5-2016

# The Economics of the Blockchain: A study of its engineering and transaction services marketplace

Dylan Bargar
*Clemson University*, dylanbargar@gmail.com

# THE ECONOMICS OF THE BLOCKCHAIN: A STUDY OF ITS ENGINEERING AND TRANSACTION SERVICES MARKETPLACE

---

A Thesis
Presented to
the Graduate School of
Clemson University

---

In Partial Fulfillment
of the Requirements for the Degree
Masters of Arts
Economics

---

by
Dylan Bargar
May 2016

---

Accepted by:
Dr. Gerald Dwyer, Committee Chair
Dr. Skip Sauer
Dr. Charles Thomas

ABSTRACT

The purpose of this document is to discuss the origins, developments, and economic issues of blockchain technology as well as the industry opportunities presented by different forms of distributed ledger systems. The engineering of digital currencies' blockchains are presented beginning with bitcoin and its blockchain. Afterwards, specific areas of contention within the engineering innovations and their interaction with the economics of blockchain transaction services with respect to the consensus process are discussed. Finally, industry opportunities are presented and specific organizations' applications are described.

TABLE OF CONTENTS

## Introduction

Digital currency technology has evolved rapidly over the past decade, beginning with bitcoin and progressing to the evolution and broad application of the blockchain. When bitcoin was created in 2009, the scarcity and security issues of digital currencies were solved with the creation of the blockchain, which allowed for the creation of an asset with no physical or digital presence that could not be replicated and was difficult to steal. This essay discusses the engineering of the bitcoin's blockchain and specifically its potential applications to future industry.

Although this essay will focus on the significance of the blockchain and its design to markets, it will begin with a brief discussion on the blockchain's origins—digital currencies and specifically bitcoin. After discussing the growth and economics of digital currencies, the essay will discuss recent developments in blockchain technology, specifically the importance of the verification process and the different forms of the blockchain which have different solutions to issues presented by the blockchain. Finally industry applications specific to financial markets as well as implications of introducing this technology certain industries will be briefly discussed along with some discussion for future research.

## Origins of Digital Currencies

Digital currencies began as asset-backed electronic tokens prior to the Dot-com Bubble. E-Gold was the first such currency and was essentially a token backed by physical gold. In 1999, the currency was proclaimed as "the only electric currency that

has achieved critical mass on the web" by the Financial Times. Although it initially appealed to those who felt that currencies should be backed by precious metals, the currency faced many of the same problems that bitcoin would later have to deal with, and eventually shut down after the currency's frequent use in illegal transactions or transactions which funded illegal purposes attracted the attention of prosecutors (Hughes et al., 2007). Other digital currencies or digital transaction services also predicated bitcoin (a notable one being the Liberty Reserve and its foreign exchange service), but the structure and associations with criminal activity allowed each to be eventually shut down by the United States Government. Although these currencies were traded on electronic platforms and lacked a physical form, they were not truly digital since they required an asset (such as gold) to maintain value. The creation of the blockchain created verifiable scarcity.

## The Bitcoin

The bitcoin was the first truly decentralized digital currency (Chowdrey and Mandelson, 2013). Bitcoin was created in 2009 by an individual or group of individuals operating under the pseudonym Satoshi Nakamoto (Dwyer 2014). In attempt to improve the financial system and its "trust based model", Nakamoto created an "electronic payment system based on cryptographic proof instead of trust". Bitcoin theoretically made this remedy possible by utilizing a peer-to-peer distributed ledger to prevent double-spending (Nakamoto). This innovation laid the foundation for many other digital currencies and innovations which used these networks to verify payments between individuals.

Bitcoin began as a published Bitcoin Protocol theory published in 2008, which grew into an open-source software released to the public in 2009 (Chowdrey and Mandelson, 2013). By solving complicated algorithms, miners generate new bitcoins and add to the system's total. As bitcoin has grown in popularity, so has its worth. As of January 2016, bitcoin trades for close to $400, a nearly 17-fold increase (Chowdrey and Mandelson, 2013). Bitcoin is essentially just a product of the blockchain, a technological innovation which prevents double-spending and counterfeiting. The blockchain dictates the buyer and seller and transactions, which simply dictates who owns a given bitcoin at any time. For this reason, a bitcoin has no physical properties in the sense that it cannot be downloaded or destroyed. To have bitcoins means "nothing more than having the ability to move these bitcoins in the Bitcoin ecosystem (Badev and Chen, 2014).

The total intended release of bitcoins will be twenty-one million, with a rate of increase that halves every four years (Nakamoto). As bitcoin's popularity increases and the rate of increase of bitcoin decreases, miners are beginning to find it significantly harder to generate new coins. The costs in terms of time, wear and tear on computers, and electricity often do not justify the effort of participating in bitcoin mining. Oftentimes, this hardware created specifically for bitcoin mining (oftentimes graphic processing unites (GPUs) or Application Specific Integrated Circuits (ASICs)) still does not net positive profits from newly minted bitcoins alone (CoinDesk, 2016).

Despite the trends of high growth of bitcoin over the past few years, "bitcoin is still in its infancy" (Wolfson, 2015). The growth of bitcoin and blockchain interest is increasing at a notable rate. For instance, total venture capital investment doubled in 2015

compared to 2014, exchange traded volume in Q4 of 2015 was four times greater than Q4 of 2014, and four times more firms were interested in bitcoin or blockchain technology at the end of 2015 than at the end of 2014 (Hileman, 2016). The early stage nature of this technology makes it difficult to analyze, especially considering much of the current buying and selling of bitcoin appears to be speculative. This can be demonstrated by the distribution of bitcoin ownership. "Of the approximately 12 million bitcoins in circulation 47 individuals hold 28.9%; 880 individuals hold 21.5%; 1 million individuals hold 20.7% and 7.42% have been lost" (Wolfson 2015).

## Ripple, Litecoin, Ether, and other Digital Currencies

Digital currencies other than the bitcoin have provided unique alternative options to the bitcoin and its blockchain. Below, the origins and engineering of a few alternate digital currencies are discussed. These currencies either provide notable alternatives to bitcoin's blockchain or have obtained a significant market capitalization.

### Ripple

Ripple was developed by the venture-backed startup Ripple Labs Incorporated. Its growth opportunities have resulted in funding and interest from numerous high impact companies and individuals, including the Chicago Mercantile Exchange Group and Google Ventures. Additionally, the firm has recruited personnel with experience in economics, finance, technology, security, and regulation (Ripple Labs). Perhaps this intrinsic infrastructure in terms of advisors and capital gives the currency the best

possible opportunity to succeed despite having just a fraction of the market capitalization of Bitcoin.

A finite number of 100 billion Ripple will be created by Ripple Labs on the frontend. Since Ripple Labs is a venture-backed startup, the company will retain 25% of all Ripples to fund operating costs, which of course has drawn significant controversy (Popper, 2013). Ripple Labs does not require individuals to use Ripples during their transactions using the Ripple protocol system but instead acknowledges that using Ripples would be the most inexpensive method of transactions. However, if a user still did not want to use the XRP currency, they could still deal in fiat currencies and experience greater liquidity relative to current global exchanges. Effectively, the system increases fiat currency's liquidity. Unlike bitcoin, Ripple was developed to improve current financial capabilities rather than replace currencies. Ripple systems and XRP are complements to modern financial infrastructure, not substitutes (like bitcoin seemingly attempts to be). Additionally, unlike bitcoin or fiat currencies, Ripple transactions are instantly settled through their protocol system (which will be discussed later), enabling lower costs and risks.

