KNOWLEDGE@WHARTON | Student Fellowship Series

Why Bitcoin Is Not a Viable Currency Option

August 2018

Why Bitcoin Is Not a Viable Currency Option

In certain political corners, the Great Recession is seen, rightly or wrongly, to have tarnished the reputation of the U.S. Federal Reserve system. Some libertarians especially have argued against the purpose and even existence of the central bank, which they think helped cause the 2008 crisis.[1] Furthermore, their anger is compounded by then Fed chair Ben Bernanke's bailout of financial institutions with distressed assets — even if it meant that he had to act to rescue the U.S. economy.

Against that backdrop, it is no surprise that digital currencies such as bitcoin have gained traction. Bitcoin seems to offer an innovative option to citizens disenchanted with the existing monetary system. The relatively new digital currency offers not only decentralization, but also a limited money supply — all working within an anonymous peer-to-peer, ledger-based transaction system. As such, it skirts concerns around the over-printing of money, privacy, and efficiency. It also implies that, perhaps, a government is not needed for the currency system.

> The bitcoin system as a whole is inherently loaded with technological issues.

Yet, underneath the claims of cryptocurrency advocates lie numerous problems and obstacles in bitcoin that would prevent it from becoming a truly efficient, independent, and widely accepted currency. First, the bitcoin system as a whole is inherently loaded with technological issues. Second, it faces transactional problems. Finally, bitcoin poses regulatory problems with respect to account insurance, illegal usage, and taxation.

Technological Problems

In most transactions today, the amount of money moved is usually recorded on a ledger that is entrusted

1 http://www.bbc.com/news/business-3507949

to a third party, such as the central bank. In the bitcoin system, the master ledger (or 'blockchain') is theoretically distributed across all users.[2] This act is intended to remove the need for a third party, and to negate the need for trust by having all users own a copy of the master ledger. The idea is that if all users own a copy, no one person can easily get away with tampering with it.

Although this seems like a good idea, the distribution of ledgers poses two problems. First, the ledger gets increasingly bigger as usage rises over time until it becomes unappealing or impractical to download and constantly update. Second, it creates a gross inefficiency in the verification process of the ledgers after transactions. As the number of users increases once bitcoin adoption gains ground, the ledger that everyone is theoretically supposed to download and update becomes more unwieldy. As of July 17, 2017, the bitcoin blockchain size was 125 gigabytes.[3] This massive size poses numerous problems.

First, it is impossible to make these transactions secure by mobile phone, since most phones don't have the capacity to hold 125 GB of data. Instead, a phone user would have to rely on an exchange that constantly updates its ledger and keeps the coins in a specific account. However, exchanges are employed not just by phone users; those with requisite storage on their computers also may open accounts with an exchange simply for convenience.

By concentrating ledgers in a few exchanges for the sake of efficiency and ease of use, security is compromised. If an attack were to happen on a provider of ledgers, then entire records of transactions could be lost.[4] No one would be able to prove who owned what, and large amounts of bitcoins could be stolen.

On the other hand, if everyone were to constantly maintain a ledger the size of 125 GB and growing, it would be a huge waste of storage space. Furthermore, most people do not have the requisite internet speeds, the technological knowhow, or the patience to constantly maintain such a large digital ledger. Instead, they would rather outsource the job to keep things simple. This problem of efficiency/convenience versus security occurs also in the process of verification of transactions.

Most people do not have the requisite internet speeds, the technological knowhow, or the patience to constantly maintain such a large digital ledger.

The bitcoin system requires a complicated and power-consuming computer activity called 'mining' to verify 'blocks' of transactions. When each chain is mined, the transactions are verified and added to the master ledger. This is why the master ledger is called the blockchain, as it is a chain of blocks containing transactions that have already been verified. To incentivize miners, the creator of bitcoin implemented a reward system in which the first miner of each block gets some bitcoins in exchange for their time and significant electricity usage. Despite the compensation, owing to the ultimate limited supply of 21 million bitcoins and the continuously extending blockchain, the return on mining decreases while the costs of mining increases.[5]

Therefore, it becomes increasingly inefficient for multiple miners to compete with one another. The only miners who can reasonably partake in this process are those who have very large computing power, or who have

2 https://bitcoin.org/bitcoin.pdf

3 https://blockchain.info/charts/blocks-size

4 http://www.japantimes.co.jp/news/2016/08/31/business/financial-markets/cryptocurrencyexchanges-attack-risking-repeat-mt-gox-debacle/#.WW-zqt-PyvdQ

5 The Macroeconomics of Central Bank Issued Digital Currencies. John Barrdear and Michael Kumhof. p6-7

unified into a group. However, this creates the problem of centralized mining.

Centralized mining is when an individual, or a group of individuals, mines more than 50% of all the blocks that need to be verified (this act is called a 50+1% attack). In this situation, an individual or group will theoretically be able to manipulate the master ledger and display transactions to their own liking. This is because the blockchain will only follow the longest and most recent chain mined. Any other branch being mined at a slower pace will be 'orphaned,' and left behind. Since such an individual or group has majority control over the master ledger, they could double-spend, choose to verify or nullify transactions at will, look at everyone's accounts, and even steal money.

