BlockChain: applications other than cryptocurrency

FP Team 3

Noah Smith & Elise Timmons | CIS 481-01 | 4 April 2020

**Table Of Contents**

[**Executive Summary**](#_uw3g37yvotmj) **1**

[**Objectives**](#_ngq0ertq1x7w) **2**

[**BlockChain**](#_6d1tbpdlv9bu) **2**

[**Cryptocurrency**](#_ap29yp3v20bg) **3**

[**Compare BlockChain and Cryptocurrency**](#_ijuspt499ews) **4**

[**BlockChain Relevancy**](#_s6nq3pxw08w4) **5**

[Proof of Ownership](#_ds4sc72o0389) 5

[Less Transaction Friction](#_82cxj2d7p7ni) 5

[Less Criminal Enticement](#_ya7tlbsgc6z1) 6

[**Applications**](#_yo5bb2cv3ms2) **6**

[Finance](#_f9y88mfkvvyy) 6

[Government](#_e4hjn7v84p8o) 7

[Healthcare](#_w0n93452vgq4) 8

[**Security Concerns**](#_y63b0t18kily) **9**

[Social Engineering and Phishing](#_39dudw2iq5d4) 10

[Endpoint Vulnerabilities](#_az9y2sh5rptm) 10

[51% Vulnerabilities and Attacks](#_ieayrhdrh74w) 10

[Exchange Hacks](#_wleodml9gh71) 11

[**Ways to Prevent Security Concerns**](#_x61dsro6d1a8) **11**

[Social Engineering and Phishing](#_l5trfgq5pdwv) 11

[Endpoint Vulnerabilities](#_g3uqqkvfehyj) 11

[51% Vulnerabilities and Attacks](#_o9cy44k96dgf) 12

[Exchange Hacks](#_nuvkh49aa929) 12

[**Conclusion**](#_9xf9weww998g) **12**

[**Works Cited**](#_v73dyftjr4iz) **14**

# **Executive Summary**

Blockchain is one of the most popular and fastest growing distributed ledger databases. The shift from in person to online sharing created a need for secure and transparent data that both companies and their customers can trust. Using Blockchain has been a great way to do just that. This is because of decentralization. All information created from data cannot be owned by one central person but instead distributed over a consensus of participators. All data is not centrally owned and therefore is more easily trusted. The use of Blockchain became a large talking point because of the increased use in Bitcoin, a cryptocurrency that used blockchain to help keep transactions trustworthy and private over the internet. However, data users have been finding additional ways to use this “distributed database” for more than just exchanging currencies.

Other applications for Blockchain have come to show just how impactful the technology can be. These other applications can include keeping secure networks for the likes of the medical, finance, government, and business worlds through healthcare, medical data, insurance, and banking. For example, blockchain use between insurance networks and medical networks would mean that neither would own personal patient info. This would allow readily available information sharing for specific patient needs, but also maintain security from external corruption so as to keep in compliance with government patient privacy acts.

While blockchain is an outstanding technology to use for anyone’s data sharing, there are still plenty of security concerns that should be addressed. Mainly, any type of threat that can affect blockchain’s distribution of data can hurt it’s users. Threats can come from social engineering that can result in phishing and malware, endpoint vulnerabilities that create attack paths for hacks, 51% attacks that result from an uneven division of owned data, and exchange attacks that hurt a current transaction.

One of the key solutions to a multitude of threats for blockchain users is to be vigilant, this means staying up to date on newly designed threats. An unknown threat is more dangerous than a known one. Understanding weak points within a company’s blockchain network is key to also understanding how to secure the network.

# **Objectives**

The primary objective of this research paper is to help the reader understand BlockChain and the ways it can be used that do not deal with cryptocurrency. Our main focus is pointing out and explaining the most crucial parts of BlockChain as well as giving a description of cryptocurrency so that the reader will be able to understand how BlockChain can be used in other ways that do not involve cryptocurrency. We will then go over several different applications of BlockChain and finally, we will go over some of the security concerns that may come from BlockChain and discuss the ways that they could be fixed...