Litecoin

Litecoin is another payment system invented by a former Google programmer Charles Lee. It was marketed as "silver to Bitcoin's gold", or a "lite version of Bitcoin" (Bitcoin Forum, 2011). It is structurally nearly identical to bitcoin, and was purposefully created as a complement to bitcoin. For instance, the currency was created to produce

roughly four litecoins for every one bitcoin. Additionally, litecoin better supports payments by having significantly faster block generation time (https://litecoin.org/). Although litecoin provides few other significant advantages over bitcoin, in tandem it could be useful for small value transactions. However, the purpose of litecoin is slightly ambiguous. The developers of litecoin stated it was "silver to bitcoin's gold" without actually stating the worth of litecoins in bitcoins. Litecoin's worth relative to bitcoin is market determined rather than influenced by a concrete relationship. Even though four times more litecoin were made than bitcoin, the price relative to bitcoin has been noticeably volatile. This indicates that, even though litecoin was envisioned as a complement to bitcoin, it is on a somewhat independent demand function than bitcoin.

Ether

Ether is a digital token created by the Ethereum Foundation. Its primary use is a transaction fee to compensate miners and also impose costs on users attempting to execute large transactions or contracts (in terms of coding requirements or total byte size) on the alternate and potentially more useful Ethereum blockchain. Additionally, it can be used as a currency which provides liquidity in transactions. Ether's success as a currency will likely be tied to the Ethereum platform's success as a transaction service. Ether denominations are predetermined by size for scalability and simplicity. The biggest denomination is a *wei* (1), followed by a *szabo* ($10^{12}$), a *finney* ($10^{15}$), and finally an ether ($10^{18}$) (GitHub Ethereum wiki). Ether has appreciated greatly since Ethereum's inception as the platform's popularity has rapidly increased.

### Other Digital Currencies

Other digital currencies exist, but with very few differences and much smaller market capitalizations. However, some notable examples include financial institutions' currencies. For instance, Goldman Sachs recently filed a patent for SETLcoin, a digital settlement currency which provides nearly instantaneous payment settlements unlike bitcoins ten minute settlement time (Cohen, 2015). Additionally, Citi Group is currently creating Citicoin, which appears to be an innovation in bitcoin's blockchain technology (Biggs, 2015). These innovations and others are perhaps most helpful because they give an indication of what these financial institutions consider to be most valuable in blockchain technology.

## Security and Regulatory Concerns for Digital Currencies

Security and regulation of digital currencies and the blockchain is a major concern for industries considering using this technology. Below, a few issues are described in detail.

### Security

The security and rigorousness of the blockchain is a major point of contention which will be discussed heavily in this essay. The possibility of double spending must not feasibly exist to ensure technology adoption. Double spending or untrustworthy blockchain may keep information on the blockchain from being scarce or reproduceable.

The engineering and design of the blockchain and its solutions to these issues are discussed extensively in this essay.

Yet another concern is the potential for individual's wallets to be "hacked", which could (and has), resulted in the rapid loss of millions of dollars of digital currency. In July of 2014, the exchange Cryptsy was hacked and lost approximately $10 million of bitcoin and litecoin, causing the website to go insolvent and threaten bankruptcy (Higgins, 2016; Cryptsy). Perhaps one of the largest issues with digital currencies and distributed verification systems is the inherent risk of hacking, which can be difficult to track and, at least with bitcoin, very profitable. Exchanges are particularly vulnerable and perhaps the unique privacy system of the bitcoin is inherently flawed concerning the potential for hacks.

Finally, bitcoin and other digital currencies are not assets in the physical sense of the word, but statements of ownership recorded by the blockchain. Digital currencies rely on public and private-key cryptography. As mentioned earlier, bitcoin users' bitcoins are associated with a "wallet" with an "address", or public key (Dwyer 2014). The owner must have a private key to be able to do transactions. If the owner loses the private key, the currency is lost. This could be a major issue in digital currencies. Over 7% of generated bitcoins are already considered lost (Wolfson 2015). Since these currencies were only engineered to generate a predetermined number, this accessibility issue presents issues with digital currencies stability.

Regulation

Regulation consideration for digital currencies have also increased with interest. The issue of cryptocurrency security and regulation is subject to significant debate following the Silk Road investigations and findings. If bitcoin and other cryptocurrencies can enable and even encourage international illegal activity, perhaps the drawbacks of this innovation outweigh potential benefits. Digital currency experts and advocates are proactively attempting to address intrinsic security and legality issues in numerous virtual currencies. The two currencies with the largest market capitalization (bitcoin and Ripple) actually directly work with legislators and regulators concerning education and healthy adoption of digital currencies (Bitcoin Foundation, Ripple Labs).

Prior to the Mt. Gox (a bitcoin exchange) collapse and the Silk Road (an internet black market) raid, Mt. Gox's U.S. accounts were seized at Wells Fargo and Bitfloor's, another bitcoin exchange, accounts were closed by Capital One Bank as news of bitcoin's use in the black market website Silk Road spread (Wolfson 2015). The collapse in bitcoin prices and the disappearance of $460 million of bitcoin from Mt. Gox (at the time, the world's largest digital currency exchange) may indicate an apparent need for regulation in the bourgeoning digital currency market (McMillan, 2014).

Bitcoin and other digital currencies fall into a "legal grey area" (Bernard, 2015). Although a few existing laws could potentially regulate the currency, the most obvious regulation opportunity is through the executive agency or Congress's constitutional right to control money (Kaplanov, 2012). Issues exist regarding the legitimacy of payments, potentials for illegal international monetary transfers, and a possible lack of control over certain aspects of inflation and monetary policy concern legislators and market makers.

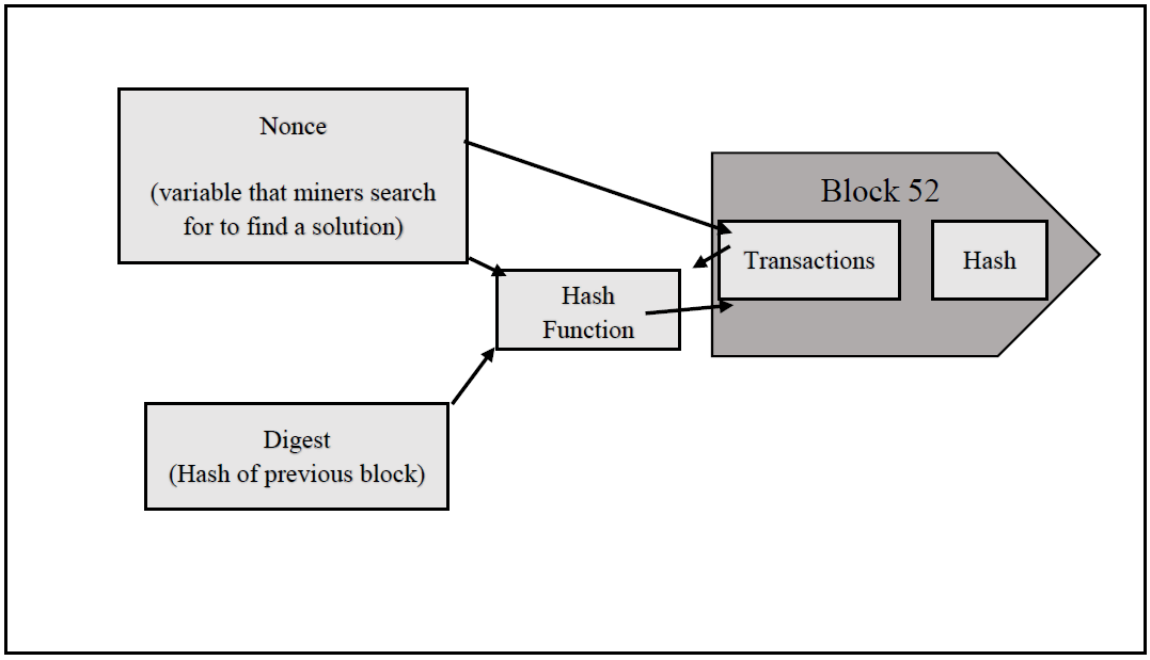
Regulators are apprehensive concerning their ability to enforce money laundering laws and collect taxes with digital currencies (Dwyer 2014). However, a few countries have already outright banned bitcoin from use (notably Iceland, Bangladesh, as well as China which banned bitcoin use for financial institution). Additionally, in the United States, the Internal Revenue Service views bitcoin as property instead of currency, meaning users must pay capital gains taxes on profitable purchases and sales of bitcoin transactions (Swan 2015).

