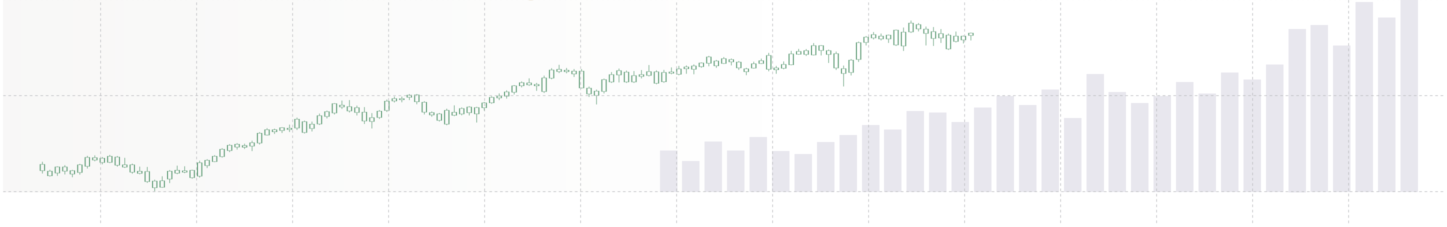
Number 2019-12
July 16, 2019

Economic Commentary



Bitcoin's Decentralized Decision Structure

*Ben R. Craig and Joseph Kachovec**

With the introduction of bitcoin, the world got not just a new currency, it also got evidence that a decentralized control structure could work in practice for institutional governance. This *Commentary* discusses the advantages and disadvantages of centralized and decentralized control structures by examining the features of the bitcoin payment system. We show that while the decentralized nature of the Bitcoin network "democratizes" payments, it is not obvious that the approach increases the equity or efficiency of markets or that the costs of the decentralized control structure won't outweigh the benefits in the long run.

In 2009, a paper appeared that established the philosophy and implementation of Bitcoin (Nakamoto, 2009). Bitcoin introduced an innovative approach to processing payments, wherein a trusted third party in a transaction, such as a bank, is replaced by anonymous people who verify the accuracy and trustworthiness of the transaction over the internet. The functions of a bank in processing a payment (establishing that the payer has the amount of currency they promise to pay and that they intend to pay the receiver of the transaction) is replaced in Bitcoin by open-source software that enables decentralized members of the network to vote with their computing power to determine whether a transaction is valid. The final sentence of Nakamoto's paper hints that the same approach to verifying a transaction can be used in broader decisions about corporate policy:

> "They [i.e., the nodes who participate in the payments] vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. *Any needed rules and incentives can be enforced with this consensus mechanism.*" (Italics ours.)

The lack of central counterparties and regulatory authorities in the Bitcoin network is viewed as a key benefit by many of Bitcoin's users. Indeed, a central revelation of the Bitcoin "experiment" is that a functioning payments system does not necessarily need a central authority, such as a central bank, or even a bank of any kind.

What are the possible advantages and disadvantages of a decentralized control structure such as used currently in Bitcoin? Every institution requires some structure, whether it is a central bank that chooses how much of its currency is in circulation or a software consensus mechanism as used by Bitcoin to decide on the rules of its transactions. This structure is used to make decisions about rules that govern the system, as well as to adjudicate disputes. However, making changes to the rules or adjudicating disputes is likely to be more difficult with Bitcoin, due to the lack of a universal enforcement authority.

This leaves uncertainty over whether the benefits outweigh the potential costs of decentralization in this market. In this *Commentary* we explore the benefits and costs of a decentralized payments system. We show that in a

*Ben R. Craig is an economic and policy advisor at the Federal Reserve Bank of Cleveland and Joseph Kachovec is a research analyst at the Bank. The views authors express in *Economic Commentary* are theirs and not necessarily those of the Federal Reserve Bank of Cleveland or the Board of Governors of the Federal Reserve System or its staff.

Economic Commentary is published by the Research Department of the Federal Reserve Bank of Cleveland. *Economic Commentary* is also available on the Cleveland Fed's website at www.clevelandfed.org/research. To receive an e-mail when a new *Economic Commentary* is posted, subscribe at www.clevelandfed.org/subscribe-EC.

