6-2021

Evaluating Security in Cryptocurrency Wallets

Judith N'Gumah
xc7934wv@go.minnstate.edu

Evaluating Security in Cryptocurrency Wallets

by

Judith Mozoun N'Gumah

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

May, 2021

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Lynn Collen
Changsoo Sohn

Abstract

The number of users who are interested in trading Cryptocurrency is tremendously increasing, however, some users of cryptocurrency wallets do not know how to protect themselves or how to use a wallet with high protection. The objective of this paper is to propose a framework to enable users to evaluate the security and privacy of cryptocurrencies wallets. This framework will provide users with a list of attributes that define the degree of user protection in cryptocurrency wallets. This work aims to improve security and privacy in cryptocurrency wallets and enable users of these platforms to interact safely.

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Introduction

Nowadays with technology, people are changing their ways of doing online transactions; they are seen using Cryptocurrency Wallets. With the prosperity of human economic activities and the development of science and technology, the currency pattern has been constantly changing. Investing Cryptocurrency is like putting money in the bank. After the 1980s, under the support of modern information technology, new currency forms such as electronic money, virtual currency, and digital cryptocurrency emerged one after another. Bitcoin is the most well-known cryptocurrency, and has been in existence since 2009, invented by Satoshi Nakamoto while publishing it in 2008. It has experienced different stages such as physical currency, silver standard, gold standard metal currency and credit currency.

Cryptocurrency wallet is a software program that stores the public and private keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance. The use of Cryptocurrency has been rising in Africa which has been one of the largest economies. According to Statista on “How Common is Crypto” mentioned that Nigeria, one of the African Country has been using and owning Cryptocurrency in which they send or receive money all around the world. They have been using Cryptocurrency in their daily lives. There has been a statistical growth since Nigeria began using Cryptocurrency more. There have been a higher rates not only in Nigeria but numerous other Countries such as Vietnam, South Africa, Turkey,

United States, Peru, Spain, Germany, and Japan (Buchholz, 2020). Below is the list of Countries and their percentages of used and owned Cryptocurrencies.

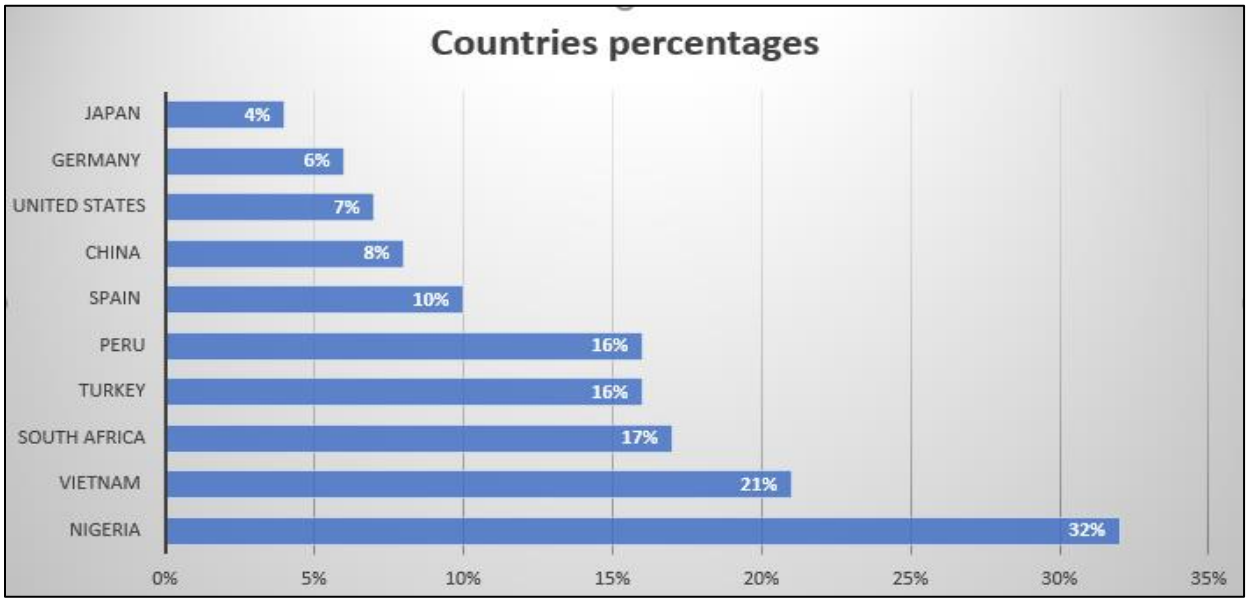
Table 1

List of Countries Using and Owning Cryptocurrencies and the Percentages of Use

Countries using and owning Cryptocurrencies	Countries percentages
Nigeria	32%
Vietnam	21%
South Africa	17%
Turkey	16%
Peru	16%
Spain	10%
China	8%
United States	7%
Germany	6%
Japan	4%

