Winter 1-15-2019

Accepting Blockchain Tech to Increase Bitcoin Acceptance

Oscar Nawrot
La Salle University, nawroto1@student.lasalle.edu

Accepting Blockchain Tech to Increase Bitcoin Acceptance

Oscar Nawrot

LaSalle University

EXECUTIVE SUMMARY

The root problem with conventional currency is all the trust that is required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. People have to trust them with their privacy, trust them not to let identity thieves drain their accounts. - Satoshi Nakamoto, Founder of Bitcoin (nakamotoinstitute, 2009).

Cryptocurrencies, with Bitcoin leading the charge, are the beginning of something new because this ideology is attempting to change the way people store and use money - led by an influx of technological innovation and success. If executed accordingly, blockchain has the chance to completely change our world for the better. With Bitcoin being driven by advanced blockchain technology, this digital currency has the ability to decentralize one of the most important aspects of life - money. This in turn would allow for people to take direct control of their money without the need for being completely dependent on bank systems and government entities. Society is beginning to realize the full potential of blockchain technology and crypto as a whole, but lack of security may be the reason why sustained growth and mass adoption is happening at a slower rate than expected.

Bitcoin and blockchain technology have life changing potential, but there are security issues holding back mass adoption and disallowing institutional money from flowing into the market. There is not a quick fix available, but starting at the root of the problem, which is in the

areas surrounding education and awareness, would certainly create a solid foundation and help bridge the gap between this innovative technology and the end-user. Additionally, regulation and insurance against possible theft need to be fully established to give users the peace of mind to accept the technology. Lastly, advancements on the technical side of securing the blockchain also need to be properly executed for all of this to come together.

Finding the proper balance between the technological innovation, user accessibility, and security is vital for the success of bitcoin and blockchain technology as a whole.

INTRODUCTION

Cryptocurrencies and Bitcoin

A generational technology has created a unique digital way to manage and use money. The future of banking may be through the innovative digital asset classes of cryptocurrencies. The main purpose of cryptocurrency is to decentralize banking which would allow for total freedom in managing and exchanging money, without the burden of having to trust a bank or government-based entities. All transactions are meant to be secured using cryptography, which reinforces the security first mindset that is driving this technological revolution.

The banking systems in the world today are all institutionally controlled. The power is centralized under one governing entity that has the ability to print money at its desired pace, print as much as it wants, and even utilize customers' funds for lending and investment purposes that involve risk of loss. This money's relative value is typically agreed upon, but corruption can impact the playing field. With cryptocurrency, new units cannot be produced at will as the circulating supplies predetermined by the creators. Trust is what is expected since every

historical transaction can be seen on the public ledger also known as the blockchain. None of the buyers or sellers are identified; only the transaction is identified. Unless a person is controlling their money through cryptocurrencies, away from centralized banking systems, then who knows if their money is actually safe? Cryptocurrencies allow for financial freedom, and when used properly, can be the most secure alternative to the mainstream option. An example of using cryptocurrencies properly is doing everything possible to be secure. This means storing the currency offline while only having enough for day to day transactions online. Also, utilizing strong passwords and two factor authentication on top of devices that are updated and operating on a hardened network.

There are many different cryptocurrencies that operate using blockchain technology, like - Litecoin, Ethereum, DASH, Ripple, ZCASH, Monero, NEO, and Bitcoin Cash - but the oldest and most popular one today is Bitcoin. Bitcoin was created by an anonymous entity known by the name Satoshi Nakamoto in 2009. He/she/it is referred to as an anonymous entity because nobody knows if this creation was made by a single person, or a collective group of people. Bitcoin was created with the purpose of being a digital currency that can be used to exchange for fiat (standard cash) currencies, and for standard transactional purposes online or in person. Nakamoto created this digital currency to allow for exchanging of money without the need for institutional oversight. It was founded in 2008 and the "code is open source and thus it belongs to the public domain" (Franco, 2015, 4).

In addition to the transactional purposes, Bitcoin is also widely considered a digital store of value. A store of value can be anything that holds value over a period of time, usually something physical. In this case Bitcoin is a currency and stores its value digitally. To help illustrate the comparison, a good example of a physical store of value is gold. This characteristic

is important because, historically, there have been many people who invested their worth into gold, as its value still holds true through rough economical stretches, but this new digital version, Bitcoin, is changing the game forever. “The final monetary base is fixed at around 21 million bitcoins and new bitcoins are minted at a planned schedule and paid to users who help secure the network. This serves the double purpose of providing the bitcoins with value due to their scarcity and creating incentives for users to connect to the network and help secure it by providing their computational power” (Franco, 2015, 5). As one can imagine, supply and demand, driven by the low supply, can equate to a huge return on a person’s investment, and people are beginning to recognize this.

Shortly after its creation, Bitcoin gained popularity fairly quickly as it was driven by public-key cryptography which allowed owners to easily transact with fellow owners by sharing their own public key for the transaction. This is also very secure since a private key is needed to fulfill the transfer of funds, almost like how asymmetric encryption works. Without both the public and private key, the Bitcoin network could not be able to successfully process and validate the transaction. “A public key is what’s available for everyone to see and a private key is known only to the owner. In a Bitcoin transaction, users receiving Bitcoins send their public keys to users transferring the Bitcoins. Users transferring the coins sign with their private key, and the transaction is then transmitted over the Bitcoin network” (Franco, 2015). Since all of the transaction data is shared over the blockchain, all peers share the responsibilities associated with validating and recording new transactions. This validation is also known as mining, and it is typically conducted by people who dedicate above average computing power to assist in block validation on the blockchain. Behind the scene, when a new block is being validated, or in technical terms, mined, a math equation is the only way of finalizing the information within a

given block and finally adding that block to the chain. The result of successfully mining a Bitcoin is a portion of that Bitcoin being paid out in commission for the work done by people who host a node to use their computer processing power for mining. The network is shared so there can be multiple miners looking to mine new blocks of data, therefore making it more difficult to take a bigger slice of the pie. Naturally, only the miners with the most computing power prevail in solving these algorithmic math problems associated with each new block. There also are mining pools that allow for miners to combine their processing power in a collaborative effort to mine new blocks, but the larger the pool, the more of the reward that needs to be split (Park, J. H., & Park, J. H., 2017). Banks in the centralized system are different from miners in the decentralized Bitcoin system because the decision-making responsibility comes from multiple areas in Bitcoin, compared to a single bank being in control of all their customers money. This promotes honesty since multiple miners validate each transaction.

So how does one obtain Bitcoin if they are not dedicating their time and energy to mining? In order to purchase Bitcoin a person needs to exchange fiat currency through a verified global digital asset exchange company (GDAX), such as Coinbase. Exchanges like Coinbase house numerous cryptocurrencies and allow for buying and selling with current market trends. Once purchased, the crypto owner can either store their new asset online through Coinbase's wallet functionality, or they could move it offline into a cold storage wallet, like a Nano Ledger S, or through a paper wallet. "Cold storage is another way to secure Bitcoins which involves storing Bitcoins offline--meaning, away from any internet access. Keeping Bitcoins offline substantially reduces the threat from hackers" (Bajpai, 2015, 1).

