Cryptocurrency

Team 3

Brandon Crosier, Aaron Gordon, Kitrina Justus, Sam Steele, Marvin Weaver

Table of Contents

Executive Summary

Cryptocurrency, a digital form of currency, is a fairly new concept revolving around the idea that money should not be tied to one government and instead should flow freely throughout the Internet. Cryptocurrency started gaining popularity with Bitcoin in 2009. The popularity came at a price though. Since it is now widespread, it is also a target for attacks, leading to the theft of millions of dollars.

This report details some of the most popular cryptocurrencies, the history of cryptocurrency, and its modern-day significance. Then it addresses the security measures taken by the industry to protect itself, and where those measures have fallen short. It also details the three most costly cryptocurrency attacks and the known vulnerabilities of cryptocurrency that could be exploited in another attack.

Then it breaks down the safeguards that the industry has utilized to keep themselves safe. The three most influential solutions the industry has implemented are the Cryptocurrency Security Standards, blockchain, and decentralization.

After that, the future of cryptocurrency is analyzed, focusing on the stability and security of current cryptocurrencies, as well as the projected popularity of a select four, namely Bitcoin, Litecoin, Ripple, and Mintchip.

1 Introduction

Cryptocurrency is a digital currency that is designed and handled through the use of exceptional encryption known to us as cryptography. Through the establishment of Bitcoin in 2009, cryptocurrency has made the leap from being nothing more than an academic concept to a part of our everyday reality. After Bitcoin started, it attracted a large following in the following years and captured significant attention from the media when its market value peaked in April of 2013 at a record of $266 per Bitcoin after surging 10-fold 2 months prior to hitting its peak. Bitcoin hit a market value of a little over $2 billion at its peak but then took a dive of around 50%. This 50% plunge initiated an intense debate about the future of cryptocurrencies. So, will cryptocurrencies become the way we start paying for the essential as well as non-essential items we purchase in everyday life or are cryptocurrencies a phase the world is going through that will eventually fade away? We hope to answer those questions with the information we have collected (Barone, 2019).

1.1 History of Cryptocurrency

First, a little history of where and how cryptocurrencies began is provided. As stated above, Bitcoin was the first established cryptocurrency, but there were other attempts at digital currencies that utilized ledgers that were protected through encryption. Two of these examples were Bit Gold and B-Money which were conceptualized and formulated beginning in 1998-2009 but never made it to the fully developed stage like Bitcoin did.

Fast forward to 2009 and the establishment of Bitcoin was made where the Bitcoin software was made available to the public. With this software becoming publicly available, mining -- the process of creating new Bitcoins --, recording transactions, and verifying the transactions on the blockchain, has begun (Marr, 2017).

According to Konstantin Rabin in his article *What is the actual use of Cryptocurrencies* on Finextra, a common misconception about cryptocurrencies is that the only thing they can be consistently used for is illegal activities. While the use of cryptocurrencies in illegal activities is, unfortunately, something that can be done, cryptocurrencies should not be defined by the illegal transactions it can be used for because it is not the only thing cryptocurrencies can do. This beautiful technology enables a large number of individuals worldwide to work with and for better purposes around the world. Things like making an investment, paying tuition, providing charity donations, in addition to paying for everyday life goods and services are all a part of what cryptocurrencies can do and account for more than 50% of all cryptocurrency transactions with the first recorded crypto transaction being the purchase of a pizza (Sedgwick, 2018). The idea behind the creation of cryptocurrencies was for it to become the way we purchase everyday things, not an easier way to purchase illegal products, and that should never be forgotten (Rabin, 2019).

1.2 Significance in the Modern World

Cryptocurrency is important in the modern world because it is a virtual currency that is secured by cryptography, making it extremely hard to counterfeit or double-spend. Double spending is an attack where a set of coins is sent that has been spent in a previous transaction.

Another important aspect of cryptocurrencies is they generally are not associated with any governing bodies, thus making them theoretically immune to government interference and/or manipulation. A couple of important aspects in today's world are that most cryptocurrencies are inflation resistant and the entire history of the currency is available to the owner. We believe that most cryptocurrencies are inflation resistant because they are not tied to any other form of currency. An example of this could be that if the U.S dollar fell in value it wouldn't affect the price of BitCoin.

