

Systematic Analysis of Cryptocurrencies, Mining Techniques and Improving Existing Security for Cryptocurrencies.

**Table of Contents**

[1 Introduction 6](#_Toc44841856)

[1.1 Background Information 6](#_Toc44841857)

[1.2 Historical Background 8](#_Toc44841858)

[1.2.1 The Birth and Evolution of Cryptocurrencies 10](#_Toc44841859)

[1.2.2 Technical Foundations 10](#_Toc44841860)

[1.2.3 The Virtual Currencies Preceding the Bitcoin 12](#_Toc44841861)

[1.2.4 The Bitcoin Era and Modern Cryptocurrency 13](#_Toc44841862)

[1.3 The Most Common Cryptocurrencies 14](#_Toc44841863)

[1.3.1 Bitcoin 14](#_Toc44841864)

[1.3.2 Ethereum 16](#_Toc44841865)

[1.3.3 Ripple 18](#_Toc44841866)

[1.3.4 Litecoin 19](#_Toc44841867)

[1.3.5 IOTA 20](#_Toc44841868)

[1.3.6 NEO 21](#_Toc44841869)

[1.3.7 Dash 22](#_Toc44841870)

[1.4 Problem Statement 23](#_Toc44841871)

[1.5 Aim and Objectives 24](#_Toc44841872)

[1.6 Research Questions 25](#_Toc44841873)

[1.7 Study Hypotheses 26](#_Toc44841874)

[1.8 Rationale of the Study 27](#_Toc44841875)

[1.9 Scope of the Study 28](#_Toc44841876)

[2 Literature Review 29](#_Toc44841877)

[2.1 Cryptocurrency Valuation 29](#_Toc44841878)

[2.2 Cryptocurrency Trading Pairs 32](#_Toc44841879)

[2.3 Legitimacy of Transactions 34](#_Toc44841880)

[2.4 Adequate Familiarity with the Team 36](#_Toc44841881)

[2.5 Extensive Research on the Whitepaper 39](#_Toc44841882)

[2.6 Token Sale as an Indicator of Legitimacy 40](#_Toc44841883)

[2.7 The Feasibility of Cryptocurrencies 41](#_Toc44841884)

[2.8 Methodology 42](#_Toc44841885)

[2.9 Security Issues in Cryptocurrencies 43](#_Toc44841886)

[2.9.1 Findings and Discussions 44](#_Toc44841887)

[2.9.3 Proof-of-Work 46](#_Toc44841888)

[2.9.4 Proof-of-Stake 48](#_Toc44841889)

[2.9.4 Malicious Proof-of-Work in Cryptomining 50](#_Toc44841890)

[2.9.5 Distributed Denial-of-Service (DDoS) Attack 51](#_Toc44841891)

[2.9.6 Sybil Attacks 53](#_Toc44841892)

[2.9.7 Transport Layer Security (TLS) 53](#_Toc44841893)

[2.9.8 TLS Handshake 54](#_Toc44841894)

[2.9.9 Poisoning Attacks 54](#_Toc44841895)

[2.8.1 Virtual Wallets 56](#_Toc44841896)

[2.8.2 Wallet Vulnerability 56](#_Toc44841897)

[3 The Blockchain Technology 58](#_Toc44841898)

[3.1 Problem with Blockchain 60](#_Toc44841899)

[3.2 How the Blockchain Technology Works 62](#_Toc44841900)

[3.2.1 Proof-of-Work (PoW) Algorithm and the Functioning of Blockchain 64](#_Toc44841901)

[3.2.2 Proof-of-Stake (PoS) 65](#_Toc44841902)

[3.3 Proposed Solution to Blockchain Scalability Problem 66](#_Toc44841903)

[3.3.1 Face Recognition System 66](#_Toc44841904)

[3.3.2 OpenFace 69](#_Toc44841905)

[3.3.3 Implementation of OpenFace in Virtual Wallets 70](#_Toc44841906)

[3.3.4 Front End 71](#_Toc44841907)

[3.3.5 Backend 71](#_Toc44841908)

[3.4 Speech Recognition System 71](#_Toc44841909)

[3.5 Protecting Transactions in Blockchain 73](#_Toc44841910)

[3.6 Blockchain and the Cloud 75](#_Toc44841911)

[3.6.1 Other Security Issues 77](#_Toc44841912)

[3.6.2 Security of Software Wallets 79](#_Toc44841913)

[4 Hardware Wallets 79](#_Toc44841914)

[4.1 Ledger Nano X 80](#_Toc44841915)

[4.2 Physical Unclonable Functions (PUF) 80](#_Toc44841916)

[4.3 General Security of Hardware Wallets 81](#_Toc44841917)

[5 Machine Learning 86](#_Toc44841918)

[6 The Economic Effects of Cryptomining on Cryptocurrencies 87](#_Toc44841919)

[6.1 The future of Cryptocurrency 89](#_Toc44841920)

[7 Conclusion 90](#_Toc44841921)

**Abstract**

One of the major impacts of globalization is that it makes it possible for people to conduct business across borders regardless of their geographical isolations. Social media has enabled businesses to overcome the geographical barriers to accessing foreign markets. In the current society, it is easier for organizations or individual sellers to access foreign markets without having to operate as multinational corporations. Therefore, people can now access services offered by overseas sellers without having to travel to the sellers’ premises. Products such as software, consultancy services, and even physical products have become easier to access from any part of the globe.

Digital evolution has also created a situation where more advanced methods of doing business are becoming more necessary to avoid the challenges associated with the traditional techniques. The concept of cryptographed transactions existed for decades. The idea of living in a society in which no physical currencies are used was proposed by the technology’s enthusiasts several decades ago. However, earlier attempts to implement these ideas were opposed by several barriers including security concerns and the legitimacy of cryptocurrencies transactions. According to a 2017 study that was done by ICO Advisory Firm Satis Group indicates that approximately 80% of initial coin offerings conducted in 2017 were scams.

Systematic Analysis of Cryptocurrencies, the Techniques Used for Mining,

and How Can They be Solved

# Introduction

## Background Information

Cryptocurrency continues to become one of the most sought after technologies in the modern corporate sector. It continues to attract the interests of even individuals who are not directly involved in the business sector. The application of this type of technology is expected to continue rising in the near future.

According to Caleb Chen, a renowned Bitcoin Advocate at London Trust Media, most national governments are expected to implement laws that drive their nations toward a cashless society (Rosic, 2018). These governments will encourage the use of centralized digital currencies. Additionally, there will be a significant increase in the use of decentralized cryptocurrencies that have always been perceived as hard money (Rosic, 2018).

The term cryptocurrency can be used to refer to an internet-based medium of exchange that facilitates financial transactions through the use of cryptographic functions. Some of the most popular cryptocurrencies are Bitcoin, Ethereum, Ripple, Bitcoin Cash, NEM, Litecoin, IOTA, NEO, Dash, Qtum, Monero, and Ethereum Classic. In the final quarter of 2017, as cryptocurrencies value surged, so did the number of cybercriminal attacks on cryptocurrency transactions (Symantec Blogs, 2020). The need for secure technology became apparent and resulted in the use of blockchain technology: a format of storing records known as blocks connected in chains, each block contains specific information of its users along with a unique serial number defined as a hash. The first block is called Genesis block which forms the entire chain. A chain contains sets of several blocks, each block must have its unique hash number connected to the previous block by having the same block’s unique hash number. If any block in a chain is tampered with by cybercriminals, it immediately deletes the chain by changing the unique hash number assigned to each block.

When using Bitcoins as means of payment, each of the associated transactions is verified and stored in a shared database known as the blockchain (Bit Degree, 2020). Blockchain contains encrypted information such that it can only be decrypted by the owner of a given Bitcoin even though it remains visible to everyone (Bit Degree, 2020). Each of the individuals who own Bitcoins within the database are issued with a private key, which they can use to decrypt the Bitcoins owned by them (Bit Degree, 2020).

Every blockchain that contains Bitcoin-related transactions is run by many individuals and organizations that take part in the associated transactions. Each of the Bitcoin owners possess computers, known as nodes, on which they run the software responsible for processing transactions within a given blockchain (Bit Degree, 2020). When nodes are rewarded for the verification of transactions, the users are said to have earned new Bitcoins (Bit Degree, 2020).

The process by which users run the verification software on their respective nodes is known as mining, while the nodes on which they run such software are described as miners (Bit Degree, 2020). The entire process is analogous to the situation where actual miners are rewarded with new gold while operating in mine fields (Bit Degree, 2020). When information describing any transaction is availed into the blockchain, it is verified by the nodes using the Proof of Work (PoW) algorithm such that new Bitcoins are given to the node that is first to verify the transaction information in the block. Overall, Bitcoin is a typical representation of blockchain technology due to its high level of decentralization.

Blockchain technology remains one of the key factors of the success of cryptocurrency. Through this medium of exchange, blockchain technology is leveraged to enjoy important features, like transparency, immutability, and decentralization (Rosic, 2018). Due to blockchain technology, cryptocurrency and the associated transactions do not require the control of a third-party trustee. It is completely decentralized, therefore it is immune to the traditional methods of interference and control (Rosic, 2018).

When using cryptocurrencies in business transactions, the transacting parties can deliver payments to their preferred recipients using keys that can either be private or public, depending on the nature of arrangements between them. Another benefit of transactions in cryptocurrencies is that they require low transaction fees. Consequently, this type of currency allows the transacting parties to avoid the hefty fees that are charged by the conventional financial institutions, like banks (Rosic, 2018). Thus, this type of currency is popular, not only due to its capacity to provide security and confidentiality but also because of its ability to lower the cost of financial transactions. Furthermore, blockchain unlike any other decentralized applications use about 6,000 validators or also known as miners on a daily basis to validate and update ledger on blockchain; this process is called proof of work.

## Historical Background

The idea of using cryptographed mediums of exchange dates back to several decades. The first attempts to establish this type of currency were observed in the 1990s when a significant technology boom was witnessed. This boom led to the birth of systems, such as DigiCash, Beenz, and Flooz (Martucci, 2020). However, these early digital currencies failed to succeed in the market due to challenges such as financial difficulties, rivalries among employees and their superiors, and fraud (Martucci, 2020).

One of the main differences between the earlier versions of digital currency and the current versions is that the former was characterized by third-party trustees whose responsibilities were to verify and facilitate the transactions involved (Martucci, 2020). This feature remains one of the weaknesses of the earlier forms of digital currency because it deprived the users of the right to anonymity (Martucci, 2020). The massive failure of the earlier attempts to create cryptocurrencies discouraged the experts involved, leading to reduced inspiration to pursue related technologies at that time.

The interest in the digital currency technology was reignited in 2009, when Bitcoin was introduced by a group of unknown programmers who operated under the pseudo name, [Satoshi Nakamoto](https://en.bitcoinwiki.org/wiki/Satoshi_Nakamoto) (Martucci, 2020). Upon its introduction, Bitcoin was intended to operate as a peer-to-peer system of electronic cash. The Bitcoin technology came with a unique feature that differentiated it from the earlier versions of digital currency. They were completely decentralized, an implication that they were not connected to any servers. Additionally, the Bitcoin streams did not rely on third-party trustees for validation and verification, as they lacked any form of centralized control systems.

According to Martucci (2020), the Bitcoin technology was inspired by the characteristics of peer-to-peer networks of sharing files. Before the birth of the Bitcoin technology, the concept of cryptocurrency had always existed as a digital construct. The earlier proponents of this technology suggested that cutting edge principles in computer science and mathematics could be used to invent digital currencies. They argued that the introduction of digital currencies would solve both the political and practical problems associated with traditional currencies (Martucci, 2020). Thus technologies, such as the Bitcoin are the result of the implementation of ideas that were previously regarded as theoretical constructs.

### The Birth and Evolution of Cryptocurrencies

Cryptocurrencies were introduced into the market around 2010 and soon they became applicable in various contexts. As highlighted above, the idea of digital currency had existence as theoretical constructs even before experts thought of its actualization. Its implementation began with the introduction of simple forms of digital currencies, most of which were never successful, before advancing to the more sophisticated versions that dominate the global markets today. Therefore, the history of digital currencies can be categorized into three stages, technical foundations, the pre-Bitcoin virtual currencies, and the modern cryptocurrency boom.

### Technical Foundations

The progressive developments that have been witnessed in digital currency technologies all stem from technical grounds that were established decades ago. The technical background can be traced back to the early 1980s when the blinding algorithm was invented by David Chaum, an American cryptographer (Martucci, 2020). This algorithm has remained a critical part of all web-based encryption systems even to the present date (Martucci, 2020).

The initial reason behind the development of this algorithm was to facilitate the exchange of information between parties in a manner that was both unalterable and more secure. It laid grounds on which future work in electronic money transfers would be based. Any currency that was transferred from one party to another using the blinding algorithm was then referred to as the “blinded money” (Martucci, 2020).

Alongside other enthusiasts in this field, Chaum tried to commercialize the concept of cryptographed money transfer or the blind money technology. During the late 1980s, he moved to the Netherlands where he started a company known as DigiCash, which was actively involved in the commercialization of currencies using the blinding algorithm (Martucci, 2020). Even though this company was involved in the production of digital currencies, it did not have a decentralized control like Bitcoin and other cryptocurrencies in the modern society. It monopolized and controlled the production, supply, and use of blind currencies using the same concepts used by central banks to control regular fiat currencies (Martucci, 2020).

Even though Chaum’s company was initially allowed to deal directly with clients, this practice was prohibited after being criticized by the Dutch central bank. Consequently, it was only allowed to deal with banks that were licensed to take part in such transactions (Martucci, 2020). After refusing a lucrative deal proposed by Microsoft for the two organizations to work together, DigiCash went bankrupt in the late 1990s (Martucci, 2020).

Chaum’s company inspired other engineers and thinkers, like Wei Dai and Nick Szabo to propose the continued production of these more secure forms of digital currencies. Nich Szabo even managed to develop and release a special type of cryptocurrency, which he referred to as Bit Gold (Martucci, 2020). Both pioneers suggested the introduction of digital currencies that used the blockchain technology for the purposes of anonymity and security. However, these attempts ended up in total failure as none of the proposed or developed ideas withstood the test of time.

### The Virtual Currencies Preceding the Bitcoin

After Chaum’s company went bankrupt most researchers became less interested in studying the concept of electronic financial transactions. Even investors were reluctant to employ their resources in such studies or related projects. Instead, a lot of research was initiated on conventional methods of money transfer using digital interfaces such as PayPal, Cash App and Venmo. Despite the fears that discouraged more individuals from any further investments in the production of cryptocurrency, several organizations, described as imitators of Chaum’s company emerged during this time (Martucci, 2020).

A typical example of such an organization was WebMoney, a Russian organization following Chaum’s lead (Martucci, 2020). The United States also followed similar trends, leading to the introduction of E-gold, the most popular digital currency in the country between the late 1990s and early 2000s (Martucci, 2020). The currency was developed, commercialized, and controlled by an organization known as E-gold, which was based in Florida (Martucci, 2020).

E-gold, began as a private company that used digital currencies to purchase jewelry. The typical customers mailed in old jewelry, coins, and trinkets to the companys’ warehouses in exchange for e-gold (Martucci, 2020). The E-gold units earned by the users could be traded with other e-gold holders, exchanged for actual gold, or traded for actual cash (Martucci, 2020).

During the peak of its popularity and operation, E-gold boasted millions of active accounts and billions of dollars of money processed on an annual basis (Martucci, 2020). These developments were encountered by the company in the mid-2000s when it was one of the most trusted cryptocurrencies in the United States (Martucci, 2020).

Nevertheless, the company had weak systems and protocols for maintaining security and protecting transactions. Consequently, it became an easy target for hackers and scammers, forcing its customers into incurring hefty financial losses. By the late 2000s, the company was subjected to pressure from experts, organizations, and other public figures who campaigned against its legality, leading to its eventual collapse.

### The Bitcoin Era and Modern Cryptocurrency

The modern cryptocurrency technology was initiated by the introduction of Bitcoin. It is also regarded as the first means of exchange with user anonymity, blockchain system of record keeping, decentralized control, and built-in scarcity (Martucci, 2020). It is also renowned for being the first cryptocurrency with these characteristics to be traded publicly.

As highlighted in earlier sections of this chapter, the technology was drafted for the first time in 2008. It was first presented on white paper by a group of programmers operating under the pseudo name, Satoshi Nakamoto (Martucci, 2020). The group began to commercialize their idea in 2009 and they enjoyed a wide reception from enthusiasts from all over the world. The supporters of the technology began to use Bitcoin through mining and exchange (Martucci, 2020). The success enjoyed by the Bitcoin encouraged several other firms to develop similar technologies.

Towards the end of 2010, several cryptocurrencies had been developed and released into the market. Such currencies include the renowned Bitcoin alternatives, such as Litecoin. Bitcoin also experienced its first appearance in the public exchange during late 2010. WordPress was the first corporate merchant to embrace the Bitcoin technology as it accepted payments using this cryptocurrency (Martucci, 2020). This company began to accept and process payments in Bitcoin by late 2012 (Martucci, 2020). Its decision to accept this currency inspired other organizations, like Expedia, Microsoft, and [Newegg.com](https://www.newegg.com/bitcoin) to adopt the same means of payment from their clients.

Bitcoin offers many advantages, such as anonymity, confidentiality, security, and reduced costs of transactions. Consequently, several merchants from various parts of the world accept it as a secure and legitimate method of payment. Overall, cryptocurrencies have undergone a series of developmental changes, leading to the collapse of some currencies and the success of others, such as Bitcoin and Litecoin, among several others.

## The Most Common Cryptocurrencies

The use of cryptographic methods of transaction has undergone a series of evolutionary changes, leading not only to the development of the initially established currencies, but also to the birth of new ones. As of 2020, there are more than ten cryptocurrencies that are used in cryptographed transactions in different parts of the globe. They include Bitcoin, Ethereum, Ripple, Bitcoin Cash, NEM, Litecoin, IOTA, NEO, Dash, Qtum, Monero, and Ethereum Classic.

### Bitcoin

Bitcoin is regarded as the most popular cryptocurrency, as it was the first ever cryptocurrency to be established. According to Bit Degree (2020), a Bitcoin is a digital currency that allows people to conduct business transactions without the use of fiat cash (Bit Degree, 2020). As highlighted in the previous sections, Bitcoin is the most popular cryptocurrency in the world. It is the most widely used type of digital currency with a popularity that is more than ten times that of the second most preferred alternative. The currency’s market cap is also ten times larger than that of Ethereum, which is the second most valuable digital currency (Bit Degree, 2020).

Due to the perceived trustworthiness of this currency, many companies have embraced it as one of their preferred methods of payment. Organizations that support the credibility and legality of the currency accept it as a means of payment from their clients. This currency, according to Bit Degree, can be sent as a gift or used to pay for goods and services (Bit Degree, 2020). It performs the same purposes as actual money except that it is a virtual medium of exchange (Bit Degree, 2020).

Just like other forms of digital currency, Bitcoin is completely decentralized, an implication that no third-party trustees are needed for verification and validation of the associated transactions (Bit Degree, 2020). All the transactions involving Bitcoin constitute peer-to-peer networks since they occur directly between the transacting parties without any external interference. Bitcoin enables parties to engage in transactions within peer-to-peer networks because it uses the blockchain technology (Bit Degree, 2020).

The blockchain technology was introduced by Bitcoin to ensure that the transacting parties can send and receive payments without requiring the interventions of third parties (Bit Degree, 2020). The benefit of the currency’s decentralized nature of transactions is that it guarantees the anonymity of the transacting parties. According to Bit Degree (2020), the transacting parties do not need to reveal their identities because they are not answerable to third-party trustees.

### Ethereum

Ethereum is completely programmable and was developed to encourage the growth of technologies that are incompatible with the Bitcoin technology. Ethereum permits the development of both smart contracts and Decentralized Applications (DApps), in a more secure and reliable manner. The system prevents such contracts and DApps from being negatively affected by issues, such as fraud, third-party interference, downtimes, and control (Reiff, 2020).

The applications that are on the Ethereum system are designed to run on Ether, the system’s token that is platform-specific (Reiff, 2020). Ether, which is regarded as one of the key functional units of the Ethereum system, provides a platform for application developers to develop and run such applications within the system (Reiff, 2020). It is also used by investors as a means of safely purchasing other cryptocurrencies in a safe manner (Reiff, 2020). Since its launching in the year 2015, Ethereum has undergone rapid growth, making it the second largest cryptocurrency technology by market cap, only second to Bitcoin (Reiff, 2020).