An additional concern is the possibility of digital currencies becoming a preferred currency or even competition for a country or group of people (similar to the American dollar in Zimbabwe). There are two distinct causes for this possibility, the first being a lack of stable monetary policy from the central authority in that specific region. In fact, the European Central Bank has carefully considered this possibility, concluding that "virtual currency schemes provide an alternative way for individuals to achieve the same end: accessing commerce and effecting payment transactions." (European Banking Authority 2014, Baron et al. 2015). An additional possibility is the "building up maintain [of] communities", or essentially a currency specific to a community to encourage growth and local production and consumption in the area (Baron et al. 2015).

Finally, monetary policy with digital currencies would be complicated. Any institution, regardless of intentions, would have an extremely difficult time influencing the real economy if bitcoin were a popular medium of exchange. The Federal Reserve's dual mandate (to promote stable prices and maximize employment) would be difficult to exercise at best with digital currencies. For instance, bitcoin has a stated limit of twenty-

one million. Many economists reason that this limit will cause a “deflationary spiral”. As the currency approaches the limit, popularity may increase and the currency will appreciate, resulting a deflating prices of goods in bitcoin. This incentivizes consumers to hold onto currency rather than spend it, resulting in more deflation (Chowdrey 2013). Perhaps a central bank, say the Federal Reserve, could influence monetary policy in digital currencies through open market operations. They could simply buy and sell bitcoin depending on monetary policy goals.

**The Blockchain Verification Process**




(The diagram above shows the method which the blockchain utilizes to verify and store transactions in block 52)

Bitcoin's success depends on a peer-to-peer distributed network which updates an underlying database of transactions called the blockchain. One of bitcoin's heralded advantages is the anonymous, decentralized nature of the currency—the strengths and weaknesses of this have already been discussed—which is only possible with the blockchain. Transactions are recorded in the blockchain.

Recording transactions requires use of recent cryptographic innovations to ensure the honesty in the system. The two cryptographic methods utilized by the system are *digital signatures* and *cryptographic hash functions.* Digital signatures are created by digital keys through hash functions and are required for transactions between individuals. They occupy a field in individual transactions. This is critical to the bitcoin market and is

further discussed in the paragraph below. A cryptographic hash function takes a string input of arbitrary input length and returns a string of predetermined length. In order to make it difficult to reproduce transactions, it is very difficult to find an alternative input which creates the same string. To accomplish this, the bitcoin system utilizes a SHA-256, a Secure Hash Algorithm written by the National Institute of Standards and Technology (Henri and Handschuh, 2003).

This cryptographic hash function is required to verify payments through a proof-of-work system which of course requires computer work and time. The proof-of-work algorithm is a transaction cost in the form of an algorithm which is difficult to produce but easy to verify (Becker et al., 2013). If one wishes to change the transaction recorded in the blocks, they must solve the proof-of-work algorithms of past blocks and the current block faster than other users, who are just competing to solve the current block (Badev and Chen, 2014; Nakamoto). After a transaction is initiated, nodes on the network require a relatively short amount of time to verify the transaction which ensures that (1) the initiated transaction between the two parties is correct as stated and (2) the sending party actually has enough funds to complete the transaction (Badev and Chen, 2014). After this initial process is verified, participants (called miners) in the network compete to be the first to solve a proof-of-work algorithm and generate a hash less than the target. Miners compete to solve a problem which is a function of *digest*, a set of transactions including the *digital signatures*, and the *nonce,* an alpha-numeric string which contributors attempt to find to solve the equation. The output of the equation must have at least N leading zeros, where N is the number of leading zeros, establishing the difficulty (since the

acceptable value is lower, meaning that there are fewer solutions) derived from the amount of time it took to find the last 2016 blocks. The first node to determine a correct *nonce* which is a solution to the problem is rewarded with newly generated bitcoins and possibly voluntary transaction fees. These contributors are known as miners. Since new bitcoins will eventually run out (or alternatively as rewards decrease over time), these voluntary transaction fees are intended to eventually replace newly generated bitcoins and some non-bitcoin blockchains (Dwyer 2014; Badev and Chen, 2014; Nakamoto).

The blockchain system by design enforces a target equilibrium for supply of transaction services. Consumers (those who use deal in bitcoins or use Ethereum) expect transactions to be bundled into the blockchain actively and consistently, and likely care little about the overall hash rate as long as the transactions reliably occur and consist of proof-of-work algorithms difficult enough to ensure system security. Suppliers are willing to contribute as much computing power as necessary as long as expected profits are positive. To ensure that consumers receive the predictability necessary for use, blockchain systems create a target rate for block generation once every ten minutes. The difficulty of the proof-of-work algorithm is automatically increased or decreased to meet this target block generation time. As can be expected, increases in the network difficulty have a positive correlation with increases in the network hash rate, which is the processing power of the particular blockchain network.

This target rate promotes an equilibrium supply and demand of transaction services. Suppliers will still continue to innovate and improve their computing power as long as expected profits are positive. Consumers will still be able to utilize transaction

services at a stable and specified rate; however, they may pay higher transaction fees due to difficulty. The benefits of this system are a stable and predictable supply of transaction services as well as a self-regulating difficulty setting for the proof-of-work algorithm which keeps up with technology. The concerns are possible higher transaction costs resulting in a decrease in potential consumer welfare since transaction services providers will have to be compensated for increased difficulty.

For example, bitcoin has a target rate of one new block generated every ten minutes, or 2016 blocks generated every two weeks. Every 2016 blocks, the difficulty is recalibrated. If it took less than two weeks for the network to create 2016 blocks, the proof-of-work algorithm increases in difficulty. Of course, as technological innovations blend with blockchain technology, difficulty will climb sharply as ASICs and other mining devices become more powerful and sophisticated assuming that positive profits are still expected.

In non-bitcoin blockchains such as Ethereum, users must use the system's recommended transaction currency (ether for Ethereum) to incentivize miners to verify transactions. Alternatively, in private or permissioned blockchains, security may not be as great of an issue and the network can efficiently function with less demanding proof-of-work functions or potentially even no proof-of-work function. Additionally, the system could theoretically function with an external agreement that requires each participant to participate in the expensive mining process to an extent to be allowed on the private or permissionless blockchain with a proof-of-stake agreement or something similar.

The successful miner broadcasts to other nodes, who verify that the hash is a solution. Again, while the proof-of-work algorithm can be very difficult to solve, it is easily verified. Once the other nodes on the network recognize the block, they move on to the next block and the transaction is added to the blockchain. The longest blockchain is used by nodes to add future blocks to the chain, which is only problematic if two chains of equal length exist in which case only one will be used for future transactions.

If one wishes to change a prior block in the blockchain from the widely recognized form, they must have over 50% of the computing power in the system. They would not only have to change the target block, but also all the blocks in the blockchain that have occurred since the target block was created. For instance, if a group of miners would like to control the details of transactions in the next two blocks (J and J+1), they could create the next three blocks (J, J+1, J+2), and add them to blockchain while other users are working on J+1. Since this blockchain would be the longest, it would be used for future transactions. However, the individual would require over 50% of computing power to accomplish this even somewhat reliably. Due to this system, "the probability of a slower attacker catching up diminishes exponentially as new blocks are added" (Nakamoto). If the attacker were to catch up and successfully beat other miners in the current block creation, the original chain would be irrelevant and the network would continue creating blocks on the new chain. The transactions recorded in the new blockchain would be the new reality

In short, the blockchain requires miners in order to not just ensure security and honesty, but also actually execute transactions. To increase probability of successful

mining, oftentimes miners join mining pools to increase total computer power and decrease risk of unsuccessful mining. However, pooled computer power increases chances of a group of miners obtaining over 50% of power in the network, which could perhaps instantaneously devalue bitcoin by removing the assurance of honest transactions.