When it comes to significant cryptocurrencies, currently Bitcoin and Ethereum are the most used. Bitcoin has a current market capitalization of $169 billion which is around 6 times larger than the next largest cryptocurrency, which is Ethereum and its current market cap is $25.7 billion. These two are the most significant cryptocurrencies currently because the next largest cryptocurrency is Tether and it's only worth $9.1 billion (Knight). We also believe that BitCoin is significant because it was the first cryptocurrency to become widely known outside of the tech world and that is shown by how much larger BitCoin is than any other cryptocurrency.

So far, the main cryptocurrency discussed has been Bitcoin; however, there are other cryptocurrencies being used, specifically Ethereum. Ethereum uses blockchain technology similar to Bitcoin. Both of these cryptocurrencies function in generally the same manner, but there are some key differences between them. For example, transactions using Ethereum may have some sort of executable code while data related to Bitcoin transactions is generally only used for keeping notes.

Another difference between the two is blocktime. Bitcoin takes a few minutes to confirm while Ethereum takes only a few seconds. The most important difference between the two cryptocurrencies is their networks have different overall goals. Bitcoin was created as an alternative to national currencies and Ethereum's intended use is as a platform for immutable, programmatic contracts, and applications through its own currency (Reiff, 2020).

Bitcoin came into existence in August 2008 when the domain bitcoin.org was registered and later that year a paper was published titled "Bitcoin: A Peer-to-Peer Electronic Cash System". It was written by a person named Satoshi Nakamoto, who is credited with the creation of Bitcoin. To this day no one is sure who Satoshi Nakamoto is or if they are even a single person. A method of using a peer-to-peer network for electronic transactions was referenced. The Bitcoin network came online on January 3rd, 2009 and the first mined block was by Nakamoto and it gave him 50 bitcoins. This block was called the genesis block and that is why they received 50 Bitcoins.

Ethereum was launched on July 30th, 2015 by Vitalik Buterin. Vitalik Buterin was a researcher and programmer when he first wrote a paper describing what is now Ethereum. In this paper he proposed Bitcoin needed a scripting language. He decided to develop a new platform with a more general scripting language. He was unable to get buy-in funding, so he developed an online crowdsale that ran between July and August 2014 (Knight). Crowdselling is similar to crowdfunding but with crowdselling you aren't pre-sold a widget but rather a token (Bradbury). With the crowdsale he was able to fund the development. Ethereum launched with over 11.9 million coins already mined which is around 13% of the total supply (Knight).

To provide additional understanding about the technologies utilized by cryptocurrencies, specifically blockchain technology. Blockchain technology is a time-stamped series of immutable records of data managed by a cluster of computers not owned by one single entity. Each of these pieces of data, the block, is “bound” to each of the other pieces of data using cryptographic techniques, making the chain. What is so special about blockchain technology? Since the blockchain network has no central authority, it is the definition of a democratized system. This is because it shares an immutable ledger data where the information on it is available for everyone to see. Thus, anything built on the blockchain is transparent and everyone involved is accountable for their actions (Reiff, 2020).

Because cryptocurrencies have not been around very long, many people think they are really hard to understand when, in reality, the concept behind them is quite simple. Bitcoin is a decentralized currency that uses peer to peer technology. While the decentralization ensures that there is no interference or manipulation from the government, it also means that there is nothing to back the value of Bitcoin. The major difference between Bitcoin and standard fiat currency is that fiat currency is backed by the full faith and credit of their government. Fiat currency is highly centralized and managed by a nation’s central bank. Local fiat currency deposits are also secured against bank failures by the government. Because Bitcoin is decentralized, it is unable to offer any kind of security against lost funds. This means that if a user were to lose any Bitcoin they had acquired, there would be no way for anyone to track the lost Bitcoin to get it back (Rosic, 2016).