It would be all too easy for the Chinese government to nationalize such enterprises in order to control bitcoin.

This problem is further compounded by the fact that not everyone has the computing power, equipment, and technological knowhow that is necessary to participate in mining the blocks (mining is more complicated than updating the blockchain, which can be set on autopilot). Instead, mining has largely become the realm of small companies who are dedicated to its execution. But users are not at fault here; it would indeed be a serious waste of electricity to compete with other miners and groups.

Thus, although those who use bitcoins like the idea of a decentralized currency, they themselves are not willing, or simply unable, to contribute to it. This phenomenon has already taken place: In 2016, China became the leader in bitcoin mining. Although the government in China has not yet consolidated its miners, the top mining companies in the nation already mine 71% of all blocks worldwide. Meanwhile, users within the U.S. only mine 1% of all blocks.[6] Many companies that are dedicated exclusively to mining bitcoin have set up shop in China, taking advantage of the nation's relatively cheaper power.[7] It would be all too easy for the Chinese government to nationalize such enterprises in order to control bitcoin.

Transactional Problems

Bitcoin also faces numerous transactional problems. The basic functions of a currency are the following: It is a store of value, a medium of exchange, and a unit of account. Although bitcoin meets the criteria as a medium of exchange, it fails as a store of value and a unit of account.

Unlike fiat currencies such as the U.S. dollar, bitcoin has proven to be too volatile to make it a reliable vehicle in which to store value over long periods of time. Its price history since its inception in 2009 has seen extreme ups and downs. Events such as cyber attacks or criminal revelations have all played a part in influencing the price of bitcoin, whether for good or ill. In recent years, signs that Wall Street might join the bitcoin party resulted in a peak price of nearly USD $20,000 in December 2017. But scarcely six months later, the price had plummeted by two-thirds.

This is because bitcoin has no inherent worth, nor does it have any government backing. The only reason why people would even consider buying bitcoin is because they believe they can sell it at a higher price in the future. Current buyers are betting that bitcoin might later become widespread.[8] Therefore, bitcoin is in a positive feedback loop. As more buyers come in, they drive the price up, which in turn attracts more buyers, and so on. However, the reverse is also true. A fall of confidence in

6 https://www.buybitcoinworldwide.com/mining/china/

7 https://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html

8 Some Simple Economics of the BlockChain. Christian Catalini and Joshua S. Gans. p24.

the currency will only cause more people to sell, leading to a downward cascade.

As of July 2017, bitcoin's market capitalization was USD $35 billion, compared to the U.S. dollar's $64 trillion.[9] In the U.K., total bitcoin value is miniscule compared to the total amount of pound sterling notes in circulation. The Bank of England, having done extensive research on cryptocurrencies, concludes that bitcoin does not pose any immediate threat to existing financial structures.[10]

Bitcoin's second major transactional problem is that it does not truly function as a unit of account. For a currency to be a unit of account, it must be able to measure the real economic value of an item. For example, an apple might be said to be worth USD $1. The item's value is always seen through the prism of fiat currency. However, that's not the case with bitcoin. For example, while some retailers might accept and list prices in bitcoin, their prices fluctuate along with the price movements of bitcoin. As such, bitcoin does not represent the real value of an item. Rather, it is an intermediary between the item and the fiat currency with which it is being exchanged. Indeed, there are few examples of parties actually negotiating a price solely in bitcoins.[11]

Regulatory Challenges

Bitcoin also faces three regulatory issues: account insurance, taxation, and illegal usage. Each of these problems may be generalized as an issue arising from anonymity. Even though bitcoin in its current state is only a tiny percentage of the U.S. dollar's total market capitalization, it has already managed to cause many problems.[12] One can only imagine what would happen if bitcoin were to become a truly efficient, independent, and widely accepted currency.

Most modern bank accounts are easily linked to their owners. Governments and financial institutions can identify the owners of monetary assets, the amount of funds held as well as the source of the monies. Although this tracking does raise privacy concerns, not only is it helpful in the event of a system failure or bank run to sort out how much one should be reimbursed in federally insured accounts, it helps authorities sniff out illegal activities such as money laundering and funding of terrorism plots.

As of July 2017, bitcoin's market capitalization was USD $35 billion, compared to the U.S. dollar's $64 trillion.

With bitcoin, personal identities are not linked to individual accounts. If one person were to steal another's account credentials and make transactions, there is no easy way to prove ownership and check whether transactions were legal or not. Furthermore, there would be no way to void and refund fraudulent transactions. This lack of identity would only compound problems in the event of an unforeseen catastrophe. Buyers of bitcoin would lose huge amounts of money, and there would be no regulating agency to insure them and find the cause of the breach. This is especially harmful to bitcoin holders who bought the cryptocurrency as an upfront, legal investment.