# **BlockChain**

What is BlockChain? According to Ameer Rosic, at the most basic level blockchain is literally just a time-stamped series of data that is managed by a cluster of computers and doesn’t have a single owner. “Blockchain network has no central authority (Rosic, 1)”. Because of this, the information is open for everyone to view. A blockchain is a simple and ingenious way of transmitting information from A to B (Reiff, 1).

When a person creates a block, a transaction is initiated. This block is then verified by thousands of computers and added to a chain. This chain is stored across the internet and creates a unique record with a unique history. If someone would want to create a false record, then they would have to create an entire false chain (Rosic, 1). Creating a false chain is virtually impossible, this makes the use of blockchain very appealing.

The batches of transactions are hashed and encoded into a merkle tree (the Economist, 1). Each block contains a hash of the previous block in the chain creating a link in the two and all the way down the chain, this creates integrity all the way back to the original “genesis” block.

Sometimes separate blocks can be produced concurrently creating a temporary “fork (The Economist, 1)”. As stated by Rosic, “The history of each chain is also secure, every blockchain has a specific algorithm for scoring different versions of the history so that the one with the higher score can be selected over others, the blocks that are not selected are known as orphan blocks”.

The use of BlockChain also creates decentralization since data is stored across peer-to-peer networks (the Economist, 1). This is great and eliminates many of the risks of storing data in a central location. Decentralization also makes it harder for computer hackers to find an exploit they can take advantage of, also, there is no central point of failure (Rosic, 1). There has been some controversy due to BlockChains permissionless design. A part of this debate tries to decide if a private system with unique varifiers should be considered a BlockChain.

Compare a blockchain to a GoogleDoc, these files are accessible and rewritable by everyone at the same time, this same idea is what allows blockchain to work. There are three main properties that have helped blockchain technology become widespread: Decentralization, Transparency, and Immutability. Blockchains that are readable by people are the ones that are used in cryptocurrencies.

# **Cryptocurrency**

What is Cryptocurrency? According to Ameer Rosic, it is a digital medium of exchange that uses cryptographic functions to conduct financial transactions. One of the most important features of a cryptocurrency is that “it is not controlled by any central authority (Rosic, 1)”. Bitcoin was first released as an open-source software in 2009 and “is generally considered the first decentralized cryptocurrency (Matonis, 2)”. Since the release of BitCoin there have been over 6,000 other cryptocurrencies released.

The idea of a cryptocurrency has been around since the 80’s when a man named David Chaum conceived the idea for “cryptographic electronic money and called it ecash (Chaum, 3)”. Later in the 90’s Chaum implemented his creation. Throughout the 90’s other people and organizations began their own research on cryptocurrencies including the NSA (Rosic, 4). Starting in the 2010’s cryptocurrencies began to take off due to the sheer number of people that use the internet at that point as well as the secrecy and perceived awesomeness of the coin.

The validity of a cryptocurrency is provided by a blockchain, therefore, one of the uses of blockchain is in cryptocurrencies (we will not go over this though because this research paper shows uses other than cryptocurrency, it is important however, to know about the link between cryptocurrency and blockchain.) As stated by Rosic, cryptocurrencies can be “mined” and stored in “wallets”. These “wallets” can be used to contain, retrieve, and spend the cryptocurrency.

# **Compare BlockChain and Cryptocurrency**

As gone over briefly in the section above, cryptocurrency is one of the many uses on BlockChain and because of this they share many similarities. Blockchain would be considered a technology while Cryptocurrency would be considered an asset class, “blockchain is the platform that allows cryptocurrencies to work (Blockchain WTF, 1)”. Cryptocurrencies are the tokens that are used within a blockchain network to send a value and pay for transactions. All of this is important to understand when trying to find different uses for blockchain, as we will go over later.

# **BlockChain Relevancy**

With the vast growth in electronic services for consumers, the relevant need for transparent data has also grown. New companies and even old ones wanting to create a new platform that allows customers to own their own data should implement blockchain technology. This is because “the software itself is a controlled and open framework that is visible to all transaction participants (Kumar, 1).” This is blockchain’s main attraction for businesses but there are also other reasons such as proof of ownership, decreasing transaction friction, and decreasing criminal activity that shows just why the technology is rising in popularity.