Figure 1

Countries Using and Owning Cryptocurrencies Percentages



The great thing about it is that you can see the records of the transactions, how they increase and how they decrease based on the assets and is stored in one's digital wallet. It can be stored using a web-based (hot) wallet or a large cryptocurrency values are at stake than in a more secure offline (cold) wallet like a USB Drive.

The private key allows you to have access to your funds through the crypto wallet. it is used to send Bitcoin and must be protected and secured. As for the public key, it is used to receive Bitcoin and can be published anywhere safely. As we noticed last decade, centralized exchanges such as MT. Gox and Binance have reported loss from hackers (Young, 2019). There has been an increased number of security breaches that lead to the loss of users' funds. As a result, investors may become reluctant to rely on centralized exchanges to store funds (Young, 2019).

In this paper, I will focus on the security and protection of the cryptocurrency's wallets from hackers; finding related articles on blockchain and cryptocurrencies wallets; gaining an understanding of blockchain and cryptocurrencies wallets security; understanding the different types of wallets and the one that is most safe and secure.

Problem Statement

A lot of people are interested in cryptocurrency, and would like to do some trading online, however, a lot of security and privacy issues are there. Furthermore, Myriads of incidents were reported in the past few years and individuals should do something about these incidents, and what really causes them. An article that was published in 2018 spoke about the numerous attacks that have been described in different aspects of the systems such as double spending, netsplit, transaction

malleability, networking attacks, attacks targeting mining, and mining pools (Conti et al., 2018). We know they have been having a lot of incidents lately, they do not know how to protect themselves and trade safely online.

Nature and Significance of the Problem

There are a lot of security breaches that affects cryptocurrency wallets; this is evidenced by the articles published in newspapers, and research. People are becoming victims of digital wallets cybercrimes as they lose money from their crypto wallets. An article that was published in 2019 discussed about Binance, one of the largest cryptocurrency exchanges, which lost approximately $41 million in Bitcoin which was the largest hack to date (Kumar, 2019). The studies show that this is the case of what has been going on in the past years.

Objective of the Study

Security of cryptocurrency wallets users is a big problem nowadays. In this paper, I present framework to enable users to evaluate the security and privacy of these cryptocurrencies' wallets. This method or tool will have a list of attributes that will define the degree of protection and prevention in these wallets. This work aims to improve security in cryptocurrency trading.

Study Questions/Hypotheses

The main research questions that this paper include:

1. What are the security measures needed to protect users of online cryptocurrency trading platforms?
2. Can these cryptocurrency wallets be stolen by hackers?

3. What are the different types of cryptocurrency wallets?
4. How can we evaluate security in cryptocurrency wallets?

Limitations of the Study

The limitation of the study is that the conclusion or information provided on this paper is not the final say meaning there are still many more things to know or say about Cryptocurrency. There are certain aspects of Cryptocurrency Wallet that this paper did not cover. This field of Cryptocurrency is an evolving one. They are still development, new research that are coming on the field daily. It is tentative, it is not conclusive, it is not the end. This paper left things unset, that was not cover which needs to be discussed in depth. I only covered what was useful for this research. The future of Crypto, as much as it is predictable, we never can tell.

Definition of Terms

This paper discusses about the cryptocurrency wallet which is a device that stores the public and private keys and can be used to track users' funds by receiving and spending cryptocurrency. My plan is to enhance the security of the users as well as protect users' funds from hackers. Moreover, one can make the apps and devices more secure for users to use by protecting their digital wallets. Below are some terms and their definitions:

- Cryptocurrencies: are a type of currencies that are relying on cryptographic proofs for confirmation of transaction (Lansky, 2018).