Cold storage through a Nano Ledger is typically the best way to go since private keys are completely inaccessible unless the Ledger is connected directly into the computer using only a

USB cable. There are no other methods for connecting this type of wallet to a computer, so attack layers are minimized, and only after a passcode and confirmation are successfully authenticated will access be granted. This is also known as multi signature validation and is the best safety feature of a cold storage wallet. Additionally, this form of storage is water proof and virus proof (Bajpai, 2015), although the owner would have to keep their computers protected because a computer is always vulnerable to attacks. So even if one uses a cold storage wallet, malicious program that tracks key strokes or other trojan horses are still something to be mindful of. Assets are securely stored on the blockchain so even if an owner's wallet gets stolen, their information and assets can be retrieved using a new wallet as long as they remember their 24-word unique recovery words, so it is important to keep personal login information secure by storing these recovery words in either a safe, bank lockbox, or secret areas within one's home. To be extra safe, a mixture of the above decreases one's chance of losing the ability to recover a wallet.

Once a person has their assets secured, they can transfer funds from their own wallets into other exchanges depending on what is available. Each exchange offers a different variety of crypto, but all are able to be traded for or with Ethereum, Litecoin, and especially Bitcoin. Bitcoin is the most popular cryptocurrency and trade volume reflects this as Bitcoin is the most traded coin in the cryptocurrency space.

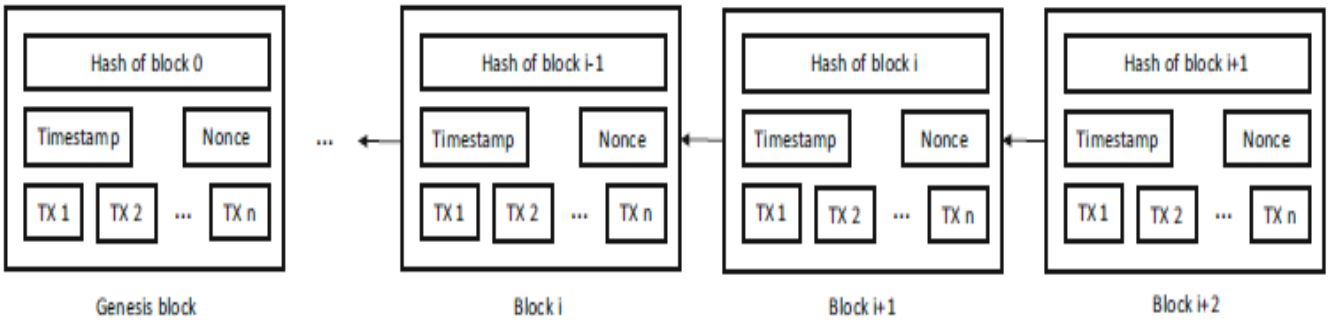
Interestingly, cold storage has initiated developments of a new concept called deep cold storage which "was introduced by a London based company which offered the security of a bank vault for securing the keys of Bitcoins. This service is insured by an underwriter thus providing protection against theft or loss of Bitcoins" (Bajpai, 2015, 1). Security enhancements to storage seem like a good starting point in bitcoin's attempt to winning over current non-adopters. This example is a good sign of things to come as the technology moves forward.

Blockchain

Initial developments of blockchain related technology dates back to the early 90's when Stuart Harber and W. Scott Stornetta spearheaded a project that revolved around the implementation of a system where timestamped documents could not be altered. Even in the early developments of cryptography, they successfully developed Merkle Trees, which allowed for efficient data collection and storage through cryptographic hashing (Bashir, I. (2018). Jump forward 20 years, an entity by the name of Satoshi Nakamoto piggybacked off the technology's early findings and anonymously invented blockchain, and, as mentioned earlier, Bitcoin.

Blockchain is best described as a digital ledger where transactions can be documented and saved in sequential order. This ledger is decentralized - meaning that its structure and functions are shared among everyone that wants to access it. The information within a decentralized blockchain is made available to the general public for reference and for validation as new blocks of information are created and solidified.

A classic example of a blockchain illustration can be seen below (Example of a blockchain, Zheng, as cited in Nofer, Gomber, Hinz, Schiereck, 2017):



At the technical level, a blockchain involves groups of data that are connected through a chain of blocks that are hashed and encrypted using the cryptographic hash from the prior block in the chain, which in turn links them to each other. A hash can be easily described as a unique sequence of numbers that enables data to be efficiently consumed and digested (Piscini, Dalton, 2017). Hashing allows for that unique string to be identified and indexed within a database. Each block can consist of numerous transactions, but once an entire block's worth of transactions gets solidified and a new block is added onto the chain, it can no longer be altered and the sequence continues. The validation between blocks is confirmed using cryptography, in addition to the block's time stamp and hash value, as well as the nonce, which represents a randomly generated number that assists with the verification process. Since hash values are randomly generated, the process allows for a seemingly secure environment that can prevent fraud and promote meticulousness (Nofer, Gomber, Hinz, Schiereck, 2017).

Understanding the technicalities behind blockchain is important because there are many industries that are already implementing this technology to improve their operations. In the health care field, some developers feel that blockchain could be implemented to help track historical records of patients in addition to keeping their personal information safe. Supply chain companies see the benefit of more easily tracking the origin of goods – an exotic fruit may have been purchased in a grocery store, but the odds are that multiple companies have handled that fruit from the point of observed planting and growth, all the way to shipment services and distribution centers – tracking this information can get very complex especially across borders. (Nofer, Gomber, Hinz, Schiereck, 2017). The same concept can be shared for medicine, as pharmaceuticals and equipment touches multiple hands before it gets to the prescribed patient. Fraud could be eliminated if the shipping methods were tracked appropriately, in such a way that

is not possible to alter historical data. Everyday news talks about the development of blockchain and finance collectively, but the truth is that even though finance is leading the blockchain charge, there are many other areas where the technology is being looked at or is already being utilized (Nofer, Gomber, Hinz, Schiereck, 2017). This is proof that blockchain technology is here to stay.