However, the gap between Ethereum and Bitcoin remains significantly large. A survey conducted in January 2020 revealed that Ethereum’s market cap size is still only a tenth that of Bitcoin (Reiff, 2020). One of the company’s largest successes was in 2014 when it launched a pre-sale for ether. The pre-sale triggered a significant response from the target market, a condition that enabled the company to establish itself in the age of initial coin offering (ICO) (Reiff, 2020).

Ether, according to Ethereum, is a useful tool for codification and decentralization while facilitating the security of user’s data and financial records (Reiff, 2020). Ethereum, like most cryptocurrencies, makes great use of blockchain technology that relies on complex algorithms. In addition to these algorithms , blockchain technology employs individuals, organizations and major internet providers and services that verify each transaction known as Proof of work

According to an article published by Investopedia, a total of 18 million ether are validated each year by miners that are paid for each transaction or distributed ledger which is updated on the platform. On the other hand, in 2018, during a U.S. Securities and Exchange Commission’s Conference, the Director of Corporate Finance, William Hinman, revealed in a speech that Ether failed the Howey test[[1]](#footnote-1) ( David Benger, 2018) and, therefore Ether is not considered a security platform on its own but more of a utility that connects the user with blockchain.

The company decided to divide itself into Ethereum and Ethereum Classic as a response to the 2016 Decentralized Autonomous Organization (DAO[[2]](#footnote-2)) attack (Reiff, 2020). This decision has proved to be beneficial to the company since it boasted of a per-token value of $142.54 and a corresponding market cap of $15.6 billion by January 2020.

Overall, Ethereum remains one of the most successful Bitcoin alternatives and one of the fastest growing cryptocurrencies of the modern times. Ether, the main platform that has been commercialized by the company, is responsible for a significant part of its success. Besides offering a secure path platform on which DApps can be built and run, Ether also promotes a secure purchase of other cryptocurrencies.

### Ripple

Ripple is a relatively unique type of cryptocurrency because it does not employ the decentralized technology as a means of reaching transaction consensus network-wide. In one sense, Ripple is more of a trusted partner just like Paypal, WesternUnion, and Cash App, this feature counts for most of its great successes. Ripple recently partnered with the American multinational financial services corporation Nasdaq-Listed Firm that was valued in 2014 at 4.2 Billion United States Dollars.

Although Ripple is a faster method than Bitcoin, this currency is relatively more vulnerable to hacking than Bitcoin. Just like Bitcoin and Litecoin, Ripple also uses blockchain technology. However, it was established to serve a relatively different purpose from the previous two currencies.

According to Bit Degree (2020), this currency is a blockchain that was developed to help financial institutions, like banks to conduct their transactions (Bit Degree, 2020). Thus, the currency is sometimes referred to as the banker’s coin due to its centralized features that introduces it more like a correspondent bank (Bit Degree, 2020). Therefore, as mentioned above this feature attracts more financial institutions to adopt Ripple into their operations.

Ripple eliminates the hefty fees used by banks to process transactions and is a faster method of payment. Apart from the deals Ripple is working on at the moment, it already boasts of several partnerships not only with major financial organizations across the globe but also with governments which allows for more success and development (Bit Degree, 2020). Nevertheless, the currency’s main challenge is that it is not decentralized, which is a mandatory requirement for any digital currency (Bit Degree, 2020).

Instead, all its tokens are owned by Ripple Labs, which is also regarded as the third-party trustee for all the parties involved in the related transactions. Centralization implies that the transacting parties have to entrust a third-party trustee with the roles of verifying transactions. Consequently, users of this currency find it impossible to operate anonymously.

### Litecoin

Litecoin was part of Bitcoin Cryptocurrncy but later it split to improve upon what Bitcoin had created. Litecoin is considered as an alternative to Bitcoin as it offers the digital silver, which is a cheaper version of Bitcoin’s digital gold technology. Litecoin basically uses the same technology that was originally used by Bitcoin. Many people would refer to Litecoin as the younger brother of Bitcoin and its main purpose of creation was to serve as a backup if Bitcoin failed. Litecoin is yet to find its primary destination and has no primary goal or objective like other cryptocurrencies.

Litecoin was separated from Bitcoin when its update was offered (Bit Degree, 2020). However, due to its capacity to provide solutions to most cryptocurrency challenges, like scalability, the Lightning Network[[3]](#footnote-3) will improve Litecoin’s overall efficiency by enabling it to process a significantly larger number of transactions per second than it does now (Bit Degree, 2020). Additionally, Litecoin transactions are cheaper, which makes them more efficient and considerable than Bitcoin, especially when dealing with transactions which involve smaller amounts (Bit Degree, 2020). Overall, Litecoin not only offers high scalability but also offers benefits, like cost efficiency and relatively faster speed.

### IOTA

IOTA also requires its users to perform Proof of Work, which is intended to approve two transactions (Rosic, 2018). This feature implies that the currency has eliminated dedicated miners from its processes (Rosic, 2018). IOTA is another platform that uses a different form of blockchain compared to conventional cryptocurrencies.

Instead of the regular blockchain technology, IOTA uses the directed acyclic graph (DAG) (Sharma, 2019). The technology comes with benefits, such as infinite scalability, secure data transfer, zero fees, and speedy transactions (Sharma, 2019). These characteristics are attributed to the system’s typical features, which encompass tangle[[4]](#footnote-4) and quantum-proof protocol[[5]](#footnote-5) (Sharma, 2019). The system also offers an unlimited number of transactions that can be confirmed in a given unit time within the network (Sharma, 2019).

Instead, the speed of the network increases with an increase in the number of transactions (Sharma, 2019). According to Sharma (2019), IOTA was established to facilitate data exchange between recording machines that are parts of the Internet of Things (IoT) (Sharma, 2019). Users of this transaction must always validate two previous network transactions before they can proceed with new transactions (Sharma, 2019).

In contrast, Bitcoin employs trusted individuals and parties to validate transactions and connect the block in one chain known as distributed ledger which all parties involved will have a copy of; this feature makes Bitcoin more secure than other cryptocurrencies. This high level of validation on the Bitcoin’s side attracts investors and developers to adopt such technology, however this validation process can take up to ten minutes to process a single transaction.

Just like Ripple, IOTA offers solutions to typical cryptocurrency issues, such as the congestion of blocks, network delays, and scaling issues, which are common in Bitcoin transactions (Sharma, 2019). Overall, IOTA is another cryptocurrency that is intended to relieve users of the challenges associated with Bitcoin-related transactions.

### NEO

NEO is one of the most successful cryptocurrencies of Chinese origin and it provides smart contract systems that facilitate the development of financial contracts and the associated apps under a single embedded system (Rosic, 2018). Neo is an open-source platform that uses blockchain technology alongside digital identities to digitize and automate the management of assets using smart contracts (Bowden, 2029). It uses distributed network systems to develop a smart economy. The platform achieves this objective through the construction of infrastructures for the next-generation internet (Bowden, 2019).

The company also tries to establish a concrete foundation for the adoption of blockchain technology in large scales (Bowden, 2019). Each of the dozens of cryptocurrencies that are available in the market aims to attain a specific objective. NEO’s primary objective is to reach out to traders, an objective that it has attained with success over the past few years. According to Bowden (2019), the company has attracted the interest of traders because it is determined to implement improvements on the foundations that were established by Ethereum (Bowden, 2019).

It is intended to improve the efficiency of smart contracts and to accelerate the development of such contracts (Bowden, 2019). Due to its capacity to meet the targeted objectives, this currency is well positioned to become a dominant force in the market, especially in Asia (Bowden, 2019). This currency made its first appearance in the Western market in 2016 when it was still referred to as Antshares (2019). The company attains its blockchain consensus using the delegated Byzantine Fault Tolerant (dBFT)[[6]](#footnote-6) (Bowden, 2019).

In 2016, up to 100 million NEO tokens were created from the 6119 BTC raised during its 2016 ICO (Bowden, 2019). Half of the token created during this ICO were sold while the remaining were distributed to NEO Council (Bowden, 2019). By the end of 2017, the currency had become one of the top 20 cryptocurrencies, as it attained a market capitalization of $5 billion (Bowden, 2019). According to a research conducted by the United States Equity Research, NEOI’s market capital is expected to encounter a 32% growth by 2023 (Bowden, 2019). Overall, NEO is one of the fastest growing cryptocurrencies because traders believe in its capacity to improve smart contracts and also due to its transparency

### Dash

Dash was launched in 2014, previously called darkcoin. is a cryptocurrency designed specifically for daily payments . Indeed , the cryptocurrency’s whitepaper, co-authored by Evan Duffield and Daniel Diaz, describes it as “the first privacy-centric cryptographic currency” based on Nakamoto’s work (Sharma , 2019). Dash's main goal is to become a medium for daily transactions and replace the need for having an ATM card , or carrying cash. For instance, in China the most used application is WeChat; Chinese WeChat links the user’s with his/her bank account and the user will be assigned a unique QR code . Merchants scan the code to take the payment and therefore cashiers can use quick pay to accept payments within 1-2 seconds without the need for any cash or change, increasing efficiency and avoiding cashier errors. Dash is trying to adopt a similar strategy and take it globally.

Dash security is equipped with a protocol that has two tiers, the first of which is similar to bitcoin and utilizes a proof-of-work consensus mechanism. The second tier uses a proof-of-service (PoSe) consensus mechanism, a type of scoring system used to determine if node operators are providing legitimate services.. The second tier of the Dash system contains features known as masternodes that are charged with the roles of relaying transactions and enabling special types of transactions known as the PrivateSend and InstantSend (Rosic, 2018). Through the PrivateSend and InstantSend, Dash system offers complete anonymity and speeds that are higher than Bitcoin’s, respectively (Rosic, 2018).

## Problem Statement

The modern society has evolved to such a stage where cross business borders have become easier to conduct regardless of the distances between sellers and buyers. Businesses rely on media platforms to access their overseas customers. Using the delivery services offered by companies, such as amazon, eBay, and other logistics companies from different parts of the world, shipping products to and from different parts of the world ceases to be a challenge to individual vendors and organizations that deal with customers from all over the world. The services offered by these logistics companies also make it possible for companies or businesses to operate businesses in multiple countries without having to establish offices in such countries. However, these organizations are forced to rely on conventional banking institutions for payment purposes. Banks and other financial organizations that process payments as third party trustees are characterized by low speed of processing payments and hefty transaction charges. financial institutions do not provide decentralization, transparency, and immutability . Additionally, such institutions act as the intermediaries between buyers and sellers, a condition that deprives both the transacting parties of their rights to confidentiality. Digital currencies help to solve all these challenges through the use of decentralized methods of transactions in which the identities of each of the transacting parties remain confidential. Therefore, cryptocurrencies have become the center of attention for researchers and developers. Attempts have been made to ensure that international and local payments are made in a manner that is both swift and cost effective. Although cryptocurrencies leverage the use of blockchain technology , most cryptocurrencies have failed to thrive in the market due to issues, such as lack of awareness, lack of technical skills to understand and use them, security issues, and distrust among the users. The study’s main problem is that a significant portion of cryptocurrency’s target market lacks adequate knowledge about mining techniques, its impacts on the economy, and the general technical knowhow of how to operate using these currencies.

## Aim and Objectives

The main aim of this paper is to use evidence-based strategies to the establishment of both general and technical knowledge about the inner sanctum of cryptocurrencies and the associated security concerns with blockchain where most cryptocurrencies transactions are processed . This paper will use evidence based research along with hands-on skills on the security aspects. Many cryptocurrencies failed due to the reluctance of investors, lack of strategies and security concerns. As many researchers have speculated that 80% of ICO in 2019 were scams, this research will investigate whether this speculation is true. Also, from a cybersecurity standpoint blockchain technology is still vulnerable to cyberattacks. This paper dissects these currencies in terms of their characteristics, origins, operational mechanisms, technical knowledge about their use, and security issues. Through this approach, the study intends to ensure that individuals and organizations who are currently using or planning to use digital currencies in the future are supplied with adequate information on the implications of being part of the cryptocurrency technology. It also provides knowledge that will enable users to understand the changes occurring in the market and react in ways that will enable them to accommodate these changes without incurring any financial losses. The final aim of the thesis is to expose the security concerns and the dangers facing the users of cryptocurrencies, thereby enabling users to take precautions that would enable them to avoid or overcome such challenges. The main objectives of the thesis are in accordance with the following list:

* To analyze cryptocurrencies based on their origins, characteristics, and technical details.
* To analyze the concept of cryptomining, unearthing the most common security issues in cryptocurrency mining.
* To investigate the issues that constitute cryptocurrency security and reveal the most common types of attacks to which such currencies are vulnerable.
* To evaluate the ways in which cryptocurrencies are economically affected by cryptomining.
* Propose new security measures to strengthen the existence security of cryptocurrencies.

## Research Questions

This thesis relies on the use of information to meet its objective of informing the society and scholars about cryptocurrencies, their benefits, how to use them, and the associated security concerns. It tends to solve the stated problem by providing answers to some of the questions asked by critics of the technology. The main study questions are as follows:

* RQ1: What are cryptocurrencies?
* What are the core benefits of using cryptocurrencies in regular business transactions?
* RQ2: What are the main characteristics of cryptocurrencies in terms of value, technical details, history, and market capital?
* What are some of the factors that affect the market value and reputation of cryptocurrencies?
* RQ3: What is cryptomining?
* RQ4: What are some of the security issues surrounding cryptomining?
* What are some of the security concerns facing the use of cryptocurrencies?
* How does cryptomining affect the economic aspects of cryptocurrencies?

## Study Hypotheses

Even though the findings of this study will be revealed by the results obtained from the analysis of the collected data, it is easy to speculate on some of the expected outcomes. These speculations are inspired by theory, public opinion, news, and logical reasoning. This research is based on seven hypotheses as highlighted below:

* *H1*: Cryptocurrencies’ main benefits include confidentiality, anonymity, immutability and low transaction costs.
* *H2*: The main characteristics of cryptocurrencies are similar to those that existed decades ago such as E-gold
* *H3*: One of the main security concerns in the use of cryptocurrencies is cryptojacking.
* *H4*: cryptomining has the effect of boosting the economic value of digital currencies.
* *H5*: Different cryptocurrencies show high levels of variation in terms of value, popularity, and market capital.
* *H6*: a cryptocurrencies transaction is irreversible and decentralized and therefore it is the ideal method of payment used by scammers. The alternative payment methods used before were PayPal, Western Union, credit card. In all these previous payment methods some sort of identification is needed where in cryptocurrencies you can operate anonymously. Moreover, if any of these financial institutions suspect foul play the transaction is subjected to further investigation.
* *H7*: The variations in the values, market capital, and popularity are affected by trustworthiness, simplicity of use, the number of individuals and customers who are already committed to a particular currency.

## Rationale of the Study

As highlighted in the problem statement section, this paper aims to educate the public about the characteristics and benefits of using digital currencies, and also to analyze the security issues that face the use of such currencies. Achieving all these objectives will be of significant benefit to society in various ways. First the decisions made by users will not be influenced by appeals from the developers of these currencies or peer pressure. Instead, they will depend on the users’ individual analysis of the technology based on the benefits, strengths, weaknesses, and cost constraints. As a result of such a transformation, the society will be able to genuinely dissect the use of digital currencies and decide to either accept or reject it based on their perception of the technology’s impacts on the economy. A detailed understanding of the security issues associated with the use of cryptocurrencies will also enable users to take precautions to avoid incurring heavy financial losses. Revealing security loopholes also sets a foundation on which further study on preventative measures can be based. The effect of cryptomining is another important factor that the study introduces. By observing the effects of this process on the economic valuation of cryptocurrencies, it becomes possible to perform a cost-benefit analysis on it and analyze its effects on both the users and service providers. A general and technical analysis of the currency mining process, on the other hand, equips users with adequate knowledge on how to harness the opportunities that come with owning digital currencies and taking part in the related transactions. It also enlightens the users on how to avoid some of the potential dangers that characterize the mining process to ensure that they optimize the associated benefits. Overall, this study intends to educate users and developers on various aspects of digital currencies that are expected to shape their future in terms of value, usability, and overall commitment from consumers.

## Scope of the Study

This research uses the facts, findings, and statistics contained in existing literature and past studies as its main source of information. several references are used as the main sources of information. Only the sources that were polished not earlier than 2000 have been considered for the review process. The entire project consists of the collection, analysis, selection, and review of references that are considered to be relevant to the study. Due to the national emergency lockdown aimed to contain Covid-19, testings were limited because of lack of proper equipment. studies will be collected from various authors and researchers regardless of their geographical locations along with some technical testings done on my personal computer. Only scholars whose works are both relevant and credible will be considered for the selection process. The study’s main deliverable comes in the form of a written report that provides satisfactory and evidence-based answers to the stated questions. This deliverable also provides a solution or recommended solutions to the thesis’ main problem. Some of the major components of the report include a detailed analysis of cryptocurrencies, a review of their characteristics, values, and market capitals, and a review of the main security issues facing the cryptomining process. Overall, the study intends to obtain its data by sampling the findings, statistics, and facts that have been presented by researchers who conducted similar studies in the past before performing a critical analysis to generate new ideas.

# Literature Review

## Cryptocurrency Valuation

The valuation of individual types of cryptocurrency implies that a given can be exchanged for another. However, the rate of exchange depends on the individual value of a given currency within the market. The valuation of each coin is given in USD to make it easier to convert a given cryptocurrency into its equivalent of the other. For instance, the valuation (in USD) of Ethereum determines the rate at which it will be exchanged against the Bitcoin. indeed, the value of cryptocurrencies are affected by the same factors that affect actual stock exchange involving various types of non-cryptographic currencies like the USD, and GBP, and the Euro (see table 1).

Table 1

The Popularity of common cryptocurrencies by market value

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Market Cap** | **Price** | **Volume** | **Circulating Supply** | **Change (24hrs)** |
| Bitcoin | $112,735,453,936 | $6760.98 | $5,136,770,000 | 16,674,425 BTC | -5.43% |
| Ethereum | $29,227,540,706 | $305.58 | $894,988,000 | 95,647,370 ETH | -4.84% |
| Bitcoin Cash | $15,121,119,942 | $901.17 | $4,500,640,000 | 16,779,413 BCH | 37.68% |
| Ripple | $8,088,155,335 | $0.209910 | $140,243,000 | 38,531,538,922 XRP | -3.47% |
| Litecoin | $3,297,343,825 | $61.33 | $294,950,000 | 53,767,732 LTC | -5.75% |
| Dash | $2,601,563,986 | $338.71 | $115,739,000 | 7,680,801 DASH | 3.18% |
| NEO | $1,893,495,500 | $29.13 | $59,589,000 | 65,000,000 NEO | -8.16% |
| NEM | $1,804,086,000 | $0.200454 | $10,806,300 | 8,999,999,999 XEM | -6.32% |
| Monero | $1,675,861,201 | $109.28 | $87,656,500 | 15,335,901 XMR | -8.11% |
| Ethereum Classic | $1,457,787,439 | $14.98 | $299,410,000 | 97,318,182 ETC | 5.69% |
| IOTA | $1,441,775,712 | $0.518712 | $48,539,100 | 2,779,530,283 MIOTA | -5.46% |
| Qtum | $862,271,130 | $11.71 | $132,988,000 | 73,651,804 QTUM |  |

Source: (Rosic, 2018).

## Cryptocurrency Trading Pairs

Traditionally, most people have always believed that cryptocurrencies can only be exchanged for cash. However, there have been remarkable developments in the field of cryptocurrency to such an extent that each of the currencies is assigned a specific value. The exchange rates may vary with time, depending on the performances of each of these currencies in the currency market (see table 2). Furthermore, cryptocurrencies can also be exchanged for goods or services.