As mentioned earlier difficulty increases as more miners participate. In fact, considering the costs of equipment and electricity, mining bitcoin may not have been profitable since 2013 (Dwyer 2014). Specific software has been created specifically for mining on blockchains and related products have been created as well. An example is the relatively new company named 21, which received $116 million in venture funding in March 2015 (Hileman, 2016; 21 Incorporated, 2016). Although the 21 computer was designed to be complementary to bitcoin in the sense that it assisted the user to develop products to work with bitcoin rather than necessarily mine, its relatively advanced GPU is much more powerful for bitcoin mining than the average computer. However, a quick calculation utilizing the specifications for the 21 computer and an efficiency calculator revealed that if 21's system was only used for mining, there would be no breakeven in the first year when accounting for energy costs. In fact, only $20 in revenue would be generated in the year (TradeBlock; 21 Incorporated, 2016). Bitcoin mining has simply become too difficult for many bitcoin miners to participate.

Recently, even more powerful, dedicated computers called Application Specific Integrated Circuits (ASICs) have been created for the specific purpose of mining bitcoins. Some of the newer computers are extremely powerful and expensive, with modules

which can produce at hash rates occasionally reaching and even topping 500 gigahertz. However, the costs in terms of time and energy expenditure as well as the very high costs of this equipment may likely not be covered by the newly generated bitcoins. Fortunately, miners are incentivized to participate in the verification process not through newly generated bitcoin, but by transaction fees paid by bitcoin users. It appears that this method works by virtue of supply and demand and these voluntary transaction fees might be the answer to future blockchain innovations. Transaction fees are already being used by the Ethereum system. This has contributed to the recent high growth in value of Ether against the dollar as demand has increased for transactions on the Ethereum platform.

Blockchain's privacy differs from traditional transactions by ensuring that the private keys associated with public keys remain anonymous. Although transactions are visible, the source or destination of transactions can only be known if observers know who owns the public keys or "addresses" similar to a stock exchange, where all transactions are visible while still remaining, to some degree, private (Nakamoto). Of course, if one knew an individual's public key, they would be able to track all transactions in which the individual participated using that address. Although bitcoin is, to some degree, private, it is not necessarily anonymous (Nakamoto; Dwyer 2014). The public key is stored on the blockchain as transactions are bunched into blocks.

As mentioned, the network peer-to-peer verification process is critical to ensuring that double spending does not occur. Nakamoto gives a few network requirements to ensure the security and use of bitcoin. "(1) New transactions are broadcasted on all nodes, (2) each node collects new transactions into a block, (3) each node works on finding a

difficult proof-of-work for its block, (4) when a node finds a proof-of-work, it broadcasts the block to all other nodes, (5) nodes accept a block only if all transactions are valid and not already spent, and (6) nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash". This process will take at least ten minutes, the target rate generation rate for the blockchain. As we will discuss later, many financial institutions seem to consider this waiting period to be a degree of added risk to the payment process and there are certain blockchain innovations which could reduce this transaction clearing time. Of course, a potential solution would be to change the target rate of block generation, but this is not easily considering current blockchain protocol. As mentioned earlier, this would automatically alter the difficulty of the proof-of-work algorithms by changing the difficulty (by altering N, the number of leading zeros in a successful solution).

Since a bitcoin is just a statement of ownership, the real innovations in digital currencies is the distributed ledger technology. As such, recent developments in digital currency have largely focused on the blockchain. As the blockchain continues to develop and improve, opportunities for further use of bitcoin as well as potential other digital currencies will continue to grow. However, the most impressive and disruptive component of bitcoin is its technological foundation, the blockchain.

The future of digital currency may very well likely be the blockchain technology utilized by bitcoin and other digital assets. The distributed ledger has numerous advantages which are directly applicable to many markets and could provide instantaneous returns if utilized correctly. Of course, there are concerns with the security

of distributed ledgers and incentives for miners to participate in the critical verification process, but the huge potential returns of blockchain technology ensure that interest and investment will continue to flow.

## The Importance of Blockchain Innovations to Adoption

Major banks seem to care most about the design of this blockchain consensus process. Concerns about the payment protocol system and security rigor are incentivizing banks to cautiously experiment with bitcoin adoptions. Although the currency has much potential, several issues must be addressed if it is to become ubiquitous as a financial tool and medium of exchange.

## Different Forms of Blockchains

Discussions of the possibilities of digital currency technology seems to mostly concern the advantages and potential issues of blockchain technology (Piscini, 2016; Hileman, 2016). The current form of the blockchain which is applied to most digital currencies including bitcoin is a public, permissionless blockchain, the security issues of which have already been discussed. Blockchains may be able to ensure that transactions and payment verification can occur without the existence of centralized oversight similar to the United States Treasury Department and the U.S. Federal Reserve or even just banking institutions. However, financial institutions and large companies must have

assurance concerning the security of outgoing and incoming transactions. As interest in digital currencies has grown, so has discourse concerning the evolution of the blockchain and methodologies for improvement of transaction verification.

The blockchain or distributed ledger technology will likely only gain traction when major financial participants (such as banks, exchanges, clearing houses, or funds) can trust the level of security and volatility of transactions. Although this is accomplished through bitcoin's blockchain, the current permissionless blockchain nevertheless has its faults. Although the technology has significant opportunity to positively disrupt the financial system especially related to remittances and transactions, there must be an industry consensus concerning the engineering of the ledger and the methodology of the verification process. Financial institutions and other firms must feel that the technology is low enough risk to utilize it in their businesses.

The blockchain, as mentioned earlier, is the distributed network system used to verify and record bitcoin transactions and their process. Distributed ledgers such as blockchain have numerous cross-industry use opportunities. To facilitate potential distributed ledger use, there are many innovations to distributed ledgers which are being explored and tested. These include distributed ledgers with limitations concerning verification, transaction recording, and access. While these major innovations impact who can view or verify transactions on any distributed ledger, they have little impact on the core engineering of the blockchain. The basic idea of the distributed ledger remains the same. As far as recent innovations within distributed ledgers, there are two separate sets of categories for distributed ledgers as described by Peters and Panayi (2015).

With regards to access protocols, distributed ledgers can either be:

- Public: Any user who wishes to do so can access the ledger and submit transactions for inclusion. This is the blockchain technology used in bitcoin. This is the true democratized form of the ledger and, by many opinions, the ideal system. Much of the discourse which can be found online concerns the public access to information and transaction submission which may have fueled much of bitcoin's surge in popularity. It seems as if the decentralized, democratized version of this technology is not only popular for potential efficiency reasons but also for some other idealistic reasons.
- Private: Only a select few participants can view as well as submit transactions. Although the market can have many participants, only certain individuals or institutions will have access to the ledger and the development of the blockchain. This better resembles a financial exchanges or modern banking due to the centralized characteristic of the process. Although only a few institutions (brokers) verify these transactions, anyone can willingly participate in the dealing of assets. This process sacrifices potentially lower transaction costs on public blockchain for increased reliability and security. Individuals or institutions who would like to participate in the verification network must be invited and approved by the overseer. This method does not adhere for the original purpose or intention of bitcoin, which was to create a completely decentralized and

anonymous currency, but uses the blockchain for other innovations. Additionally, a private blockchain which is applied to a market could create concerns with the selective nature of the technology (when applied to industries like finance), especially in terms of ease of entry into the market.

