5-9-2017

Blockchain Technology: Digitizing the Global Financial System

John Frechette

Blockchain Technology: Digitizing the Global Financial System

John Frechette

Submitted in Partial Completion of the
Requirements for Departmental Honors in Accounting and Finance

Bridgewater State University
May 9, 2017

Prof. Eric Disbrow, Thesis Director
Dr. Jeffrey Stark, Committee Member
Dr. Caitlin Finning Golden, Committee Member

Blockchain Technology: Digitizing the Global Financial System

John Frechette
Bridgewater State University
Honors Thesis

Abstract: Recent technological innovations have sparked massive restructurings across the entire global economy. Despite the changes that have already taken place, an underutilized and emerging technology, known as "blockchain," has the potential to disrupt every segment of the financial services sector. Using information and data accessed through the Bridgewater State library database, analyst reports, news articles, and the Bloomberg Terminal, this paper details the intricacies of blockchain technology, determines its potential effect on the global financial system, and reflects on its initial implementation with the creation of Bitcoin currency. While Bitcoin, a new cryptocurrency first invented in 2008, drew attention to the potential "digitization of money," the incredible underlying technology that makes the transfer of digital currency possible was mostly ignored. Utilizing the power of the Internet and complex mathematical algorithms, two parties are able to transfer assets to each other in a safe and efficient manner. A "distributed ledger" of historical transactions is published to every network participant, enabling verification that the transferor possesses the asset(s) that he/she claims to. While the technology is complex by nature, its potential effect is straight-forward: elimination of the need for financial intermediaries in the payment process. Consequently, financial services organizations that do not take the appropriate steps to remain proactive to the implementation of blockchain may see their business models become entirely obsolete.

I. Introduction

Individuals often do not concern themselves with the process of transferring assets from one party to another. Operating in the current "trust-based model," an intent to transfer ownership of assets is mediated by a financial institution, such as a bank, mutual fund, or broker. That organization checks its

own records and verifies that each party possesses the resources that he/she claims to. While this model has driven down costs for individuals and improved safety in financial markets, a certain percentage of fraud is still deemed to be acceptable and a large amount of bureaucracy is inevitably involved in the process.

In November of 2008, the *Cryptographic Mailing List* published a report written by Satoshi Nakamoto entitled, "Bitcoin: A Peer-to-Peer Electronic Cash System." The report details a new currency that is transferable without the use of a financial intermediary, evidenced by the first sentence of the document: "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008).

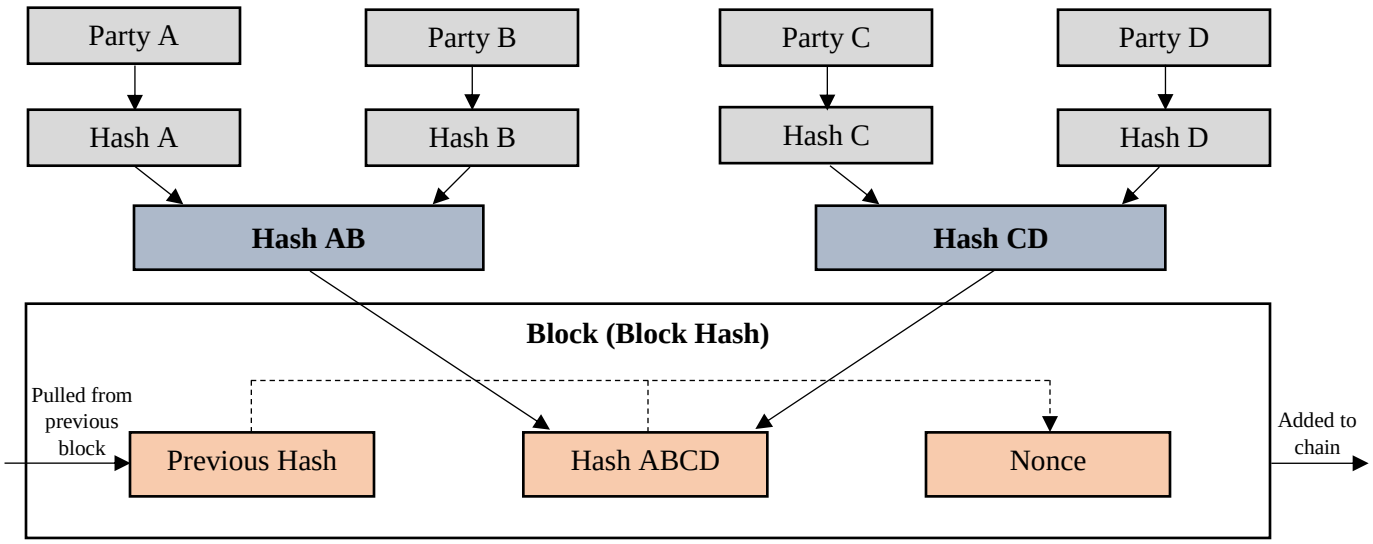
While the story of Satoshi Nakamoto, who remains unidentified, and Bitcoin gained traction, a large majority of readers failed to recognize the most crucial element of Satoshi's invention: the underlying technology that made the transfer of Bitcoin possible. Referred to as "blockchain," the program uses a public record of transactions to allow parties to transfer assets in a safe and efficient manner. While end users would benefit from increased speed and lower costs associated with transactions, eliminating the need for intermediaries would have a direct impact on firms operating within the financial services landscape.