Table 1

The exchange rates for various cryptocurrency pairs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Symbol** | **Name** | **Price** | **Change** | **%Change** | **Volume** | **Previous Close** |
| [BTC-BITSTAMP](https://www.cnbc.com/quotes/?symbol=BTC=) | Bitcoin/USD Bitstamp | 5,144.04 | -180.99 | -3.396 | 9,662 | 5,329.7 |
| [BTC-COINBASE](https://www.cnbc.com/quotes/?symbol=BTC.CO=) | Bitcoin/USD Coinbase | 5,144.79 | -297.67 | -5.469 | 39,616 | 5,442.46 |
| [BTC-GEMINI](https://www.cnbc.com/quotes/?symbol=BTC.GM=) | Bitcoin/USD Gemini | 5,145.46 | -303.08 | -5.563 | 4,944 | 5,448.54 |
| [BTC-BITFINEX](https://www.cnbc.com/quotes/?symbol=BTC.BF=) | Bitcoin/USD Bitfinex | 5,142.3 | -304.4 | -5.589 | 15,012 | 5,446.7 |
| [BCH-BITSTAMP](https://www.cnbc.com/quotes/?symbol=BCH.BS=) | Bitcoin Cash/USD Bitstamp | 173.95 | -11.94 | -6.423 | 12,235 | 185.89 |
| [BCH-COINBASE](https://www.cnbc.com/quotes/?symbol=BCH.CB=) | Bitcoin Cash/USD Coinbase | 174.47 | -11.41 | -6.138 | 73,281 | 185.88 |
| [ETH-COINBASE](https://www.cnbc.com/quotes/?symbol=ETH=) | Ether/USD Coinbase | 112.5 | -5.96 | -5.031 | 301,778 | 118.46 |
| [ETH-GEMINI](https://www.cnbc.com/quotes/?symbol=ETH.GM=) | Ether/USD Gemini | 112.47 | -6.16 | -5.193 | 26,479 | 118.63 |
| [ETH-BITFINEX](https://www.cnbc.com/quotes/?symbol=ETH.BF=) | Ether/USD Bitfinex | 112.63 | -6.03 | -5.082 | 97,210 | 118.66 |
| [LTC-COINBASE](https://www.cnbc.com/quotes/?symbol=LTC.CB=) | Litecoin/USD Coinbase | 33.23 | -1.67 | -4.785 | 336,527 | 34.9 |
| [LTC-BITFINEX](https://www.cnbc.com/quotes/?symbol=LTC.BF=) | Litecoin/USD Bitfinex | 33.243 | -1.773 | -5.063 | 65,759 | 35.016 |
| [XRP-BITSTAMP](https://www.cnbc.com/quotes/?symbol=XRP.BS=) | XRP/USD Bitstamp | 0.143 | -0.007 | -4.806 | 162,095,446 | 0.15 |
| [XLM-BITFINEX](https://www.cnbc.com/quotes/?symbol=XLM.BF=) | Stellar Lumens/USD Bitfinex | 0.035 | -0.003 | -7.398 | 784,523 | 0.038 |
| [ZEC-BITFINEX](https://www.cnbc.com/quotes/?symbol=ZEC.BF=) | Zcash/USD Bitfinex | 24.81 | -0.815 | -3.181 | 8,610 | 25.625 |
| [ZRX-BITFINEX](https://www.cnbc.com/quotes/?symbol=ZRX.BF=) | Ox/USD Bitfinex | 0.136 | -0.009 | -6.073 | 289,462 | 0.145 |
| [BAT-BITFINEX](https://www.cnbc.com/quotes/?symbol=BAT.BF=) | Basic Attention Token/USD Bitfinex | 0.115 | -0.005 | -3.783 | 15,029 | 0.119 |

Source: Consumer News and Business Channel (2020).

## Legitimacy of Transactions

Legitimacy is the most important factor for consideration before deciding to become part of the people using digital currencies. Failure to observe this factor exposes people to significant financial dangers because it makes them vulnerable to the activities of scam. According to Reiff (2019), legitimacy refers to the capacity of cryptocurrencies to conform to the required ethical and legal standards. Earlier discussions of the valuation of these currencies have revealed that they are highly valued. It also suggests that their values continue to surge with time. Therefore, they attract high rates of people who would like to make financial gains at the expenses of users (Gagarina, Nestik, & Drobysheva, 2019). One of the most common ways through which malicious persons try to gain financial benefits from this type of currencies is through scam (Gagarina, Nestik, & Drobysheva, 2019). Others are also trying to create fake versions of the most popular currencies with the aim of stealing large amounts of money from the users of these currencies. Consequently, a proper knowledge of the legitimacy of various cryptocurrencies is a critical piece of information for users and the institutions that accept digital currencies and methods of payment from their customers (Gagarina, Nestik, & Drobysheva, 2019). The number of cryptocurrencies that operate in the market keep increasing with time. Increases in the number of currencies, coins, and tokens always result in the emergence of more initial coin offerings (ICO) (Reiff, 2019; Gagarina, Nestik, & Drobysheva, 2019). one very deceptive approach used by scammers is creating cryptocurrency with an identical name of the original cryptocurrency and offering their fake currencies on the market. This approach is similar to someone who is trying to pass fake money.

Another trend that comes with the increasing number of coins and tokens within the market is the increase in demand among investors. The investors from various parts of the world retain their desire to exploit the opportunities that are presented by the emergence of new coins in the market (Reiff, 2019). A combination of factors, such as the birth of new coins, new tokens, and the introduction of new initial coin offers attract the interest of scammers.

Another problem that faces such a situation is that the investors’ heightened hunger to make heavy investment in cryptocurrencies, which is a highly speculative market, is that they remain vulnerable to making investments in fraudulent ICO or tokens (Reiff, 2019). People who invest in the cryptocurrency business, as well as the users of this currency find it very challenging to act in a way that enables them to harness the full potential of the opportunities that come with this line of business while maintaining their safety in the business. According to Reiff (2019; Ornes, 2019), this challenge stems from the fact that cryptocurrency is based on the blockchain technology, which is relatively new and not easily understandable to all people (Ornes, 2019; Esmaeilzadeh & Mirzaei, 2018). Additionally, the speedy rate at which this technology develops makes it difficult for even experienced investors to keep up with the associated changes (Ornes, 2019). Even though there is no specific protocol that can be used to evaluate the legitimacy of cryptocurrencies, the most common methods of telling between legitimate and fraudulent tokes or ICOs include a proper knowledge of the team offering these services, monitoring the token sales, assessing the feasibility of currencies, and extensive research to stay informed about the latest trends in the market and any proposed changes.

## Adequate Familiarity with the Team

The developers of a given currency are regarded as the most important factors determining the legitimacy of such a currency. Alongside the administrators of such services, the currency developers have a direct impression on the capacity of their coins, ICOs, or tokens to conform to legal and ethical standards within their respective regions of operation. When legitimate currencies are introduced into the market, they are only accepted when the creators are known to have followed the required protocols when introducing them into such markets (Pesch & Ishmaev, 2019; Esmaeilzadeh & Mirzaei, 2018). Additionally, the legal reputation of currencies depends on the public image of the creators. Under this criterion, users and investors are advised to ignore digital currencies whose creators remain anonymous and fail to make public declarations about their involvement in the development of such currencies as well as willingness to take responsibility for the security concerns facing their currencies (Pesch & Ishmaev, 2019; Esmaeilzadeh & Mirzaei, 2018). The creators of legitimate currencies always the interests of consumers at hand and will always make public declarations regarding the measures that will be taken to ensure that their clients or the users of their currencies do not incur hefty losses due to poor adherence to security regulations.

The legitimacy of digital currencies, as highlighted above, becomes even harder to determine as more currencies continue to enter the market. According to Reiff (2019; Pesch & Ishmaev, 2019), the digital currency space is characterized by both popular and relatively less popular developers. In such a space, the more established brands, like Vitalik Buterin, the founder of Ethereum, can always support or destroy new brands by having their names listed as a development team (Reiff, 2019). This argument implies that the most established brands, like Bitcoin and Ethereum are also considered as part of the security team. They have already been trusted by investors, individual clients and organizations for such a long time that they are considered to be the pioneers of this market (Reiff, 2019) These developers are also believed to have direct contact and a more inside knowledge about emerging developers than everyone else (Pesch & Ishmaev, 2019; Esmaeilzadeh & Mirzaei, 2018). Consequently, the same that they recommend to investors and consumers of these currencies are believed to be legitimate developers. As a result of such trends, the developers of fake currencies and scammers are developing the tendency of creating counterfeited versions of the reputed brands to help in popularizing their brands (Reiff, 2019; Pesch & Ishmaev, 2019). For instance, a company that creates new coins can decide to develop a fake version of Vitalik Buterin and use it to promote their fake brands. such activities result in situations where investors are misled into incurring heavy financial losses when they put their money into currencies that are created by scammers. Additionally, many investors think that more regulations should be implemented in regards to the offered cryptocurrencies in the market.Most of the regulatory discussion gravitating blockchain has been at the agency level, including the Department of Treasury, Securities and Exchange Commission , Federal Trade Commission , Internal Revenue Service and Financial Crimes Enforcement Network . All the mentioned agencies have had different opinions in regards to the legitimacy of cryptocurrencies. For Instance, the Financial Crimes Enforcement Network in late 2019 started regulating decentralized applications (dApps) (Blog, F, 2020). Also, the IRS has begun considering cryptocurrencies properties and has issued tax guidance accordingly. New York State was the first state to regulate virtual currency companies through state agency rulemaking. As of the year 2020, the US federal government has not exercised its constitutional legislative, executive and judicial power to regulate blockchain (Dolan, 2020).

Investors are advised to take specific actions toward protecting themselves from the actions such as the creation of fake reputed brands to promote or popularize fraudulent tokens. According to Reiff (2019), the most effective method of protecting investors from this type of scam is by conducting a thorough research on the individual creators of the brands in which they intend to invest and make necessary decisions. For instance, funders whose profiles are not available on reputed social media sites, like LinkedIn may not be trusted since they are trying to hide their identities from the public (Reiff, 2019). Reiff (2019) warns that the existence of such profiles is also not enough to confirm the legitimacy of currency developers. Therefore, investors and users who are researching them should continue to verify their rates of activity by assessing common social media features, such as the number of followers or likes accrued by them (Reiff, 2019; Esmaeilzadeh & Mirzaei, 2018). Even the verification of the number of likes and followers should be proceeded with further evaluation, like the extent to which such developers engage with their followers. Conventionally, legitimate developers have busy social media websites since they are always actively involved in interactions with their customers and the followers of their brands (Reiff, 2019). The final step taken to verify the legitimacy of currency developers is a verification of their stated qualifications with existing information (Pesch & Ishmaev, 2019; Esmaeilzadeh & Mirzaei, 2018). Apart from the consistency between the qualifications claimed by the developers, such qualifications must also be relevant to projects in which they are involved. Overall, a proper knowledge of the developers of cryptocurrencies acts as an essential technique of determining the legitimacy of such currencies (Pesch & Ishmaev, 2019). Legitimate currencies are those that are developed by highly qualified individuals whose legitimate credentials are available for access by the members of the public as such people are said to be operating their businesses in the open public without hiding their identities.

## Extensive Research on the Whitepaper[[7]](#footnote-7)

The white paper of a given cryptocurrency or an initial coin offer forms a principal foundation for the information that is known about such a currency or ICO. It refers to the foundational document for the cryptocurrency project (Reiff, 2019). The main components of a typical cryptocurrency whitepaper include background information, strategy, goals, concerns, and the implementation timeline (Reiff, 2019). This document is always a mandatory requirement for all projects that are based on blockchain technology (Reiff, 2019). According to Reiff 92019), evaluating a currency based on this criterion can be very challenging in many ways. For instance, there are companies that obviously lack sound concepts even though they may have ostentatious websites (Reiff, 2019). Additionally, there are companies with properly developed white papers even though their websites are characterized by issues, like spelling errors and other misrepresentations. Therefore, it is necessary to be careful when evaluating a company’s legitimacy on such grounds. Legitimate whitepapers should always contain useful information, like the adopted financial models, SWOT analysis[[8]](#footnote-8), legal issues, and roadmaps for implementing the project’s main objectives (Reiff, 2019; Pesch & Ishmaev, 2019).

Failure to offer a whitepaper is one of the key signs that a company is not legitimate and should be avoided at all cost. Nonetheless, the Whitepaper does not necessarily reflect the legitimacy of a company . For instance, PlexCoin, an illegitimate company in the United States, managed to collect up to $15 million using a fake whitepaper before it was discovered and shut by the [U.S Securities and Exchange Commission (SEC)](https://www.investopedia.com/terms/s/sec.asp) (Reiff, 2019; Esmaeilzadeh & Mirzaei, 2018). A good whitepaper is that which offers answers to stakeholders’ most asked questions, like success drivers of the company, actions that will be taken to meet its principal goals, and how its products are different from those of investors (Reiff, 2019; Pesch & Ishmaev, 2019). The knowledge about a company’s whitepaper is as important as having proper information about the developer of a given cryptocurrency as this information differentiates between legitimate and fraudulent currency providers.

## Token Sale as an Indicator of Legitimacy

Another method through which the legitimacy of a cryptocurrency developer or provider can be evaluated is through an inspection of the token sales made by such an organization or developer. Any agency that offers cryptocurrencies will always depend on a currency system known as tokens to enhance crowdfunding (Reiff, 2019). The companies that provide various cryptocurrency services always avail all the information on token sales available to investors and the public in general (Esmaeilzadeh & Mirzaei, 2018). This method can be considered as another criterion through which the legitimacy of such organizations can be determined, especially considering that only legitimate organizations will prefer to avail such information for public consumption. The token sales registered by a company as the ICO progresses can always be accessed through the providers. The sales trends can also be viewed over time to identify the pattern with which they progress (Reiff, 2019; Stewart, Ilie, D., Zamyatin, Werner, Torshizi, & Knottenbelt, 2018). Any attempts by an organization to prevent investors from charting the ICO progress is a typical sign of scam (Reiff, 2019). Another common practice by scammers is that they hide the progress of their token sales under the pretense of specific contribution addresses (Reiff, 2019). Such activities are considered as signs of scam as they prevent users and potential investors from monitoring the funds that have been raised from token sales and the remaining time in the sale (Reiff, 2019). Scammers also use such techniques to fabricate a sense of urgency among the investors even in cases where there is no evidence of successful sale of tokens (Reiff, 2019; Stewart et al., 2018). Overall, the progress of token sales reflects the legitimacy of a company in the exchange market. Legitimate companies will always make their tokens available for public purchases. Such organizations also avail all the information describing such sales for access by the members of the public and potential investors.

## The Feasibility of Cryptocurrencies

Feasibility is a factor that determines the practicality of all projects. Feasibility studies consist of analyses that focus on the relevance or projects. They also involve studying important aspects of such projects, like legality, technical possibilities, and economic implications (Kenton, 2019). Information about feasibility studies is essential to decision makers as it enables them to conduct cost-benefit analyses of the alternatives at their disposal and make the most suitable alternatives (Kenton, 2019). It also helps people or project managers to evaluate projects in terms of the capacity to implement them without incurring too much losses and encountering severe difficulties (Kenton, 2019). In essence, feasibility studies determine the soundness of a project in terms of the ability to implement it successfully (Stewart et al., 2018). Investors are attracted to ICOs that show signs of the ability to outperform their competitors. They tend to favor such organizations because they offer the best deals and the best rates. Consequently, companies that have shown low capacities to compete effectively in the market have been forced out of business due to their inability to attract investors (Reiff, 2019). Consequently, scammers always try to hype their abilities to make their ICOs attractive to investors.

However, it is worth noting that even ICOs that seem highly successful can collapse if not selected with caution (Reiff, 2019). Therefore, the secret to making successful investment lies with the investors ability to invest in organizations with achievable sets of goals (Reiff, 2019; Esmaeilzadeh & Mirzaei, 2019). Such organizations have goals that are both compelling and achievable over short and long periods into the future (Reiff, 2019). Feasibility is emphasized in the cryptocurrency business because it goes hand in hand with transparency (Reiff, 2019; Esmaeilzadeh & Mirzaei, 2018). The rationale behind this argument, according to Reiff (2019), is that companies that boast of feasible goals and business models are more willing to be transparent with their clients than their counterparts with unattainable ambitions. Legitimate companies, based on feasibility criteria, will always have feasible goals and are willing to update their investors with the latest details of their progress in the market (Stewart et al., 2018). Such updates are made through company websites or social media accounts; they also provide updates of the goals that have already been achieved and the progress made so far.

## Methodology

This study used the literature review as the method of data collection along with great testings on the security aspects of cryptocurrencies. The review process was undertaken in three principal steps. The first step involved the identification of the references that would be appropriate for the project. Several readings were identified from various online libraries, like ResearchGate, ScienceDirect, and online university libraries. The search terms used include cryptocurrencies, the blockchain technology, cryptomining, the popularity of cryptocurrencies, legitimacy of cryptocurrency transactions, security issues in cryptocurrencies, the economic impacts of cryptomining, sybil attacks, DDoS attacks, virtual wallets, hardware wallets, machine learning, proof-of-work, and the future of cryptocurrencies.

The selected references were then evaluated based on credibility, year of publication, and the closeness or relevance to this thesis. Only books, articles, and online sources with the most relevant content were considered for inclusion in the list of sources to be reviewed. This process was done by assessing the closeness of the studied topics or discussed concepts with the search words used in the study. the evaluation process reduced the references to only a few that were considered to be most applicable. The selected references were reviewed by analyzing the information presented and supporting such discussions with auxiliary studies obtained from reliable sources, like journals and magazines.

### 

### 2.9 Security Issues in Cryptocurrencies

Cryptocurrencies are very characterized by high monetary values in the current market. Statistics also indicate that these values are expected to continue increasing with time (Kadyrov, 2019). These trends imply that large sums of money are at stake, especially when the situation is viewed from the investors’ perspectives. Therefore, security remains one of the biggest concerns when dealing with digital currencies. According to Kadyrov (2019), investors and other stakeholders in the digital currency market have lost large sums of money due to the activities of digital thieves who are always determined to interfere with transactions and valuable information for monetary benefits. The cryptocurrency market is occupied by large numbers of investors who take part in various activities at different times (Kadyrov, 2019). All the parties to such transactions are determined to optimize their financial benefits to such an extent that they are never concerned about harsh conditions, like the developers’ reluctance to account for the losses incurred by investors. According to the rules governing the trading of digital currencies, no companies are accountable for the losses incurred from digital theft (Kadyrov, 2019). Therefore, there are no guarantees that the transaction activities and the associated assets are secure, a condition that makes such investments extremely hazardous (Kadyrov, 2019). The increased number of digital currencies used in the cryptocurrency market makes it easier for hackers to invade and steal valuable information from investors (Kadyrov, 2019). According to Kadyrov (2019), the current digital currency market is characterized by over two hundred crypto-exchanges that provide various services. The growing number of crypto-exchanges also imply that decline or hacking of a particular service provider will not cause a drop in the market for its competitors as witnessed in the past (Kadyrov, 2019). Additionally, the regulatory laws that are being implemented by most governments are not adequate to protect all the players in the market. The most common security concerns for cryptocurrencies include wallet vulnerability, cyberattacks, selfish mining, percent attacks, and double spending.

## 2.9.1 Findings and Discussions

After a thorough investigation of cryptocurrencies and the surrounding technology associated with this market, it was determined that cryptocurrencies still lack the properties of actual money. Furthermore, the security measures of cryptocurrencies including the hashing algorithms, cryptomining and blockchain technology are still vulnerable to cyberattacks. There have been minimal efforts from the federal government to regulate cryptocurrencies that are oftentimes used as a legitimate form of payment.

In fact, some of the world's biggest retailers including Whole Foods, Nordstrom, and Starbucks are now accepting cryptocurrency payments in the form of bitcoin, ethereum, bitcoin cash and the Gemini dollar (Cuthbertson, 2019) . Aside from fake offerings of cryptocurrencies some legitimate cryptocurrencies are still struggling to secure their digital assets. On the other hand, sadly some cryptocurrencies offer deceptive information in regards to their application security to gain more investors.

Cryptocurrencies are mostly decentralized which makes it very challenging for agencies to implement regulations. Decentralization is one of the features that makes cryptocurrencies more appealing to investors, yet it lacks transparency. Despite the efforts cryptocurrency developers use to secure their systems including hashing algorithms such as SHA-256, sha-512, directed acyclic graph, PrivateSend & InstantSend, Proof of Work, Proof of Stake, Proof of Authority and cryptoming, the technology is not hack-proof. At the present time, all the previously mentioned technologies alongside blockchain technology securities still have room for enhancement.

Although they are many different possible cyberattacks and weaknesses within the existing technology of cryptocurrencies, the focus here will mainly be on the common attacks and vulnerabilities such as malicious Proof-of-Work (PoW) attacks, Distributed Denial-of-Service (DDoS) Attacks, Sybil Attacks, Poisoning Attacks, Transport Layer Security within blockchain, Transport Layer Security Handshake, and the obvious weakness with the blockchain technology authentication process.