In addition to public and private ledgers, blockchain can be divided into two similar but independent categories:

- Permissionless: Bitcoin's blockchain is a public, permissionless ledger which is verified by all nodes on a network with weight distributed based on computing power. Permissionless means that anyone can contribute to the blockchain. As mentioned above, once a transaction has been verified, it is added to the blockchain. In a permissionless ledger, anyone can choose to participate in this verification network and obtain potential rewards of participation. However, no matter the difficulty required to participate in the verification or mining process, the possibility of an organization or individual successfully threatening the system always exists since sufficient concentrated computing power can overpower the system.

  Another issue with permissionless blockchains is scalability. Growth potential is hurt by the data requirements of the blockchain. In the permissionless blockchain, every transaction needs to be processed by every node on the network. The current size of bitcoin's (permissionless)

blockchain is fifteen gigabytes and growing at a rate of one megabyte per hour. If the amount of transactions on bitcoin grew to the amount of transactions process by Visa, the growth rate would increase to 1 megabyte per second, or eight terabytes per year (GitHub Ethereum wiki). This is likely not feasible or efficient especially with an increasing supply of transaction services (participating nodes). Bitcoin's and Ethereum's systems require users to store the entire blockchain history on their system which could be a major flaw for future growth.

- Permissioned: Permissioned blockchains are gaining traction within financial firms and digital ledger-based startups. Just like non-cash payments between individuals must be verified by a financial firm for the transaction to be complete, financial firms would understandably like the same degree of control over the verification and recording process of digital currencies in order to minimize risks. Transactions could possibly take less time and potentially be cheaper because the supply of transaction services will be smaller resulting in a lower network hash rate and lower difficulty of the proof-of-work solution, meaning that transactions are less expensive to suppliers of transaction services. Alternatively, participants could decide to do away with the proof-of-work system altogether, especially since it is in the best interest of financial firms, exchanges, clearing houses, and funds participating in the verification and recording process to deal in good faith with one another. Additionally, the

> permissionless blockchain exists and thrives because individuals are willing to lend computing power to the network to solve the complex algorithms, which means that expected mining profits must still be positive.

An additional innovation which attempts to meet at the middle-ground is the sidechain. The sidechain is essentially a separate permissioned, private distributed ledger operated by an organization which periodically adds some of the information concerning its transactions to a public, permissionless ledger (Yermack, 2015). However, efficient industry use of this technology and permissioned or private blockchains is still being determined.

Although these different forms of the blockchain may seem to have insignificant differences, the occurrence of a transaction and the ability to verify that transaction in the future is absolutely critical for transfers of wealth regardless of whether they concern digital currencies or other physical assets. The added value of the blockchain is the instantaneous competitive verification of transactions including their details and destinations. While this could potentially lower costs and increase liquidity in the market, this will only happen if the blockchain is determined to be adequately secure and transaction costs are lower.

**Industry Opportunities for Blockchain**

There are numerous opportunities for these innovations to positively disrupt the financial sector. Due to the often expensive nature of money transfers (in terms of costs

and time), there is great opportunity for reductions in costs that could benefit institutions and their shareholders as well as consumers. The only potential downsides are security issues of digital systems and the displacement of workers whose jobs are no longer necessary. However, these issues are synonymous with many technological developments. These potentials are listed below.

Smart Contracts

Perhaps one of the most obvious and easily applicable uses of the blockchain concerns smart contracts. Many firms, such as Ethereum, have attempted to create digitally recorded and executed projects utilizing blockchain technology. Smart contracts have seemingly vast opportunities in many industries, and the mechanics of the contract will be discussed here while the work of the not-for-profit firm Ethereum will be discussed later in this essay.

These contracts take some form of a conditional if-then statement involving different parties. For instance, a contract concerning a bitcoin transaction might simply be "If the S&P 500 is negatie tomorrow, give Julie 1 BTC. If else, give Julie 0 BTC" written in a scripting language, which would imply that an individual made a contract with Julie to pay her one bitcoin if the sky was blue tomorrow. This information is distributed throughout the blockchain for the cost of a small token and automatically executed upon occurrence of the event. This application could be used heavily in finance and governance, and can provide quick remedies to issues such as strategic default and save on potential legal and enforcement costs. In fact, the need for legal services would likely

dramatically decrease if all contracts on a platform were self-enforcing (Yermack, 2015; Peters and Panayi, 2015). A significant advantage of blockchain enabled smart contracts is that it eliminates much of the need for extensive regulation in contracts since the network is self-regulating. There is no necessity for trust of a central institution or regulator if the smart-contract itself mechanically executes the terms of the contract (Kosba et al., 2015). Since default risk will always occur, it will be necessary to code details of a potential default into the contract. Of course, when combined with other potential uses of blockchain technology in finance, these items could have huge potential efficiency benefits to the financial system.

*Smart Contracts in Financial Markets*

A very impactful and immediate use of smart contracts includes finance, namely, derivatives trading including "the mechanical exercise of options embedded in derivative securities and other contingent claims, the instant transfer of title to collateral in the event of default, and the payment of employee compensation if performance goals are achieved" (Yermack, 2015). Although smart contracts could apply to all derivatives including those traded on exchanges, the most immediate use may very well be in over-the-counter derivatives markets (including swaps, options, forwards). Until now, most OTC derivative trading has been limited to funds, institutions, or sophisticated investors due to the complicated and risky nature of these investment vehicles. Because they are not highly regulated and since an OTC derivatives contract is between two parties, smart contracts have a very immediate opportunity to increase efficiency and decrease legal or execution costs in these markets. In fact, companies such as HitFin are already attempting

to expand this market by providing platforms for OTC derivative trading using Ethereum-based blockchain technology.

A specific example of smart contracts in trading would be the execution of "swaptions". If one party purchases an option to execute an interest rate swap with another party, the terms of the contract can be programmed to automatically execute in the event the first party chooses to do so. In the code, the options of the swap (say, collect LIBOR + 1% on a $1 million notational principle in return for a 5% fixed rate) will be set and will automatically occur of the first party exercises the option. Since default risks exists, the contract could include collateral or other terms which will be available to the trustee or lawyers. This will require a generally accepted set of laws which recognize the legitimacy of smart contracts. This contract decreases transaction time, removes the necessity for much of the labor involved in the transaction, and does not require legal or regulatory intermediation. This is because the contract is fulfilled and regulated by the network. Not only are these contracts inexpensive, but they also increase liquidity in some markets and could still decrease some risk associated with these deals concerning counterparty risk while lowering legal costs if some form of margin requirement is included in the coding. In this way, smart contracts could be a powerful tool for institutions and funds.

However, smart contracts' financial impact can go much further than OTC derivatives. Companies like NASDAQ are attempting to use smart contracts and other blockchain possibilities for trading exchange traded securities (Grygo, 2016). Even more interesting, the firm Symbiont is creating platforms for utilizing smart contracts to trade

corporate debt, syndicated corporate loans, or private equity deals inexpensively and rapidly (Symbiont, 2016). Symbiont claims that their "technology can aid the numerous other markets and asset classes that suffer from high administrative costs, excessive settlement times and / or reduced liquidity" (Symbiont). Blockchain technology concerning smart contracts has the potential to significantly increase efficiency in the financial system.