1.3 Acceptance of Cryptocurrency

Today cryptocurrency is much more accepted than it has ever been. Since Q3 of 2016, the number of blockchain wallets has increased 5-fold from 8.95 million to 47.14 million (Szmigiera). This is a good metric to judge the acceptance because it shows a significant increase in the number of users using blockchain-based cryptocurrencies. According to a survey from Hartford Steam Boiler (HSB), 36% of small and mid-sized businesses accept cryptocurrency and 59% of these businesses use this cryptocurrency for purchases. Many companies using cryptocurrencies have only been in operation for less than 5 years (Milewski).

2 Security Measures

Security is the implementation of regulations to ensure safety. In terms of cryptocurrency, security would be the act of protecting the personally identifiable information of users, the currency stored in users' accounts, and the cryptocurrency itself. Hackers can make money from two ways: selling data they find and transferring money from the accounts they hack. For cryptocurrency, a hacker will infiltrate an account and transfer funds. So, how secure is cryptocurrency?

2.1 Security Weaknesses

First, there have been successful attacks on cryptocurrency companies in the past. They occurred due to weaknesses within the company. Those weaknesses consist of identity fraud, distributed denial of service attacks, and cryptojacking, among others.

Identity fraud occurs when someone pretends to be someone else. In this case, a hacker may discover someone's personal information and access his/her account. When the hacker gains access, funds can be transferred, purchases made, or any number of things.

A distributed denial of service attack, or DDoS attack, occurs when an attacker makes a service or machine temporarily offline by overwhelming the target with traffic, usually service requests. Since this is a distributed attack, it comes from many sources, making it hard to stop. As such, the company is susceptible to downtime from these attacks, costing money.

Cryptojacking occurs when hackers use someone's computer or phone's processing power to help mine their attacks, like with DDoS. Hackers will access this often without users even knowing it. This allows hackers to commit attacks like DDoS.

There are a number of security weaknesses that cryptocurrency companies need to address. One way to help combat these issues is to inform customers of best security practices and ensure they are following them, so companies are not held liable if they get hacked. They also need to implement policies regarding firewalls and secure passwords.

2.2 Security Strengths

Security is lacking in some areas, but cryptocurrency is still secure, some at the level of most banks. They have installed new hardware and software, like wallet management systems, to help improve their security. They also have implemented policies, like two-factor authentication and reporting hackers' addresses to help their customers be secure.

A wallet management system serves as a digital, encrypted wallet. It is a software program that stores credit card information and encrypts it, allowing the customer to safely store their information without worrying about hackers accessing it. Cryptocurrencies use them to manage their funds as well as to connect customers' outside banking to them.

Two-factor authentication requires two password entries to access the system. For example, requiring someone to enter his/her username and password and then confirming it with a code sent to a device. The device would have to be set up ahead of time, but if the hacker does not have the approved device, they will not be able to access the account, even with the other credentials.

Finally, a third security strength is the cryptocurrency industry is working together to combat these cybercriminals. As soon as one of the companies gets hacked or a hacker is caught in the act, the offender's address is added to a list of addresses to block. This is known as blacklisting and it helps prevent other companies from facing the same fate.

While cryptocurrency may seem unsafe, companies have taken several precautions to ensure customers have the best experience possible. They have taken many security measures, but it is difficult to know what is out there until it is attacking you. As such, cryptocurrencies may seem like they are not safe for widespread use yet. However, in a few years, that conclusion may change.

2.3 Previous Attacks

There have been a few notorious hacks on cryptocurrency companies resulting in losses up to millions of dollars. The most well-known are the BITPoint hack, NiceHash hack, and the Mt. Gox hack.

2.3.1 BITPoint

In July 2019, Japanese cryptocurrency company BITPoint was hacked and half of its customers were targeted. This resulted in the company needing to shut down to assess the damage. Originally thought to be around $32 million, the investigation revealed that the actual damages were $28 million. While that isn't a small number, it is less than expected. Unfortunately, since half the users were affected, their reputation as a trustworthy cryptocurrency company may never recover.

2.3.2 NiceHash

The NiceHash hack occurred in December 2017. NiceHash is an industry leader in mining and trading, so when they got hacked, it rocked the industry. They offer services to cryptocurrency miners and traders and sell hash power. The hack occurred at a time when Bitcoin was peaking, resulting in a loss of 4700 Bitcoin, totaling around $64 million. The site had to suspend all operations for a day to recover and are still paying back the customers who lost their funds.