ISSN 0428-1276

FEDERAL RESERVE BANK *of* CLEVELAND

discussion of benefits, the problem of "time consistency"—enforcing commitments over time—is central. The costs of decentralization are that a consensus approach to decisions is at times clumsy and can lead to outcomes that are not optimal.

Bitcoin Transactions

Bitcoin was envisioned as a more democratic method of processing transactions and a way to prevent financial power from becoming too concentrated in a few institutions' hands. As opposed to a central counterparty such as a bank approving a transaction, bitcoin transactions are sent to be verified and cleared by the Bitcoin network—anonymous, unconnected individuals all over the globe who have chosen to work as transaction processors (or "miners" in Bitcoin parlance). Verifying a transaction in bitcoin means making sure that the sender owns the bitcoin in question, and completing the transaction means adding the transaction to the public record of all bitcoin transactions (called the blockchain).

How this decentralized system can actually work in practice rests on several of Bitcoin's features. The authenticity and integrity of the messages are maintained through an extremely secure encryption process (which is why bitcoin is called a "cryptocurrency"). Miners are incentivized to do the work of verifying transactions and adding them to the blockchain because they earn bitcoin by doing so; the accuracy of the blockchain is ensured through a process called "proof of work"[1] in which miners compete for the right to add sets of pending transactions ("blocks") to the blockchain. The miner who "wins" the right to add the block is the first to solve a difficult math problem that requires significant computing power and electricity because it can only be found by trial and error. The transaction process is final when the miner[2] submits the block for verification to the network and 51 percent of the miners in the network agree that the transaction is valid.

Benefits of a Decentralized Network Structure

A payments system incorporating a trusted third party with decision-making authority has an inherent problem: The goals of the third party can diverge from the goals of the users of the system. For example, the users of a paper currency would prefer that the currency not be inflated, but a government issuing the currency might decide to inflate it to increase the revenue it makes from putting money into circulation ("seigniorage").

There are many ways that payments systems work to minimize the problems created by divergent goals such as these. Separating some of the powers of the central authority into independent or interdependent parts is one common solution. For instance, the centralized authority governing the inflation rate of a national currency might be vested in an independent central bank that is somewhat separated from the taxing authority. Separating powers in this way makes it more difficult to introduce changes to the system (deciding to inflate in this example).

In spite of such solutions, the goals of those in control of a system can still diverge from the users of the system over time. In economics, the problem of decision makers having different goals at different times is referred to as "time inconsistency." The roots of the problem are in the discretionary authority of a centralized decision maker. In a currency such as bitcoin, such decisions are made by the entire body of users of the payment system and this reduces the ability of a group to discretionarily change the rules of the game.[3]

Another example of the advantage of the decentralized decision structure of Bitcoin lies in its open-source software. Open-source software can be maintained and improved by a large enough consensus of users, and these decisions are transparent. By contrast, with a central decision maker, software can be changed or even removed on the whim of this decision maker with little recourse on the part of the software's users. A program can be bought by a competing company and then not developed further because the program competes with another of the company's products, or the program can be shut down because the firm has decided that the software does not fit its new business model. The possibility of this removal can cause fewer users to invest in learning the new software or in the capital to run it. In the case of Bitcoin, its open-source code removes this time-inconsistency problem because the users maintain the code. The decision to discontinue Bitcoin, if it happens, will occur only when so many participants decide not to accept bitcoin that no one will use it as a medium of exchange. In this sense, the termination of the system is made by a large majority of the system's users rather than the simple convenience of a director of a company. This control over the system's termination factors into the decision of users to adopt it.

Costs of Decentralization

The decentralized environment of Bitcoin introduces several potential problems that could be harder to solve than they would be within a centralized decision-making structure. We discuss two. The first is that the democratic nature of Bitcoin sometimes forces an outcome that is less efficient than the optimal outcome. We illustrate this through a recent Bitcoin example. The second is more speculative in that when fraud occurs, it is harder to enforce accountability in a decentralized environment than in one with a central decision maker.