*Issues with Smart Contracts*

There remain many issues with smart contracts, but currently there are only three which are concerning. First, a smart contract is an automated execution of an operation, not a transfer of data like a bitcoin transaction. If the code written in were a loop (endless execution), it could bring down network. Firms like Ethereum have solved this by requiring transaction fees based on the size or duration of the transaction, but the solution is less than ideal to some who fear excess transaction costs especially if the currency used to fund transactions is appreciating. Second, smart contracts have no legal precedent. Although the action will be automatically enforced, it might not stand in court. A legally binding contract only requires an offer, acceptance, and consideration, but there is still no precedence for smart contracts. Fortunately, efforts are being made to combat this. Additionally, if smart contracts become popular, it would be extremely taxing on the network to have every node verifying every contract and its execution (Peters and Panayi, 2015). Further research must be done to remedy this scalability issue. Finally, smart contracts are not private. Although public keys can be ambiguous and steps toward privacy can be taken, the terms of the contract will be broadcasted across the entire

network and recorded in the blockchain, which could remove incentives for many institutions or individuals to utilize smart contracts for transactions. Fortunately, it is possible to program separate private and public contracts according to the Hawk framework described by Kosba, el al. (2015), where the public contract written on the blockchain and the private contract is encrypted in a set of logic in the public contract which is executed by the blockchain. Although current mediums for smart contracts cannot yet accommodate private smart contracts, this innovation will likely soon be implemented for smart contracts to become a legitimate option in industry (Kosba et al. 2015).

Remittances

International remittances are an additional opportunity for digital currencies. This $514 billion industry has transaction costs that can be extremely high—between 7 and 30 percent (Swan 2015). Conceptually, a consumer who wanted to switch his U.S. Dollars to Euros could do so much more inexpensively by buying bitcoin and trading for Euros rather than going through the financial system. In fact, Goldman Sachs analysts stated that "bitcoin and cryptocurrencies allow for the decentralized transfer of assets without a central clearing authority" and that these technologies would eliminate 20% of the revenue from consumer-to-consumer currency transfers and save businesses $74 billion in costs (Braithwaite and McLannahan, 2015).

Theoretically, an individual or institution wishing to exchange euros to U.S. dollars, for instance, could buy bitcoin (or any other digital currency for that matter) in

euros and sell bitcoin in dollars and pay cheaper transaction costs than utilizing institutions to exchange euros for dollars. A basic analysis of the exchange rates of fiat currencies and bitcoin shows that bitcoin does display efficient markets in the sense that, based purely on FX rates, the above transaction is roughly equal prior to factoring in transaction costs. However, this is likely due to financial institutions, who can trade for a lower transaction cost than individuals or non-financial institutions who would stand to greatly benefit through this new market. Individuals in countries like Samoa, where much of the GDP is from expatriate family members sending support funds back home would see a significant increase in income. Additionally, international firms could see a decrease in overhead from foreign expenditures. Remittance services could be the largest impact digital currencies have on individuals or non-financial firms since they essentially allow them to participate in FX markets which were previously closed to them.

Settlement Speed

Fast payments are a major advantage of distributed ledger innovations. Trading U.S. equities generally takes around three days to clear due to transaction risks and back office operations (Yermack, 2015). Perhaps decreasing settlement times will positively impact market stability by increasing institutions or money managers' ability to quickly buy and sell assets, or increasing liquidity, and decreasing transaction risks. Faster payments ensures that institutions can respond to potential crises or concerns quicker in addition to actively responding to information or investment opportunities without having to wait for funds to clear using credit lines. Specifically, this would help funds who anticipate margin calls or institutions who anticipate margin calls or bank runs in the

event of a crisis. In good times, this would assist in the more efficient use of funds and investment opportunities. For instance, a money manager closes a position in the morning and would like to open a new position within a few hours. Since their funds have not cleared yet, they must leverage themselves to "fill the gap" until the funds have cleared (which could take as long as three days). However, if this digital technology was used, the money manager would not have to leverage themselves to open a position, but instead could use the debt to strengthen a position and potentially increase returns.

Financing

In addition to remittances and fast settlements, distributed ledger technology could also change the financing mechanisms in terms of issuing equity or debt. Opportunities to finance using blockchain technology would result in "faster, cheaper trade execution and greater transparency of ownership" (Yermack, 2015). First, due to the nature of distributed ledgers, there would likely be an even greater transparency of ownership concerning ownership of shares in a given company if the shareholders of a firm can determine the ownership of certain management's public keys. This increases market efficiency and creates additional profit-making opportunities for other shareholders of a firm. For instance, due to the nature of the blockchain, shareholders could conceivably see instantly determine if a manager was buying or selling shares. Finally, this could conceivably decrease corporate executive pay since managers are paid extensively in stock options. Since the public would be aware of a manager's desire to legally liquidate their position in real time, the market would likely react unfavorably. In addition to increasing information, the blockchain could also positively impact corporate

voting procedures for shareholders by making them relatively cheaper and quicker (Yermack, 2015). This will likely not occur, and managers would certainly not favor this option. However, it is a technical possibility.

### Accounting

A final possibility for blockchain use is real-time accounting. Currently, accounting is relatively labor intensive and time-consuming. The blockchain could be used as long as the firm used digital currencies or tokens. This proposition seems potentially very helpful for firms as long as they can solve they can merge their business's cash flow with the token requirements of the blockchain. It could save costs related to third-party accounting as well as detecting earnings fraud and other suspicious activity (Yermack, 2015).

Blockchain technology has the opportunity to drastically speed up commercial banking ledger operations which would result in faster settlements and increased visibility in terms of finances at any given point. If a financial institution were to adopt this technology, the potentially lengthy process of unsettled funds or unbalanced budgets would not exist like it does today. As mentioned earlier, the negative sides to this innovation in this case are potential security issues.

## Initiatives and Organizations Utilizing Distributed Ledger

Financial services are “low hanging fruit” for blockchain implementation (Allison, 2015). The lengthy settlement times required in finance are significant considering the relatively instantaneous transactions which could occur with technology. For these reasons, there appears to be an “arms race” for companies which would like to leverage technology to fill needs in the massive financial industry. For this reason, companies and organizations like Ethereum, R3 CEV, Ripple Labs, and Digital Asset Holdings are obtaining extensive funding and support to develop the blockchain for use in finance. However, the innovations of these companies, specifically Ethereum, could provoke huge future innovations in blockchain use across industries.

Below, a few specific initiatives are listed and their contributions to blockchain development are described:

Ethereum

Ethereum might have the most potential of these innovations. Ethereum is a Turing-complete and a customized blockchain to enable smart contracts and other blockchain based operations. Turing Completeness refers to a languages universality, or its ability to use “a certain set of primitive operations, which are then strung together in different ways to create programs for different tasks” (Wolfram 642). This idea of system universality can be traced back to the Turing machine, created by the mathematician Alan Turing in 1936 (665). Most popular imperative programming languages, including C++, Python, and JavaScript, are Turing-complete. Ethereum, unlike bitcoin, exclusively uses Turing-complete languages for more modularity.

The firm is a crowd-funded, not-for-profit market-maker developed by the research and development firm ETHDEV. The platform claims that it operates contracts "without any possibility of downtime, censorship, fraud, or third-party interference" (Ethereum). Currently, Ethereum's frontier release was developed as a JavaScript platform for developers to create systems which use smart contracts. Ethereum's remarkability comes from their ability to give users the opportunity to employ smart contracts for many different uses. The organization developed a platform which utilizes very basic imperative coding to develop executable contracts that have already proven to be useful in a variety of industries.

An Ethereum transaction is a simple process which concerns three parties—the sender, the receiver, and the miner. The sender, or one who initiates the contract, must pay a fee (referred to as gas) to complete the transaction. Gas is a tradeable asset which has historically been worth a very small amount of ether. The gas for this transaction, plus five ether, is a reward for the miner who successfully completed the proof-of-work algorithm and created the block. The sender specifies the maximum gas they are willing to pay in the code of the transaction and Ethereum contract. This amount is used by miners to rank transactions to be included in the blockchain. After the code of the transaction is executed, the transaction will show up in the blockchain when miners include it in a newly created block. Again, executing the transaction requires gas, and if the sender's transaction runs out of gas (by including a lengthy loop or multiple bytes of information), the transaction will be cancelled and gas not used will be returned to the sender (Ethereum Foundation).