2.3.3 Mt. Gox

Mt. Gox was the leading cryptocurrency exchange company in 2013, with a majority of Bitcoin transactions occurring there. While it had been hacked in the past, the most catastrophic hack occurred over three years, from 2011-2014. This hack slowly emptied the cold wallets of the company, resulting in a loss of $460 million. The head of the company was tried(fired?), and the company had to file for bankruptcy. Fortunately, this attack led to new regulations in the cryptocurrency industry to prevent this from happening again.

While these attacks were significant, most attacks are either prevented by detection software or immediately handled to mitigate the losses. Overall, these attacks were from new companies still trying to figure out how to operate in a new industry. As the years pass, hacks of this magnitude should decrease.

2.4 Known Vulnerabilities

Cryptocurrencies are considered fairly safe and secure. This is primarily because cryptocurrencies utilize blockchain technologies, which are notorious for being nearly impossible to hack. With blockchain, information about cryptocurrency transactions is encrypted within the blocks, making unauthorized access to information difficult (“Blockchain”). Despite the security of blockchain use within cryptocurrencies, there are several vulnerabilities regarding cryptocurrency transactions, namely, the storage and exchange of currency.

2.4.1 Cryptocurrency Wallets

Cryptocurrency wallets are a major vulnerability in the cryptocurrency world. Vulnerabilities for wallets include both digital and physical theft. First, there are two different types of cryptocurrency wallets: digital and hardware. Hardware wallets are exactly what they sound like: a physical object token used to access your “coins”. Something physical like this is at risk of being misplaced or stolen. One could steal a consumer’s wallet and have a greater chance of accessing the cryptocurrency. However, the hardware does not grant automatic entry to the cryptocurrency. The wallet is paired with a private key that allows the consumer to decrypt the wallet (“Protect”). Despite the extra security protocol, hardware wallets are still vulnerable to being stolen and potentially costing access to all of the user’s cryptocurrency.

The other type of wallet is a digital wallet. Digital wallets make cryptocurrency vulnerable because they are susceptible to hacks and scams. The most common scam is creating fake wallet sites or cloning existing wallets. In 2018, four different fake cryptocurrency wallets were found on the Google Play app store (Alexandre). One of the wallets was a “phishing wallet” that allowed users to input banking information, which in turn was stolen. The other three were wallets that tricked people into depositing coins into the hacker’s account (Alexandre).

2.4.2 Cryptocurrency Exchanges

Cryptocurrency exchanges share the same issues with wallets: being hacked and having fake sites created. Unlike wallets, more attacks have been executed on cryptocurrency exchanges. Per the MIT Technology Review, the majority of the $2 billion in stolen cryptocurrencies have come from exchanges (“Once”). Of that $2 billion, it is estimated that nearly half was stolen from only two groups, both cybercrime organizations (“Once”). Needless to say, these fake exchange sites have become an issue in the world of cryptocurrency.

2.4.3 Blockchain

Blockchain is a fairly secure technology because it is virtually impossible to edit the blocks of information. It is too time-consuming and would require an astronomical amount of power to do. This fact also makes it vulnerable in the case of bugs. One such “bug” allowed for $80 million in Ethereum to be stolen (“How”). The problem lied in a smart contract bug. A smart contract is a connection between blockchain and the real world that allows users to automate transactions (“How”). These contracts can be used to sign legal contracts or conduct financial transactions. The “bug” allowed hackers to continually request money without the system knowing that the money had already been withdrawn (“How”). Because of this flaw, the money could not be recovered once it was stolen. The only way to return the money would be to rewrite “history” in the blockchain blocks.

3 Safeguards and Solutions

This section outlines the security precautions that have been put in place since the invention of cryptocurrency. This includes new standards, encryption methods, and mindsets regarding cryptocurrency.