- A Cryptocurrency wallet: is a piece of software that keeps track of the secret keys used to digitally sign cryptocurrency transactions for distributed ledgers (Mearian, 2019).
- Bitcoin: a piece of digital currency, otherwise known as BTC. As a general concept, Bitcoin is a system for securely buying, storing, and using money digitally.
- Blockchain: a digital ledger of economic transactions that is fully public, continually updated by countless users, and considered by many impossible to corrupt. It is a list of continuous records in blocks (Zhang et al., 2019).
- Cryptocurrency mining: the process in which transactions between users are verified and added into the blockchain public ledger (IT, 2020).
- Hash rate or Hash Power: the measuring unit that measures how much power the bitcoin network is consuming to be continuously functional (Coinsutra, 2019).
- Proof-of-Work: the validation of the work that happened and proving it is correct. It currently account for more than 90% of the total market capitalization of existing digital currencies (Gervais et al., 2016)
- Proof-of-Stake: it confers decision power to minters that have a stake in the system. Unlike the Proof-of-Work in which everyone can become a miner, not everyone can join the network in the POS system (Seang & Torre, 2018).
- Address: a destination where a user sends and receives digital currency.

- Blocks: Many digital currencies make use of blocks, which contain transactions that have been confirmed and then combined (Zhang et al., 2019)
- Cryptography: the process of encoding and decoding information so that would be observers are unable to understand the information being sent (Hartnett, 2019).
- Fiat currencies: are currencies that have value because they are minted by a central bank. Fiat means “by decree”, and these currencies have value because some central authority have decreed that they have monetary value like British pound, Euro and Japanese Yen (Gobry, 2013).
- Exchanges: are just marketplaces where traders can make digital currency transactions. If a person wants to buy bitcoin, going to an exchange is the fastest way to accomplish this objective (Kharif, 2019).
- Private key: a piece of information, presented as a string of numbers and numbers that an investor can cause to access their digital currency.
- Public key: an address where an investor can receive digital currencies. This public key, like the private key, is a combination of numbers and letters.
- Satoshi Nakamoto: the pseudonym for the creator of bitcoin, and more than one individual has claimed to be Nakamoto.
- Token: it is a unit of digital currency, such as a bitcoin.

Summary

This paper will aim to educate people about the cryptocurrency wallets; it will present the identification of threats or attacks as well as security measures needed to protect users of online cryptocurrency trading platforms. This essay will present a literature review and will relate to methodology and the future work based on the evaluation of cryptocurrency wallets.

Chapter II: Background and Review of Literature

Introduction

This section of the literature review shall look at the findings in other areas of study and by other researchers on cryptocurrency wallets. Effectively, Cryptocurrency Wallets can be hacked by attackers if it is not well protected and secured. Nevertheless, the focus of this essay for now be based on the problems and security; this section will discuss about the major hacks and other cryptocurrency related services that occurred from 2011 to 2020, when users experienced money stolen from their cryptocurrency wallets due security issues. It is important to highlight about the problems facing on the cryptocurrency wallets and decide how it can be protected it, as well as secured along with how to solve the problem.

Background Related to the Problem

Recent hacks into cryptocurrency wallets of users from such systems have raised serious questions about whether this technology can be secured from ongoing, evolving cyberattacks; these hackings happened in chronological orders based on the year from 2011 through 2020 in which it will be mentioned and discuss in the literature related to the problems such as the Proof-of-Stake and the Proof-of-Work problem. The next part of the literature review would be about the methodology given by other researchers and area of study in which the solutions were provided.

Literature Related to the Problem

First, the article explained about the problems of cryptocurrency thefts and shutdowns of the exchanges that occurred from 2011 through 2020; these drew a lot of

attention from investors and users who had their funds safe and secured with any of the cryptocurrency wallets.

The online magazine SSRN demonstrated in their article titled “The Problems of Cryptocurrency Thefts and Exchange Shutdowns”, how Cryptocurrency, specifically Bitcoin, shed a light on the lack on of accountability when it came to cryptocurrency. Furthermore, It defended the need for stricter oversight and more transparency (Usman, 2018).

The article that was published in 2017 by MEDIUM “Mt. Gox Hack Technical Explanation” discussed how Mt. Gox got hacked by attackers in which they stole their Hot Wallets private keys. Unfortunately Mt Gox was not really good at security during that time, but they were able to figure out how now to make it more secure for users (Song, 2017).