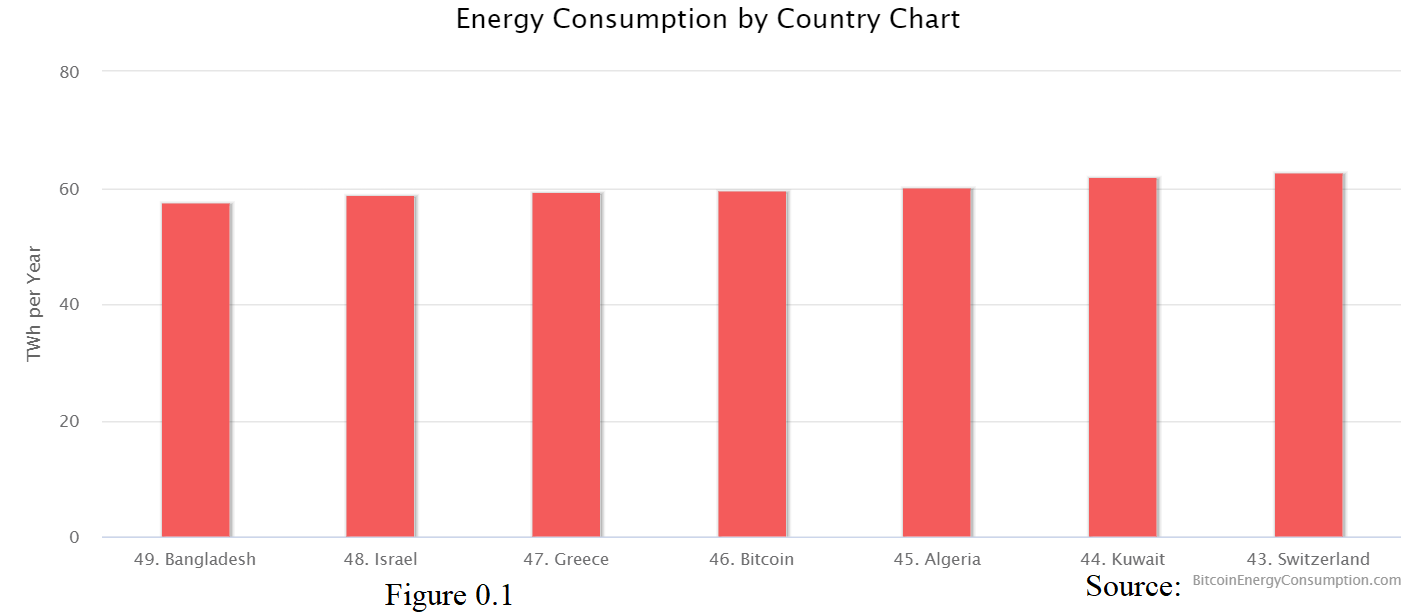
**2.9.2** **SHA-256 Hash Function**

The SHA-256 hash function is one of the most important cryptographic hash algorithms. The cryptographic hash, which is also known as the digest, is a special signature that applies to data files or text (Wustrow & VanderSloot, n.d.). The main function of the SHA-256 is to generate a 256-bit hexadecimal number, which translates to 32-byte signature for a given text (Wustrow & VanderSloot, n.d.). The signature generated by this function can be considered as the text’s identity since it is almost unique (Wustrow & VanderSloot, n.d.). Thus, SHA-256 mainly generates unique signatures that can be used to differentiate one text file from another.

### 2.9.3 Proof-of-Work

The concept of Proof-of-Work (PoW) remains one of the core features of all or most systems that utilize blockchain technology. It is one of the methods used to validate and verify the legitimacy of the parties to various transactions. PoW can be described as the original consensus algorithm in a given blockchain (Wustrow & VanderSloot, n.d.). It enables miners to compete against one another for the completion of transactions on the network so that they can be rewarded accordingly (Wustrow & VanderSloot, n.d.).

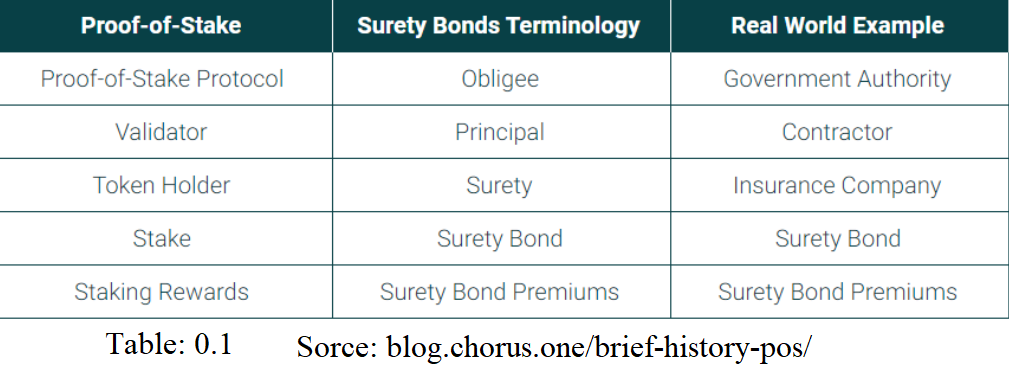
The main activities that occur in a typical mining network is the exchange of tokens amongst the miners (Wustrow & VanderSloot, n.d.). All the transactions that are conducted by the miners are gathered and recorded into a block by a decentralized ledger (Wustrow & VanderSloot, n.d.). Research indicates that powered blockchains constitute more than 90% of the entire current market capitalization. Such studies also refute the claim that the performances of blockchains that are based on the Proof-of-Work strategy can be improved without any negative security consequences. PoW acts as the third party trustee in the centralized financial institutions.

Although the PoW process is an essential security feature of blockchain technology , it consumes a great amount of electricity. Digiconomist reported that Bitcoin mining alone consumes 54 TWH (Digiconomist 2020). To fully understand how huge this number is, 54 TWH is enough to power 5 million households in the US, enough to power the entire country of New Zealand or Hungary. Figure 0.1 below shows that Bitcoin mining consumes more electricity than Algeria ,and Kuwait. 

One of the main reasons why PoW consumes massive amounts of electricity is because PoW gives more rewards to miners with better equipment and therefore the higher hashing rate you have; the greater chance to create the next block. This led some miners to build massive mining centers with better and more equipment. Nowadays, Miners rely on ASICs to mine as many transactions as they possibly can, which led to a great monopoly in the market. Furthermore, miners that share geographical connections starting investing their sources in what is called “Mining Pools”. Ultimately, PoW not only is causing miners to use massive amounts of electricity but also encouraging mining pools which makes the blockchain centralized as opposed to decentralized.

### 2.9.4 Proof-of-Stake

As an alternative to PoW algorithms, PoS was first introduced by QuantumMechanic in 2012 as a secure, and more efficient method to achieve distributed consensus. Peercoin was the first cryptocurrencies to implement the PoS along with PoW. In order for someone to start mining, she/he has to put a security deposit on the nodes network that is why it is called Proof of Stake. The greater deposit you put on the nodes network the greater chance of mining and essentially earning money for each successful transaction completed. For instance, if John deposits 100$ and Ruth deposits 1,000$, Ruth has a great chance of being chosen to validate transactions.

Table 0.1 below shows the easiest way that you can think of PoS, it can also be translated into as a collateral loan where the bank bonds the loanee house for collateral damage. PoS unlike PoW, Miners are chosen by how much stake they have deposited. The security deposit will be used as collateral damage when a miner validates a fraud transaction. The validator verifies all the transactions and adds the block to the chain. The user's stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can validate the new block. As soon as the block is verified the user will get the stake and the given rewards. Even though, this approach is a greater alternative to PoW favorites rich people. PoS, however, does not let anyone validate transactions in the blockchain leading to less energy consumed and it is also more decentralized because it does not encourage the use of mining pools. Chart 0.1 below shows the dominant mining pool in the PoW processes, so if three of these dominant mining pools merge together that can lead to validating fraudulent transactions on the network. 

Pool mining can lead to what is known as 51% attack which is when a mining pool controls 51% of the computational power of the network and creates fraudulent blocks of transactions while invalidating the transactions of others in the network. In PoS validators are chosen and assigned specific blocks to verify where in PoW miners are working simultaneously to mine the same block which leads to the high energy consumption.

### 

### 

### 

### 2.9.4 Malicious Proof-of-Work in Cryptomining

Bitcoin is one of the cryptocurrencies that has extensively employed the concept of Proof-of-Work (POW) since its introduction in 2009. This currency employs the hash-based system of POW to generate new blocks and to create a single public ledger of transactions (Wustrow & VanderSloot, n.d.).

This strategy is regarded as one of the key security measures used by this currency and the related transactions. Its main objectives are to prevent sybil attacks and to make it difficult for double spending to occur during the related transactions (Wustrow & VanderSloot, n.d.). Double-spending is essentially spending the same single digital token more than one time. Despite its capacity to prevent the stated security issues, research indicates that this technique is not as efficient as one would think (Wustrow & VanderSloot, n.d.). It is characterized by a number of security vulnerabilities that can be exploited to pose threats to bitcoin transactions or the transactions involving any other similar currencies that employ the POW system of validation and verification.

Due to these loopholes, alternative methods of validation have been proposed for use to enhance security (Wustrow & VanderSloot, n.d.). One of these alternative methods is the DDoSCoin, which is a special type of cryptocurrency with a malicious proof of work. The DDoSCoin is designed to allow users or miners to prove their participation in distributed denial of service attacks against particular target servers (Wustrow & VanderSloot, n.d.).

The validation and verification processes involves the creation of many TLS connections to a target server before using cryptographic responses to validate that many connections have been created (Wustrow & VanderSloot, n.d.). However, DDoSCoin validation methods are both expensive to validate and may become difficult to solve.

### 2.9.5 Distributed Denial-of-Service (DDoS) Attack

The distributed denial-of-service is a form of a security attack that is common to most online cryptocurrency wallets. The system is also used by attackers to paralyze operations on internet or network-based systems of communication or data exchange.

Conventionally, DDoS attacks occur when the bandwidth of resources of a targeted system or network is flooded with many systems (Wustrow & VanderSloot, n.d.). Such a system usually includes one or more web servers (Wustrow & VanderSloot, n.d.). The attack results in a situation whereby the operation of most systems is compromised such that the targeted system becomes flooded and nonfunctional.

Conventionally, the proof-of-work in cryptomining is designed to ensure that miners can prove their participation in a distributed denial of service attack (DDoS) against a given target. To ensure that miners can produce valid proofs-of-work, they are incentivized to be able to send and receive voluminous network traffic to and from the target (Wustrow & VanderSloot, n.d.). Just like in the case of other cryptocurrencies, this proof-of-work can be verified by others at low costs such that the original miner can be rewarded accordingly (Wustrow & VanderSloot, n.d.).

In return, the reward can be exchanged for other currencies, which makes it possible for botnets and other attacks to earn revenues for participating in the decentralized DDoS attack (Wustrow & VanderSloot, n.d.). The malicious proof-of-DDoS operates in a slightly different manner. It allows miners to create many TLS connections to a target web server such that they can now use the signed responses of the target server as proof of connection (Wustrow & VanderSloot, n.d.).

The server signs the parameter given by the client during the handshake and the server-provided values that are used in the exchange of keys during the connection (Wustrow & VanderSloot, n.d.). Consequently, the client is allowed to provide the proof of having communicated with the server to the others (Wustrow & VanderSloot, n.d.). Additionally, the signed value that the server returns is unpredictable to the client, as it is randomly distributed (Wustrow & VanderSloot, n.d.).

Therefore, it becomes possible for the clients to only report the connections that match some rare threshold. This mechanism has been used to design the DDoSCoin, a special type of coin that uses the proof-of-DDoS mechanism in cryptomining. This coin allows currency miners to select preferred victim servers by consensus using the proof-of-stake mechanism. The consensus selection of the victim servers ensures that such a selection is collective, fair, and acceptable to all the participants of the given DDoSCoin.

### 2.9.6 Sybil Attacks

Sybil attacks constitute another category of security concern facing cryptocurrency and the cryptomining processes. It refers to the process by which cyber attackers create multiple accounts, or use multiple computers or nodes to enable them to take over networks (Wustrow & VanderSloot, n.d.).

In the cryptocurrency world, sybil attacks are executed by running several nodes on a specific blockchain (Wustrow & VanderSloot, n.d.). Sybil attacks come with several impacts on the networks and the holders of the affected accounts. Through this method, attackers outvote legitimate nodes within the network, especially in the case where they manage to create adequate fake identities (Wustrow & VanderSloot, n.d.). After outvoting legitimate nodes, the attackers proceed to block other users from the network through refusal to transmit or receive blocks (Wustrow & VanderSloot, n.d.).

Sybil attacks that are executed on a large scale can enable the attackers to reverse transactions made while in control of the network, leading to the problem of double spending (Wustrow & VanderSloot, n.d.). Apart from enabling attackers to interfere with transactions and network flow, sybil attacks make it possible for attackers to control and manage a significant portion of the hash rate and computing powers of a network.

### 2.9.7 Transport Layer Security (TLS)

Transport layer security (TLS) is one of the most common components of the validation systems in cryptocurrency mining and the related transactions. It refers to a widely adopted security measure that is designed to enhance privacy and security for all the communications that are undertaken over the internet (Wustrow & VanderSloot, n.d.).

One of the specific areas in which this technique is employed, is the encryption of communication that occurs between servers, like in the case where a website is loaded by a web browser (Wustrow & VanderSloot, n.d.). Overall, TLS is mainly a system of security and privacy for internet-based communication.

### 2.9.8 TLS Handshake

Just like the TLS, the TLS handshake also deals with the encryption of communication that occurs over an internet connection. It refers to the process that triggers a communication session that is characterized by TLS encryption (Wustrow & VanderSloot, n.d.).

A handshake is said to have occurred when there is a successful exchange of information between the two sides of communication (Wustrow & VanderSloot, n.d.). Other activities that constitute the handshake include mutual verification of the two sides of communication, the establishment of the algorithms to be used by both sides, and a mutual agreement on session keys (Wustrow & VanderSloot, n.d.). TLS handshakes mainly involve exchange of information and mutual verification of the sides that are communicating over internet connections.

### 2.9.9 Poisoning Attacks

Poisoning attacks are cookies, which gather information that a website saves on a user’s hard disk so that it can remember something about the user at a later time. They contain bits of texts that can be user ID or session IDs ([Hoffman](https://www.howtogeek.com/author/chrishoffman/), 2017). They include information such as the configurability of webpages or hide links that hide specific items found on a webpage ([Hoffman](https://www.howtogeek.com/author/chrishoffman/), 2017). Websites that are characterized by cookies always use the bits of information that they contain to keep track of users and to allow their users to gain access to given features or applications ([Hoffman](https://www.howtogeek.com/author/chrishoffman/), 2017).

Cookies also enable the fundamental functionalities of websites, including electronic commerce shopping carts ([Hoffman](https://www.howtogeek.com/author/chrishoffman/), 2017). Despite being a critical part of a website’s functional unit, cookies are also considered as principal threats to both security and confidentiality ([Hoffman](https://www.howtogeek.com/author/chrishoffman/), 2017). Therefore, cookies can be used to create security compromises that allow cyberattackers to invade the computers or nodes that verify transactions in blockchain-based transactions.

Web-based cookies attacks pose a serious danger to the security of cryptocurrency transactions, which are performed using computers and browsers. According to studies conducted in Poland in 2020, cyberattackers can use various forms of cookie fraud to pose security threats using web-based cookies. The main categories of cookie fraud are cross-site scripting (XSS), session fixation, cross-site request forgery attack (XSRF), and cookie tossing attack (Poland, 2020). XSS attacks occur when a user visits a malicious website and receives a cookie that targets another specific website. Such cookies are designed to resemble the ones of legitimate websites such that when the user visits the legitimate website then the information pertaining to that website is sent to the attacker. This type of attack can be used to acquire user IDs for important websites such as virtual wallets (Poland, 2020). Session fixation occurs when a user receives malicious cookies containing the session ID of the individual who issues them (Poland, 2020). When the user tries to log into the targeted domain, the details are logged into the system of the cookie issuer instead of the legitimate user. The end result is the issuer’s acquisition of vital session or login information. XSRF occurs when a user visits a legitimate site and obtains a legitimate cookie before visiting a malicious site instructing it to perform actions that render the legitimate site vulnerable for attack (Poland, 2020). The legitimate site then receives a request together with the legitimate cookie and performs the instructed actions as they appear to originate from the legitimate user (Poland, 2020). The final type of cookie fraud is the cookie tossing attack, which occurs when a user visits a malicious site that is designed to provide cookies that appear to be subdomains of the targeted site (Poland, 2020). The attacker then manipulates the provided cookie to overrule any data that is contained by the legitimate cookies from the targeted website (Poland, 2020). Therefore, the concept of cookie fraud poses a significant threat to the security of cryptocurrency transactions, especially considering that such transactions are verified by computers.

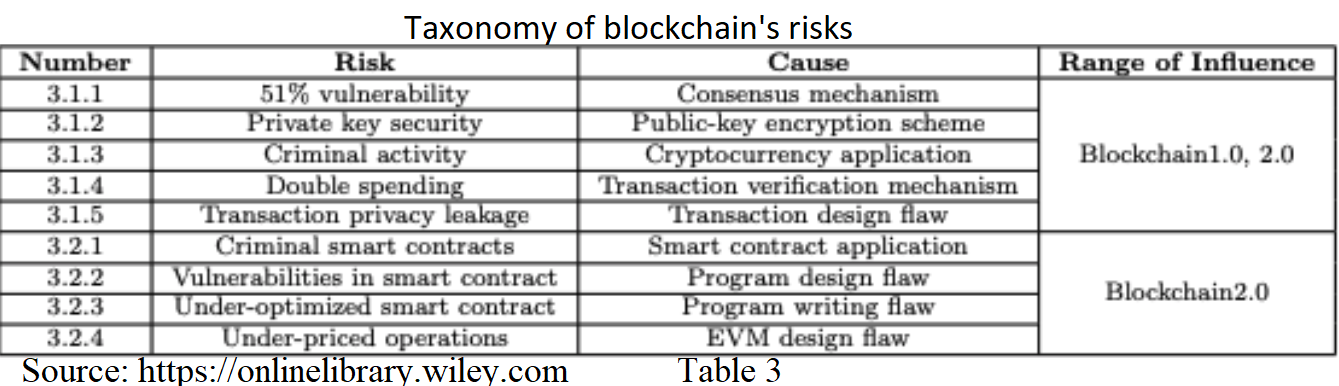
### Virtual Wallets

Virtual wallets, also referred to as online wallets, are software or web-based services that allow users to store and control their virtual currencies alongside vital information, such as transaction records, logins, passwords, and shipping details, among other pieces of vital information.

### Wallet Vulnerability

Wallet vulnerability has been identified by many scholars as one of the leading security concerns facing cryptocurrency and the associated transactions. Wallets are the devices in which people store their cryptocurrencies (Agrawal, 2019). Wallets are designed in different ways such as certain versions have features that make them more secure than others (Agrawal, 2019). The ones that lack adequate security features are said to be more vulnerable than the ones that are integrated with compact security features. Each of the desktop, web, and mobile wallets are characterized by specific security issues that make them valuable to hacking and cyberattacks (Agrawal, 2019). Research indicates that all waits, including Bitcoin wallets have certain vulnerabilities that can easily be exploited by cyber criminals 9 Kadyrov, 2019). A study conducted by a group of scholars from Edinburg University revealed that wallets are characterized by loopholes that make even them vulnerable to attack regardless of the level of encryption implemented on them (Kadyrov, 2019). This research also established that a special set of malwares can be used to intercept communication between personal computers and malware, especially for desktop wallets (Kadyrov, 2019). Consequently, Bitcoin users are at risk of losing their funds since attackers can use this loophole to divert users’ funds into their own accounts (Kadyrov, 2019). According to Agrawal (2019), mobile wallets are always online, a property that makes them very risky. The tendency of other mobile wallets to offer the functionality of exporting private keys makes such wallets even more vulnerable to security breaches (Agrawal, 2019). Virtual wallets are all very similar in the way how they operate and authenticate users. Indeed, virtual wallets all use an online server to store data of users, and also they all are almost identical in the way they authenticate users. For instance, in the case of Blockchain.com and coinbase.com, a user is authenticated by the traditional username and password. In case the system is suspecting foul-play , the further authentication process is sending an email to the user associated email. This process is not secure enough and if a hacker was able to obtain the user’s ID and password, the cybercriminal could have easily obtained the user’s email credentials.