## **Proof of Ownership**

An important use for this technology is eliminating the main issue with exchanging data from one platform to another. Blockchain can be used as proof of ownership of any data that is being presented. A large issue today is security of personal information. Large sums of personal data for multitudes of people can be found through insurance groups, hospitals, online banking, and online companies. These collections of data are enticing for hackers. But if a company went through blockchain, “Each data element is secured and encrypted with a blockchain member’s key, a cybercriminal would need to have access to each key of each member” (Kumar, 1). Online personal data would be owned only by the person it belongs to and when in need to share info, the recipient user would be able to securely receive the data from a trustworthy source. For example, if an applicant for a job wanted to send their credentials from a University, the chain of that information would clearly show where the credentials came from. Sending the data would authorize the employer to check that their credentials are not fabricated and are in fact owned by the applicant.

## **Less Transaction Friction**

Blockchain reduces transaction and data sharing friction. Use of a “self-governed” blockchain network that can be used between two participants would have close to zero interference and allow for direct and efficient connections. Blockchain creates a simple foundation for businesses that want to come in and use indisputable data storing tactics. No way to question anything if all the information pertaining to that data is laid out right before your eyes. Blockchain is relevant to us because it creates a distribution of power for a transaction. There is no one person that owns the data within blockchain technology because everybody owns their own data. As an open source uses blockchain, participators remain equal when any data is introduced or exchanged.

## **Less Criminal Enticement**

Criminals are able to be easily identified. Hackers are hesitant to try and alter a block. As data cannot be overwritten, data manipulation is extremely impractical, thus securing data and eliminating centralized points that cyber criminals often target (Joshi, 1). This is because without a great deal of experience and a large amount of time, trying to change the already presented data would be useless. Trying to modify one block of data will affect the whole chain and compromise all connected data, making it apparent that there was an attempt made to the block.

# **Applications**

Blockchain has hundreds of possible applications with more being developed all of the time. The uses for this technology are almost limitless and as we continue to advance and build more powerful computing machines the importance of these chains will be even greater. A few of the different applications of blockchain would include...

## **Finance**

One of the many uses of blockchain is in finance. Blockchain provides many different benefits to the finance world, the chain allows more “open, inclusive, and secure business networks (Finance, 1)”. There is also a higher level of customization given by blockchain. There is a great increase in security with blockchain, the way that the distributed architecture works helps eliminate single points of failure which in turn, helps transfer agents. There are also big performance gains from blockchain. As stated by Engineering, due to the engineering of the hybrid and private networks, hundreds of transactions per second can be sustained and monitored.

The digitization of financial instruments have many different effects on the finance world. Any new technology helps the world do things faster, and in turn, helps the global economy and nothing is different here. “The automatization allows for more efficient processes that help reduce infrastructure costs, operating costs, and transaction costs (Finance, 2)”. There are also many added programmable capabilities that allow greater market reactivity and allows more products to reach more markets.

There are many different use cases that blockchain brings to the financial market, a few of them would include:

* Capital Markets- There is an elimination of a single point of failure.
* Trade- The documentation is authenticated digitally and removes the cost of physical travel.
* Payments- Secures cross border transactions and multiple forms of payments.
* Investment Management- Funds can be launched automatically and seamlessly.

## **Government**

Another great use for blockchain is in the governmental sector. Governments can use blockchain to streamline processes and protect their data. Governments that work on the blockchain model all share resources and models with themselves, businesses, and individuals. According to Government, “A blockchain-based government has the potential to solve legacy pain points and add many new advantages.” One of the issues that can be fixed is voter security and fraud. Citizens can gain their own private key that they could use on an app, this app could then generate private keys that are locked to the individual. The keys could then be tied into the country's governmental bodies and used as a means of voter tracking and fraud prevention.

A country could also “Issue your identity” through a blockchain (Government, 1). There is already a product that has this capability out there called Zug. Zug creates a person's identity on the Ethereum network, this gives the government the ability to sign and verify data through their account and use it for a number of tasks. In the future, citizens could use their Zug profile to enter a governmental office or building, this could be done by a scanner that reads a citizens information and pulls an instantaneous background check on that individual, this check could then be used to decide if they could have access or not. This technology has many different uses, both good and bad, that governments could use to protect, or even harm their citizens.