Some of the ether created will go to the Ethereum Foundation to "compensate early contributors and pay ETH-denominated expenses before the genesis block" as well as the creation of "a long-term reserve". Specifically, this is includes 0.099x of the total amount sold which will compensate early contributors and pay ether-denominated expenses and an additional 0.099x which will go to the long-term reserve. The proceeds of the initial ether sale (in BTC) went to pay salaries and "bounties" of early contributors in the Ethereum system (GitHub Ethereum wiki).

Ethereum does have a few issues which may need to be resolved prior to future growth. Unfortunately, Ethereum does not allow for the existence of private contracts, as mentioned earlier in the section on smart contracts. A second issue is Ethereum's scalability. Since Ethereum uses a permissionless blockchain, it faces many of the same problems as bitcoin in terms of growth potential. For more information on this, refer to the "Permissionless Blockchain" section above.

R3 CEV

R3 CEV (an abbreviation for R3 "Crypto 2.0, Exchanges, and Ventures") is an organization which is attempting to establish a consortium of banks to bring blockchain technology to the financial system. They plan to use a private, permissioned blockchain to decrease the time required to verify transactions. Additionally, this movement would reduce transaction costs for these banks and, as stated before, will increase systematic liquidity. This organization is attempting to apply distributed ledger technology directly to the business operations of these major banks. R3 CEV and its consortium appear to

have three goals: (1) to apply the cryptographic methods found in digital currency to finance, (2) to explore opportunities for this technology in trading through use of smart contracts and other technologies, (3) to invest in and assist new financial technology companies which could also assist R3 and the banks in the consortium (R3 CEV).

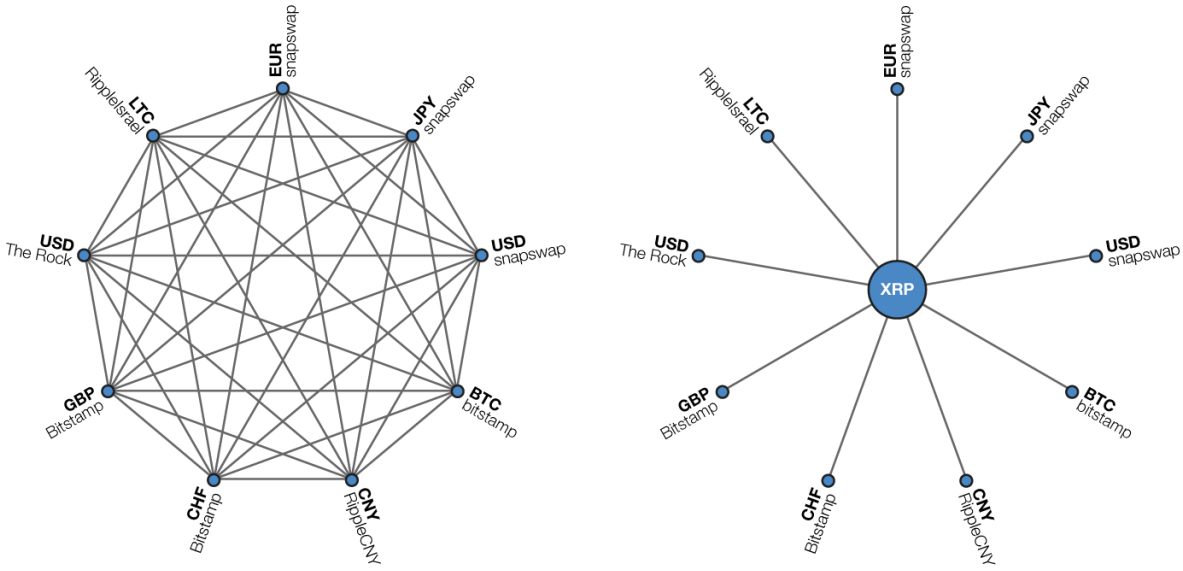
So far, this organization has accomplished some tests using the blockchain. However, most notably, they have succeeded in gathering many reputable institutions together to attempt to utilize the innovative technologies. Fortunately, R3 CEV appears to be open to testing other organizations' technology rather than exclusively creating their own. For this reason, they are utilizing a Microsoft-based blockchain (which utilizes Ethereum-based smart contracts) for their experimentations (Baert, 2016; Allison, 2015)

Ripple Protocol System

Ripple was designed exclusively to create faster, cheaper, and ultimately more efficient global payments. Unlike Bitcoin's open source framework and distribution, Ripple's intended growth is through partnerships between global banks. Bitcoin seems to be created for consumers, while Ripple was openly designed to exclusively apply to banks. At its core, Ripple is a centralized payment protocol system with a distributed ledger which trades using ripples or other currencies (XRP) (Ripple Labs). Ripple's Gateway protocol system is essentially a permissioned form of bitcoin's anonymous distributed ledger (Swanson, 2015). This centralized payment protocol system (referred to as Gateways) may give Ripple an edge over Bitcoin or Ethereum in terms of costs. Perhaps a decentralized permissionless blockchain would not be scalable enough to apply

to financial institutions (Todd, 2015). Ripple Labs has attempted to mimic the properties of centralized currencies while removing transaction costs and inefficiencies specific to traditional currencies.

The payment protocol system works through three different types of nodes—users, market makers, and validating servers. Users can send payments to each other cryptographically in XRP or any other currency. Two individuals can trade without using XRP if they are willing to establish a credit network while the transaction occurs, which essentially means a level of trust between the two parties must be established while the transaction is being completed since the amount of time required is greater relative to a pure XRP transaction. The XRP currency accelerates the transaction and also opens markets for currency pairs that are not regularly traded. Ripple, like Bitcoin, guarantees some user anonymity through anonymizing networks like TOR, a network which gives anonymity by moving users' traffic across other TOR servers and encrypting the traffic so that it is difficult to trace back to the original user. Additionally, the Ripple payment system has many centralized features. For instance, Ripple Labs controls most of the validating servers, ensuring stability and transparency but introducing concerning risks such as malicious intent if servers are compromised. Considering these potential security issues, many suggest rigorous analysis of the Ripple system before further implementation (Schwartz, et al., 2014).




As shown in the illustration above, Ripple's protocol system utilizes XRP to increase liquidity of currencies against each other (Ripple Labs, 2013)

Ripple Labs markets itself to financial institutions as an efficiency tool. They are proactively addressing potential legal issues by corresponding with numerous regulators such as the New York State Department of Financial Services. Companies such as Tembusu Systems are utilizing Ripple's Gateway network in lieu of the bitcoin system to serve the globally unbanked and underbanked. Tillit is creating an integrated financial "Platform" for businesses by utilizing Ripple's distributed, permissioned ledger (Swanson, 2015).

Digital Asset Holdings

Digital Asset Holdings, a firm led by ex-JP Morgan Managing Director Blythe Masters, is another effort spread blockchain technology use to banking (Higgins, 2016). In fact, they won a bid (out of four hundred applicants) to redesign ASX, the Australian Securities Exchange. This opportunity and their growing popularity has secured them

extensive support from Goldman Sachs, Citi, JP Morgan, IBM, and others (Digital Asset Holdings; Leising, 2016). Similar to R3 CEV and Ripple, Digital Asset Holdings is another large venture-backed firm in the race to adapt blockchain technology to finance.

## Conclusion

This essay began by discussing the origins and evolution of digital currency technology and concluded by discussing the design, industry applications, and importance of the bitcoin technology, the blockchain. While the value of actual digital currencies is yet to be determined, innovations in the blockchain could lead to massive long run reductions in transactions costs across many industries. In the short term, the blockchain is already beginning to be used in financial transactions involving mostly OTC products.

Before blockchain adoption can obtain broad industry adoption, issues concerning the source and design of supply for transaction services (essentially miners) must be solved in the protocol. Different forms of the blockchain offer unique solutions to issues such as the security and scalability of blockchain technology. It is reasonable to suspect that different solutions will be applied to different industries. At this moment, it appears that the financial industry favors permissioned blockchains, which could offer cost-cutting solutions to expensive back-office operations.