Contrary to a traditional, centralized system where intermediaries hold private ledgers to ensure validity of ownership, Blockchain technology utilizes a public (distributed) ledger where all historical transactions are broadcasted to the entire network. This core principle of the technology enables participants to know exactly what each party, with a coded identity for anonymity, possesses and has the ability to transfer. To demonstrate a simple example, assume A transfers $5 to B. The network is aware of B's ownership of $5 as the transaction is distributed to each participant. While B will be able to transfer $2 or $3 to another party, the network will reject a proposal to transfer $6.

II. Technology

Once a potential transaction is publicly announced on the server, "miners," nodes within the network that attempt to verify the legitimacy of transactions, use the ledger of previous transactions to ensure each party possesses the assets being transferred. Proposed transactions are packaged into a "block." Each new block contains the "hash," or assigned code, of the previous block, with each additional block reinforcing the ones before. Miner nodes, utilizing complex algorithms and powerful computing, compete to verify each block first. After initial verification, the entire block is published on the ledger for a majority of nodes to confirm the collection of transactions as legitimate. As each block of transactions is eventually published, generally in approximately ten minute increments, the blocks form a chain. As the process continues, nodes always consider the longest chains to be the correct ones.

Specifically, to ensure that the process remains decentralized and that concentration of miners does not emerge, each block contains a difficult "proof-of-work." In addition to the collection of proposed transactions and the hash of the previous block, a "nonce" is included for the sole purpose of complicating the verification of the block. The nonce is ultimately a random value that eliminates the possibility of one miner outpacing the majority of the network. The diagram below provides an overview of a simplified block.