There are many countries that are already using blockchain in their governments including Australia and the United Kingdom. Australia has decided to use blockchain in voting, and according to them, “the system is tamper-proof (Chin,1)”. They want to start testing the systems in small community elections before they bring it to the federal level. According to Chin, the ballot would be integrated cryptographically within the blockchain. The United Kingdom has also begun using blockchain to track the distribution of welfare funds. Due to the nature of blockchain, this is a great use. There is a lot of belief within the United Kingdom that blockchain would be great at replacing, “large legacy IT systems located within a single institution (Chin, 1)”. If these countries continue to implement blockchain in various ways they could save money, protect the citizens, and make everyday tasks faster and more protected.

## **Healthcare**

One of the most useful applications of blockchain is in the healthcare industry. Currently, the healthcare industry is being plagued by rising hospital costs and constant data breaches. Many of these problems can be solved with a little innovation and blockchain allows just that. “Keeping our medical data safe and secure in the most popular healthcare application at the moment (Daley, 1)”. BlochChain’s ability to protect data from corruption is a great reason for the industry to use the chain, and the industry is beginning to do just that.

BlockChain can be used as a “network” for all of the healthcare institutions to use, because of this, they wouldn’t own a patient's data. Each patient could be identified by their HashID providing the ability to store all of the health information of a person into one long chain that can be viewed wherever the patient goes.

There are also many benefits for the drug industry. As stated by Daley, there is a company known as Chronicled that builds blockchain networks that show the chain-of-custody of drugs. This solution allows drug firms to track all medications and analyze that data to see what is used the most and where it is used. There is a lot of regulation when it comes to the user privacy of drugs and the encryption in blockchain helps protect that privacy.

The CDC is using blockchain to “monitor diseases in a supply chain-like manner (Daley, 1)”. The impacts of this could help the CDC learn about diseases faster and be able to treat them faster than they would have been able to otherwise. Genomics also comes into play here as well, the blockchain can allow the CDC to store genetic data of different diseases and watch how they mutate over time. All of this information will be time stamped and safely encrypted.

The healthcare uses stated above aren’t the only ones, there are tons of them and people are using blockchain in new ways all that time that help the healthcare industry. Well regulated products built off blockchain would help the healthcare industry innovate and provide the medications that millions of people need around the globe each day as well as prove the world new ways to do research that could possibly stop a pandemic.

# **Security Concerns**

As more uses for blockchain develop, the more widely known the technology has become. This results in increased interest in others learning how to threaten blockchain using applications. Cryptocurrencies built on top of blockchain are subject to hackers learning how to exploit the systems for a significant time now because of a focus for growth and not a focus for security. The best way to understand a blockchain’s security concerns is to look at previous successful security take downs throughout blockchain history. In LedgerOps – 2018 Blockchain Threat Report, a total of about $1 billion was reported lost in blockchain cryptocurrency related hacks in 2018. Some concerning security threats that we can learn from cryptocurrency and apply to the other blockchain applications are as follows…

## **Social Engineering and Phishing**

This type of threat is most common because there are always going to be social engineering threats to all companies, whether they use blockchain technologies or not. In 2018, the LedgerOps - 2018 Blockchain Threat Report reported that over $2 million was lost to attacks related to social engineering and phishing. This type of threat uses the user as the main form of attack, and without the user there would be no way to attack. Social Engineering creates a loss of trust within employees of a company and tries to chip away at the social behavior of human beings. Taking over an employee’s social behavior can lead to criminal use of malware or DNS hijacking that tricks a user into trusting a link or program that intends to threaten the security of a network. Ransomware and malware are large issues when pertaining to social engineering because once a hacker has tricked an employee, they are able to slip many threats through the employee’s connections.

## **Endpoint Vulnerabilities**

Endpoint vulnerabilities can also be found in other systems besides those that use blockchain. However, they can still be a large issue when in use with exchange hacks that we will talk about later. This type of attack is used against the user and the blockchain system. When another device connects to a system it creates a liable access point for a hacker to attack. These are called attack paths. If a user is connected to a system through a desktop, laptop, or smartphone there is a chance for security to be less than optimal. This is why an endpoint attack is a user and a system attack. An endpoint attack can lead to malware use or even an exchange hack.