To be sure, the anonymity that bitcoin offers is an appealing feature to people who don't want to be tracked, including criminals. Some contend that citizens who have nothing to hide should be less concerned when governments can see their information. The argument is that if citizens cannot trust their government, why should they place more trust in a system designed

9 http://data.worldbank.org/indicator/CM.MKT.LCAP.CD?end=2016&start=2015

10 https://internationalbanker.com/banking/impact-bitcoin-central-banks/

11 The Economics of Digital Currencies. (2014). Bank of England. p281.

12 https://coinmarketcap.com/currencies/bitcoin/

by an unknown person or a group of persons, which cannot be regulated at all? An anonymous system is advantageous only to those who wish for their identities to remain hidden, especially if they commit illegal acts.

Already, bitcoin has been used by terrorists and organized crime groups globally.

Already, bitcoin has been used by terrorists and organized crime groups globally. One infamous user of bitcoin was Ross Ulbricht, creator of Silk Road, a black market website best known for transactions of illegal drugs on the dark web. On this site, all transactions were made in bitcoin. Eventually the site drew the attention of the U.S. Federal Bureau of Investigation and shut down. Ulbricht was convicted and is currently serving a life sentence without the possibility of a parole.[13]

Criminal hacker groups have also used bitcoin. When they lock people's computers for ransom, they ask for bitcoin instead of fiat currency, which is more easily traceable. For example, in May 2017, the computers of a hospital in the U.K. were locked and hackers demanded a ransom in bitcoin.[14]

The second attack occurred just one month later, in which many key Ukrainian infrastructure facilities were hit.[15] Yet the nature of this attack was different: After the ransom was paid, the computers remained locked. Given that the targets attacked Ukrainian infrastructure, speculation arose that the bitcoin ransom was a ruse to cover the hackers' true intent: cyber warfare.[16] If true, this marks the first instance of bitcoin being used in a massive cyber attack against a country. The perpetrator behind the second attack still has not been found.

China's Bitcoin Crackdown

However, the nature of bitcoin is a major plus for those who want to move money out of regulated areas. For example, China's government mandates that its citizens can only bring out of the country a set amount of cash (50,000 RMB).[17] This is in order to prevent its own assets from leaking to other nations. China wishes to discourage citizens from investing elsewhere (and emigrating), and instead encourage them to invest in their own country (and staying).

However, Chinese citizens realized that they could essentially transfer money out of the country by investing in bitcoin and then selling it. This explains why 60% to 80% of all global bitcoin transactions are conducted in RMB.[18] Furthermore, it also explains why the Chinese government has cracked down on bitcoin transfers: The currency must be held by a verified Chinese exchange instead of the investor. This essentially locks the currency in China, and allows the country to monitor any transactions that occur within its jurisdiction. As such, the government can easily monitor and tax such transactions.

Regulating Bitcoin in the U.S.

The U.S. government has not yet taken substantial steps to regulate bitcoin. One issue could be the lack of a clear definition. Is bitcoin a security, currency or property (commodity)? Future legislation on bitcoin would do well to hash out the blurred lines of its nature.[19] Currently, the

13 https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentencedto-life-in-prison.html
14 https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/
15 https://www.forbes.com/sites/leemathews/2017/05/25/services-interrupted-as-hospitals-pushfixes-for-wannacry-ransomware-exploit/#3b9390ef26bf
16 https://www.forbes.com/sites/janetwburns/2017/06/29/experts-massive-petya-attack-looksmore-like-state-cyber-warfare-than-a-data-heist/#4f096ca47c27
17 http://money.cnn.com/2015/09/30/news/china-overseas-atm-cash-limits/index.html
18 The Economics of Digital Currencies. (2014). Bank of England. p279. https://internationalbanker.com/banking/impact-bitcoin-central-banks/
19 Conversation with Professor Kevin Werbach. July 13, 2017. Wharton, University of Pennsylvania.

U.S. Internal Revenue Service considers bitcoin a taxable property. But its function as an investment vehicle for some makes it a security. Further complicating matters is that it was created to be a currency.

As long as the U.S. government does not take far reaching measures to control the movement of bitcoin, it will not be able to tax bitcoin users properly. This is especially the case given that bitcoin accounts have no identity linked to them. Again, the power of bitcoin's anonymity works primarily to the advantage of criminals, and to the disadvantage of the state and its honest citizens.

Conclusion

Bitcoin has a long way to go before it can become viable, efficient, independent, and widely accepted. It has major technological hurdles, and its acceptance in society is currently limited at best. In its present state, the bitcoin system is controlled by a few major mining companies (it is too costly for individuals), traded through a few major platforms (finding other bitcoin users without a meeting place is difficult), and held in wallets provided by various companies (holding your own key and ledger is too inconvenient). Already, the idea of decentralization has fallen apart simply due to humanity's tenancies towards being frugal, social, and free from hassle.

Bitcoin has a long way to go before it can become viable, efficient, independent, and widely accepted.

Even if bitcoin becomes a viable currency — efficient in power consumption, independently run, and widely accepted — the problems it brings would likely offset any benefits to citizens. The idea that individuals scattered around the world can work to maintain such a system is simply against human nature. In such a decentralized monetary system, there would exist a state of economic war that pits people against people.

This paper was written by William Wu, a Knowledge@Wharton student fellow in 2017. He is a recent college graduate and is now working towards obtaining his real estate license.