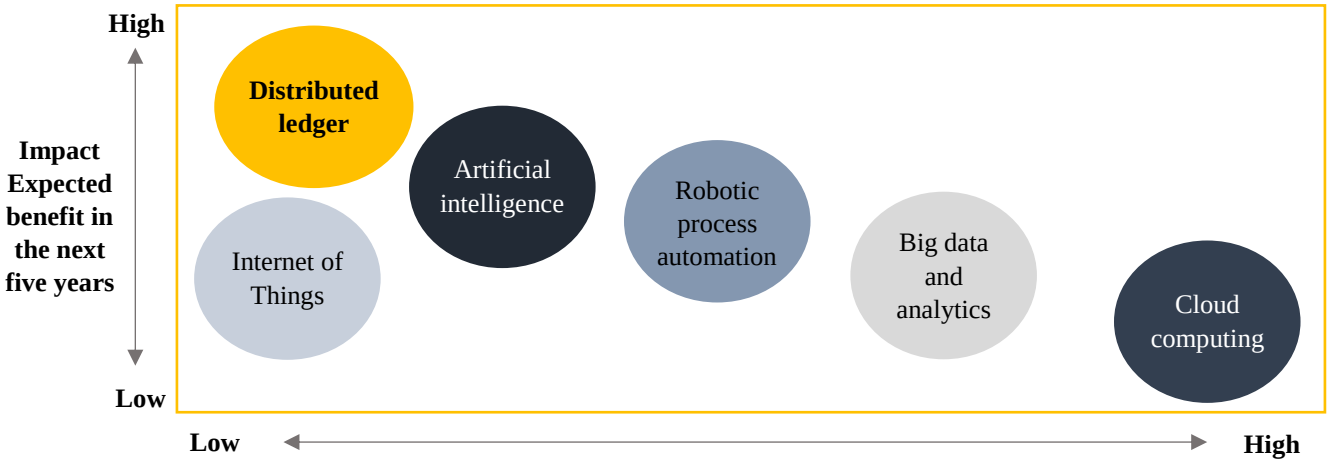


Guessing the correct nonce requires rapid trial-and-error. According to The Economist, miners generally try 450 thousand trillion solutions per second to guess the correct nonce. A correct nonce is evidenced by a block hash with predetermined characteristics, generally related to the number of leading zero "bits." Once a miner configures the correct hash, all other nodes confirm the block. As the properties are random and verification requires the majority of the network, no one node is able to gain a significant advantage. Nodes communicate their acceptance by working on verifying the next block in the chain, including the hash of the previously accepted block. Therefore, modifying a previous block in the chain would require the modification of the block and all blocks after it, rendering an attack on the system to be nearly impossible.

III. Applications

In today's environment, the automation of traditional business processes is necessary to remain competitive, particularly with financial services organizations who have been relatively slow to adapt to new technological innovations. Given the fact that a large majority of these firms exist for the sole purpose of mediation, decentralization of what could be argued as the core function of the financial services sector will have an enormous effect on these firms. A 2016 Ernst & Young case study of new technologies in the banking industry highlights the massive potential impact of distributed ledger technology:

Diagram of the comparative maturity and impact of new banking technologies



"As a solution for currency, blockchain is essential. As a solution to sharing information across disparate parties, blockchain is truly revolutionary" (Price, 2017). While Satoshi Nakamoto initially introduced blockchain technology as a way to facilitate the implementation and transfer of cryptocurrency, mainly Bitcoin, blockchain's potential applications are seemingly infinite. Given the sector's concentration of market share and the scope of the largest financial institutions, a breakdown of each core function is more useful than a breakdown of each sub-sector.

A. Payments

Blockchain's disruptive potential relative to the payments function of financial services stems primarily from increased transparency and therefore, the elimination of demand for a third-party processor. The distributed ledger of transactions allows for the rapid transfer of currency and eradicates the potential consequences of a trust-based model. In fact, it can be said that blockchain and Bitcoin were created under the assumption that no one can be trusted.

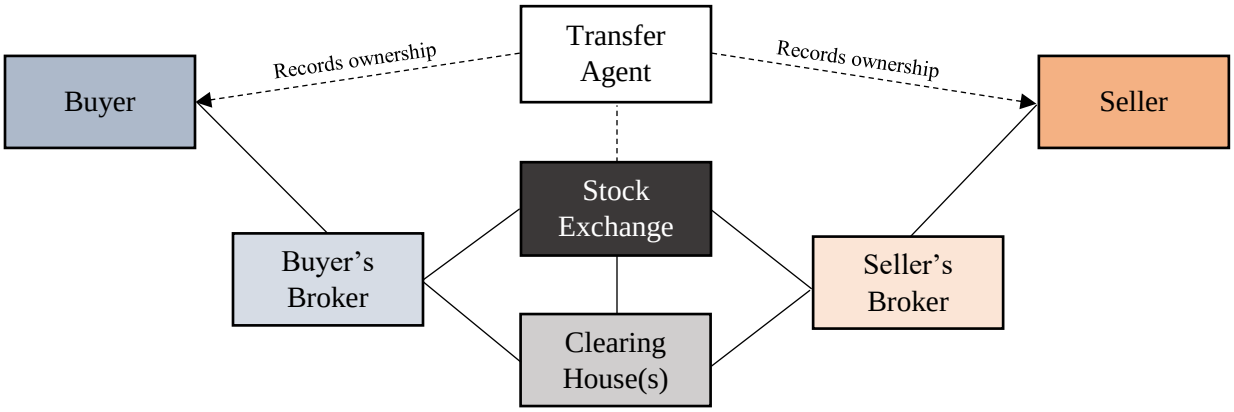
For perspective, IBISWorld estimates the U.S. credit card processing and money transferring industry to generate $75 billion in annual revenue. One of the largest players in that space, PayPal, a payments support company with an enterprise value of $52.6 billion, is a key example of a company whose business model could become, all else being equal, completely obsolete. Central parties like PayPal would no longer be necessary to verify and execute on transactions. The blockchain network itself performs this function, in a quicker and more accurate manner.

B. Securities

The mechanics behind the exchange of securities represents one of the most outdated systems in finance today. Amazingly, computing power and the internet allow some traders to execute orders in a matter of microseconds. According to "Flash Boys," a book written by Michael Lewis detailing the emergence of "high-frequency trading," some traders are even able to execute orders in a window of 465 microseconds, or one two-hundredths of the time it takes to blink an eye. However, despite new

technology enabling this magnitude of speed, the actual infrastructure of the stock market has been based on the same model for over 300 years.