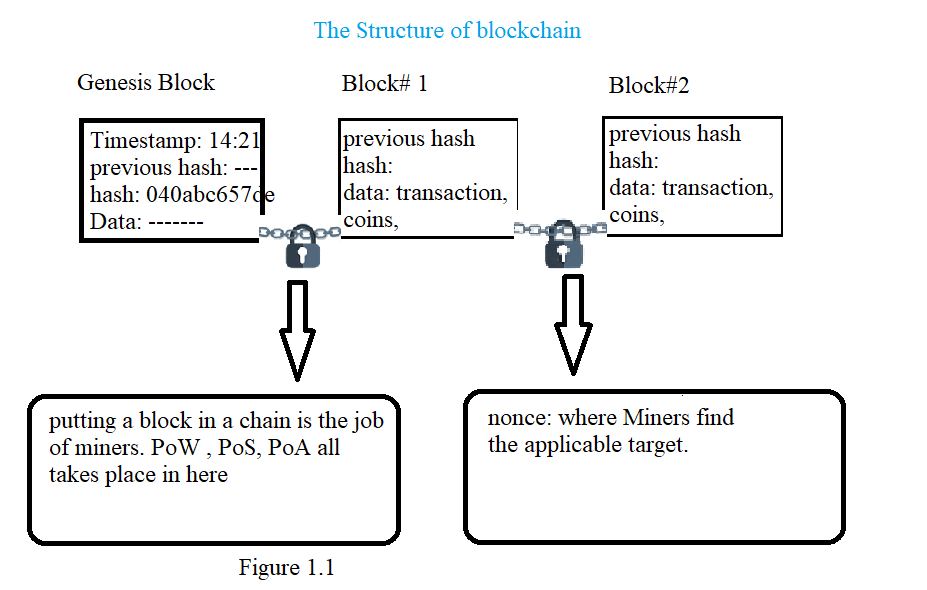
This paper will further assess the blockchain technology to understand its current vulnerabilities. In January 2019, A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures published on Wiley that elucidate the main risks with blockchain technology. Table 3 below shows the vulnerabilities is at 51% so if a miner’s hashing power accounts for over 50% of the total hashing power of the entire blockchain, a 51% cyber-attack can be launched. The 51% vulnerabilities in this assessment is only considering the system weakness, so adding human errors will add a great chance of cracking down on the blockchain technology. Human errors can be as simple as manginig one’s account using public Wi-Fi, or using very guessed username and password. consequently, this paper will closely evaluate the blockchain technology and propose new security measures.



# The Blockchain Technology

Due to the decentralized nature of blockchain transactions, they form the principal foundation on which cryptocurrency transactions are based. According to Reiff (2020b), blockchain technology refers to a structure that helps to store transactional records in databases. In this case, the series of transactional records are the blocks, while the databases on which they are stored are referred to as the chains (Reiff, 2020b). In a typical blockchain system, the constituents of the network are connected by peer-to-peer nodes (Reiff, 2020b). Due to these properties, blockchain technology is always regarded as a particular type of digital ledger (Reiff, 2020b).

The blocks in a chain, which are made of digital pieces of information, consist of three main components. First, they store important transactional information, such as time, date, and the amounts involved (Reiff, 2020b). The blocks also contain information about the parties who are participating in a given transaction. However, unique digital signatures are used to identify the transacting parties instead of their actual identities (Reiff, 2020b). The final component of a block, in a blockchain, is the information that distinguishes one block from the others within the chain (Reiff, 2020b). According to Reiff (2020b), each of the blocks within a chain contains a unique code known as the hash, which differentiates it from all the other blocks in the chain. Conventionally, a blockchain can store up to 1 MB of data in each block, eventually blocks are connected translating to several thousand transactions. to better understand the blockchain technology Figure 1.1 has the main structure of blockchain. As fIgure 1.1 shows that a Genesis block does not have a previous hash or any specific data. The Genesis block was the first block of bitcoin ever mind and it is the parent block of the blocks in blockchain. The Genesis value does not have specific information to a specific user and also does not have a previous has and its hash value is used for add blocks in a chain.



## Problem with Blockchain

Although blockchain has the potential to construct future cloud and Internet systems, it is facing challenges. Firstly, blockchain suffers from scalability issues. For example, the Bitcoin block is limited to 1MB, while one block of Bitcoin requires 10 minutes of mining (Zheng et al., 2016). Subsequently, the Bitcoin system can process only seven transactions per second, which makes it incapable of processing high-frequency trading transactions (Zheng, 2016). According to such frequencies, only 144 and 210,000 blocks can be mined in one day and four years consecutively. In practice, a more massive block requires a considerable storage location and slower transmission in the network. These issues can lead to centralization since fewer consumers would like to maintain such a large blockchain (Zheng et al., 2016). Even though blockchain offers the security of transactions, the tradeoff between security and performance (block size) is a high price to pay.

The performance of blockchain cannot compare to the efficiency of current Visa systems. Visa systems can process, on average, 2000 transactions per second (Maharjan, 2018). According to Visa (2020), VisNet handles 150 million transactions daily and can manage over 24,000 transactions per second. Hence, based on the 150 million confirmed transactions, Visa can process 1700 transactions per second. Indeed, the difference between the two technologies in terms of speed is significant. Tata Communications’ (2018) report shows that 44 percent of companies are adopting blockchain but admit that the scalability of blockchain is a hindrance to its success. Indeed, blockchain’s sluggish processing of transactions is a concern to enterprises that rely on speed to meet their objectives. Currently, Visa is the most popular brand in the US and Canada because it is setting industry standards of reliability in terms of speed (Visa, 2020). Even though blockchain experience is a scalability bottleneck, it still remains the most secure network compared to Visa.

Secondly, miners are expected to earn more than they should through a selfish mining strategy. In this strategy, miners hide blocks to earn more money in the future (Zheng et al., 2016). Consequently, branches could emanate frequently and hinder blockchain development.

The scenario of a selfish miner can be explained using Figure 1. This figure illustrates a baseline attack involving a selfish miner that is producing two blocks, BS1 and BS2. The baseline attacker forks the main blockchain and invalidates the genuine miner’s block BH (Saad et al., 2018). This attacker obtains 50 percent of rented hash power in Bitcoin from NiceHash for 10 minutes (Saad et al., 2018). The attack sequence happens in two rounds. In the first round, the attacker computes a first block, BS1, using his or her hash power (Saad et al., 2018). Moreover, the attacker withholds the block (BS1) and observes the legitimates’ block BH being accepted in the network.

In the second round, the attacker utilizes the rented hash power to compute the next block (BS2) before other participants in the network. After the block has been computed, the attacker forks the main blockchain using its private chain, as shown in Figure 1 (Saad et al., 2018). Consequently, the network discards BH and adopts both blocks (BS1 and BS2) to the longer chain (Saad et al., 2018). The selfish miner ultimately wins because the network flushed the BH block out of the main blockchain.

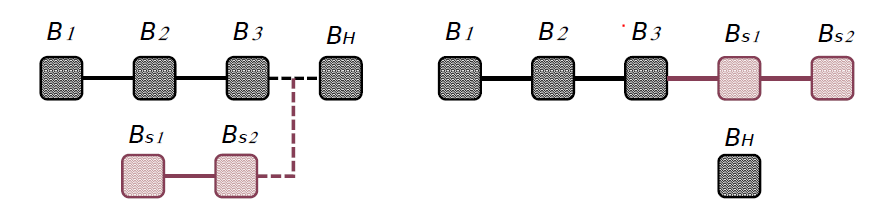


Figure 1: Selfish Mining (Saad et al., 2018)

Thirdly, blockchain’s consensus algorithms face setbacks. The proof of work (PoW) consumes more electric energy in its operations. Moreover, the Proof of Stake (PoS) technique (alternative to PoW) favors the richer over the poor; hence, the rich get more productive, and the poor get poorer (Zheng et al., 2016). Thus, this technology requires more research on how to improve both performance and security without missing on other vital components of the blockchain.

## How the Blockchain Technology Works

The functionality of blockchain heavily depends on the protocols and consensus mechanisms employed. From a simplistic view, the blockchain is explained as a distributed ledger system that holds records consolidated in timestamped blocks. Each time stamped block is replicated and shared among the members of the blockchain network (Laabs & Đukanović, 2018). Blocks in the blockchain are identified using cryptographic hash and points to the hash of its predecessor. Therefore, members of the node can read the data structure of the blockchain and calculate the current state.

A blockchain network contains a set of nodes making a peer-to-peer network where each node implements the blockchain protocols and holds copies of blockchain and asymmetric keys (Laabs & Đukanović, 2018). Nodes that are used in contributing to the blockchain to create and add new blocks are called the mining nodes. Moreover, nodes use private keys to sign transactions (Tx) cryptographically. In contrast, the mining nodes use blocks to sign transactions that should be processed by the network (Laabs & Đukanović, 2018). Specific nodes in a blockchain are addressed using a public key or the hash of the public key.

A node is critical in broadcasting a signed Tx to the neighboring peers. The validity of a Tx depends on the rules defined by the blockchain’s protocol of a specific network. Eventually, valid Tx is sent across the whole blockchain network (Laabs & Đukanović, 2018). Moreover, the mining nodes are responsible for collecting and ordering a set of validated Tx and wrap them into a timestamped block. A reference of the timestamped block is added to the previous block on the chain through hashing and sent back to the network (Laabs & Đukanović, 2018). Consequently, when a node validates the Tx and hash of the new block, it adds the new block to its chain, applies the Tx, and updates its status.

A critical activity of blockchain technology is building consensus between nodes. The consensus in nodes refers to the agreement on the Tx and the order of the Tx in the newly designed blocks (Laabs & Đukanović, 2018). An intuitive method of reaching an agreement is through a majority decision. However, doing so can make the blockchain vulnerable to the Sybil attacks. A Sybil attack is a threat to online work where one person tries to create multiple accounts, nodes, or computers to take over the network (Laabs & Đukanović, 2018). In social networking, this attack relates to an online user creating multiple profiles on Facebook, Twitter, or any other social media platform. In cryptocurrency, a Sybil attack allows someone to run multiple nodes on a blockchain network. Thus, blockchain requires consensus algorithms to manage communication between blocks and prevent the Sybil attacks.

### Proof-of-Work (PoW) Algorithm and the Functioning of Blockchain

PoW is a mechanism to prevent Sybil attacks in Blockchain. PoW makes it complicated for an attacker to create multiple nodes. In essence, PoW makes mining a computing-intensive activity. Hence, the benefit of joining the network using multiple accounts reduces since a single entity cannot manage the resources required to join the network (Laabs & Đukanović, 2018). This idea of PoW is used in Bitcoin to prevent the ledger from being changed. Figure 1 shows the PoW contained in Bitcoin.

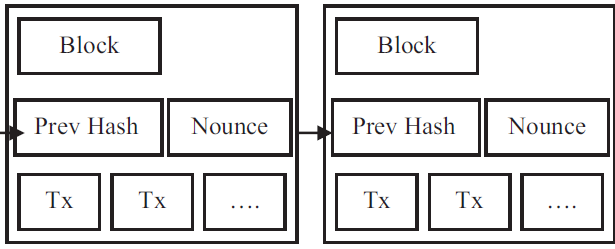


Figure 2: PoW in Blockchain Technology (Gemeliarana & Sari, 2018, p.127)

PoW operates in several steps. First, information stored in a target block is calculated using a hash value. The hash value generated must meet the complexity level determined in the system. Secondly, if the hash value generated does not meet the criteria, then the calculation must be repeated, and the value of the nounce is changed (Gemeliarana & Sari, 2018). A nounce is a value that is meaningless to the system. However, it is intentionally included in the calculation to generate a hash value according to the conditions (Gemeliarana & Sari, 2018). Thirdly, if the hash value calculation does not meet the desired rules, then the nounce value is changed again, and the processes repeat. The solving of the puzzle continues until a node that can find the solution is found and granted access to attach its block to the head of the blockchain. After verification of the hash value, the miner is provided with copies of the ledger; however, creating duplicate transactions will be visible to other nodes and cannot be accepted.

Apart from preventing the Sybil attack, the PoW has other benefits and challenges. While solving the puzzle is difficult for the mining node, every other node in the blockchain can verify the solution. PoW also adds the flexibility to change the difficulty of finding a solution by altering the length of the nounce to support a steady generation of blocks over a period. On the flip side, the PoW engages nodes in finding the correct value of the random number simultaneously; hence, consuming CPU time and electricity (Laabs & Đukanović, 2018). According to Laabs & Đukanović 2018, the PoW algorithm can make one transaction in Bitcoin to consume an equal amount of energy as that of approximately 22 U.S. homes on an average day. Moreover, PoW slows down the network performance, which is a massive problem because of the timing restrictions of online transactions. Nonetheless, the challenges of PoW can be mitigated using the proof-of-stake (PoS) method.

### Proof-of-Stake (PoS)

Unlike PoW, PoS is an energy-saving algorithm. In its functioning, PoS expects miners to prove the ownership of the currency. The assumption is that people with more currency are less likely to attack a network (Zheng et al., 2016). Nonetheless, this selection is more biased since "richer" nodes will dominate the network. Blockchain uses a randomized system to predict the next generator. This system looks for the lowest hash value that can match the size of the stake (Zheng et al., 2016). Comparatively, PoS is better than PoS; however, one has to pay the cost of attacks because the mining cost is minimized.

## Proposed Solution to Blockchain Scalability Problem

A favorable solution to blockchain scalability problems should not interfere with its security framework since it is considered to be the best. However, it should enhance the security of blockchain and increase the efficiency of doing transactions. In this work, the author is proposing a novel face and speech recognition authentication method for virtual wallets in blockchain transactions. Therefore, the face recognition algorithm should be used to capture users’ images compared with a stored one in the database and allow authentication. Equally, the speech recognition system can also be used to capture a person’s voice and compare it to a stored voice for authentication.

### Face Recognition System

Face recognition is a required biometric method and it is attracting attention from researchers. In its operation, face recognition works in two steps. Figure 3 depicts the two face recognition steps (Zong & Huang, 2011). Firstly, a face recognition system defines an adequate representation of the face images, including the sufficient details of the face for future classification. Secondly, the classification of a new face image is done against the chosen representation.

Moreover, the approaches of image classification can be placed as holistic-based and feature-based (see Figure 3). Examples of holistic methods include Eigenfaces and Fisherfaces, which take the whole face image as raw input and feed the image into a face recognition system (Zong & Huang, 2011). The feature-based method collects the characteristics of the nose, mouth, eyes, and then captures the locations and locus statistics of those face parts classification (Zong & Huang, 2011). Therefore, a programmer decides, based on the objective of the system, which classification methodology to use when implementing the face recognition system.

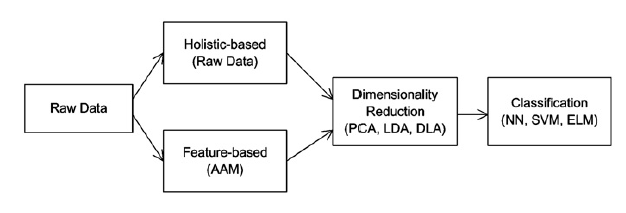


Figure 3: Face Recognition Steps (Zong & Huang, 2011, p. 2542)

Regardless of the classification methodology in a face recognition system, dimensionality reduction must be deployed. Often, natural images have statistics redundancies; hence, dimensionality reduction helps in transforming the image data from high-dimensional to a low dimensional space to reduce redundancies and noises (Zong & Huang, 2011). Dimensionality reduction also aids in unveiling vital features of face images. Dimensionality algorithms that are commonly used include the principal component analysis (PCA) and linear discriminant analysis (LDA).

Although face recognition is a robust technology, it has some challenges. An issue in the implementation of Face recognition is that a face is not rigid. Hence, a face image can be taken from different viewpoints of the face. Moreover, face representations should be resilient to intrapersonal image variations, such as expressions, styling, and age, while differentiating interpersonal image traits from a wide range of people. Achieving these objectives with high precision requires more than a statistical technique presented, such as PCA and LDA.

In this project, the author prefers an artificial intelligence (AI) technique over PCA and LDA methods. Systems, such as Google’s FaceNet, and Facebook’s DeepFace, uses convolutional neural networks (Amos, Ludwiczuk, & Satyanarayanan, 2016). Thus, neural networks-based face recognition systems are considered to be more accurate and reliable than statistical based systems.

This can be approached by forcing each user on the platform to store face pictures taken from 3 different angles and storing them in the Genesis block. The Genesis block 1 MB space is not used to its full potential, and has the capacity to hold more data. As soon as the user's picture is stored, machine learning algorithms will be implemented so the system can identify a user with as much as 92% accuracy. If the system recognizes the user, it will perform all tasks assigned to it, and eventually generates more blocks and connects them to the chain (Figure 0.2). a code was developed in Python. However, if the system does not recognize the user , the system will display “we cannot identify you and your account will be noted for a miner to review” and the account will be subjected to miners reviews. The code can be found at the end of this paper.



### OpenFace

The proposed system uses an open-source OpenFace face recognition library to build a face recognition that can be embedded in portable devices, such as a phone, laptop, or a desktop computer. This system will leverage the power of cameras in mobile devices to authenticate users to their virtual wallets through the OpenFace library. OpenFace is a general-purpose library that was released to the public in 2015. The library can be integrated into applications that implement face recognition.

Figure 4 describes the implementation of OpenFace in image recognition and processing. The system obtains a low-dimensional image and passes it through a neural network for classification. The training and inference model of this system uses Torch, luajit, and Lua. Python library (VRDJ95) will run using NumPy for array processing and linear algebra operations. Computer vision operations will be done using OpenCV while the classification will be performed through scikit-learn (PVG+11).

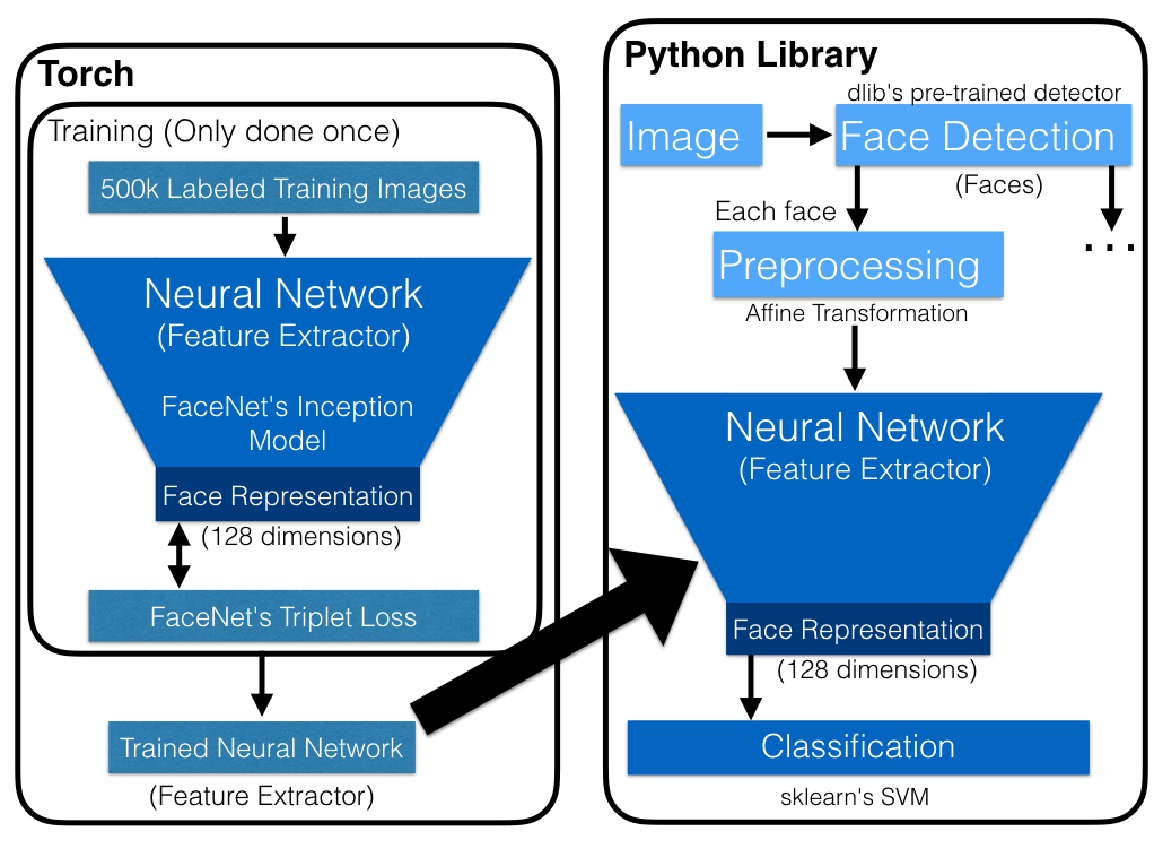


Figure 4: Logic of Face Recognition using Neural Networks (Amos et al., 2016, p. 5)

The operations of this model are expected to be shown in Figure 5. The figure illustrates how OpenFace affine transforms an image into 68 landmarks. The offline resizes and crops the image into a 96 X 96 pixels. This step is vital for the preprocessing of the image for training.