For a major change to be implemented in the Bitcoin network, every member of the network essentially votes to adopt the changes to the operating software in that members of the system will accept only those blockchains that have the software features that they accept.[4] If a group of miners chooses a new type of blockchain and the change is not acceptable to a large enough group of other miners, then the new blockchains will not circulate, and the work of the miners who worked at mining the new blockchains will be wasted. This system can lead to compromise solutions as the system accommodates minority stakeholders. Such solutions may be less efficient than those that might have been achieved by a central authority.

One such instance happened in early 2017. Bitcoin faced the problem that it was taking too long to process transactions.[5] A portion of the Bitcoin network, notably bitcoin miners, favored a solution of increasing the block size above the standard 1 megabyte. The developers in the Bitcoin network, however, did not like this solution as it made the network more susceptible to hacking. Their preferred solution was to separate the blockchain functionality from the actual transaction processing in a scheme called Segregated Witness (SegWit for short). Because not all members of the Bitcoin network agreed to adopt the software changes implementing SegWit, it was possible for the network to fracture into distinct and separate networks. This fracture occurred on August 1, 2017, with the Bitcoin network splitting into two cryptocurrencies.[6]

The Bitcoin blockchain split into two new blockchains (a fork) and caused the creation of a new cryptocurrency called "bitcoin cash" (or BCH) that is supported by the newly created second blockchain that satisfied the objections of the miners.[7] At the time of the fork, owners of bitcoin maintained their exact bitcoin (often abbreviated BTC or BCC) balances, but they were also credited with the exact same number of the new currency, bitcoin cash. Transactions from the two different currencies are cleared through different blockchains. As shown in figure 1, the two blockchains have a common past and are updated differently going forward.[8]

The new BCH was not successful. As figure 2 shows, the miner-favored currency, BCH, was never heavily used, and its price fell quickly to nothing as it stopped being used by any significant part of the network. Further, it introduced complications for the sellers of derivatives that were based on bitcoin with respect to handling the "short sales" of bitcoins that were contracted before the split and then settled after it.[9] In a centralized system, a security decision such as this could have been debated, decided upon, and then efficiently enforced unilaterally. It is unlikely that the observed fork would have been chosen as an outcome by any centralized decision maker.

The second problem a decentralized control structure might have a harder time handling than a central authority is dispute resolution. Our current legal system is set up to adjudicate disputes and enforce regulations upon people or corporations, their analogous counterparts in business. For both of these entities, there is a central decision maker who can be held accountable. In a transaction that goes wrong or results in a dispute, the bank handling the payment can be fined if it does not do its duty to enforce the trust placed in it by the counterparties of the payment. The bank itself might also create a fraud department to adjudicate whether the payer or the payee is guilty of fraud or whether compensation to the victim should be quickly paid. We have a long history of jurisprudence to rely on for precedence in such cases. A regulatory body can be set up in those difficult cases that cannot be settled this way, and the regulator can also rely on legal precedent in enforcing its decisions.