3.1 Cryptocurrency Security Standard (CCSS)

The Cryptocurrency Security Standard is a security standard that aims to hold accountable cryptocurrency providers and those companies who use/accept cryptocurrency (Psaila). It holds cryptocurrencies to elevated levels of security and transparency. There are three levels of security within the standard: level 1 establishes that an information system can protect crypto wallets with increased security; level 2 involves enhanced security with a formalized policy that is enforced through every step in the business process; in level 3, “multiple actors are required for the all-critical actions, advanced authentication mechanisms are employed to ensure the authenticity of data, and assets are distributed geographically and organizationally,” (Psaila). In addition, there are 10 security points that information systems can utilize: key/seed generation, wallet creation, key storage, key usage, key compromise policy, keyholder grant/revoke policies & procedures, third-party security audits/pen tests, data sanitization policy, proof of reserve, and audit logs (Psaila).

3.2 Blockchain

As mentioned earlier, blockchain is the driving technology behind cryptocurrencies. Blockchain has its vulnerabilities; however, overall it is a very secure technology and would require unthinkable time and power in order to hack it. To start, blockchain is a “public encryption method that keeps transactions secure and ensures each one is unique” (Regan). All transactions are also recorded in a public ledger. What makes blockchain an inherent safeguard is the way it is designed and how information is stored within the blocks.

To summarize how blockchain works, per Business Insider, transaction data is stored in hash functions within the blocks (Joshi) and encrypted. It is time stamped so the data cannot be tampered with (Joshi). The newly encrypted block joins a chain of blocks, hence blockchain. The blocks also contain a hash code that will change is any information within the block is changed ("Blockchain". This is important because in order to remain undetected, the hash for every single block following the block you changed must also be changed ("Blockchain"). This security feature serves to deter would be hackers for trying to gain access as it would take an enormous amount of time and power to change the blockchain.

3.3 Decentralization

Many, but not all, cryptocurrencies are decentralized. Decentralization means that the cryptocurrency is a universal currency. No one country can dictate what happens with the currency ("Frequently"). Bitcoin is the most notable decentralized currency. By being decentralized, Bitcoin has servers all over the globe (Regan). This offers the currency added security because if an attack is being attempted on one server, all the other servers globally can pick up the slack to prevent the attack from being successful (Regan).

4 Moving Forward: The Future of Cryptocurrency

Cryptocurrency is defined as "a digital currency that is created and managed through the use of advanced encryption techniques known as cryptography. (Barone)" Cryptocurrency took the leap to where it is now back in 2009, with the creation of Bitcoin. Bitcoin steadily rose in market value, peaking at a value over $2 billion. But, shortly after that the market plunged, this plunge left everyone in the dark about the future of cryptocurrencies. According to Adam Efrima, a Forbes technology council member, there are 5 predictions for the future on cryptocurrency and blockchains: "(1)The U.S. economy's bull run will end, and crypto interest will soar, (2)The gaming industry will emerge as a major use case, (3)The U.S. will maintain a 'wait and see' regulatory approach, (4)Stablecoins will gain popularity, or (5)The industry will recognize that blockchain's 'killer app isn't coming." (Efrima)

First, the meaning of Efrima's statement "The U.S. economy's bull run will end, and crypto interest will soar" is cryptocurrencies will attract the attention of investors when the current bull run ends. Cryptocurrencies would “soar” because cryptocurrencies are not tethered to any one nation’s market. This gives cryptocurrency the ability to hold its value much better during a time of economic strife. (Efrima)

Next, what Efrima means by “The gaming industry will emerge as a major use case” is gaming companies have the capability to appeal to a more tech savvy generation. In his article he points out that the gaming world has been comfortable with cryptocurrency for years. This gives the gaming world a competitive advantage over competitors interested in the cryptocurrency world. (Efrima)

Third, the statement Enfrima makes regarding regulation, “The U.S. will maintain a ‘wait and see’ regulatory approach”, means the U.S. will take a hands-off approach to the global contribution of technology to blockchains. The U.S. will maintain its position as the global tech leader but will become “hands-off regulators. “(Efrima)

Furthermore, what Enfrima means by “Stablecoins will gain popularity” is, that stable coin will become the new favorite of the cryptocurrency market. He believes this because stablecoins take cryptocurrency innovation to the next level. In his article he says, “In simple terms, stablecoins are cryptocurrencies that tie their values to real-world assets like the U.S. dollar.” This tie to an asset like the U.S dollar is huge because governments will have more to do with the stabilization of stablecoin, compared to other cryptocurrencies. (Efrima)