Table 1 Applications of blockchain

Type	Application	Description	Examples
Financial applications	Crypto-currencies	Networks and mediums of exchange using cryptography to secure transactions	Bitcoin Litecoin Ripple Monero
	Securities issuance, trading and settlement	Companies going public issue shares directly and without a bank syndicate. Private, less liquid shares can be traded in a blockchain-based secondary market. First projects try to tackle securities settlement	NASDAQ private equity Medici Blockstream Coinsetter
	Insurance	Properties (e.g., real estate, automobiles, etc.) might be registered using the blockchain technology. Insurers can check the transaction history	Everledger
Non-financial applications	Notary public	Central authorization by notary is not necessary anymore	Stampery Viacoin Ascribe
	Music industry	Determining music royalties and managing music rights ownership	Imogen heap
	Decentralized proof of existence of documents	Storing and validating the signature and timestamp of a document using blockchain	www.proofofexistence.com
	Decentralized storage	Sharing documents without the need of a third party by using a peer-to-peer distributed cloud storage platform	Storj
	Decentralized internet of things	The blockchain reliably stores the communication of smart devices within the internet of things	Filament ADEPT (developed by IBM and Samsung)
	Anti-counterfeit solutions	Authenticity of products is verified by the blockchain network consisting of all market participants in electronic commerce (producers, merchants, marketplaces)	Blockverify
	Internet applications	Instead of governments and corporations, Domain Name Servers (DNS) are controlled by every user in a decentralized way	Namecoin

The table above from Nofer, Gomber, Hinz, Schiereck (2017) illustrates many of the top application benefits thought to be available through the use of blockchain technology. There are many specializations that could use the functionality enhancements that blockchain technology brings to the table, and the technology is only at its early stages of development.

Blockchain Security

At a coding level, "cryptographic open source software has the advantage that it allows users to check that the code does not contain any backdoor or security vulnerabilities" (Franco, 2015, 7). This alone amplifies confidence in a blockchain's foundation since anyone is allowed to go into the open source code to run diagnostic checks and look for issues.

Blockchain security is commanded by the consensus mechanism which says that the validity of a block can only be determined if majority of the network nodes can all come to an agreement on the block itself – only then will a block be determined as sufficient to forever be added to the chain. In other words, validating the integrity of the data within the blocks is everyone's responsibility as the results are collectively agreed upon. Once an agreement has been made through this joint effort, hash values get 'engraved' into the blocks solidifying the data. Since there is a direct correlation between the hash value and the integrity of the data within the blocks themselves, everyone can feel comfortable trusting the information within the entire blockchain. Mistakes could occur among the many miners within the validation process but only the correct answer gets applied. "In contrast to centralized systems, the functionalities of the network persist even if particular nodes break down. This increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network" (Nofer, Gomber, Hinz, Schiereck, 2017, 182). Because everyone that uses the blockchain powers it, one person going offline or experiencing a network related issue will not hinder the overall performance of the blockchain.

Blockchain was created to be tough for hackers to attack, and the cryptographic link that appends each block of information cannot be fabricated without massive computational resources at ones disposal (Franco, 2015). Security is blockchain's philosophy. At its core, it

succeeds at this, so people should continue to educate themselves while accepting this innovative technology without worrying too much about risks.

BITCOIN AND THE BLOCKCHAIN

As touched on earlier, blockchain technology and Bitcoin go hand in hand – their development and popularity have grown together. Blockchain, acts as the decentralized database which provides a more secure way to track and store information. Next, there is Bitcoin, which is the most innovative digital cryptocurrency in existence that is attempting to become the next generation of banking, but in a safer and less restricted way. “By utilizing the blockchain third parties can become obsolete, ultimately increasing user’s security” (Nofer, Gomber, Hinz, Schiereck, 2017, 184).

With Bitcoin working on blockchain technology, there is a way to accurately record and track every single historical transaction in the cloud, with, allegedly, no possible way to ever manipulate previously recorded data. Not only is the information accessible to anyone that wants to see it, but it also prevents one governing body from being in control of everything and gives the power and trust back to the people who fuel the smart economy. “The bitcoin transaction information is disclosed over the network such that all peers can verify it and so currency issuance is limited. The peers participating in the network have the same blockchain and the transaction data are stored in blocks in the same way as the distribution storage of transaction” (Park, J. H., & Park, J. H., 2017, 3). Although minimal, there are transaction fees that get paid out to the miners who help with validation. Even with transaction fees in place on the users, “Bitcoin’s transaction fees are lower than credit cards’ fees” (Franco, 2015, 26). This is a major

positive that Bitcoin provides and credit card companies have trouble matching this. “Fees are still a small fraction of total miners’ compensation, currently below 1% of their total compensation. It is expected that as the issuance of new bitcoins shrinks, transaction fees will take over as the principal compensation to miners” (Franco, 2015, 17). Block rewards from the validation payout more for successful mining.

It is a very simple concept that attempts to provide a sense of security when used appropriately. All that is involved is the user’s Bitcoin address, and the block where that transaction’s information sits, which will be validated by fellow miners on the network. Before the transaction goes through, a set of electronic signatures must be completed between both participants using both the public and private key of each participant. The way Bitcoin functions on a blockchain is fairly similar to the way money moves in and out of bank driven checking accounts, but with no middle man, and no trust issues. The people are in full control of their money and their security. Since Bitcoin uses cryptography, a user can trust anyone from around the world when they are moving their digital assets.

In addition to safe and secure digital transactions, what else does this combination of Bitcoin and blockchain bring to the table? In the centralized banking system, everyone is reliant upon an institution to complete a transaction. If that institution sells out or does something to scam its customers, there is not much a victim can do unless they have the proper insurance or funds to take a case through the legal system. That centralized power is needed for our banking systems to function properly. A centralized banking system also houses all of a customer’s personal information which could be breached at any point in time if the entity has not squared away an adequate amount of resources for protection. Banks should have the proper resources allocated for protection, both preventative measures and recovery measures, but not every bank

operates the same way. Simply said, a lot can go wrong when someone else is in control of another person's money and their highly confidential information.

Opposite to that, with the Bitcoin economy operating on a decentralized blockchain, one node going offline would not do anything to hinder transaction validation or to weaken the security that protects user information. Since all peers on the network work together, others can make up for the loss of computing power in order to uphold the standards of the blockchain. There will always be somebody else looking to make that extra commission for successfully mining a new block, therefore nodes are continuously running to keep everything afloat. This should make users feel more comfortable when comparing blockchain's infrastructure with a centralized bank. If a denial of service attack happens to a bank's network, all users get kicked off their online banking systems, sometimes for a very long time. "As a result of additional network traffic, the victim's network starts responding slow or it drops some packets. The loss of packets may cause a flood of retransmitted requests, which further increases the network traffic. Increased network traffic saturates the network and it becomes unavailable for the intended users" (Kumar, 2016, 9). Denial of service attacks can certainly cause trouble to businesses and users, but blockchain has a safety net that allows for its infrastructure to continuously run since the network operates across many nodes, and not just by one centralized authority giving fuel to the whole blockchain. This essentially makes denial of service attacks nonexistent on the blockchain - "This increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network. It is sufficient if people solely build trust in the system as a whole" (Nofer, Gomber, Hinz, Schiereck, 2017, 184). Trusting the system as a whole makes for a more efficient economy that gives users full control.