In the current centralized model, an order to buy or sell securities passes through an assortment of intermediaries, generally including a broker, a clearing house, an exchange and a transfer agent. Clearing houses and brokers primarily operate to facilitate the coupling of buyers and sellers of securities at centralized venues for trading, known as exchanges. Similar to payments processors, transfer agents, who are appointed by the Securities and Exchange Commission, keep records of who owns a company's stocks and bonds and how those securities are held in an internal ledger. It is important to note that transfer agents are contracted by public companies to maintain records and therefore, the fees associated with their services are not directly reflected in each trade. However, the costs of these agents are, of course, indirectly reflected in the value of the company's stock and earnings, a cost to shareholders that is not immediately apparent to individual investors.



Blockchain technology eliminates the need for third parties in the securities transfer process. The transfer of securities would work in a similar way to currency, with each transaction of stocks or bonds automatically confirmed by the public ledger of previous transactions. As peers transact directly through the network, brokers and clearing houses would no longer be required to seek out counterparties for trades and a centralized, physical exchange would no longer be a necessary venue. Transfer agents would not be

needed as the distributed ledger would not only ensure validity of transfer power in a quicker and more accurate manner for individuals, but it would still provide companies with the necessary data while cutting the high costs associated with a transfer agent.

For perspective, IBISWorld estimates that securities brokering in the U.S. generates $143 billion in revenue and that stock and commodity exchanges in the U.S. generate $12 billion in revenue. Combining data from Audit Analytics and annual reports of the largest transfer agents by market share indicates that transfer agents generate a combined annual revenue of roughly $5 billion. Based on information published by Harvard Business School, Select USA, Voxeu and Investopedia, estimates for total revenue of the entire U.S. financial sector range anywhere between $1.2 and $3.3 trillion. Therefore, with these three segments of business alone accounting for roughly 5 to 10 percent of the entire financial services space, it is easy to see from initial examples that blockchain's disruption potential is not limited to specific industries within finance, but will instead have an impact on the entire system.

C. Smart contracts

Despite blockchain's enormous potential applications involving the immediate transfer of assets, "smart contracts" are likely to have the largest visible impact on both individuals and institutions. Also known as self-executing or blockchain contracts, smart contracts are essentially computer-programmed contracts that enable parties to (anonymously) create, monitor, and automatically execute on the terms of an agreement.

The traditional model for formulation and execution of legal contracts is time-consuming and often, extremely costly. The process generally involves a trusted third-party (normally lawyers) and the physical agreement often contains countless pages of complicated legal language. Furthermore, a valid contract far from guarantees that each party will honor their terms and there is frequently no medium for enforcing those terms in a cost-effective manner. "Part of the reason (why contracts are broken so often) is because participants in a contract know that the cost of going to court will be too much effort for the

other holder of the contract," (Price, 2017). Examining these inefficiencies exposes yet another outdated process that results in an unproductive use of resources and a lack of accountability for both organizations and individuals.

Consistent with blockchain technology's primary benefit of automation, smart contracts are designed to eliminate the pitfalls of transacting business on the basis of trust. Broadly speaking, obligations of each party, such as an exchange of value, are programmed into the smart contracts and therefore, there is no possibility for parties to alter the terms or refuse to honor the agreement.

Specifically, the contract terms are stated in conditional programming functions, essentially ensuring that if one event takes place, another event (the obligation) is triggered. That code is encrypted then sent out to the network on the distributed ledger. Network participants then update the distributed ledger to record the execution of the contract. Similar to an attempt to transfer assets not in possession, if one party attempts to alter the terms of the contract, the network majority will not approve. As can be assumed, obligations are immediately executed on with no possibility of alteration, holding each party accountable for the terms originally agreed upon. These incredible capabilities, which fall well outside the scope of what is required to facilitate the transfer of Bitcoin, are evidence of the improvements that are being continuously made to blockchain technology.

To demonstrate the potential impact of smart contracts utilized in the financial sector, it is useful to detail an example, break down the process of disruption, and speculate on the outcome. While smart contracts will eventually have an impact on all businesses, an immediate example within financial services is the $11 billion industry of collections (IBISWorld). In the context of either outsourced collection agencies or internal corporate accounts receivable teams, smart contracts will replace the necessity to collect by automating the repayment of debt or payables to suppliers.