An Atlantic Archive Technology that was published in 2012 highlighted the hacking that happened to BitFloor online bank robbery without the FDIC protection in which the owner of the company decided to shut down the site. They were concerned whether or not they can repay coins (Greenfield, 2012).

An article that was published in 2012 by ARS Technical demonstrated how Bitcoinica users filed a lawsuit in a San Francisco court for neglecting the safety of user’s money. Users were promised full refunds due to the hacking that occurred while making sure the security was protected (Geuss, 2012).

According to the Hacker News website published in 2013 which explained about how Bitcash.cz got hacked by attackers; these hackers got access to employee’s

personal emails by sending malicious scam while pretending to be the Bitcash.cz. The system unfortunately has been down for maintenance and the server was compromised by unknown hackers (Mohit, 2013).

The CSO online article that was published in 2018 talked about Cryspty that got hacked by inserting malicious viruses to their system named Lucky7 Coin. They lost 300,000 Litecoin's that were worth approximately $10 million. The owner of Cryspty Paul Vernon was sued by users with an amount of $8.2 million for destruction of evidence and stealing the Bitcoins (Schwarz, 2018).

Based on the newspaper article that was published in 2014 which mentioned that Mt. Gox have been experiencing one of the biggest hacks at all time. It was one of the world's largest Bitcoin exchanges and Investors were very concerned about the situation as large amount of funds were invested in Bitcoin, hence they were seeking answers for what really happened to their product on the unregulated Tokyo-based exchange. Eventually, the former CEO got arrested in 2015 in which they found roughly $2 billion of Bitcoin stolen in the hack (Yoshifumi & Sophie, 2014).

According to the website on CoinDesk that was published in 2014, the article discussed how Poloniex, one of the Bitcoin exchanges got hacked and suspected an employee who worked for the company that was behind the hacking. The owner D'Agosta suggested that the only way that bitcoins could be distributing fairly among affected users was to pay back customers using exchange fees as well as personal contributions (Rizzo, 2014).

An article that was published in 2015 by Cointelegraph highlighted BTER from China that had been hacked from their cold wallet. Cold wallet was one of the hardest and especially difficult one to hack. Apparently, it was not the first time that they have been hacked. Anyone who would be willing to find the stolen funds would be recompensated (Samman, 2015).

An article that was published in 2015 mentioned that the Chinese bitcoin exchange called KipCoin had lost over 3000 Bitcoins in the hack. KipCoin taught they were secured but the hacker was able to have access to KipCoin's servers and downloaded the wallet.dat file at the time. Even when the hacker was able to steal the funds at KipCoin stolen during that time, since this hacker even left some clues or their identities that could be traceable (Demartino, 2015) .

An article that was published in 2015 by CoinDesk illustrated that at Bitstamp company, the hacker was able to communicate with few employees by sending malicious malwares through their skypes. Without knowing what it was, some employees automatically clicked on the file malwares that the hackers sent. The hackers were able to have access to at least two servers that contained the wallet.dat file for Bitstamp's hot wallet and their passphrase (Stan, 2015).

According to Cryptonews website on local bitcoin in 2019 mentioned that it was hacked by attackers who distributed malwares through the local bitcoin live chat. They got access to the funds that was approximately 7.9 BTC. The company was trying to figure it out how they can reimburse affected users (Fredrik, 2019).

An article that was published in 2016 by Reuters discussed how Bitfinex one of the cryptocurrency exchange got hacked extremely. Hackers stole the Bitcoins user's accounts. Bitfinex did not know how to address the situation to users who lost their funds (Baldwin, 2016).

According to the website on Finance Magnates that was published in 2016 which discussed about Hong-Kong based exchanges called GateCoin that had been hacked in 2016 for an amount of $2 million in cryptocurrencies; they did so by having access to GateCoin hot wallets, the exchange then set up a payment plan called Payment Service Provider to be able to reimburse all the funds belonging to investors who got hacked during that time (Mizrahi, 2016).

An article that was published in 2019 by Crypto News Website mentioned the cryptocurrency exchange ShapeShift had been hacked three times. It was one of the employees working for the company who was behind these attacks, but they were able to rebuild it. it was important to prevent these kinds of attacks from happening, hence they tried to secure it by providing suggestions like keeping your keys in a secured area and transferred it into a hardware wallet (Sead, 2019).