Another opportunity Bitcoin and blockchain technology creates is the ability for third world countries to improve their society. Many third world countries are not fortunate enough to develop appropriate banking facilities and operations to properly serve most of their population; there simply is not enough funding for banks to expand throughout their countries, so accessibility is limited (Johnston, Walton, 2017). However, there are more people that have a cell phone than people that have bank accounts, and all a person needs for cryptocurrency is a cell phone with limited network coverage. Telcoin, which is a cryptocurrency based out of a third world country, says that 90 percent of the adult population in Kenya has a bank account. Additionally, there are five times less bank accounts than cell phones. This makes for an ideal situation to leverage phones for using and storing money (Telcoin Whitepaper, 2017). Their philosophy is to bank through mobile devices in third world countries since more people have access to a phone than a bank, with their main focus being Nigeria. (Telcoin Whitepaper, 2017). Other countries like these are also considering switching their main currency into either Bitcoin or their own version which also operates on blockchain, mostly due to decreased cost and convenience. As an example, Venezuela just converted to an oil backed cryptocurrency, which they named the Petro. Hope is that this will assist in stabilizing their economy which has been on a downfall (Warwick Business School, 2018).

The study recently conducted in South Africa shows that “Bitcoin users consider it as a universal currency which makes cross-border payments cheaper” (Johnston, Kevin A., and Aiden J. Walton, 2018, 166). This was piloted using online surveying methods and they concluded that “the volatility and trust-related risks such as scams and hacking attempts were seen as the main risks for South African Bitcoin adopters” (Johnston, Kevin A., and Aiden J. Walton, 2018, 178). Their study also brought to light the worries surrounding the difficulty some people have with

setting up their wallets and transacting safely. Ever since the boom of 2017, one of the common opinions was exactly this – how user accessibility is well below what a new adopter would expect, and this makes it difficult for people to catch on since education and research is a prerequisite to using Bitcoin safely. South Africa's opinions towards Bitcoin sheds some light on how this new digital currency is perceived, and although it is not guaranteed, it is possible that many more countries around the world also have similar opinions. Feeling discouraged or intimidated by new technology is a normal feeling shared by many, but this obstacle is surmountable. Risk and difficulty of use can often be countered with proper education and awareness.

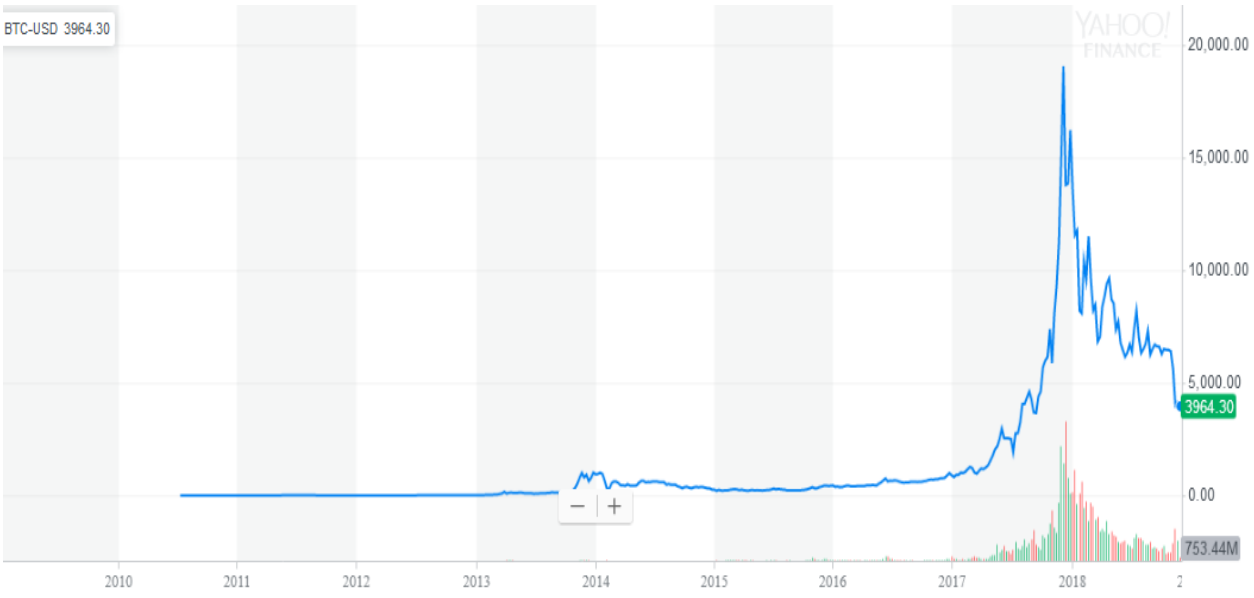
It is obvious that there are many benefits to Bitcoin and blockchain: it decentralizes money, removes the need for banks and governing institutions, takes away third parties, gives the owner direct control of their assets, protects personal information, and gives opportunity to second and third world countries to assist with development. But what problems does it create?

First and foremost, adding a decentralized banking system into the economy can divide the people and their government. An official switch would certainly cause more trust issues that could leak into other aspects of government associated activities. The power would be almost completely taken away from the entities that held it throughout history, and with any change as drastic as this, there will be a backlash in some way, shape, or form. The issues Bitcoin creates does not end with social uproar, there are also many fears "related to security and privacy. Apart from these, a few other challenges are interoperability, lack of standards, legal challenges, regulatory issues, rights issues, emerging IoT economy issues, and other developmental issues" (Kumar, N. M., & Mallick, P. K., 2018, 2). Put that all together and it is easier to understand just how complicated it could be to successfully adopt Bitcoin on a broader basis. There are many

positive aspects where actual worldwide problems are being solved, but with every positive, there is also a negative.

BITCOIN ADOPTION RATE AND VALUATION

Now that Bitcoin has been around for almost a decade, it is a good time to take a look at some historical price statistics that help paint the picture of where its value was at the beginning, versus where it is today (from publicly available trading information through Yahoo Finance - (https://finance.yahoo.com/):



During the first year of its existence in 2009, one Bitcoin was worth $0, but its first ever recorded price was $0.39 in 2010 - once awareness started to spread. Comparing the first ever price point with our current price of $3,964.30 (at the time of research), one can see that Bitcoin has come a long way at increasing its value by over 130,000% (https://finance.yahoo.com/).

During the ride, intense price fluctuations frequently occur swinging both ways in aggressive fashion. This “volatility is explained by regulatory uncertainty, low liquidity, low market capitalization, limited market access, and narrow adoption” (Franco, 2015, 34). Supporters counteract this argument by stating that if these areas of concern improve, volatility will decrease over time. As the technology improves, there could be updates on the technical side that improve the issue of volatility, but adoption seems to be the most reliable fix (Franco, 2015).

Just as supply and demand directly impacts stocks and their trade value in the stock market, supply and demand directly correlates to the real-time price of Bitcoin (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017). Now the difference between stocks and the Bitcoin market is that stocks are backed up by their company. Companies and their yearly profits add an extra dimension to price action because the price can fluctuate based on company performance. Dividends also get paid out to dedicated investors. Bitcoin is considered one dimensional because its value is just in the supply and demand (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017). If more people want it, whether it be for investment purposes or to actually use it to buy a coffee, those people will be willing to pay more for it. When looking at Bitcoin’s recent rise in value, one can conclude that popularity has increased in the trading space, but does that really mean that adoption is taking place?