While costs will surely decline for most organizations, often ignored is the extent to which the guaranteed payments will eliminate risk. Supplier credit terms and loan interest rates for businesses and

consumers intrinsically price in the possibility of a recipients' unwillingness to repay. Confirming Miles Price's assertion above, entities with small outstanding balances understand the cost of collections as well as the complex process of bankruptcy. This imbalance, for some corporations, leads to a large amount of small uncollectable balances. Particularly at risk are small to medium-sized businesses who do not have the same legal power and scale as large corporations.

As the risk of uncollectable loan repayments and receivables diminishes, initial credit terms and interest rates will become more favorable. Theoretically, this will lead to an increase in the amount of credit available to businesses and consumers which will stimulate economic growth, increase the value of assets in circulation, and reduce costs for individuals.

IV. Headwinds

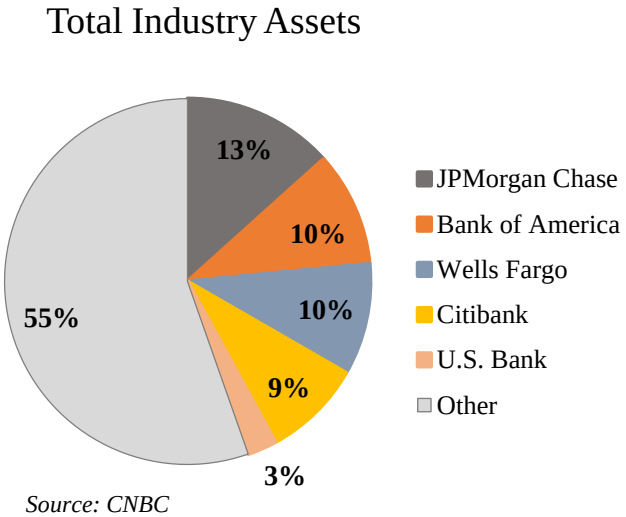
Interestingly enough, the implementation of blockchain faces few headwinds related to the technological capabilities of the system. While there are countless instances of cryptocurrencies stolen from owners, it is important to note that these attacks were not conducted through the distributed ledger, but rather at the level of specific computers. Hackers are able to gain access to the private key of users in the same way they would go about obtaining a bank account number. Some experts do believe, however, that while blockchain's fundamental system is extremely secure, constant updates are always required to ensure security in any widespread implementation of new technology.

The lack of regulation and the anonymity involved in the distribution and transfer of a cryptocurrency, like Bitcoin, naturally attracted a large amount of illegal activity. "Dark" marketplaces such as Silk Road, a well-known hidden online platform primarily used for selling illegal drugs, emerged (Silk Road was shut down in October of 2013, when the FBI seized $3.6 million of Bitcoin). Although this has inadvertently cast a dark image on the applications of the technology, it can be argued that an unfavorable perception of blockchain as a result of this criminal activity is misplaced. The potential benefits of widespread access, particularly in underdeveloped and underbanked countries, to an efficient

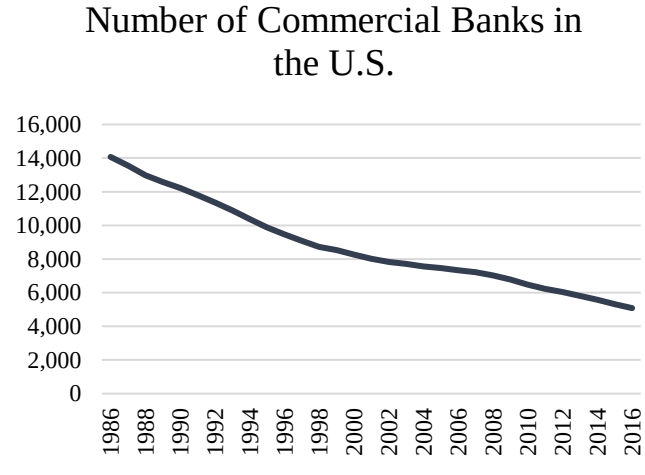
form of payments substantially outweighs the costs of a select group of individuals using the same access to conduct illegal activities.

Although it is not detailed in online articles and blockchain reports, the largest headwind by far that faces the implementation of blockchain use into the core functions of financial services is the exact characteristic that the technology is poised to eliminate: bureaucracy. Ironically, despite it being the most influential sector in the entire economy, financial services has a history of slow adaptations that results in radical inefficiencies. As evidence, traditional, high-cost organizations like banks and large brokers are losing market share rapidly to online lending companies and commission-free or low-cost brokerage platforms. Active stock managers and hedge funds who have underperformed their benchmark indices for decades are unprepared for a price war, and it is reflected in the tremendous amount of business being lost to index and exchange-traded fund providers charging extremely low expense fees.