Finally, Enfrima is simply pointing out the fact that ever since blockchain came into fortition, investors and inventors have been expecting an amazing app to be developed and released in blockchain, but this is very unlikely to happen. (Efrima)

4.1 Stability

Cryptocurrencies have the capability to bring about big change in the market. According to Investopedia, there is a possibility that cryptocurrencies will be floated on the Nasdaq, this would add credibility to blockchain and increase its use as an alternative to conventional currencies. Furthermore, some experts predict that all the cryptocurrency world needs are verified exchange traded funds (ETF)(Barone). An ETF would make it much easier for someone to invest in cryptocurrency, but just because it has an ETF, is formed for the cryptocurrency market, doesn't mean that you have demand from investors to invest in cryptocurrencies.

4.1.1 Investing in Cryptocurrency

Cryptocurrency supporters claim that the financial platform that cryptocurrency is on is a trustless system, meaning they are not directly tied to any nation-state, government, or body. These supporters would argue that cryptocurrency is superior to traditional currency for this reason. Cryptocurrency is not dependent on a centralized form of government regulation. (Stanford Online)

4.2 Increased Security

According to Sandro Psaila, an IT Audit Senior Manager, cryptocurrencies current biggest challenge is confidence, people are concerned about the authentication, authorization and/or confidentiality limitations of cryptocurrency transactions. The current security standard for all cryptocurrencies is called the Cryptocurrency Security Standard (CCSS). The CCSS has three levels of security that increases as you increase the level.

- "An information system that has achieved Level I security has the ability to protect crypto wallets with strong levels of security.
- A higher level II of CCSS translates into enhanced levels of security with formalized policies and procedures that are enforced at every step within the respective business processes.
- In level III of CCSS, multiple actors are required for the all-critical actions, advanced authentication mechanisms are employed to ensure authenticity of data, and assets are distributed geographically and organizationally. "(Psaila)

I believe the next big hurdle to overcome in the cryptocurrency world is the physical custody of the cryptocurrency. Cryptocurrency custody solutions as defined in Investopedia is a "third party providers of storage and security services for cryptocurrencies." Right now, there is no definite way to track currencies or prove who is the custodian of the cryptocurrency at hand. Northern Trust has been making strides in the cryptocurrency custody. Northern trust also made it first venture into the cryptocurrency world, with the backing from Bakkt, a digital currency exchange custody service. (Watkins)

4.2.1 Government Regulation

Currently cryptocurrencies are not legal tender in any nation or state. They are not controlled or regulated by any central governing authority. The question you should be asking yourself is should there be government regulation of cryptocurrencies? Currently there are no regulations by any government; by adding regulation, cryptocurrencies protect the stability of their market. The regulation of government could in the long run make cryptocurrencies a safer investment, but by doing so it takes away from the privacy aspect that cryptocurrencies are known for. Currently there is a public ledger of all cryptocurrency transactions, you may not be able to trace it back to the person who made the transaction, but you can see all the other details: time, amount, date, etc. With government control comes the SEC, the SEC is looking at regulating ICO's as securities and is cracking down on fraud. (Sharma)

4.3 Alternative Cryptocurrencies

Alternative cryptocurrencies outline the most popular cryptocurrencies to date. The top four are Bitcoin, Litecoin, Ripple, and MintChip.

4.3.1 Bitcoin

"Each Bitcoin is basically a computer file which is stored in a 'digital wallet' app on a smartphone or computer. People can send Bitcoins (or part of one) to your digital wallet, and you can send Bitcoins to other people. Every single transaction is recorded in a public list called the blockchain." Bitcoin is currently the top selling and used cryptocurrency. (Newsround)

4.3.2 Litecoin

"Litecoin is regarded as Bitcoin's leading rival at present, and it is designed for processing smaller transactions faster. It was founded in October 2011 as "a coin that is silver to Bitcoin's gold," according to founder Charles Lee.13 Unlike the heavy computer horsepower required for Bitcoin mining, Litecoins can be mined by a normal desktop computer. Litecoin's maximum limit is 84 million – four times Bitcoin's 21-million limit – and it has a transaction processing time of about 2.5 minutes, about one-fourth that of Bitcoin." (Barone)