Figure 1. Bitcoin Blockchain Fork

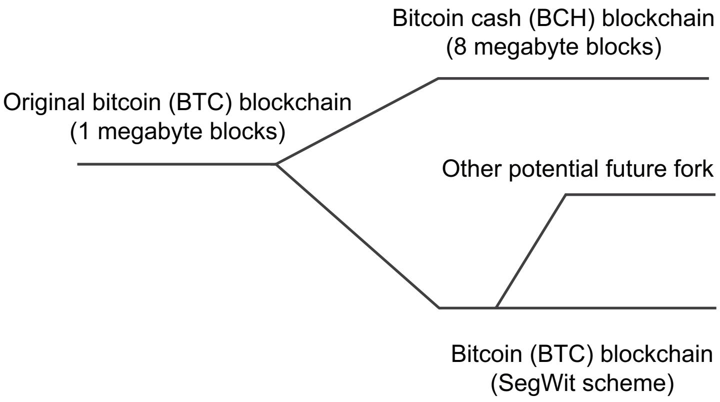
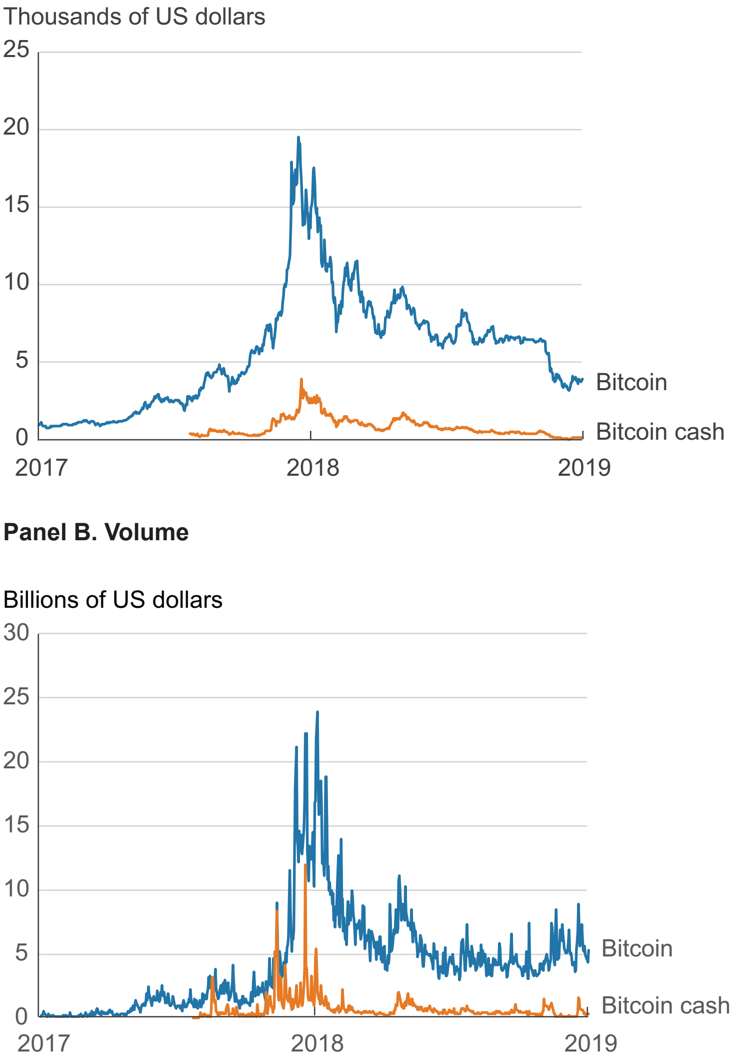

Bitcoin cash (BCH) blockchain
(8 megabyte blocks)
Original bitcoin (BTC) blockchain
(1 megabyte blocks)
Other potential future fork
Bitcoin (BTC) blockchain
(SegWit scheme)

Figure 2. Comparison of Bitcoin and Bitcoin Cash by Price and Volume

Panel A. Price

Panel B. Volume



Source: "Top 100 Coins by Market Capitalization." CoinMarketCap. https://coinmarketcap.com/coins/.

Bitcoin disputes, when they arise, are harder to resolve. The legal precedent is not very rich in cases where it is not clear who wrote the program (as in the case of open-source code) or even in cases where programmers had a complete idea of the effect their code would have as it interacted with the code of many others (for example, if new code is introduced that creates a security vulnerability in the system). Regulation in this context can be challenging because it is not only difficult to attribute responsibility but also to determine how to implement penalties once fault is ascertained because there is very little jurisprudence precedent to rely on.

Even simple disputes can be tricky to resolve quickly in a context where the agents are often anonymous, and the blockchain permanent. A bank can quickly assess a fraud, invalidate a transaction, and supply a quick refund, while in the Bitcoin network, solving this problem is much more complicated, as blocks added to the Bitcoin blockchain are permanent and all transactions are pseudonymous (which is seen as a key feature to many users). It would theoretically be possible to return to the point on the blockchain before a fraud occurred, resulting in the restoration of bitcoin to its proper owners. However, this is an incredibly complicated endeavor as transactions are stored in blocks, and presumably not every transaction in each block is fraudulent. Returning to a previous point on the blockchain would create winners and losers from a monetary standpoint. Receivers of cryptocurrency (providers of goods and services) would be net losers because they would have already provided a product or service only to have their currency in payment of it taken away at a later date. The primary beneficiaries would be entities whose cryptocurrency had been fraudulently removed from their accounts on the original blockchain. As a result of these complications, the welfare consequences of returning to a previous point on the blockchain after frauds occur are unclear.[10]