The power of these organizations coupled with a financial market environment driven by quarterly earnings reports and short-term profits, unconsciously results in an unwillingness to make favorable long-term, proactive decisions. While in most industries, disruptive forces are quick to drive change, the consolidated nature of the financial sector allow the benefits of scale at large organizations to outweigh the costs of inefficiencies for an extended period of time. The U.S. banking industry exemplifies this consolidation, with a 64 percent reduction in the total number of firms over the last 30 years and the assets of the largest five institutions accounting for over 45 percent of the industry total:



Source: CNBC



Source: FRED

V. Bitcoin Case Study

Countless articles and books can be found on blockchain technology, with Satoshi Nakamoto's Bitcoin introduction being one of the most technologically in-depth and informative. The differentiation of this report arises from the benefit of hindsight and the ability to reflect on blockchain's first application introduced on a large scale: cryptocurrencies.

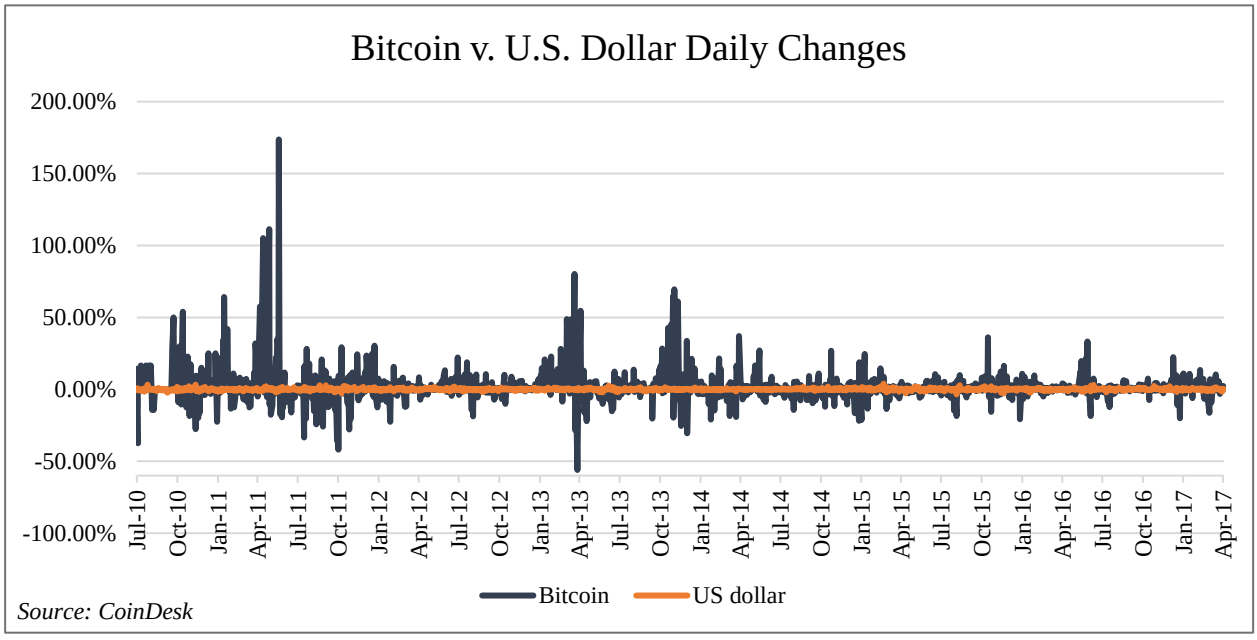
As mentioned previously, blockchain technology was developed specifically as a necessity for the transfer of Bitcoin. The creator(s) of Bitcoin also were not interested in the efficiencies and cost-savings that would arise from a peer-to-peer network. Rather, the main purpose was to return to a (digital) gold standard, where the value of currency is not reliant on trust in one centralized party, namely the government. The idea was that the current faith-based monetary system, a system where fiat currency is printed by the government and holds value with the sole belief that the government will not print beyond what's appropriate, leaves too much room for human error. To achieve a digital gold standard, Mr. Nakamoto capped the amount of Bitcoin to be issued at 21 million BTC. After the issuance of 21 million bitcoins (projected to be reached around 2140), the free market alone will determine its value.