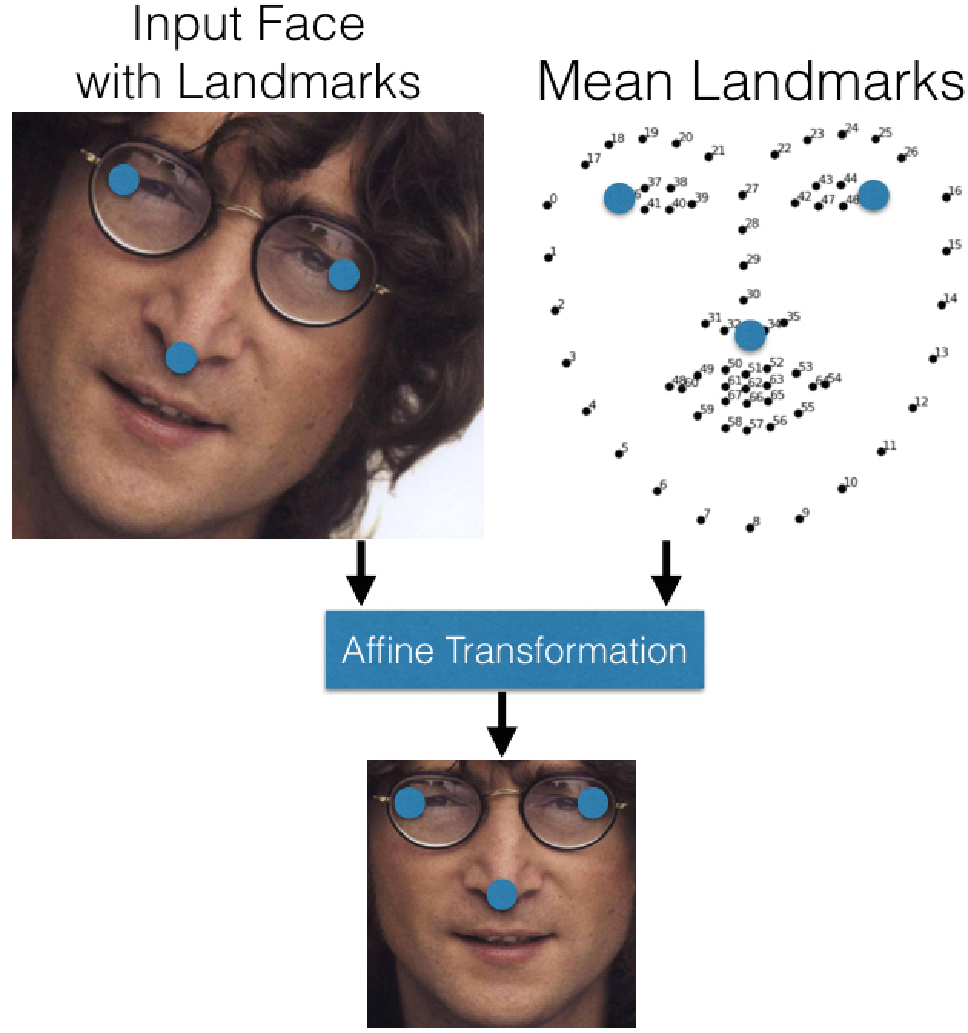
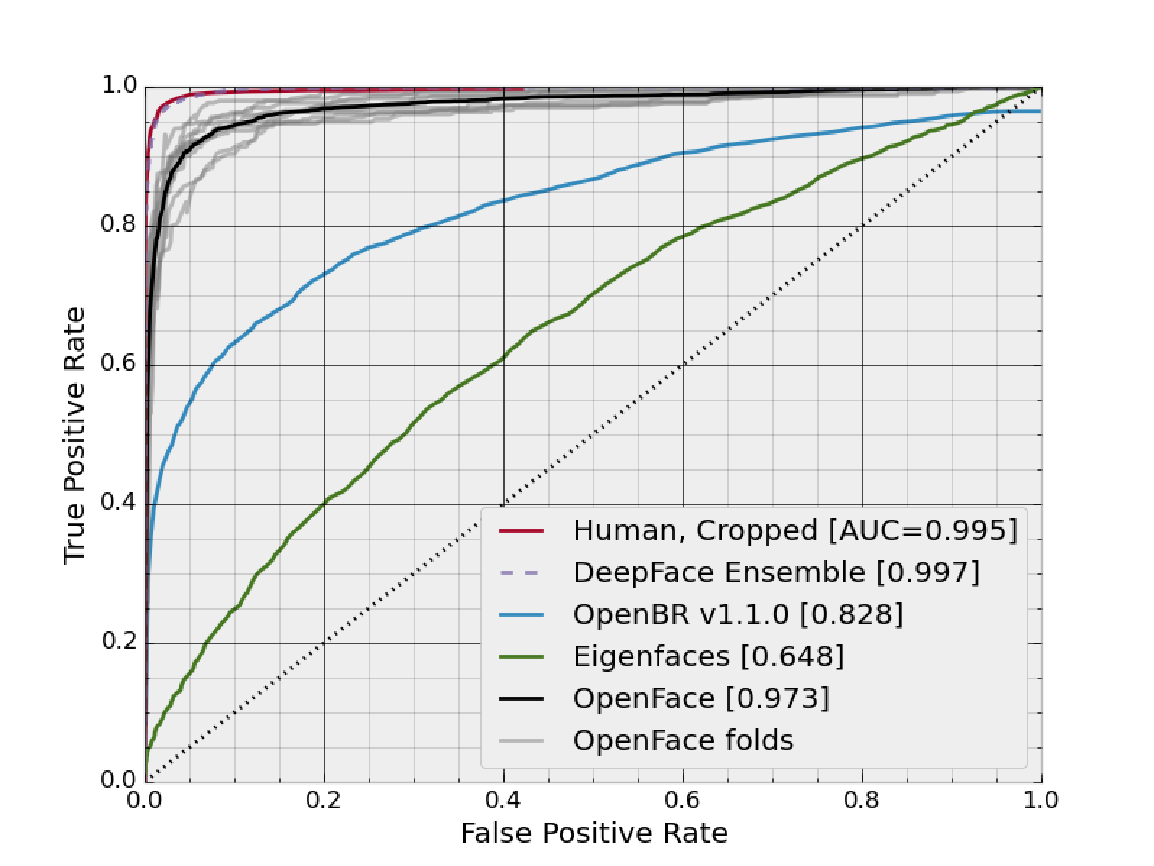


Figure 5: OpenFace’s Operation (Amos et al., 2016, p. 6)

In Amos et al. research, the authors use OpenFace for face recognition. In the paper, the authors determined that OpenFace has an accuracy of 0.9292. Furthermore, the authors tested the accuracy of OpenFace against the LFW(Labeled Faces in the Wild) benchmark. As shown in Figure 6, OpenFace shows a near-human accuracy.



*Figure 6: Receiver operating characteristics (ROC) curve (Amos et al., 2016)*

### Implementation of OpenFace in Virtual Wallets

Software wallets are applications that can be downloaded on a laptop or mobile device. Moreover, other users prefer working with online wallets that run on the cloud. In online wallets, the private key is stored in the cloud and controlled by a third party. Therefore, it is essential to have an additional layer of security using the proposed facial recognition system.

The implementation of extensive user authentication will rely on the camera of the portable device the user prefers to use. In practice, this new system will identify the user sitting in front of a PC or holding a phone through capturing the photo and comparing it with an existing photo stored in the cloud. If the photos match, the user is asked to use their voice as the login password; hence, a two-factor authentication mechanism is being proposed..

### Front End

The frontend of this application will implement an open-source library to integrate with the camera of the hardware used. For example, iMac users can utilize the open-source JPEG Camera library, which is on GitHub (Sabaratnam, 2017). The library allows one to use the web browser with HTML5 to capture an image. Furthermore, Android phones and tablets models can utilize the Tensorflow objection detection API (Al-Azzo, Taqi, & Milanova, 2018). Tensorflow API can be modified to meet the requirements of images captured in a smartphone or tablet.

### Backend

The backend of the proposed system will run the OpenFace library. The OpenFace will receive the image and process it, as shown in Figure 5. The preprocessed image will be run against a trained data set of users’ images to authenticate.

## Speech Recognition System

Machine learning (ML) and automatic speech recognition systems (ASR) collaborate to produce robust products. ASR and ML are being used in the market in products, such as iPhone’s Siri, Amazon’s Alexa, and Google Assistant. However, the poor performance of voice assistant renders ASR a frustrating experience to consumers (Deng & Li, 2013). Nonetheless, speech recognition remains an important technology that can also be used in blockchain to improve on user authentication mechanisms.

A speech recognition system has a client-side application and a server-side. The client-side can be embedded in another application or run on its own. However, for this blockchain implementation, it is imperative to embed voice recognition into the virtual wallet application to avoid cross-application communication, which can compromise the security of the application. The server side is responsible for analyzing the audio, fingerprinting the audio, and verifying whether the person is legitimate. The imperfection of this system can be covered by designing it as being the second factor in a two-factor authentication system. The server side also stores information about a user’s audio through the enrollment phase where multiple audio samples are provided.

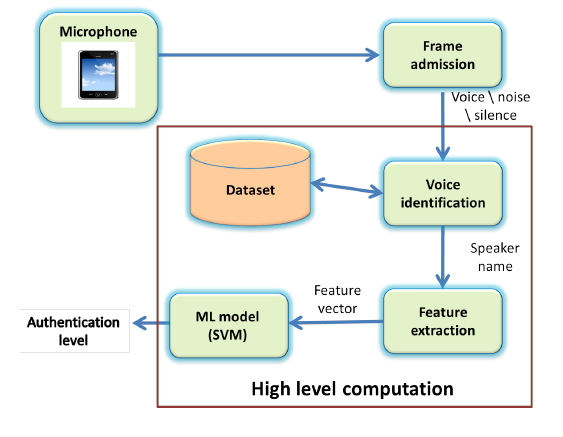


Figure 7: Voice Recognition System (Amin et al., 2014)

The ML model resides in the cloud, for example, Windows Azure or Amazon Web Service. A machine learning algorithm, such as Support Vector Machine (SVM) can be used to process the audio and authenticate a person to a virtual wallet. The advantage of a speech recognition system is that implementation does not require new hardware. In its operation and implementation code, the system utilizes the microphone of the phone or personal computer to capture the voice. In this case, the cost of implementation is low.

The implementation of both speech and face recognition will help deal with the security problems of blockchain’s virtual wallets. In 2018, phishing and social engineering scams stole approximately $2.728 million worth of cryptocurrency (LedgerOps, 2018). The majority of this scum happened through phishing using fake social media accounts (Twitter, Facebook, and Instagram), where attackers stole the login credentials of users. Hence, the introduction of speech and facial recognition systems’ virtual wallets will be secure because biometric technology’s security relies on personal characteristics, but not passwords.

## Protecting Transactions in Blockchain

Blockchain should adopt the attribute-based encryption (ABE) methodology. ABE methodology defines and regulates factors for ciphertext encryption using a secrete key of an account user (Zhang & Xue, 2019). Through a user accounts secrete key, it is possible to decrypt data if the attributes are agreed with the attributes of the ciphertext. Traditionally, an encryption mechanism is seen as a technique of encoding data for the target recipient. For example, Alice encrypts data using a public key and sends it to Bob, who decrypts the data using a private key. Although the technique of public key management applies in blockchain, an increased layer of protection can be enforced using ABE which uses a slightly different approach from the traditional key management technique. In an ABE system, only users with known attributes or credentials, that match the policy defined, can collude to access data. Thus, collision-resistance is a critical attribute of ABE.

ABE can be a solution to the security of completed transactions in the blockchain. Notably, transactions, in a blockchain, can be altered in two ways: miners attempt to change a transaction’s information or adversaries attempt to tamper with the data stored in the blockchain (Zhang & Xue, 2019). If an attacker colludes with miners, he cannot access or alter completed transactions because of attribute mismatch. Moreover, a significant number of nodes can be given permission to protect completed transactions by receiving an access token (Zhang & Xue, 2019). For that matter, all nodes with the token are assigned exclusive rights and privileges related to the token. The tokens will act as a pass to track who has specific attributes. Checking of attributes will be done through an algorithmic and consistent fashion from the token issuing authority.

Although relying on issuing authority to distribute the tokens can be dangerous, it is also possible to work without a fixed authority. According to Zhang and Xue (2019), authorities can be used to release the tokens. For instance, a blockchain can rely on witnesses to act as the authorities. Technologies, such as Steemit, Storj, among others, can be implemented on the decentralized network to fulfill the same action (Zhang & Xue, 2019). Indeed, transactions can remain intact in a blockchain through ABE.

In addition to blockchains’ internal security, it is essential for the virtual wallets to implement one-way hashing before the client’s details are stored in the database (Ajao et al., 2019). A user authentication system should permit blockchain customers to register their details and subject the values in a one-way hash function. The hash values can be used in authentication of customers as shown in Figure 8.

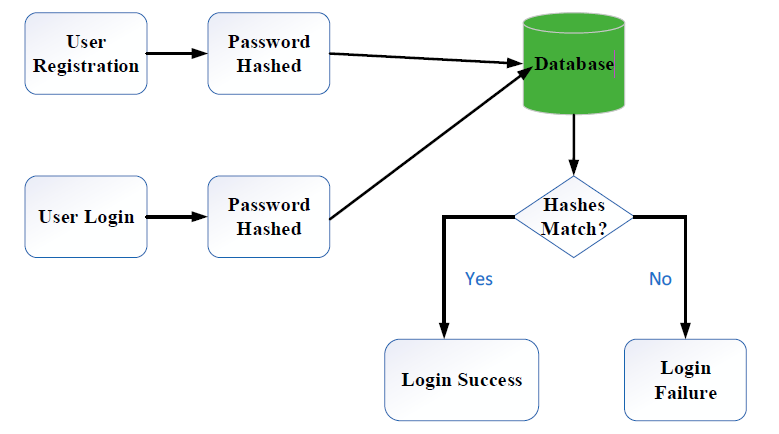


Figure 8: Additional Security for Authentication (Ajao et al., 2019)

## Blockchain and the Cloud

Cloud security is a challenge for blockchain systems because all its data is stored online. The exposure of the user’s sensitive data online can pause both psychological and monetary damages to cryptocurrency consumers. According to Park and Park (2017), the security of blockchain’s transactions and storage in the cloud depends on the security of the electronic wallet. For example, a secure wallet must provide a measure for secure restoration of infringed records, verification of binary files installed for self-protection, and protection of data online in case restoration is required. A secure wallet must ensure security for stored data in the electronic wallet and the settings required for the utilization of wallets (Park & Park, 2017). Moreover, it should allow the deletion of the remaining data securely when the consumer no longer requires the electronic wallet. The deleted wallet and data should also be securely discarded (Park & Park, 2017).

Park and Park (2019) proposes a secure bitcoin protocol. In this protocol, a user installs an electronic wallet on a portable device or PC. The system should send electronic data to the secure environment. When a user downloads and installs an electronic wallet software to operate on bitcoin, the public key of the installed system should be sent to the electronic wallet immediately after installation is complete. The exchange of the public key follows the Diffie- Hellman technique, where both the electronic wallet and platform owns the shared key (Park & Park, 2017). Therefore, when a user requests a transaction for a bitcoin, the ledger data containing the timestamp between the wallet and the platform are encrypted using the shared key and sent via the network (Park & Park, 2017). When a cloud user requests disposal, the system detects the client’s certificate and deletes it from the electronic wallet, and the message is sent to confirm the transaction has been securely discarded (Park & Park, 2017). Moreover, all relevant data is deleted to ensure the user remains anonymous. Leakages of user data are prevented when traces of user records are securely deleted.

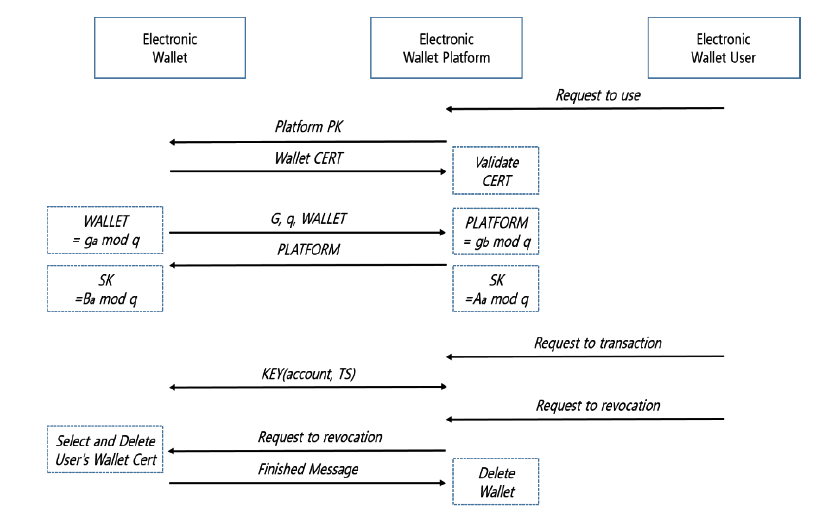


Figure 9: Secure Cloud Bitcoin Protocol (Park & Park, 2017, p. 10)

According to Park and Park (2017), the proposed bitcoin protocol is better than other studies on confidentiality, anonymity, integrity, privacy protection, and residual information protection. Overall, if this proposal is implemented, blockchain transactions can be secured in the cloud.

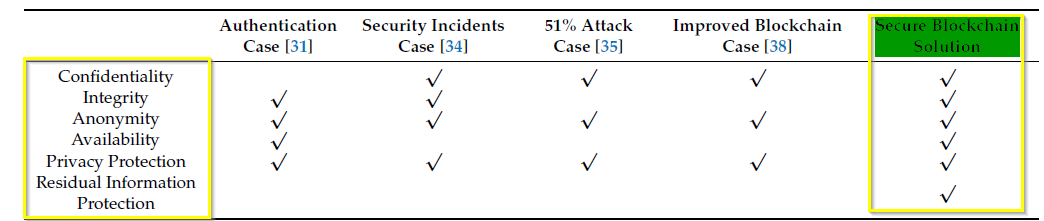


Figure 10: Comparison of Related Studies (Park & Park, 2017, p. 11)

Besides the cloud issues, cryptocurrency faces a challenge when a person dies. In essence, the crypto data can disappear if no one knows the cryptocurrencies’ details of the deceased (Roberts, 2017). Industry experts believe between 2.3 billion and 3.7 billion coins are lost (Deathio Limited, 2020). Although a variety of reasons are involved, the vast amount of the lost bitcoin is because of death.

One can think of naming beneficiaries to cryptocurrencies. However, most cryptocurrency exchange facilities, such as Coinbase, do not accept naming a contact person. Another solution is to put the cryptocurrency in one’s will. Even though this solution will help family members to know one had a huge asset in crypto, wills are not meant to store private information because they are public entities in courtrooms (Silva, 2018). Thus, doing so can jeopardize the security of the cryptocurrency.

A solution to cryptocurrencies' inheritance is to subdivide the private key among trusted individuals and family members. After death, the members can piece them together to retrieve the wallet. Indeed, forging this document will be difficult because several parties are involved.

### Other Security Issues

Blockchain transactions hope to handle security issues, such as double spending, chargebacks, data security, frauds, cross-border transactions, and currency reproductions. Double spending in the blockchain is handled using two methods: “total currency” and “longest chain wins” (Park & Park, 2017). Total currency means that a transaction can be terminated if a total currency exceeds the maximum of 21 million in the double transaction (Park & Park, 2017). In the second method, the next block is created when a double transaction forks a blockchain. Consequently, the longest chain will always win.

Chargebacks are a nightmare to most merchants. When a blockchain transaction happens, it is recorded instantly across the network; hence, they cannot be hacked (Vaccaro, 2019). Thus, processing chargebacks can take a shorter period than standard weeks or months.

Moreover, blockchain is handling data security issues. The cryptographic signature in blockchain can be used to secure a document against tamper (Callahan, 2017). Thus, comparing the cryptographic signature can help data owners confirm that their documents are secure.

Blockchain was designed to handle fraud in digital transactions. For example, identity fraud can be handled entirely through blockchain. Through hash codes and digital signatures, only legitimate account holders can access an account and cannot be traced back (Vaccaro, 2019).