Conclusion

The rise of Bitcoin competitors and additional cryptocurrencies[11] shows that demand exists in the marketplace for these products. However, questions still remain about how viable a decentralized platform can be long term. While the decentralized nature of the Bitcoin network "democratizes" payments, it is not obvious this approach increases either the equity or efficiency of markets. In fact, many of the recent criticisms of Bitcoin's governing structure concern whether a more concentrated computational power could result in decisions made by only a few users of the system, rather than the more democratic consensus envisioned by many of its users.[12]

Centralized decision making comes with both costs, such as arbitrary decisions, and benefits, such as being able to realize fast decisions in a changing environment. This *Commentary* suggests that the democratic principles of Bitcoin also involve tradeoffs, where solutions are likely to be contentious and consensus decisions difficult to achieve.

Footnotes

[1] An alternative to Bitcoin's "proof of work" is "proof of stake." Proof of stake allows users devote a percentage of their coins to mining. Instead of whoever first completes the "proof of work" being awarded cryptocurrency, the block creator is determined deterministically based on the amount of cryptocurrency each miner pledged. Therefore, having superior computing power will not increase your probability of mining more blocks. This system eliminates much of the hardware arms-race problem that has emerged in bitcoin mining.

[2] For a more thorough account of the processing of a bitcoin transaction see: Nielsen, Michael. 2013. "How the Bitcoin Protocol Actually Works." *Data Driven Intelligence* (blog) (December 6, 2013).

[3] The literature on time consistency is very large, but a seminal work in this area is Kydland, Finn E., and Edward C. Prescott. 1977. "Rules Rather Than Discretion: The Inconsistency of Optimal Plans." *Journal of Political Economy* 87: 473–492.

[4] Voting on code changes is somewhat different than the CPU-voting power of the miners described in the discussion on voting to add blocks to the blockchain. When miners vote on the validity of a transaction, their votes are weighted by the amount of CPU that they use. For a change in policy in a blockchain, voting is more like a mechanism with each member having one vote.

[5] Increased transactions had expanded the computing power needed to effectively mine a bitcoin with the current size of the block.

[6] Actually, there were many forks occurring in 2017 and 2018. See, Cryptocurrencies.com. 2017. "A List of Upcoming and Past Forks." (Originally posted 2017 but continuously updated.)

[7] See Bitcoin.com. 2017. "Bitcoin Cash Is Bitcoin." (October 16).

[8] What technically happened was that bitcoin "soft forked" by adopting the SegWit protocol while bitcoin cash "hard forked" by increasing the block size from 1 megabyte to 8 megabytes. This technicality, along with widespread support in the bitcoin community was why the SegWit chain maintained the original bitcoin name. For more information, and an explanation of a hard versus a soft fork see Light, John. 2017. "The Differences between a Hard Fork, a Soft Fork, and a Chain Split, and What They Mean for the Future of Bitcoin." *Medium.* (September 25).

[9] See Levine, Matt. 2017. "Bitcoin Exchange Had Too Many Coins." *Bloomberg Opinion* (August 27). Incidentally, the futures price of bitcoin cash was quickly discounted compared to the original bitcoin before the fork had even occurred, trading at 0.103 of a bitcoin the day before the fork.

10. Such an example happened with Bitcoin's largest competitor, Ethereum, which resulted in a fork of the Ethereum blockchain into "ethereum classic" and "ethereum."

11. As of September 20, 2018, bitcoin's market cap represents 54.7 percent of the overall cryptocurrency market.

12. See for example Orcutt, Mike. 2018. "Bitcoin and Ethereum Have a Hidden Power Structure, and It's Just Been Revealed."*MIT Technology Review* (January 18).

References

Courtois, Nicolas T. 2016. "Features or Bugs: The Seven Sins of Current Bitcoin." In *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century*, edited by Paolo Tasca, Tomaso Aste, Loriana Pelizzon, and Nicolas Perony, 97–120.

Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System." Unpublished Manuscript.