In a popular benchmark study done by Cambridge University, an “estimated number of unique active users of cryptocurrency wallets has grown significantly since 2013 to between 2.9 million and 5.8 million today” (Hileman, G., & Rauchs, M., 2017, 27).

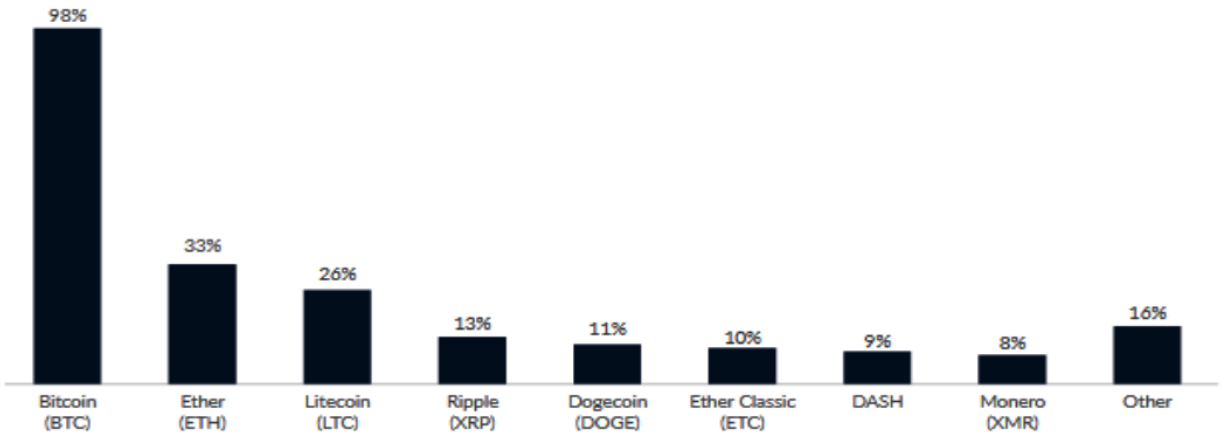
Table 1: Average daily number of transactions for largest cryptocurrencies

	Bitcoin	Ethereum	DASH	Ripple	Monero	Litecoin
Q1 2016	201,595	20,242	1,582	N/A	579	4,453
Q2 2016	221,018	40,895	1,184	N/A	435	5,520
Q3 2016	219,624	45,109	1,549	N/A	1,045	3,432
Q4 2016	261,710	42,908	1,238	N/A	1,598	3,455
January - February 2017	286,419	47,792	1,800	N/A	2,611	3,244

Data sourced from multiple block explorers[a]

As seen above in 'Table 1' it is evident that Bitcoin has the largest daily transaction volume within the space.

Figure 6: Bitcoin is the most widely supported cryptocurrency among participating exchanges, wallets and payment companies



In 'figure 6' from the same study, Bitcoin is shown to be the most supported cryptocurrency among exchanges and wallets.

The Cambridge University benchmark study was conducted in early 2017, right before the cryptocurrency surge which took place at the end of that year. Since then, it has been estimated that the current number of active wallets is well above 30 million, while the daily

transaction rate is still in the upper 200,000's per 24 hours (Hileman, G., & Rauchs, M., 2017). This truly looks like a 25 million increase in active user wallets within one year during a time of so much uncertainty, and this is only the beginning of fully adopting Bitcoin and blockchain technology. The increase in active wallets and a sustained high daily transaction rate tells the story of new users coming into the market and accepting cryptocurrency and doing their due diligence to protect their funds by opening wallets for storage. Since the transaction rate hasn't increased significantly, the numbers might indicate that a learning curve could still be prevalent - that users only chose to buy and invest, and not use the asset for further transactional purposes. Still, an increase in wallets that store the asset is an inspiring accomplishment as adopters build for the future.

So how does the United States of America's philosophy on Bitcoin compare with the rest of the world? Depending on the country, there are many factors that come into play for adoptability. There may be a country like Venezuela that is looking for a way to stabilize its economy. While another country may be full of people that are looking for financial freedom. Also, there are areas in the world that are very driven by technology advancement, like parts of Asia (Parino, Francesco, Mariano G. Beiro, and Laetitia Gauvin. 2018). Every country has its own story, but a study on different socio-economic factors showed results that the general picture of Bitcoin adoption reveals that if there is a presence of policies that present obstacles in exchanging money, the likelihood of adoption is higher (Parino, Francesco, Mariano G. Beiro, and Laetitia Gauvin. 2018). This study was driven by search trends and they discovered that Brazil and Venezuela make banking very difficult for their citizens with their policies that drive their unstable economy, but they also have a much higher Bitcoin Google search trend than countries with stable economies, like the USA and Australia (Parino, Francesco, Mariano G.

Beiro, and Laetitia Gauvin. 2018). One can assume from this study that these countries with financial constraints are looking to learn about alternatives that can be beneficial to their people. This is not to say that US citizens are less likely to fully adopt Bitcoin; it just means that adoption can be driven by different factors depending on the country. Just looking at the transaction numbers, the US is already well ahead of the game when it comes to adoption with more than 50% of all transactions coming from and into the US, (Parino, Francesco, Mariano G. Beiro, and Laetitia Gauvin. 2018), but the need and interest may be a little more prevalent in other parts of the world.

Our world has been slow in adopting Bitcoin – it is almost like a mixture of curiosity and acceptance. People are curious about the new technology and want to learn about it – some are already accepting it based on how much they know and how much experience they have had with it – but then there is a risk versus reward variable that sways a person's opinion on the subject. There is still a lot to discover and learn for adoption to truly take off, but the end of 2017 surely gave the industry a sneak peek on what the world can expect as we move into the future.

Bitcoin Security

More recently, people have been experiencing somewhat of a digital revolution where all personal information is stored online; credit card information, personal contact information, passwords, social security numbers, and so much more. All of this is saved either locally or by vendors that hold onto this information so that people can use their services. It is very difficult to cover our digital footprints nowadays, especially since our lives are completely engulfed with

IoT devices that are constantly working to keep everyone connected. So how does this impact Bitcoin and users' lives during this phase of adoption?

Like anything in cybersecurity, or security in general, it starts and ends with the user. The user should do everything necessary to minimize vulnerabilities. This includes doing basic network hardening, anti-virus installation, and performing regular system updates. The best technology can be implemented but is it still has to be used correctly. People also need to be aware of the risks before getting involved. The only way to solve all of this is with education and awareness, especially since something like Bitcoin is so new, innovative, and complex. It is unlike anything people have seen before, and they are anticipating for this to become a mainstream currency. When the internet started gaining traction in the nineties – it was hard to foresee the advancements that would bring us to where the technology is today but in order to get it to where it is today, everyone had to take the time to educate themselves on how to operate it.

The internet of things started coming to fruition in the mid-nineties when wireless communications and digital electronics finally showed advancements (Ibarra-Esquer,Gonzalez-Navarro, Flores-Rios, 2017). Then came business integration where network infrastructure enhancements were used directly with new IoT devices for them to interact with one another. Through the times, it was important to understand these changes and to take the time to learn how things could be improved upon. The same analogy can be applied here where the world is in the early phases of adopting Bitcoin – it is new and exciting, but there is a steep learning curve.