4.3.3 Ripple

“Ripple was launched by OpenCoin, a company founded by technology entrepreneur Chris Larsen in 2012. Like Bitcoin, Ripple is both a currency and a payment system. The currency component is XRP, which has a mathematical foundation like Bitcoin. The payment mechanism enables the transfer of funds in any currency to another user on the Ripple network within seconds, in contrast to Bitcoin transactions, which can take as long as 10 minutes to confirm.” (Barone)

4.3.4 MintChip

“Unlike most cryptocurrencies, MintChip is actually the creation of a government institution, specifically the Royal Canadian Mint. MintChip is a smartcard that holds electronic value and can transfer it securely from one chip to another. Like Bitcoin, MintChip does not need personal identification; unlike Bitcoin, it is backed by a physical currency, the Canadian dollar.” (Barone)

In conclusion, the cryptocurrency field has a long way to go in terms of security. There are many different types of cryptocurrency, but they all seem to have the same root issues. Thankfully, through the installation of clear standards, regulations, and security software, they are on the rise. If they keep up to date on security measures and follow the protocols outlined here, they should have no issue becoming as widespread as banks like Chase and Discover.

References

Barone, A. (2019, June 25). *The Future of Cryptocurrency in 2019 and Beyond.* Retrieved from Investopedia: https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp

Marr, B. (2017, December 6). *A Short History Of Bitcoin And Crypto Currency Everyone Should Read.* Retrieved from Forbes: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#38a7dc6f3f27

Rabin, K. (2019, August 1). *What is the Actual use of Cryptocurrencies.* Retrieved from Finextra: https://www.finextra.com/blogposting/17706/what-is-the-actual-use-of-cryptocurrencies

Reiff, N. (2020, June 16). *Bitcoin vs. Ethereum: What's the Difference?* Retrieved from Investopedia: https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp

Rosic, A. (2016). *What is Blockchain Technology? A Step-by-Step Guide For Beginners.* Retrieved from BlockGeeks: https://blockgeeks.com/guides/what-is-blockchain-technology/

Sedgwick, K. (2018, November 26). *Eight Historic Botcoin Transactions.* Retrieved from Bitcoin: https://news.bitcoin.com/eight-historic-bitcoin-transactions/

Knight, Oliver. "Top 10 Cryptocurrencies by Market Capitalisation." *Yahoo! Finance*, Yahoo!, 22 Apr. 2020, finance.yahoo.com/news/top-10-cryptocurrencies-market-capitalisation-160046487.html.

Bradbury, Danny. "What Is a Crowdsale?" *The Balance*, 25 May 2020, www.thebalance.com/what-is-a-cryptocurrency-crowdsale-391277.

Kech, Alex. "Blockchain and Crypto: Will Security Issues Finally Be Dealt With in 2020?" *Cointelegraph*, Cointelegraph, 9 Jan. 2020, cointelegraph.com/news/blockchain-and-crypto-will-security-issues-finally-be-dealt-with-in-2020.

Jordan Heal January 20, 2019, et al. "Five Security Concerns Faced by the Cryptocurrency Community." *Coin Rivet*, 20 Jan. 2019, coinrivet.com/guides/what-are-cryptocurrency-security-issues/six-security-concerns-faced-by-the-cryptocurrency-community/.

Rouse, Margaret. “What Is Wallet? - Definition from WhatIs.com.” *WhatIs.com*, TechTarget, 31 Jan. 2006, whatis.techtarget.com/definition/wallet#:~:text=A%20wallet%20is%20a%20small%20software%20program%20used%20for%20online%20purchase%20transactions.&text=When%20the%20consumer%20selects%20%22Pay,in%20the%20Wallet%20and%20clicks.

Vinayak, Heena. “Crypto Under Attack: The Five Worst Hacks That Shook the Crypto World.” *Cointelegraph*, Cointelegraph, 4 Nov. 2019, cointelegraph.com/news/crypto-under-attack-the-five-worst-hacks-that-shook-the-crypto-world.