Mining for Bitcoin requires substantial computing power, resulting in a significant required investment for hardware and continuously high electricity costs. To incentivize individuals to set up mining nodes, Mr. Nakamoto designed a system where mining is rewarded with the creation of new Bitcoin each time a new block is correctly verified. As the currency gains popularity, the reward per block verified decreases. Specifically, with each 210,000 blocks mined, the number of bitcoins rewarded halves. Eventually, rewarded bitcoins will become a small percentage of revenue for mining, and transaction fees paid by transferors will instead serve as the primary incentive. The magnitude of that transaction fee is determined by the transferor based on the speed with which verification is required. Naturally, transactions with higher fees attached take priority in the verification process. The cheapest and fastest

transaction fee is around 31,641 satoshis (0.00000001 BTC per satoshi) which translates into a U.S. dollar fee of 40 cents (four-tenths of a percent in a $100 equivalent transaction).

Despite the ingenious mechanics behind Bitcoin, headlines revolved around the exciting concept of a new digital currency, one that could result in a return to the gold standard. As Miles Price describes it: “For years after the launch of Bitcoin, the fascination came from the currency itself, and the libertarian paradise that a gold standard could bring” (Price, 2017).

In accordance with the flashy headlines and the innovative concept of Bitcoin, the currency’s value has and continues to be extremely volatile relative to other established currencies. While this volatility can be seen in exotic currencies around the world, mainly in underdeveloped countries, those currencies are generally still used to transact business as it may be the only form of payment. On the contrary, Bitcoin is an alternative to the customary form of payments and only a small number of stores accept cryptocurrencies online. As a result, owners often choose to hold on to Bitcoin and use traditional currency, anticipating future gains in the value of their holdings. This problem results in a lower-than-optimal volume of transactions that would otherwise allow Bitcoin to scale appropriately. Evidenced by the following seven-year price chart comparing Bitcoin to UUP, an ETF tracking the value of the U.S. dollar, owners holding their positions have benefitted greatly, but at the cost of outstanding volatility.



At its core, Bitcoin is a virtual asset created and maintained by computer programmers. However, the incredible potential for disruption attracted interest from a different group of professionals: the venture capital community. Startups like Coinbase and Braintree initially secured over $150 million in funding collectively, with a portion coming from venture capital firms specifically dedicated to Bitcoin, such as Lightspeed Venture Partners. Although venture capitalists have a long history of investing in and managing early-stage technology companies, the cryptocurrencies space presents a new challenge for operating partners striving to achieve growth in accordance with their fiduciary duties to investors.

In addition to a limit on the amount of Bitcoin issued, Mr. Nakamoto also decided to cap the size of a block at one megabyte. This translates into a capacity of roughly seven transactions per second, which pales in comparison to the 1,736 transactions per second that Visa handles in the U.S. Since changes to the source code would involve agreement among many people in the Bitcoin network, a civil war has broken out within the community, with one camp worried that an increase in the size of the block, which would enable quicker processing of transactions, would lead to further concentration in the mining industry, eventually turning the platform into a traditional centralized network. The counter party points to the massive backlog of transactions in Bitcoin waiting to be verified, up more than four times from six months ago according to CNBC. They argue that the system will never achieve its potential scale if its promise of fast and cheap transactions cannot be met.

Bitcoin Unlimited is an initiative that aims to “remove the only point of central authority in the Bitcoin economy – the blocksize limit.” It is a platform for miners that contradicts the customary platform, Bitcoin Core, originally developed by Satoshi Nakamoto by allowing miners to customize the size of the block. Bitcoin Unlimited’s growing market share of all nodes (presently 11 percent according to CNBC) underscores a unique risk to the value of Bitcoin: if Bitcoin Unlimited secures 50 percent of all nodes, a fork in the data may occur, also referred to as “a crisis of differing public ledgers.” While Bitcoin Unlimited and Bitcoin Core would both continue to operate, the currency would be split into two different coins.

Changes to the source code of Bitcoin's underlying technology is absolutely an issue that should be debated strenuously. However, it can be argued that a future split of the currency into two separate coins would confirm a failed implementation of Bitcoin. To speculate, the vast amount of data and information available after Bitcoin's seven years of widespread use should be sufficient to determine an appropriate strategy allowing for the processing of a higher volume of transactions. Accordingly, it is important to note that the blockchain itself has operated for seven years with no hacks or errors. It can be reasonably assumed that the failure to arrive at a solution and the development of the largest risk facing the value of Bitcoin currency today is the result of a collection of personal conflicts of interest. "Incredibly the downfall of the network might come down to politicizing the issue of changing a measure that must be changed for the survival of the network" (Price, 2017).