Blockchain technology is always changing which means Bitcoin always has the chance to improve as there are constant improvements being made to the infrastructure to make it more scalable and to help its network perform better. The main concern was addressed with the addition of a transaction related protocol called The Lightning Network. This protocol acts as a

second layer to the blockchain and promotes faster communication between nodes. There is now much less congestion on the network and payment authentication happens more rapidly, (Poon, Dryja, 2016). It takes time and effort to absorb the complexities, but it is worth the effort because Bitcoin solves actual problems (Nofer, Gomber, Hinz, Schiereck, 2017). According to public course listings on Duke University's website (https://law.duke.edu/dclt/blockchain/), classes revolving around Bitcoin and blockchain already exist within our educational system – it is a good first step but more is needed. With further evolution of the technology, more education should follow.

Beyond education and awareness, what else can go wrong when using Bitcoin? First and foremost, on a transactional level, transacting on an unsecured network "opens the possibility of a Man-in-the-Middle attack" (Franco, 2015, 54), which could intercept the communication between the public and private keys interacting with one another. Users need to be mindful of this and aim to transact over secure networks to eliminate the possibility of these types of attacks.

When it comes to Bitcoin wallets, at their core they are extremely secure, almost more secure than a physical wallet holding its owner's private information – an example of a Bitcoin wallet address would be "1N3rjCLXhuuWFCweLV88GrDym4pryx7tkq – sending Bitcoin to this address without having the corresponding private key is very unlikely. The probability that an incorrect address is accepted as valid is about 1 in 4.29 billion" (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017, 6). In other words, the only way to successfully send funds from a wallet is by utilizing the private key that matches with the public address. It is almost impossible to guess a public address's matching private key according to the aforementioned statistic. The problem is not the security behind the technical details that make

Bitcoin function, it is the problem on the surface that is driven by improper password use and lack of 2 Factor Authentication (2FA), and to a lesser extent, falling victim to hacks.

Two of the most vital features of a Bitcoin wallet are the wallet password and the two factor authentication associated with the account. These are key aspects to sound security but people overlook their importance, which can possibly be attributed to the overall security issue that is driven by lack of education and awareness surrounding the space.

Passwords need to be complex including a combination of lower and upper case letters, along with special characters and numbers used throughout. Another important point to note is that a person's wallet password should not be a password that is being recycled from a different account's login credentials. An effort should be made to make a Bitcoin wallet's password as complex as possible in order to eliminate the chances of falling victim to dictionary attacks or database driven hacks. In addition to this, 2FA is a requirement and needs to be used with every Bitcoin wallet. 2FA can be confusing to people who have never used it, but a popular analogy heard throughout the space is that a credit card can be used, but the pin also needs to be known in order to use it. With 2FA, a password needs to be correctly input before a verification code can be sent either to the user's mobile device or through an authentication application like google authenticate. Digital wallets need to be treated just like a standard physical wallet where nobody but the owner is allowed access. The key to successfully protecting a Bitcoin wallet is 2FA – "two-factor authentication is considered to be the leading method for strengthening the authentication process. For bitcoin, the two-party signature protocol by ECDSA can be used for authentication (figure 3 from Park, J. H., & Park, J. H., 2017, 2):"

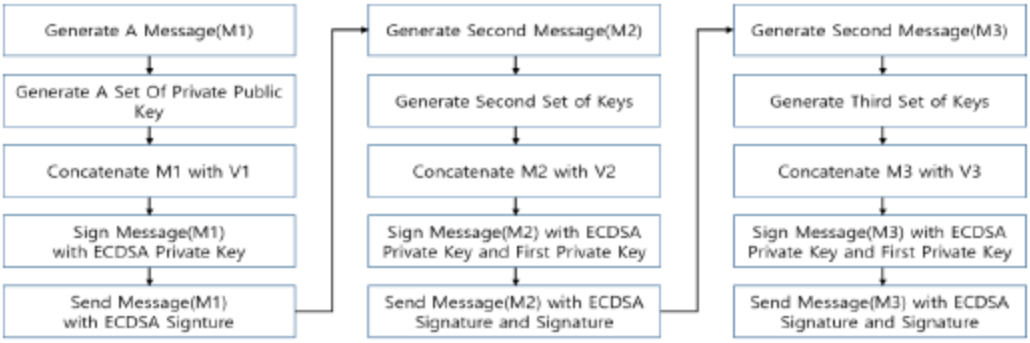


Figure 3. ECDSA two-party signature.

In the Bitcoin world, message 1 would come from the wallet's server; it would generate a set of private/public key information to a third party application, like Google Authenticate, or to a cellular phone via text message. Once the user confirms receipt of that message, the wallet application then generates a second set of keys for validation to be successfully performed. The third set gets generated once both the first and second message get authenticated thereby granting access to the wallet and its contents. It is very important to enable this type of encryption or owners will run the risk of using a wallet with major security vulnerabilities. If not taken seriously, security becomes an issue that holds back adoption. If assets aren't properly secured, cyber-attacks could exploit the vulnerability. The Mt. Gox hack is an example of this. Many people lost their Bitcoin that was being stored on the exchange's network. It was a large hack that wiped millions of dollars' worth of Bitcoin directly from the company's wallet which stored all user assets. The Mt. Gox private key was unencrypted and hackers took advantage of this and stole the information. Knowing that the exchange operated offshore, with minimal regulation, and that insurance policies were not guaranteed - if people were aware of the dangers maybe they would have gone the extra mile in order to securely store their funds on their own wallets and not rely on an unregulated exchanges (McMillian, 2014). This type of news can deter people from wanting to jump on board, but when it comes to the details, all Bitcoin users can avoid this type

of situation very easily by storing all of their Bitcoin in cold storage. As mentioned previously, cold storage is the safest way because you own the private keys and are not reliant on anybody else.

When it comes to using Bitcoin in the retail space, users do not need to worry about their information being stolen in case of the company being hacked. “A compromise of a retailer that uses Bitcoin payments can lead to financial loss for the retailer, if the attacker gets access to the retailer’s private keys. However, the compromise does not threaten the user’s funds, as Bitcoin users are in control of their private keys” (Franco, 2015, 25). As with the Mt. Gox example, users taking advantage of being in control of their private keys eliminates the chance of personal information being stolen.

At Bitcoin’s core, “technical measures such as proof of work and proof of stake have been implemented to improve the security of Blockchain (Park, J. H., & Park, J. H, 2017, 11).” Bitcoin uses Proof of Work currently, which is a new innovative algorithm that further promotes validity in the Blockchain. This scripting enables the Bitcoin network to regulate if a miner is valid and is working within the rules and regulations of the Blockchain while comparing each miner and their ledger to the rest of the miners across the network. This keeps all the nodes in the environment in sync and actually helps fight against DDoS attacks (Park, J. H., & Park, J. H, 2017).