An attack through an endpoint uses a combination of strategies and use of the systems functionality. The threat of using a system's functions to attack the system is called an abuse of functionality. This can include password recovery, sending email functions, or sending unrestricted proxy requests.

## **51% Vulnerabilities and Attacks**

51% Attacks are created when “a single entity controls the majority of a blockchain’s hashrate” (LedgerOps, 1). Hashrate is the speed at which a Bitcoin operation takes place. When affecting cryptocurrencies, controlling hashrate causes a disruption that can lead to attackers reversing transactions where they can then spend the coins a second time, this is how a split will occur within a chain, or even halting operations between other users.

51% attacks are highly damaging and effective because they create an uneven distribution of power within the applications network, known as a loss of decentralization. These attacks cannot alter past exchanges but can easily affect current and new ones. In a blockchain there should not be one overall owner of the data. This gives too much power and gives the owner the ability to control how any blockchain system would operate.

This type of attack can also be replicated in other non-cryptocurrency blockchain applications. An entity would still have control of over 51% of the “hashrate”, but instead it would be computing power and instead of stopping other crypto “miners” from earning rewards, an attacker would be able to stop exchanges of data or money.

## **Exchange Hacks**

This is an attack on the blockchain itself and while it does affect the end user it is not an actual user attack. Exchange attacks resulted in about $907.5 million lost in 2018 according to LedgerOps. A transfer of money or data during an exchange can lead to a vulnerability during the exchange. This is also one of the most popular targets for cyber criminals.

There are a couple of ways that threats can come from exchange hacks. One threat is due to access to databases. If a cyber criminal can access any form of a company’s database, the attacker will have full control of that part of the network. Data is stored in a hot or cold “wallet” that if used during an exchange can be subject to an attack because an attacker can figure out where the wallet is located.

If an attacker can find a way to fabricate an exchange it is more difficult to figure out what is accurate data compared to fake data because all data is stored the same in a block and not able to be accessed after the initial exchange.

# **Ways to Prevent Security Concerns**

## **Social Engineering and Phishing**

Social engineering is simple and easy to use because people can be easy to use. Use of private keys as access to data is a great way to protect valuable data that others may want. Private keys make access more difficult for the wrong user and allow for more security. Clear policies are also another way to create a way for employees or users to not be the last barrier between essential information and criminals.

## **Endpoint Vulnerabilities**

Some of the best ways to protect against endpoint vulnerabilities is to continue accurate decentralization methods. An endpoint attack occurs because of an insecure path from a network or system to a user. Allowing a system to not be dependent on one user or allowing data to not be owned by one centralized company is the best way to protect the data. An attacker will have less benefits from an attack because data is not all stored in the same place.

The use of better consensus methods results in a great way to secure a blockchain technology. This is where a large sum of nodes must validate any exchanges. A large amount of computing power is needed to secure via consensus method, but the security results are well worth it. Many cryptocurrencies use Proof of Work or Proof of Stake as a way to check another system for access. This ensures that there is a barrier between a new user’s system and the secure blockchain technology.

A couple other ways to protect against endpoint attacks or attack paths are to incorporate antivirus protection, to incorporate strong security protocols, or to lean on other networks that are secure.

## **51% Vulnerabilities and Attacks**

51% attacks are created because of decentralization of data. Therefore, the best way for a company to protect against an attack is to correctly store data in a non-central way. This can be through leaning on other networks, allowing system users to own their own data that can then be used when needed like patient information, or using consensus methods that check for systems outside of the blockchain to ensure protection.

## **Exchange Hacks**

When an exchange is taking place, be that a transaction with cryptocurrency or money, or even an exchange of data from one place to another, using a multi-signature protocol is the best way to ensure unwanted exchanges do not slip past. “Using this protocol provides additional layers of security, (that) without approval from the managers, the transaction (will) fail.” (LedgerOps, 1)

Another fix would be to store data or money in a cold (offline) database or wallet that would only need to become accessible, hot (online), when actually in use. This creates a secure database that is not connected to any external entities while not in use. Exchange hacks are used to take data or money from users during an exchange, so if any incentives to take the data or money is hidden from a criminal user would not become subject to vulnerabilities as long as there is no physical way to access the data.