Raymond Pompon, Sander Vinberg. “Cryptocurrency Hacks 2019.” *F5 Labs*, 11 Sept. 2019, www.f5.com/labs/articles/threat-intelligence/cryptocurrency-hacks-2019.

Palmer, Daniel. “Hacked BITpoint Exchange to Refund 50,000 Affected Users in Crypto.” *CoinDesk*, CoinDesk, 17 July 2019, www.coindesk.com/hacked-bitpoint-exchange-to-refund-50000-affected-users-in-crypto.

Alexandre, Ana. “Four Fake Cryptocurrency Wallets Found on Google Play Store.” *Cointelegraph*, Cointelegraph, 15 Nov. 2018, cointelegraph.com/news/four-fake-cryptocurrency-wallets-found-on-google-play-store.

“Frequently Asked Questions.” *Bitcoin*, 2020, bitcoin.org/en/faq#general.

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.

Orcutt, Mike. “How Secure Is Blockchain Really?” *MIT Technology Review*, MIT Technology Review, 25 Apr. 2018, www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/.

Orcutt, Mike. “Once Hailed as Unhackable, Blockchains Are Now Getting Hacked.” *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

Psaila, Sandro. “Cryptocurrency Security Standard (CCSS).” Deloitte, 26 Jan. 2018.

Regan, Joseph. “Is Bitcoin Safe?: 3 Reasons Bitcoin Is (Mostly) Secure.” *AVG*, AVG Technologies, 2019, www.avg.com/en/signal/is-bitcoin-safe#:~:text=Reason%20%231%3A%20Bitcoin%20is%20encrypted,happen%20on%20the%20Bitcoin%20system.

Reiff, Nathan. “Blockchain Explained.” *Investopedia*, Dotdash, 5 Feb. 2020, www.investopedia.com/terms/b/blockchain.asp.

Reiff, Nathan. “Protect Your Bitcoins Against Theft and Hacks.” *Investopedia*, Dotdash, 29 Jan. 2020, www.investopedia.com/tech/ways-protect-your-bitcoin-investment-against-theft-and-hacks/.

Barone, Adam. “The Future Of Cryptocurrency.” *Investopedia*, Investopedia, 3 May 2020, www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp.

Efrima, Adam. “Council Post: Five Predictions For The Future Of Blockchain And Cryptocurrency.” *Forbes*, Forbes Magazine, 13 June 2019, www.forbes.com/sites/forbestechcouncil/2019/06/13/five-predictions-for-the-future-of-blockchain-and-cryptocurrency/#5448424665a9.

Newsround. “Guide: What Is Bitcoin and How Does Bitcoin Work? - CBBC Newsround.” *BBC News*, BBC, www.bbc.co.uk/newsround/25622442.

Psaila, Sandro. Senior Manager spsaila@deloitte.com.mt +356 23432000 . “Cryptocurrency Security Standard (CCSS): Bridging the Confidence Challenge: Deloitte Malta: Technology.” *Deloitte Malta*, 5 Nov. 2018, www2.deloitte.com/mt/en/pages/technology/articles/mt-article-cryptocurrency-security-standard-CCSS.html.

Sharma, Rakesh. “What Does Government Regulation Mean for Privacy-Focused Cryptocurrencies?” *Investopedia*, Investopedia, 29 Jan. 2020, www.investopedia.com/news/what-does-increased-government-regulation-mean-privacyfocused-coins/.

“Stanford Online.” What Does the Future Hold for Cryptocurrency? | Stanford Online, 2019, online.stanford.edu/future-for-cryptocurrency.

Watkins, Jonathan. *The TRADE Crypto*, www.thetradenewscrypto.com/current-crypto-ecosystem-not-yet-viable-institutional-investors-says-northern-trust/.

Szmigiera, M. “Number of Blockchain Wallets 2020.” *Statista*, 19 May 2020, www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/.

Milewski , Dennis. “HSB Survey Finds One-Third of Small Businesses Accept Cryptocurrency.” *Business Wire*, 15 Jan. 2020, www.businesswire.com/news/home/20200115005482/en/HSB-Survey-Finds-One-Third-Small-Businesses-Accept.