Overall, the technical foundation of POW and POS, using secure passwords, as well as 2FA are the most important aspects of security to a Bitcoin user. Education and awareness drive proper implementation of both, but even if properly executed, there are still major vulnerabilities that can turn new adopters away from trusting this technology.

The consensus mechanism is what drives Bitcoin on the blockchain – "generally 51% of users in public and private blockchains need to agree a transaction is valid before it is then subsequently added to the platform" (Piscini, Eric, David Dalton, 2017, 7). This functionality drives the way information within the Bitcoin network gets authenticated and gives users peace of mind, because it's not possible for one centralized entity to control the validation. Although highly unlikely, some argue that it is possible to fool this consensus mechanism. It is called a 51% attack, and this can happen if an attacker had the ability to harness more than 50% of all Bitcoin node processing power which essentially allows for the user to have full control. (Park, J. H., & Park, J. H. 2017)

These types of attacks are possible in theory, but close to impossible, as it would just require a huge mining pool that collectively works together to generate a computation rate of above that consensus threshold, all while sharing the same intention of controlling the entire Bitcoin network. This is all theoretical, however, the potential for a collective attack down the road may be enough to deter newcomers from using Bitcoin for investment purposes or even just for day to day transactions, as nobody wants to lose their money.

A more realistic scenario which was covered earlier is a Distributed Denial of Service (DDoS) attack. This attack floods the targeted servers with superfluous requests that overload the system and prevent the provision of normal service to other users (Park, J. H., & Park, J. H. 2017). This is a major concern for online banking users in the mainstream banking systems our society has in place, usually leading to many issues among customers. Blockchain services are distributed across many nodes, so the likelihood a DDOS attack knocking Bitcoin's Blockchain offline is highly unlikely, but this is not to say that a DDOS attack can't impact an exchange like Coinbase, or Binance - they are very much at risk since those exchanges are on a

centralized network whereas Bitcoin's blockchain is decentralized. It's important to differentiate between the two.

A popular way to avoid the risk of being a victim from an attack like this is to make sure all Bitcoin is moved away from these types of exchanges, specifically into a cold storage wallet. If funds are not being housed on an exchange, security risk is diminished vastly as the owner is in control of their own keys (wallet) and doesn't rely upon a centralized entity to look after their funds. One can "transfer the risk of the individual to a Bitcoin business" (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017, 3), but it may not be a good idea to transfer the risk to a Bitcoin business because most times, the customer isn't insured. Mt. Gox was unable to fully pay back their customers after the $350 million hack (McMillian, 2014). Attacks of this magnitude don't happen often, but better to be proactive and set up a cold storage wallet before transacting.

Phishing attacks, however, do represent a vulnerability on both Bitcoin wallets and on centralized exchanges. Everyone should put in extra effort to make sure their personal information is secure since all of it is stored on IoT devices which are connected to the network. Even though Bitcoin wallets hold the owner's private keys that are directly linked to the blockchain, a phishing attack on a person's login credentials is enough for an attacker to take control of a user's account.

This can also be said for Bitcoin exchanges, as many owners utilize these for trading and storage purposes. All it takes is a little carelessness when opening up a suspicious email or clicking on ad bait, and malware involving anything from key loggers to information dumping software can be installed on the device. One recent example of this "had to do with malicious code that looted video game accounts for their associated bitcoin accounts" (Park, J. H., & Park,

J. H. 2017, 7). As video gaming has entered a phase driven by in-app purchases, many companies are now allowing users, especially on PC, to pay with digital currencies. Just like with all other technological enhancements, there is now another vulnerability that users need to be aware of to ensure safety.

Another example directly related to malicious programs being used for theft comes from an example spotted by anti-virus companies which was called DevilRobber. They said this "Trojan targets Mac computers and spreads with pirated software downloaded from torrent sites such as Pirate Bay. This is a much more complicated malware. It destroys wallet files, but it also manages Bitcoin, collects system information such as shell and browser history, and collects user names and passwords" (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017, 21). The complexity of programs like these are certainly powerful enough to deter people from utilizing Bitcoin. Malicious programing is developing at a very high rate, to the point where society may have a difficult time keeping up on the defensive end. There are also many theoretical attacks that haven't happened yet but are possible – like a Preimage Attack. "The Preimage Attack on the hash function searches for the original message from the hash value produced by the hash calculations. If they found a way to get rid of one of the hashes that encounters the difficulty required for a given block, they could present it as proof of work while collecting discovery fees and bonuses to find a new block and add it to the chain" (Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A., 2017, 12) What is being described is very difficult to do because of the complicated hashing process, but the thought brings uncertainty.

With the way IoT technology is evolving, it is becoming increasingly difficult to protect user assets when everything is connected to the network because with every new connection lies another opening that needs protection, and Bitcoin is falling victim to that same exact way of

thinking. Unless users take the time to harden their networks and invest in protection resources, in addition to spreading the word of how important security is, adoption may never fully take off.

Other security issues that are outside the technical realm generally fall into the category of social issues. Besides Bitcoin owners having to worry about losing their wallet login credentials, which is very much a cause of anxiety for some, the space is severely under-regulated when it comes to protecting a user's assets. Unfortunately, this also promotes scammers to come out of the woodwork and seize the opportunity to make money off innocent people's lack of awareness. Exchange scams is a common theme of how users get scammed in the crypto space (Liebkind, 2018). Exchange scams can leave investors with empty pockets if they are not careful by stealing private information and also directly draining accounts. These scams can be spotted by suspicious URL's but a way to fight against this is by checking to see if the web address begins with HTTPS to ensure the online traffic is being encrypted. Most recently, South Korean exchanges were exposed for this type of fraud but fraud can happen anywhere (Liebkind, 2018).

All Bitcoin related businesses, like exchanges or companies that host wallet services, face little to no regulation on the business end. That means that in many cases when an exchange gets hacked and loses all of their customer's Bitcoin, the exchange isn't responsible to retrieve the lost funds in order to refund their customers (Hughes, 2017). It becomes a case of ethics, the lack of regulation promotes business owners to make their own decisions and decide if they want to close shop or go the extra mile to make things right – all depending on the situation and the intentions of the business owner. Proof that scenarios like this do exist can be found when looking at the history of Bitcoin. Back in 2014, the Mt. Gox exchange crumbled after a $350 million-dollar hack. This translated to losing 744,408 Bitcoins, all owned by the exchange's

clients who were housed on the exchange-based wallets. “Mt. Gox was once the world's largest bitcoin exchanges, but ultimately ended up going offline, apparently after losing hundreds of millions of dollars due to a years-long hacking effort that went unnoticed by the company” (McMillian, 2014, 1). There were rumblings of the company trying to pay back customers for their lost money via arbitraging trading methods, which is still legal in crypto trading but not in the stock market. It ended up folding as the loss was too great. Situations like these where customer money is lost and the company folds without repayment creates concern among Bitcoin enthusiasts.