Cross-border payment is a challenge for most people. In a cross-border transaction, a person sends funds to a receiver who is in a different jurisdiction (Beyers, 2019). Thus, the sender and the receiver do not have a similar ledger. Often, these transactions involve third parties and take more time to complete. Through blockchain, one can send money from company to company or individual to individual without directly.

Cryptocurrencies can be regulated to control the rate of crime. Even though this technology is secure, humans are involved in this trade. Thus, it is possible to have fraudsters disrupting the system. Methods, such as initial coin reporting and taxation, should be employed on cryptocurrencies (Edmondson, 2019). Capital gains, through crypto earnings, are underreported in several lands. Indeed, this is an area of concern for taxation. If someone earns in cryptocurrency, the income should be reported before the IRS declares the capital.

### Security of Software Wallets

The security of software wallets, such as Bread, Copay, Coinbase, Jaxx, among others, is the least compared to other types of wallets. This wallet application highly depends on the security of the smartphone. If a phone is stolen, there is a high probability that the malicious user can gain access to a software wallet based on the level of security on the phone. For example, an attacker can hack into a user’s Gmail account and then obtain credentials to access the Coinbase account through the lost phone numbers. Moreover, the private key stored in the mobile device can be stolen and used to access the cryptocurrency (Beigel, 2019). Overall, mobile wallets are less secure because they store private keys into the phone’s memory and relates the phone details with the private key, mobile number, and geolocations through platforms, such as Gmail and Google Maps.

# Hardware Wallets

Hardware wallets also form an integral part of the cryptocurrency security systems. They refer to the types of cryptocurrency wallets that are characterized by secure private keys that can be stored in physical devices (Mitra, 2019). The hardware wallet has been considered by many people as the safest and the most convenient option for storing and securing cryptocurrency (Mitra, 2019). This system of wallets safeguards the cryptocurrencies that are stored in it from any act of hacking as they remain offline while in storage (Mitra, 2019). Despite being offline and dormant while in storage, the stored coins are always readily available when required for any form of transaction (Mitra, 2019). Overall, a hardware wallet provides both ease of use and security.

## Ledger Nano X

Ledger Nano X is the latest hardware wallet in the market. Ledger, a leader in hardware wallets and cryptocurrencies solutions apps, designed Ledger Nano X after Ledger Nano S to solve the problems of its predecessor (Beigel, 2019). This product can hold up to 100 apps simultaneously and support over 1000 coins and tokens (Beigel, 2019). Examples of coins supported are bitcoins, Ethereum, bitcoin gold, among others. Besides, Ledger Nano X pairs with a mobile phone through Bluetooth and controlled through the Ledger Live mobile application.

Ledger Nano X is better than software wallets. This device offers a more robust security strategy than the software wallet. For example, Ledger Nano X provides a 24-word passcode, during installation, that should be written down and stored away from the device (Ankney, 2019; Beigel, 2019). Ledger Nano X also supports a phone’s biometric security mechanisms; hence, making it flexible to manage transactions while moving (Ankney, 2019). Overall, this product is secure and flexible than a software wallet.

## Physical Unclonable Functions (PUF)

PUF are hardware security primitives useful in generating long sequences of random bit strings. The strings are reproducible and can be stored in a nonvolatile memory (NVM) (Calhoun et al., 2019). Compared to cryptographic hash functions, PUFs do not leverage the infeasibility of computing power for special functions (Calhoun et al., 2019). However, PUF obtains its strength from the random behaviors of physical processes. PUFs can be applied in the development of hardware tokens that can be used as a building block for authentication protocols.

PUF can be used to identify hardware devices. PUF can authenticate and identify Field programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs). FPGAs are semiconductor devices developed under a matrix of configurable (CLBs) through programmable interconnects (Xilinx, 2020). Thus, FPGAs can be reprogrammed to the desired applications or functionality, which is a distinguishing feature from the ASICs, which is customed designed from the specific design activities (Xilinx, 2020). In brief, these two technologies can be used to program hardware components.

FPGAs can be used in programming hardware wallets to improve security. For example, programming hardware wallets, against Internet interference, can be a significant input to cryptocurrency. Internet interference is a gateway to malware and bugs. Currently, FPGA is being used in mining cryptocurrencies because of its higher hash rates and flexibility in managing algorithms (FPGA Guide, 2019). Indeed, FPGA can be used in cryptocurrencies.

## General Security of Hardware Wallets

Hardware wallets remain protective of a user’s private keys as long as they remain within the wallet. One of the most important security features of the hardware wallet is that the verification of all the transactions involving the funds stored in the wallet is done within the wallet itself (Mitra, 2019). This feature offers a remarkable security boost because it ensures that the device is not subjected to any interference by hackers who may have access to computer networks that control blockchains (Mitra, 2019). The wallet also remains offline when not in use, a property that keeps it away from any forms of cyberattack (Mitra, 2019). As discussed above, the main security threat associated with virtual wallets is that they remain vulnerable to security threats. Since the private keys in the virtual wallets are stored in the decrypted form, the user will need to decrypt them before they become usable (Mitra, 2019).

According to Mitra (2019), the decrypting process makes these keys vulnerable to any cyber-related security concerns (Mitra, 2019). Hardware wallets solves this problem by ensuring that private keys are not exposed even during transactions (Mitra, 2019). The hardware wallet only requests the software running on the user’s computer or smartphone to provide payment details and await user confirmation upon receiving such information (Mitra, 2019). The user will then be required to sign the transactions done, which triggers the system to send a digital signature back to the software, leading to the completion and closure of the process.

The Samsung blockchain platform SDK is one of the most recent developments in this field (Mihai, 2019). The platform is designed to allow developers to develop DApps on websites and integrate them into the mobile platform (Mihai, 2019). It includes a dedicated mobile DApp browser that allows web-based blockchain applications to run effectively (Mihai, 2019). Overall, hardware wallets are designed to minimize security concerns that are associated with virtual wallets, which are online and web-based.

The level of security that is offered by a hardware wallet depends on the type of wallet used by an individual. There are two principal categories of hardware wallets, the Trezor and the Ledger Nano S. The Trezor is a simple type of hardware wallet that is powered by a micro-USB connector (Kreder, 2017). It consists of a simple injection modeled plastic that is installed with two buttons and an LCD screen (Kreder, 2017). This type of wallet uses only the [STM32F205](http://www.st.com/content/ccc/resource/technical/document/datasheet/bc/21/42/43/b0/f3/4d/d3/CD00237391.pdf/files/CD00237391.pdf/jcr:content/translations/en.CD00237391.pdf) microcontroller, a feature that has been considered to encourage insecurity by creating a large hardware-based surface for attacks (Kreder, 2017). The device’s MCU harbors the entire process that results in the generation and storage of private keys (Kreder, 2017). Therefore, Trezor hardware wallets do not have common criteria security certifications (Kreder, 2017).

On the other hand, the Nano S hardware wallet is relatively more complex that the Trezor. Just like the Trezor, this type of wallet is also characterized by two input buttons, a micro USB power system, and an on-board screen (Kreder, 2017). However, the ledger Nano S is different from Trezor I in the sense that it has two microcontrollers. The device possesses both the  [STM32F042K](http://www.st.com/content/ccc/resource/technical/document/datasheet/52/ad/d0/80/e6/be/40/ad/DM00105814.pdf/files/DM00105814.pdf/jcr:content/translations/en.DM00105814.pdf) and the [ST31H320](http://www.st.com/content/ccc/resource/technical/document/data_brief/ac/ed/36/cb/1c/04/43/a8/DM00240763.pdf/files/DM00240763.pdf/jcr:content/translations/en.DM00240763.pdf) microcontrollers (Kreder, 2017). The ledger’s STM32F042K is similar to Trezor’s STM32F205 microcontroller with the only difference being the fact that it has it is installed with an internal clock unlike STM32F205, which has an external clock (Kreder, 2017). The private keys for the Ledger Nano S wallet are generated in the proper bank grade ST31H320 secure enclave, which also stores the device key to differentiate the ledger device from potential counterfeits (Kreder, 2017). Based on the above analyses, it is apparent that the Ledger Nano S wallet is more secure than the Trezor.

Despite the above stated security measures, the security of hardware wallets is still threatened by various vulnerabilities. The main vulnerabilities that make these wallets less secure include the $800 man-in-the-middle attacks, USB device firmware upgrade vulnerabilities, bypassing PINs, and surveillance.

The $800 man-in-the-middle attacks mainly target the ledger Nano S wallets, which are considered to be more secure than the Trezor wallets. This type of wallet is vulnerable to MIM attacks because it only displays eight digits of the recipient’s address. According to Kreder (217), it is easy for attackers to defeat the eight-digit confirmation of transactions at a relatively low cost, which is only $800 (Kreder, 217). Therefore, connecting a ledger Nano S wallet to a compromised computer and using it to transfer large amounts of money between various accounts on a regular basis subjects such a wallet to MIM attacks (Kreder, 2017). When a user transfers money regularly to an exchange account owned by him or her, any compromises on their computers would enable the attacker to identify the accounts or addresses to which they transfer funds as well as the amounts involved. They could proceed to create that are apparently identical or nearly identical to these addresses and wait for the user to make the next transfer of large amounts of money (Kreder, 2017). The addresses or accounts 8 for the case of ledger Nano S wallet and each of them costs $800 for apparently identical addresses and $30 for nearly apparently identical (Kreder, 2017). When transactions are made, the attacker substitutes the connected ledger for their accounts such that the user ends up confirming transactions that result in the transfer of funds to the attacker’s accounts. Cyber attackers have used this type of attack to transfer large sums of money from hardware wallets, leading to hefty financial losses.

The USB device firmware upgrade vulnerability affects both the ledger Nano S and the Trezor wallets. Generally, both wallets are upgraded using a system that is similar to the micro’s [USB Device Firmware Upgrade (DFU)](http://www.st.com/content/ccc/resource/technical/document/application_note/6a/17/92/02/58/98/45/0c/CD00264379.pdf/files/CD00264379.pdf/jcr:content/translations/en.CD00264379.pdf) (Kreder, 2017). The USB DFU features makes it possible for the wallets’ software to be upgraded through the USB port and device manager on the connected computer (Kreder, 2017). Attempts have been made to use just the DFU for the remote dumping of the memories of STM32F microcontrollers (Kreder, 2017). For Trezor wallets, this type of firmware upgrade facilitates the remote extraction of private keys from the wallet (Kreder, 2017). However, the remote dumping of memory does not affect the ledger wallet, since the private keys are stored in the ST31 secure enclave and not the STM32, which is affected by the remote control (Kreder, 2017).

Another potential danger of using the USB DFU firmware upgrade protocol is that it opens avenues for attackers to re-flash the device with malicious code when the upgrade is in progress (Kreder, 2017). The malicious code helps to spoof the check-sum that is used by the Trezor and the ledger Nano S wallets for on-screen verification, enabling the attacker to gain total control of the funds in the wallets (Kreder, 2017). However, all these activities are only possible if the upgrade is done at the time when the user’s account has been compromised. While this type of attack exposes the private keys in the Trezor, the private keys in the ledger Nano S wallet will still remain secure in the enclave, preventing the attacker from creating any malformed transactions.

Bypassing PINs occur when the hardware wallet is accessed by the attackers. Conventionally, all hardware wallets are designed in such a manner that the PIN can be reset if an incorrect version is entered three times. This feature is intended to ensure that attackers cannot use brute-force attacks methods to reveal the PIN (Kreder, 2017). However, the keys are not much of a barrier to attackers who intend to take control of a given wallet. According to Kreder (2017), the using both Vcc and clock glitching attacks can be used to create security glitches on the STM32F205 microcontrollers in Trezor. Consequently, it becomes possible for attackers to access the private PINs in Trezor without PIN verification (Kreder, 2017). However, the ledger Nano S is less vulnerable to this type of attack due to the fact that it has an internal clock and a secure enclave (Kreder, 2017). Additionally, the secure enclave in ledger Nano S requires the PIN before the device signing message, which ensures that the funds in the ledger cannot be compromised even after a successful attack of the STM32F042K microcontroller (Kreder, 2017). Overall, the ledger Nano S wallet is relatively more secure from bypassing PIN attacks compared to the Trezor.

The final vulnerability is the surveillance, which refers to the process where attackers gain control of a user’s web camera without their knowledge. In this type of attack, the attackers use a series of remote surveillance mechanisms that enable them to turn on the webcams of given computers and use them to monitor the activities of the user without being noticed. The principal objective of this type of attack is to steal the user’s PIN directly from then when they use them on their computers. Overall, both types of hardware wallets are subjected to various vulnerabilities that make them less secure for holding large sums of funds. However, the ledger Nano S wallet has systems and features that make it relatively more secure than the Trezor.

# Machine Learning

FPGAs can be used in training cameras for facial recognition. Facial recognition adds an increased layer of security on the proposed blockchain wallets security. Through deep learning neural networks, one can train FPGA on facial recognition (Easics NV, 2020). Existing frameworks, such as Python’s Tensorflow, ONNX, C, C++, or Caffe, among other types of designs, can be used on designing image recognition systems (see Figure 11) (Easics NV, 2020). The input of such a network will be the description of the network and the weights of the trained deep learning model. The network description is done using C++, while the weights of the model are converted into a fixed-point image (Easics NV, 2020). An application programming interface (API) and an image can be uploaded to the system and stored in the static, dynamic random-access memory (SDRAM) connected to the FPGA component (Easics NV, 2020). The output of the deep learning algorithm will be sent to the virtual wallet system for user authentication. Consequently, it will invoke the speech recognition system of the next authentication mechanism.

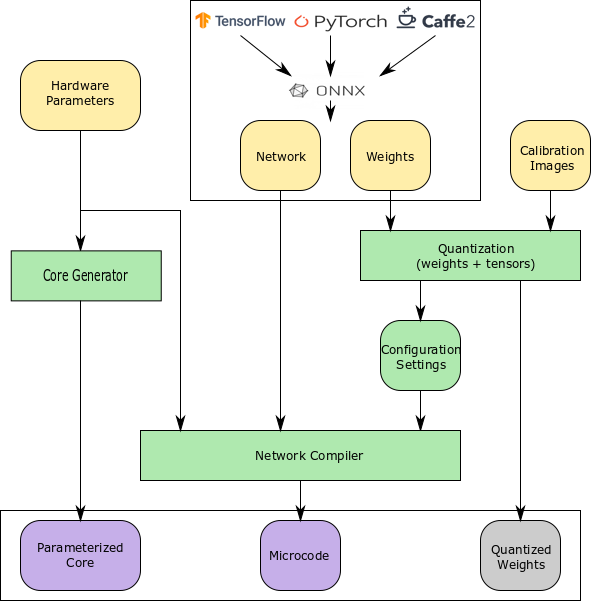


Figure 11: Deep Learning Framework

Implementing FPGA on image recognition systems has advantages. Firstly, this product has high performance per watt and offers low latency (Easics NV, 2020). Secondly, FPGA can be shaped into specific types of neural network architecture (Easics NV, 2020). Thirdly, FPGA designs offer future proof and scalable solutions; hence, making it favorable for blockchain products (Easics NV, 2020).

# The Economic Effects of Cryptomining on Cryptocurrencies

Cryptomining and the overall practice of trading in the cryptocurrency exchange markets is to generate profits. As highlighted in the previous chapters in this thesis, cryptomining refers to the process where miners are rewarded for working as auditors (Hong, 2020). The main role of the miners, in each mining process is to verify previous cryptocurrency transactions (Hong, 2020). The main reason behind the auditing process is to prevent fraudulent activities, such as double spending (Hong, 2020). According to Hong (2020), the concept of cryptocurrency mining is painstaking, expensive, and only periodically rewarding. Miners can always earn cryptocurrencies even without having to inject an initial investment into the process. Miners receive cryptocurrencies as their rewards for having participated in the completion of blocks of verified transactions. Verified blocks are generally added to blockchains within the networks (Hong, 2020). The miner who is first to offer a solution to a complex hashing puzzle becomes the one to be rewarded (Hong, 2020). Mining rigs can be facilitated by application-specific integrated circuits (ASIC) or graphics processing units (GPUs) (Hong, 2020). Based on the characteristics of these transactions, it is apparent that the mining process is of financial consequence both to the miners and the companies that offer the digital currencies.

The situation can be perceived in a two-way pattern such that whenever the currency provides gains, the miner loses. However, it is evident that miners can always earn rewards even if they do not have initial investments into the process. Such a property lowers the currency provider’s stake in the mining process. Every transaction that leads to the reward of a given number of coins of currency units to a particular miner is considered to cost the company offering such currencies by the same amount that is earned by the miner (Hong, 2020). For the case of bitcoin, transactions are compiled into groups known as blocks, which are confirmed at ten-minute intervals (Hong, 2020). Various models will always try to solve a block using a series of mathematical models such that the first node to provide a solution is awarded 12.5 bitcoins (Hong, 2020). The rewards that come with bitcoin mining are reduced by half after every four years (Hong, 2020). When bitcoin was first introduced in 2009, miners earned 50 BTC for every solution offered. This value was halved to 25 BTC in 2016 before being reduced to 12.5 BTC, its value in 2019 (Hong, 2020). The expected value for the year 2020, based on the above pattern is 6.25 BTC (Hong, 2020). In 2019, the bitcoin was valued at $9,300, an implication that the node that completes a block would be rewarded with 12.5 BTC x $9,300/BTC = $116,250 (Hong, 2020).

An exponential increase in the value of bitcoin has been witnessed in the past few years, making this currency the most popular in the world by a significant margin. According to Marquit (2019), the currency’s value per coin increased steadily from $300 in 2015 to $20,000 by the end of 2017. The same trend has been observed among other cryptocurrencies. For instance, by 2019, Litecoin and Ethereum had market capitals of $2.9 billion and $15 billion, respectively (Marquit, 2019). Cryptominers are obliged to account for the costs incurred in the mining process. In certain instances, such costs may include graphic cards, which have a unit cost of $700 (Marquit, 2019). In other cases, it is possible to negotiate basic rigs costing $3,000 for less reputed cryptocurrencies, while some miners spend up to $10,000 on their rigs (Marquit, 2019). Other expenses that are incurred by the cryptominers include the cost of electricity used in mining coins, which can go as high as $6,000. Overall, cryptomining comes with high costs that are incurred by either the miner or the company offering the currencies. A cost breakdown also indicates that the process is extremely risky since it is very costly yet there are no guarantees that a given node will be rewarded at any point in time.

The existence of cryptocurrencies has opened avenues for both positive and negative practices within the American society. The main positive aspect of this technology is that it encourages the birth of cashless transactions. The cryptocurrencies, as highlighted earlier in the thesis are characterized by low transaction costs, which make them economical. However, these currencies also encourage fraud in many ways. Fraudsters use cryptocurrencies to pay for illegal transactions as they know that such transactions are always untraceable. They also take advantage of the decentralized nature of blockchain technologies to steal funds from people using fake identities of government agencies, like the IRS.

## The future of Cryptocurrency

The future of cryptocurrency has been predicted by many economists who have mixed interpretations of what they expect the future of digital currency to look like. The first prediction that has been made by such scholars is that cryptocurrencies will be floated on Nasdaq, further adding credibility to blockchain and its role as an alternative to conventional currencies (Barone, 2019). Another development that is predicted by these scholars is the establishment of a verified exchange traded fund (ETF), which will make it easier for people to invest in digital currencies, like Bitcoin (Barone, 2019). Based on bitcoin’s mining pattern, which is 25 coins for every ten minutes, the currency is expected to reach 21 million caps by 2140 (Barone, 2019). Other predicted developments include increased security and the emergence of more alternative currencies.

# Conclusion

Cryptocurrencies constitute some of the latest technologies in the world today. However, the concept of digital currency dates back to several decades when it was considered as a mental construct. The earlier versions of the currency that were introduced failed to thrive in the market because of opposition from legal enthusiasts and lack of trust from the general public. Currently Bitcoin, Litecoin, Ethereum, and NEO are some of the most common digital currencies. However, Bitcoin remains the most popular currency by a significant margin. Since cryptocurrency involves the use of decentralized systems of transactions, it is considered as a better alternative to physical cash, which requires validation and verification from third-party trustees, like banks. However, these types of currencies are vulnerable to security threats, which include DDoS attacks, sybil attacks, and other forms of cyber-related attacks. Cryptomining is an expensive process that requires proper planning and a deeper understanding of cryptocurrency market dynamics to avoid incurring hefty losses. Overall, the cryptocurrency market is expected to increase in the future with the introduction of new currencies and a significant improvement of security in the related transactions.