There has been much talk recently concerning the potential for financial technology ("FinTech"), increased regulation, and slowing global economies to disrupt

the financial industry. Although many of these innovations may never occur, distributed ledger technology will lead to increased efficiency in finance as well as possible increase market liquidity, which may reduce fees and risks for consumers of financial products and perhaps even a displacement of workers who traditionally filled back office transactional services roles at financial firms. This could lead to net welfare benefits, but there are also potential costs to these innovations. The potential risks of market disruptions upon initial technology adoption and other issues should be carefully accounted for in regulations developed in response to these innovations.

Additionally, firms developing blockchain innovations were discussed. Regulators should pay careful innovation to the disruptive power of these firms and their respective innovations. Although these firms seem to only open up exchange opportunities for financial firms, they could create barriers to entry for certain competitors offering transactional services. Additionally, the legality of smart contracts must be carefully considered. Firms and regulators would be wise to diligently research and solve many of these issues immediately to encourage industry adoption.

In conclusion, blockchain technology could increase efficiency and lower transactional costs. However, the technology still requires extensive design and testing before firms will be willing to apply this technology to their specific industries. These include access to the blockchain's information (private or public), ability to participate in the transaction process (permissionless or permissioned), the actual efficiency of payment verifications (the costs of mining), and potential coding issues in technologies using blockchain (infinite loops in smart contracts). Specifically, the cost, source, and supply of

transaction services is a point of contention. Fortunately, individuals and firms across many industries are collaboratively addressing these issues and innovative solutions are tested daily. Because of bitcoin's elegant design and proof-of-concept, industries utilizing blockchain technology could become more efficient and potentially experience more stability due to greater liquidity.

WORKS CITED

"About Digital Asset Holdings." *Digital Asset Holdings*. N.p., n.d. Web.

"About Ethereum Frontier." *Ethereum Frontier*. N.p., n.d. Web.

"About R3 CEV." *R3 CEV*. N.p., n.d. Web.

Allison, Ian. "Bitcoin's Smart Sibling Ethereum Is 'the Only Game in Town' for Banks to Build Blockchains." *International Business Times*. N.p., 27 July 2015. Web.

Allison, Ian. "Symbiont's Adam Krellenstein: There's Really Only Two Smart Contract Systems - Ethereum's and Ours." *International Business Times RSS*. N.p., 25 Nov. 2015. Web.

Baert, Rick. "11 Banks Complete Experiment Using Blockchain Technology." *Pensions & Investments*. N.p., 22 Jan. 2016. Web.

Baron, Joshua, et al. "National Security Implications of Virtual Currency." (2015).

Baron, Joshua, et al. "National Security Implications of Virtual Currency." *Rand Corporation*. (2015).

Becker, Jörg, et al. "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency." *The Economics of Information Security and Privacy*. Springer Berlin Heidelberg, 2013. 135-156.

Bernard, Robert. "Bitcoin: How Government Regulation Will Lead to a Brighter Future for the Online Currency." (2015).

Biggs, John. "Citibank Is Working On Its Own Digital Currency, Citicoin." *TechCrunch*. N.p., 7 July 2015. Web.

Bitcoin Forum. "Litecoin - a Lite Version of Bitcoin. Launched!" *Bitcoin Forum*. N.p., 9 Oct. 2011. Web.

Braithwaite, Tom, and Ben McLannahan. "Masters Joins Cryptocurrency Start-up - FT.com." *Financial Times*. N.p., 10 Mar. 2015. Web.

Chowdhury, Abdur, and Barry K. Mendelson. *Virtual Currency and the Financial System: The Case of Bitcoin*. No. 2013-09. Marquette University, Center for Global and Economic Studies and Department of Economics, 2013.

Cohen, Brian. "Goldman Sachs Files Patent Application For Securities Settlement Using Cryptocurrencies." *Bitcoin Magazine*. N.p., 01 Dec. 2015. Web.

CoinDesk. "How to Set up a Bitcoin Miner." *CoinDesk*. N.p., 26 Nov. 2013. Web.

Cryptsy. "Cryptsy Blog." *Cryptsy Blog*. N.p., n.d. Web.

Dwyer, Gerald P. "The Economics of Bitcoin and Similar Private Digital Currencies." *Journal of Financial Stability* 17 (2015): 81-91.

Ethereum Foundation. "Ethereum Frontier Guide." *Gitbook*. Web.

Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters." Selected areas in cryptography. Springer Berlin Heidelberg, 2003.

GitHub Ethereum wiki. "Ethereum wiki: White Paper." *GitHub*. Web.

Grygo, Eugene. "Why Nasdaq and Symbiont Vie for Blockchain Firsts." *FTF News*. N.p., 4 Jan. 2016. Web.

Higgins, Stan. "Blythe Masters Blockchain Startup Raises $50 Million From 13 Financial Firms." *CoinDesk*. N.p., 21 Jan. 2016. Web.

Higgins, Stan. "Cryptsy Threatens Bankruptcy, Claims Millions Lost in Bitcoin Heist - CoinDesk." *CoinDesk*. N.p., 15 Jan. 2016. Web.

Hileman, Garrick. "State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass." *CoinDesk*. N.p., 28 Jan. 2016. Web.

Hughes, Sarah Jane, Stephen T. Middlebrook, and Broox W. Peterson. "Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products." *The Business Lawyer* 63.1 (2007): 237-269.

Kaplanov, Nikolei. "Nerdy money: Bitcoin, the private digital currency, and the case against its regulation." *Loy. Consumer L. Rev.* 25 (2012): 111.

Kosba, Ahmed, et al. *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. Cryptology ePrint Archive, Report 2015/675, 2015. http://eprint. iacr. org, 2015.

Leising, Matthew. "Goldman Sachs and IBM Join Investment in Digital Asset Holdings." *Bloomberg*, 2 Feb. 2016. Web.

McMillan, Robert. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster." *Wired*. Conde Nast Digital, 3 Mar. 2014. Web.

Peters, Gareth William, and Efstathios Panayi. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money." *Available at SSRN 2692487* (2015).

Piscini, Eric, Andrew Garfrerick, and Simon J. Lapscher. "Deloitte: Blockchain Will Become a Reality in 2016 - CoinDesk." *CoinDesk*. N.p., 10 Jan. 2016. Web.

Popper, Nathaniel. "The Rush to Coin Virtual Money With Real Value." *DealBook*. N.p., 11 Nov. 2013. Web.

Ripple Labs. "Solutions." Ripple. N.p., n.d. Web.

Schwartz, David, Noah Young, and Arthur Britto. "The Ripple Protocol Consensus Algorithm." (n.d.): n. pag. *Ripple*. Ripple Labs, 2014. Web.

Swan, Melanie. *Blockchain: Blueprint for a New Economy*. " O'Reilly Media, Inc.", 2015.

Swanson, Tim. *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*. Working paper. 6 April. Retrieved from http://www. ofnumbers. com/wp-content/uploads/2015/04/Permissioned-distributedledgers. pdf, 6 April 2015.

Symbiont. "Solutions." *Symbiont.io*. N.p., 2016. Web.

Todd, Sarah. "Banks Can Cherry-Pick the Best Bits from Bitcoin: Report." *American Banker*. N.p., 7 Apr. 2015. Web.

TradeBlock. "Mining." *TradeBlock*. N.p., n.d. Web.

Wolfram, Stephen. *A New Kind of Science*. Vol. 5. Champaign: Wolfram Media, 2002.

Wolfson, Shael N. "Bitcoin: The Early Market." *Journal of Business & Economics Research (Online)* 13.4 (2015): 201.

Yermack, David. *Corporate Governance and Blockchains*. No. w21802. National Bureau of Economic Research, 2015.

21 Incorporated. "About 21." 21. N.p., 2016. Web.