Another way the lack of regulation impacts the space negatively is through manipulation. Given Bitcoin’s small circulating supply, it is easier to manipulate the price seen on exchanges either by trading with large sums or by taking part of trading signal groups who collectively work together to either drive the price up or down. Hacks also can have a major implication on price fluctuations as well. “Bitcoin futures derive their final value from prices at four bitcoin exchanges: Bitstamp, Coinbase, itBit and Kraken. Manipulative trading in those markets could skew the price of bitcoin futures that the government directly regulates” (Chatham, 2018, 1). Coinrail was hacked back in 2018 which apparently lead to a major dip in price, and because of this dip, the overall Bitcoin market price was negatively impacted. The impacts are even felt on major exchanges which is directly related to the government based future price. There needs to be some more confidence injected into the market, almost like an insurance policy that protects investors, big and small, from scenarios where a company runs out of business or the market becomes manipulated.

CONCLUSION

Many of these security issues will stay with the existence of Bitcoin. There are vulnerabilities that come with utilizing technology that operates over a network, and Bitcoin is no exception. But just as there are ways to minimize the vulnerabilities on the internet, there are ways to minimize vulnerabilities while being a Bitcoin user. Mainstream adoption could very well be sabotaged by the lack of accessibility to the common user as plenty of work is required just to be able to safely secure the asset by storing it properly and taking the extra effort to set up 2FA. Once the technology gains momentum it will be easier to overcome this obstacle because people will need to learn it at that point, but realistically we are still a ways away and some sort of regulation to protect users' needs to be introduced.

Technically speaking, cold storage wallets provide the peace of mind necessary to give new adopters confidence that their assets are safe. Cold storage enables users to keep their Bitcoin offline and it cannot be accessed unless the USB stick is connected to their own computer and verified with their personal login credentials. There even are methods to back up the wallet by a 16 word passphrase which can be used to authenticate a wallet on a new ledger in case of theft or the user misplacing it. System and network hardening is also vital to the overall health of the user's digital world. Security loopholes can be found on multiple layers, the network layer, and the physical layer. Configuring administrative settings in a strict manner and using a reliable anti-virus program can go a long way in protecting a person and their digital information. If cold storage wallets are used appropriately and the user's network and machines are hardened, using and storing Bitcoin while minimizing vulnerability is possible.

People seem to forget that Bitcoin adoption is still in the early stages so improvements still need to be made in an effort to keep owner's assets safe. It takes education and awareness as

well as security enhancements to the Blockchain itself. This can be seen already with the implementation of POW and POS in Blockchain technology.

Ultimately, many people do not feel comfortable using a currency that is driven by blockchain technology, nor do they want to spend the time necessary to educate themselves on how to properly use it in a secure fashion. Institutional money will not flow in unless the government promotes some sort of regulation that protects users and investors. A more confident outlook on blockchain security in wallets and among exchanges definitely would inject more institutional money into the market which would in turn enhance development overall. There is more than enough potential in this technology to make the world a better place, but as with everything else in technology, there needs to be a balance between innovation and security if the early adopters expect new users to come into the space. The early phases of adoption are still happening and there is a lot of work that needs to be done to spread awareness on how useful this new technology is, and to educate on how to properly use it in a manner that minimizes security vulnerabilities and improves quality of life.

Bibliography

- Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, *9*(8), 164. doi: http://dbproxy.lasalle.edu:2101/10.3390/sym9080164

- Latifa, E., My Ahemed, E. K., Mohamed, E. G., & Omar, A. (2017). BLOCKCHAIN: BITCOIN WALLET CRYPTOGRAPHY SECURITY, CHALLENGES AND COUNTERMEASURES. *Journal of Internet Banking and Commerce*, *22*(3), 1-29. Retrievedfrom http://dbproxy.lasalle.edu:2048/login?url=https://dbproxy.lasalle.edu:6033/docview/1992203656?accountid=11999

- Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia ComputerScience,132*, 1815-1823. doi: https://www.sciencedirect.com/science/article/pii/S187705091830872X

- Piscini, Eric, and David Dalton . "Blockchain & Cyber Security. Let's Discuss." Delloite.com, 2017, Retrieved from: www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187. doi: http://dbproxy.lasalle.edu:2101/10.1007/s12599-017-0467-3

- Franco, P., & ProQuest (Firm). (2015;2014;). Understanding bitcoin: Cryptography, engineering and economics. Chichester, West Sussex, [England]: John Wiley & Sons.

- Johnston, Kevin A., and Aiden J. Walton. "Exploring Perceptions of Bitcoin Adoption: The South African Virtual Community Perspective." *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 13, 2018, pp. 165–182., doi:10.28945/4080. Accessed 9 Sept. 2018.

- Parino, Francesco, Mariano G. Beiro, and Laetitia Gauvin. "Analysis of the Bitcoin Blockchain: Socio-Economic Factors Behind the Adoption.", 2018.

- Hileman, G., & Rauchs, M. (2017). 2017 Global Cryptocurrency Benchmarking Study. *SSRN Electronic Journal*. doi:10.2139/ssrn.2965436

- *Phil's stock world: Bitcoin tumbles after major crypto exchanges subpoenaed for manipulation,* *Chatham:Newstex(*2018).. https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2052684221?accountid=11999

- *Robert McMillian Bitcoin exchange mt. gox goes offline amid allegations of $350 million hack* (2014). . Chatham: Newstex(2014).Retrieved https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1502333421?accountid=11999

- Bashir, I. (2018). Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Birmingham: Packt.

- Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 1-59. Retrieved September 30, 2018, from https://lightning.network/lightning-network-paper.pdf.

- Bitcoin open source implementation of P2P currency. (n.d.). Retrieved from https://satoshi.nakamotoinstitute.org/quotes/economics/

- Prableen Bajpai *Investopedia stock analysis: What is cold storage for bitcoin and why does it matter?* (2015). . Chatham: Newstex. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1660615934?accountid=11999

- Gulshan Kumar (2016) Denial of service attacks – an updated perspective, Systems Science & Control Engineering, 4:1, 285-294, DOI: 10.1080/21642583.2016.1241193

- *Telcoin Whitepaper*. (n.d.). doi:https://icorating.com/upload/whitepaper/S6jcOtWjm2kV8akhvqReHO8SxHrHbbCLQILXhpYb.pdf

- *Warwick Business School, Phil's stock world: Don't be fooled - venezuela's petro is not really a cryptocurrency* (2018). . Chatham: Newstex. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2008119346?accountid=11999

- Ibarra-Esquer, J., González-Navarro, F.,F., Flores-Rios, B., Burtseva, L., & Astorga-Vargas, M. (2017). Tracking the evolution of the internet of things concept across different application domains. *Sensors, 17*(6), 1379. doi:http://dbproxy.lasalle.edu:2101/10.3390/s17061379

- Joe Liebkind, 2018. *Investopedia stock analysis: Beware of these five bitcoin scams* (2018). . Chatham: Newstex. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2115903019?accountid=11999

- Hughes, S. D. (2017). Cryptocurrency Regulations and Enforcement in the U.S. *Cryptocurrency Regulations and Enforcement in the U.S, 45*(1).