In conclusion, it would be misleading to use Bitcoin's go-to-market as an indication of blockchain technology's future. Blockchain's inevitable effect will not be the introduction of new digital assets but will instead reform the infrastructure of organizations across all industry verticals. The issues that have interfered with Bitcoin's ability to achieve scale deal with the difficulty of introducing a new cryptocurrency rather than the limitations of its underlying technology. Although a valid argument can be made that the possible split is a result of blockchain's limitations, a counter argument can also be made that the absolute benefits of preparing and responding to a higher volume of transactions was not properly weighed against the hypothetical possibility of increased concentration of nodes.

VI. Conclusion

Theoretically, blockchain technology has the capabilities to automate most of the core functions performed by financial institutions. However, the same can be said for businesses across multiple verticals. Instead, blockchain will enable firms to drive efficiencies to an extent previously unattainable with existing technologies. The availability and reliability of data produced by the distributed ledger will allow internal and external auditors to make informed decisions without the problem of asymmetric

information. “If an accurate (blockchain) record of all of Lehman’s transactions had been available in 2008, then Lehman’s prudential regulators could have used data mining tools, smart contracts and other analytical capabilities to recognize anomalies” (Giancarlo, 2017). Smart contracts will instill a renewed trust in the system, reduce the burden of legal fees, and inadvertently increase liquidity in financial markets. In short, increased transparency and assurance in the absence of regulatory authority will stimulate financial market participation, benefitting organizations that are sufficiently prepared.

References

What is Bitcoin Unlimited? Retrieved from http://www.bitcoinunlimited.info.

Blockchains: The great chain of being sure about things (2015, October 31). Retrieved from http://www.economist.com.

CoinDesk BPI. *Price Chart*. Retrieved from http://www.coindesk.com.

Computershare Limited. (2016). *Annual report 2016*. Retrieved from https://www.computershare.com/News/CPU_Annual_Report_FY16.pdf.

Cox, J. (2015, April 15). *5 biggest banks now own almost half of the industry*. Retrieved from http://www.cnbc.com.

Credit Card Processing & Money Transferring in the U.S. (2017, February). IBISWorld Industry Report 52232.

Debt Collection Agencies in the U.S. (2016, December). IBISWorld Industry Report 56144.

Desjardins, J. (2017, April 23). *New technology could change the way the stock market operates*. Retrieve from http://www.businessinsider.com.

Draupnir, M. (2016, April 29) *How do Bitcoin Mining Fees Work?* Retrieved from http://www.bitcoinmiining.com.

Faulkner, J. (2013, May 16). *What is Bitcoin, and How Does it Work?* Retrieved from http://howtogeek.com.

Federal Financial Institutions Examination Council (US), Commercial Banks in the U.S. [USNUM], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/USNUM, April 23, 2017.

Financial Services Spotlight (2015). Retrieved from http://www.selectusa.gov.

Fritz, J. (2016, October 25). *2016 Transfer Agent Market Share*. Retrieved from http://www.auditanalytics.com.

Greenwood R. & Scharfstein, D. (2013). *The Growth of Finance*. Harvard Business School. Retrieved from http://www.people.hbs.edu.

History of Bitcoin: The world's first decentralized currency. Retrieved from http://historyofbitcoin.org.

Kharpal, A. (2017, March 17). *Nearly $2 billion has been wiped off bitcoin's value in three days all because of a fork.* Retrieved from http://www.cnbc.com.

Lewis, M. (2015). *Flash Boys*. New York, NY: W.W. Norton & Company, Inc.

Nakamoto, S. (2008, November). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from http://bitcoin.org.

Philippon, T. (2011, December 2). *Has the finance industry become less efficient? Or Where is Wal-Mart when we need it?* Retrieved from http://voxeu.org.

Price, M. (2017). *Blockchain: The complete guide to understanding blockchain*. Middletown, DE.

Securities Brokering in the U.S. (2016, October). IBISWorld Industry Report 52312.

Stock & Commodity Exchanges in the U.S. (2016, October). IBISWorld Industry Report 52321.

Tepper, F. (2016, July 9). *The reward for mining Bitcoin was just cut in half*. Retrieved from http://techcrunch.com.

The digital bank: tech innovations driving change at US banks (2016). London, England: Ernst & Young.