# **Conclusion**

BlockChain has grown a lot over the past few decades going from just an idea to a product with tons of different applications. In order to understand the benefits of BlockChain and how it can be used, one must first understand what BlockChain is as well as what Cryptocurrency is so that a distinction can be made and the applications can be understood.

There are many different applications for BlockChain but some of the main applications are in Finance, Government, and Healthcare. These applications benefit the world creating more security, diversity, and protection of data. Also, the creation of BlockChain has allowed these groups to increase their efficiency and overall production speed while also making things easier for the end user and employees.

Over the next few decades BlockChain will continue to be developed and added to. This will create many new applications and uses that at the moment we may not even be able to imagine. The future will continue to be enhanced by BlockChain and the products that come out of it.

# 

# **Works Cited**

“Blockchain and Cryptocurrency: What's the Difference?” *Blockchain WTF*, blockchain.wtf/what-the-faq/blockchain-cryptocurrency-difference/.

Chaum, David. “Blind Signatures for Untraceable Payments.” *University of California*, 1998, [www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF](http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF).

Chin, Charlene. “Charted: Blockchain Use in Governments.” *GovInsider*, 30 Aug. 2016, govinsider.asia/smart-gov/charted-blockchain-use-in-governments/.

“Cryptocurrencies: Looking beyond the Hype.” *BIS Annual Economic Report*, 2018, Cryptocurrencies: looking beyond the hype.

Daley, Sam. “15 Examples of How Blockchain Is Reviving Healthcare.” Built In, 1 July 2019, builtin.com/blockchain/blockchain-healthcare-applications-companies.

“Finance.” *ConsenSys*, Enterprise Ethereum, consensys.net/blockchain-use-cases/finance/.

“Government.” *ConsenSys*, 2020, consensys.net/blockchain-use-cases/government-and-the-public-sector/.

“The Great Chain of Being Sure about Things.” *The Economist*, The Economist Newspaper, [www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things](http://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things).

Joshi, Divya. “How Secure Is Cryptocurrency and Blockchain Technology? Security Benefits and Issues of DLT.” Business Insider, Business Insider, 14 Jan. 2020, www.businessinsider.com/cryptocurrency-blockchain-security.

Kumar, Ajay. “Four Things Other than Cryptocurrency That Blockchain Can Do for You.” *The Economic Times*, Economic Times, 25 Aug. 2018, economictimes.indiatimes.com/small-biz/security-tech/technology/four-things-other-than-cryptocurrency-that-blockchain-can-do-for-you/articleshow/65539901.cms?from=mdr.

*LedgerOps - 2018 Blockchain Threat Report*. LedgerOps, 2019, *LedgerOps - 2018 Blockchain Threat Report*, documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:eae0e5e7-d798-4854-b3fa-4dae1686eb3f.

Matonis, Jon. “Bitcoin 101.” *Web Archive*, 2016, web.archive.org/web/20160813163512/www.trssllc.com/wp-content/uploads/2013/05/White\_Paper\_Bitcoin\_101.pdf.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.org*, bitcoin.org/bitcoin.pdf.

Reiff, Nathan. “Blockchain Explained.” *Investopedia*, Investopedia, 5 Feb. 2020, [www.investopedia.com/terms/b/blockchain.asp](http://www.investopedia.com/terms/b/blockchain.asp).

Rosic, Ameer, and Blockgeeks. “What Is Blockchain Technology? A Step-by-Step Guide For Beginners.” *Blockgeeks*, 15 Aug. 2019, blockgeeks.com/guides/what-is-blockchain-technology/.

Rosic, Ameer, and Blockgeeks. “What Is Cryptocurrency: [Everything You Need To Know!].” *Blockgeeks*, 15 Aug. 2019, blockgeeks.com/guides/what-is-cryptocurrency/.

World Economic Forum, and Deloitte. “The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services.” *World Economic Forum*, 2016, www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/.