**Codes:**

**import face\_recognition as fr**

**import os**

**import cv2**

**import face\_recognition**

**import numpy as np**

**from time import sleep**

**import datetime**

**import hashlib**

**def get\_encoded\_faces():**

**"""**

**looks through the faces folder and encodes all**

**the faces**

**:return: dict of (name, image encoded)**

**"""**

**encoded = {}**

**for dirpath, dnames, fnames in os.walk("./faces"):**

**for f in fnames:**

**if f.endswith(".jpg") or f.endswith(".png"):**

**face = fr.load\_image\_file("faces/" + f)**

**encoding = fr.face\_encodings(face)[0]**

**encoded[f.split(".")[0]] = encoding**

**return encoded**

**def unknown\_image\_encoded(img):**

**"""**

**encode a face given the file name**

**"""**

**face = fr.load\_image\_file("faces/" + img)**

**encoding = fr.face\_encodings(face)[0]**

**return encoding**

**def classify\_face(im):**

**"""**

**will find all of the faces in a given image and label**

**them if it knows what they are**

**:param im: str of file path**

**:return: list of face names**

**"""**

**faces = get\_encoded\_faces()**

**faces\_encoded = list(faces.values())**

**known\_face\_names = list(faces.keys())**

**img = cv2.imread(im, 1)**

**#img = cv2.resize(img, (0, 0), fx=0.5, fy=0.5)**

**#img = img[:,:,::-1]**

**face\_locations = face\_recognition.face\_locations(img)**

**unknown\_face\_encodings = face\_recognition.face\_encodings(img, face\_locations)**

**face\_names = []**

**for face\_encoding in unknown\_face\_encodings:**

**# See if the face is a match for the known face(s)**

**matches = face\_recognition.compare\_faces(faces\_encoded, face\_encoding)**

**name = "Unknown"**

**# use the known face with the smallest distance to the new face**

**face\_distances = face\_recognition.face\_distance(faces\_encoded, face\_encoding)**

**best\_match\_index = np.argmin(face\_distances)**

**if matches[best\_match\_index]:**

**name = known\_face\_names[best\_match\_index]**

**face\_names.append(name)**

**for (top, right, bottom, left), name in zip(face\_locations, face\_names):**

**# Draw a box around the face**

**cv2.rectangle(img, (left-20, top-20), (right+20, bottom+20), (255, 0, 0), 2)**

**# Draw a label with a name below the face**

**cv2.rectangle(img, (left-20, bottom -15), (right+20, bottom+20), (255, 0, 0), cv2.FILLED)**

**font = cv2.FONT\_HERSHEY\_DUPLEX**

**cv2.putText(img, name, (left -20, bottom + 15), font, 1.0, (255, 255, 255), 2)**

**# Display the resulting image**

**cv2.imshow('Video', img)**

**if cv2.waitKey(0):**

**cv2.destroyAllWindows()**

**cv2.waitKey(1)**

**return face\_names**

**def blockchain\_run():**

**class Block:**

**blockNo = 0**

**data = None**

**next = None**

**hash = None**

**nonce = 0**

**previous\_hash = 0x0**

**timestamp = datetime.datetime.now()**

**def \_\_init\_\_(self, data):**

**self.data = data**

**def hash(self):**

**h = hashlib.sha256()**

**h.update(**

**str(self.nonce).encode('utf-8') +**

**str(self.data).encode('utf-8') +**

**str(self.previous\_hash).encode('utf-8') +**

**str(self.timestamp).encode('utf-8') +**

**str(self.blockNo).encode('utf-8')**

**)**

**return h.hexdigest()**

**def \_\_str\_\_(self):**

**return "Block Hash: " + str(self.hash()) + "\nBlockNo: " + str(self.blockNo) + "\nBlock Data: " + str(self.data) + "\nHashes: " + str(self.nonce) + "\n--------------"**

**class Blockchain:**

**diff = 20**

**maxNonce = 2\*\*32**

**target = 2 \*\* (256-diff)**

**block = Block("Genesis")**

**dummy = head = block**

**def add(self, block):**

**block.previous\_hash = self.block.hash()**

**block.blockNo = self.block.blockNo + 1**

**self.block.next = block**

**self.block = self.block.next**

**def mine(self, block):**

**for n in range(self.maxNonce):**

**if int(block.hash(), 16) <= self.target:**

**self.add(block)**

**print(block)**

**break**

**else:**

**block.nonce += 1**

**blockchain = Blockchain()**

**for n in range(10):**

**blockchain.mine(Block("Block " + str(n+1)))**

**while blockchain.head != None:**

**print(blockchain.head)**

**blockchain.head = blockchain.head.next**

**labels = classify\_face("test.jpg")**

**if 'Unknown' in labels:**

**print('we cannot identify you and your account will be noted for a miner to review')**

**else:**

**print('Running blockchain!!!')**

**blockchain\_run()**

**References**

Agrawal, H. (2019). Security Risks of Mobile, Web & Desktop Bitcoin Wallets [Must Know]. Retrieved from <https://coinsutra.com/security-risks-bitcoin-wallets/>

Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019, June 16). Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. *Multidisciplinary Scientific Journal, 2*, pp. 300-325.

Digiconomist 2020, . “Bitcoin Energy Consumption Index.” *Digiconomist*, 30 Feb. 2020, digiconomist.net/bitcoin-energy-consumption.

Gorman, Brigid O. “Cryptojacking: A Modern Cash Cow.” *Symantec Blogs*, 5 Mar. 2020, symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cryptojacking-modern-cash-cow?utm\_content=79386076&utm\_medium=social&utm\_source=facebook.

Al-Azzo, A., Taqi, A. M., & Milanova, M. (2018). Human related-health actions detection using Android camera based on TensorFlow object detection API. *(IJACSA) International Journal of Advanced Computer Science and Applications, 9*(10), 9-23. Retrieved 2020

Amin, R., Gaber, T., ElTaweel, G., & Hassanien, A. E. (2014, February). Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. 1-26. Ismailia, Egypt.

Amos, B., Ludwiczuk, B., & Satyanarayanan, M. (2016). OpenFace: A general-purpose face recognition. Pittsburgh.

Ankney, L. (2019, April 4). *Is ledger's new Nano X wallet worth It?* Retrieved from Forbes: https://www.forbes.com/sites/leslieankney/2019/04/04/is-ledgers-new-nano-x-wallet-worth-it/#aaf1ee53779f

Aoki, Y., Otsuki, K., Kaneko, T., Banno, R., & Shudo, K. (2019, March 19). SimBlock: A Blockchain Network Simulator. Tokyo, Japan.

Barone, A. (2019). The future of cryptocurrency in 2019 and beyond. Retrieved from HYPERLINK "https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp" https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp

Author, Guest. “The History and Evolution of Proof-of-Stake.” *Cointelegraph*, Cointelegraph, 15 Oct. 2017, cointelegraph.com/news/the-history-and-evolution-of-proof-of-stake.

Beigel, O. (2019, November 13). *Best bitcoin wallets for android review*. Retrieved from https://99bitcoins.com/bitcoin-wallet/android/

Beyers, J. (2019, August 20). *How blockchain is used to solve cross-border payments*. Retrieved from https://blog.apruve.com/how-blockchain-is-being-used-to-solve-cross-border-payments

Bit Degree. (2020). Understanding the Different Types of Cryptocurrency. Retrieved from HYPERLINK "https://www.bitdegree.org/tutorials/types-of-cryptocurrency/" https://www.bitdegree.org/tutorials/types-of-cryptocurrency/ Neo Trading 2020: Here's

Bowden, S. (2019). Everything you need to know about china's leading crypto. Retrieved from HYPERLINK "https://commodity.com/cryptocurrency/neo/" https://commodity.com/cryptocurrency/neo/

Calhoun, J., Minwalla, C., Helmich, C., Saqib, F., Che, W., & Plusquellic, J. (2019, July 16). Physical Unclonable Function (PUF)-Based e-Cash Transaction Protocol (PUF-Cash). *Cryptography, 3*(3), p. 18. Retrieved from <https://www.mdpi.com/2410-387X/3/3/18/htm>

Dolan, Shelagh. “How the Laws &amp; Regulations Affecting Blockchain Technology and Cryptocurrencies, like Bitcoin, Can Impact Its Adoption.” Business Insider, Business Insider, 3 Mar. 2020, www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global#:~:text=The%20U.S.%20maintains%20a%20generally,rules%20have%20actually%20been%20introduced.&amp;text=While%20FinCEN%20does%20not%20consider,transmitters%20subject%20to%20their%20jurisdiction.

Callahan, M. A. (2017, November 7). *How blockchain can be used to secure sensitive data storage*. Retrieved from Dataversity: https://www.dataversity.net/blockchain-can-used-secure-sensitive-data-storage/#

Consumer News and Business Channel. (2020). Cryptocurrency pairs. Retrieved from HYPERLINK "https://www.cnbc.com/cryptocurrency/" https://www.cnbc.com/cryptocurrency/

Crypto-ML. (2018). How to Use Machine Learning to Trade Bitcoin and Crypto. Retrieved from HYPERLINK "https://crypto-ml.com/blog/how-to-use-machine-learning-to-trade-bitcoin-and-crypto/" https://crypto-ml.com/blog/how-to-use-machine-learning-to-trade-bitcoin-and-crypto/

Deathio Limited. (2020). *What happens to your cryptocurrency after you die?* Retrieved from https://death.io/what-happens-to-your-cryptocurrency-after-you-die/

Deng, L., & Li, X. (2013). Machine Learning Paradigms for Speech Recognition: An overview. *IEEE Transaction on Audio, and Language Processing, 21*(5), 1-30.

Easics NV. (2020). *How to start? Deploy AI algorithms on FPGA*. Retrieved from https://www.easics.com/products/deep-learning-fpga

Edmondson, B. (2019, March 11). *Can bitcoin regulations make cryptocurrency safer?* Retrieved from The Balance: https://www.thebalance.com/can-bitcoin-regulation-make-cryptocurrency-safer-4173836

Esmaeilzadeh, P., & Mirzaei, T. (2019). The Potential of Blockchain Technology for Health Information exchange: Experimental study from patients' perspectives. *Journal of medical Internet research*, *21*(6), p. e14184. doi: 10.2196/14184

FPGA Guide. (2019, June 27). *Cryptocurrency mining: Why use FPGA for mining? FPGA vs GPU vs ASIC explained*. Retrieved from https://medium.com/fpga-guide/cryptocurrency-mining-why-use-fpga-for-mining-fpga-vs-gpu-vs-asic-explained-5aaa400082b9

Gagarina, M., Nestik, T., & Drobysheva, T. (2019). Social and Psychological Predictors of Youths' Attitudes to Cryptocurrency. *Behavioral sciences (Basel, Switzerland)*, *9*(12), 118. HYPERLINK "https://doi.org/10.3390/bs9120118" https://doi.org/10.3390/bs9120118

Gemeliarana, I. G., & Sari, R. F. (2018). Evaluation Of Proof Of Work (POW) Blockchains Security Network on Selfish Mining. *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)* (pp. 126-130). Depok: University of Indonesia.

HYPERLINK "https://www.howtogeek.com/author/chrishoffman/" Hoffman , C. (2017). What is a browser cookie? Retrieved from HYPERLINK "https://www.howtogeek.com/119458/htg-explains-whats-a-browser-cookie/" https://www.howtogeek.com/119458/htg-explains-whats-a-browser-cookie/

Hong, E. (2020). How does bitcoin mining work? Retrieved from HYPERLINK "https://www.investopedia.com/tech/how-does-bitcoin-mining-work/" https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

Kadyrov, I. (2019). Security problems of crypto exchanges. Retrieved from HYPERLINK "https://hackernoon.com/security-problems-of-crypto-exchanges-d5e2f595fb79" https://hackernoon.com/security-problems-of-crypto-exchanges-d5e2f595fb79

Kenton, W. (2019). Feasibility study. Retrieved from HYPERLINK "https://www.investopedia.com/terms/f/feasibility-study.asp" https://www.investopedia.com/terms/f/feasibility-study.asp

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association: JAMIA*, *24*(6), 1211–1220. HYPERLINK "https://doi.org/10.1093/jamia/ocx068" https://doi.org/10.1093/jamia/ocx068

Laabs, M., & Đukanović, S. (2018, February 21). Blockchain in Industrie 4.0: Beyond. *De Gruyter Oldenbourg*, pp. 143-153.

LedgerOps . (2018). *Blockchain Security Threat Report.*

Maharjan, P. S. (2018, August). Performance analysis of blockchain platforms. *University of Nevada Thesis*. Retrieved from https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=4370&context=thesesdissertations

Marquit, M. (2019). Is bitcoin mining profitable? Retrieved from HYPERLINK "https://www.thebalance.com/can-bitcoin-mining-make-a-profit-4157922" https://www.thebalance.com/can-bitcoin-mining-make-a-profit-4157922

Martucci, B. (2020). What is cryptocurrency: How it works, history & bitcoin alternatives. Retrieved from HYPERLINK "https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/" https://www.moneycrashers.com/cryptocurrency-history-Bitcoin-alternatives/

Mihai, M. (2019). Samsung Blockchain Platform SDK announced, opens new doors for developers. Retrieved from HYPERLINK "https://www.sammobile.com/news/samsung-blockchain-platform-sdk-announced-opens-new-doors-for-devs/" https://www.sammobile.com/news/samsung-blockchain-platform-sdk-announced-opens-new-doors-for-devs/

Benger, D. (2018, June 14). A top SEC official said that Ether is not a security. Retrieved April 18, 2020, from https://coincenter.org/link/a-top-sec-official-said-that-ether-is-not-a-security

Mitra, R. (2019). Five best hardware wallets: [The most comprehensive list] – Blockgeeks. Retrieved from HYPERLINK "https://blockgeeks.com/guides/best-hardware-wallets-comparative-list-blockgeeks/" https://blockgeeks.com/guides/best-hardware-wallets-comparative-list-blockgeeks/

Ornes S. (2019). Core Concept: Blockchain offers applications well beyond Bitcoin but faces its own limitations. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(42), pp. 20800–20803. HYPERLINK "https://doi.org/10.1073/pnas.1914849116" doi: 10.1073/pnas.1914849116

Park, J. H., & Park, J. H. (2017, August 18). Blockchain security in cloud computing: use cases, challenges, and solutions. *Symmetry, 9*(164).

Pesch, U., & Ishmaev, G. (2019). Fictions and frictions: Promises, transaction costs and the innovation of network technologies. *Social studies of science*, *49*(2), pp. 264–277. HYPERLINK "https://doi.org/10.1177/0306312719838339" doi:10.1177/0306312719838339

Poland, J. (2020). Browser cookies: What are they & why should you care? Retrieved from HYPERLINK "https://www.whoishostingthis.com/resources/cookies-guide/" https://www.whoishostingthis.com/resources/cookies-guide/

Roberts, J. J. (2017, September 26). *What happens to cryptocurrency when you die?* Retrieved from https://fortune.com/2017/09/26/cryptocurrency-bitcoin-death/

Reiff, N. (2019). How to identify cryptocurrency and ICO scams. Retrieved from HYPERLINK "https://www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/" https://www.investopedia.com/tech/how-identify-cryptocurrency-and-ico-scams/

Reiff, N. (2020a). The 10 most important cryptocurrencies other than Bitcoin. Retrieved from HYPERLINK "https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/" https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

Reiff, N. (2020b). Blockchain explained. Retrieved from HYPERLINK "https://www.investopedia.com/terms/b/blockchain.asp" https://www.investopedia.com/terms/b/blockchain.asp

Rosic, A. (2016). What is blockchain technology? a step-by-step guide for beginners. Retrieved from HYPERLINK "https://blockgeeks.com/guides/what-is-blockchain-technology/" https://blockgeeks.com/guides/what-is-blockchain-technology/

Rosic, A. (2018). What is cryptocurrency? Everything you need to know! Retrieved from HYPERLINK "https://blockgeeks.com/guides/what-is-cryptocurrency/" https://blockgeeks.com/guides/what-is-cryptocurrency/

Saad, M., Njilla, L., Kamhoua, C., & Mohaisen, A. (2018, December 17). Countering Selfish Mining in Blockchains.

Sabaratnam, D. (2017, March 3). *Building a face recognition web app in under an hour*. Retrieved from Hackernoon: https://hackernoon.com/building-a-face-recognition-web-app-in-under-an-hour-345aa91487c

Silva, M. D. (2018, October 24). *What happens to your cryptocurrency after you die?* Retrieved from Quartz: https://qz.com/1432471/what-happens-to-your-bitcoin-after-you-die/

Sharma, R. (2019). What is IOTA? Retrieved from HYPERLINK "https://www.investopedia.com/news/closer-look-iota/" https://www.investopedia.com/news/closer-look-iota/

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. F., & Knottenbelt, W. J. (2018). Committing to quantum resistance: a slow defense for Bitcoin against a fast quantum computing attack. *Royal Society open science*, *5*(6), p. 180410. HYPERLINK "https://doi.org/10.1098/rsos.180410" doi: 10.1098/rsos.180410

Tata Communications . (2018, December 12). *Decision makers are optimistic about the impact of AI, IoT, predictive analytics and blockchain on business and society - but cost and security concerns and lack of skills are barriers to adoption*. Retrieved from https://www.tatacommunications.com/press-release/tata-communications-discovers-digital-transformation-disparity-in-new-study/

Tripwire. (2018). Security concerns and risks related to Bitcoin. Retrieved from HYPERLINK "https://www.tripwire.com/state-of-security/security-awareness/security-concerns-risks-related-bitcoin/" https://www.tripwire.com/state-of-security/security-awareness/security-concerns-risks-related-bitcoin/

Vaccaro, S. (2019, April 2). *The Role of blockchain in fighting chargeback and ecommerce fraud*. Retrieved from https://chargeback.com/the-role-of-blockchain-in-fighting-chargeback-and-ecommerce-fraud/

Visa. (2020). *Visa acceptance for retailers*. Retrieved from https://usa.visa.com/run-your-business/small-business-tools/retail.html

Wustrow, E., & VanderSloot, B. (n.d.). DDoSCoin: Cryptocurrency with a malicious proof-of-work. Retrieved from HYPERLINK "https://benvds.com/papers/woot16-paper-wustrow.pdf" https://benvds.com/papers/woot16-paper-wustrow.pdf

Xilinx. (2020). *What is an FPGA?* Retrieved from https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html

Zhang, R., & Xue, R. (2019). Security and privacy on blockchain. *ACM Comput. Surv, 1*(1). Retrieved from <https://arxiv.org/pdf/1903.07602.pdf>

Blog, F. (2020, May 12). How FinCEN Set Up Its 2020 Cryptocurrency Regulation in 2019. Retrieved June 29, 2020, from https://www.sygna.io/blog/fincen-digital-asset-cryptocurrency-regulations-2020-vs-2019/

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2016). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE 6th International Congress on Big Data*, 557-567.

Zong, W., & Huang, G.-B. (2011, May 26). Face recognitionbasedonextremelearningmachine. *Neurocomputing, 74*, 2541-2551.

Cuthbertson, Anthony. “Bitcoin Is Now Accepted at Starbucks, Whole Foods and 100s of Other Shops.” *The Independent*, Independent Digital News and Media, 14 May 2019, www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-stores-spend-where-starbucks-whole-foods-crypto-a8913366.html.

1. A test created by the Supreme Court to determine if a transaction qualifies as an investment contract. If it does, then the transaction is considered a security and therefore subject to registration requirements and certain details of disclosure. [↑](#footnote-ref-1)
2. Decentralized autonomous organizations are companies or businesses that operate through smart contracts. Its financial transactions and rules are encrypted on a blockchain, efficiently removing the need for a central governing authority. [↑](#footnote-ref-2)
3. The Lightning Network is a "Layer 2" payment protocol that operates on top of a blockchain-based cryptocurrency. [↑](#footnote-ref-3)
4. The Tangle is the data structure at the heart of IOTA, first introduced in the Tangle whitepaper. The IOTA Tangle is a stream of interlinked and individual transactions. [↑](#footnote-ref-4)
5. Cryptographic algorithms that are generally perceived as secure against attacks launched by quantum computers. [↑](#footnote-ref-5)
6. Is an algorithm used to achieve consensus that confuses many blockchain and cryptocurrency adopters. [↑](#footnote-ref-6)
7. Crypto Whitepaper: The Ultimate Guide for Beginners [↑](#footnote-ref-7)
8. SWOT stands for Strengths, Weaknesses, Opportunities, and Threats [↑](#footnote-ref-8)