An article that was published in 2017 by Bloomberg Businessweek spoke about a cryptocurrency exchange named Yapizon from South Korea currently changed the name to Youbit had been hacked twice in less than a year. South Korea thought it was the North Korea that spied on them and stole 3800 Bitcoins, but there was no information released to prove that it was the North Korea (Yuji & Sam, 2017).

An article that was published in 2017 by Cointelegraph Bithumb, recalled about one of the top five largest cryptocurrency exchanges that had been hacked by attackers, they stole their user data, and money. Furthermore, the crypto exchange Bithumb confirmed its intention of reimbursing the users affected of the theft (O'Neal, 2018).

According to the CNBC website, there was an article that was published in 2017, focusing on how NiceHash was part of the cryptocurrency mining, allowing users to rent out their hash-rate, had been hacked. NiceHash did not specify how many bitcoins were stolen but the users estimated the amount to be roughly $60 million. They did some investigation by trying to figure out how or what had happened, and they can reimburse users funds (Browne, 2017).

An article that was published in 2019 by Cointelegraph implied that about the employee's personals computers that had been infected by malicious malwares or viruses. They suspected that it was a group of unknown hackers who installed the viruses to have access to their private keys (Huillet, 2019c).

In the year of 2018, there were more attacks from hackers in few Cryptocurrency exchanges which are listed as follows: CoinCheck, BitGrail, Coinsecure, Taylor, Bitcoin Gold, Coinrail, Zaif, MapleChange, and QuadrigaCX, Cryptopia, Coinmama, Bithumb, DragonEX, Binance, GateHub, Bitrue, Bitpoint, VinDax, UpBit, and AltsBit.

An article that was published in 2018 mentioned that unfortunately for CoinCheck, the process was simple for the hackers to access to it. They were having issues with the security; and the hackers managed to send malware or viruses through

employee's emails and were trying to steal their private keys. They had been sued by other Crypto traders and investors for not securing their funds. Coincheck decided to reimburse the funds stolen as promised to all affected people, and they had been able to "bounce back" after the massive attacks (O'Neal, 2018).

An article that was published in 2018 by Cointelegraph described that BitGrail, an Italian Cryptocurrency Exchange, had its wallets hacked and claimed that an amount of 17 million Tokens were stolen. They accused the founder of BitGrail and Nano for stealing the funds. unfortunately, BitGrail keeps pointing fingers at Nano that they had nothing to do with the hacking (O'Neal, 2018).

An article that was published in 2018 by Cointelegraph explained about Coinsecure, an Indian Cryptocurrency exchange, that had been hacked from the company bitcoin wallet. They suspected the Chief Scientific Officer to be part of the hacking. At the end of the day, the Chief Scientific Officer was arrested for that. The company eventually reimbursed the users while the investigation was still ongoing (O'Neal, 2018).

An article that was published in 2018 by Trending discussed how Taylor, cryptocurrency trading app had been hacked and hackers stole most of their funds with an amount of $1.35 million. They have decided to investigate by tracking the hacker's activities and let the law enforcement agencies to oversee the situation. Even though they lost a ton of amount, they had a backup plan of revealing a new TAY Token which will block hackers' addresses (Sam, 2018).

The researcher mentioned that Bitcoin Gold had been hacked by attackers and they stole $ 35 million. Hackers have been using some techniques by putting their Bitcoin Gold into exchanges and traded them with other cryptocurrencies to be able to withdraw their funds (Sharma, 2018).

An article that was published in 2018 by CoinDesk website mentioned that Coinrail which was one of the small Cryptocurrency exchanges in South Korea had been hacked and lost $ 40 million. They were able to save some of their funds in a cold wallet and freeze the rest of their funds so they can continue to investigate and figure it out the issue (Wolfie, 2018a).

An article that was published in 2018 by CoinDesk discussed about Zaif, Japan based Cryptocurrency exchanges had been hacked. Due to the loss of funds, they decided to keep some funds in a hot wallet for immediate transactions and in the cold wallets where the attackers would try different methods but would not have access to their funds. The hackers did not steal on Zaif cryptocurrency wallets but few others also like Bitcoin, MonaCoin and Bitcoin Cash. The great thing with Zaif was that they were able to pay back the affected customers that got their funds stolen by hackers (Wolfie, 2018b).

An article that was published in 2018 by Coinspeaker website discussed how MapleChange, which is a small Cryptocurrency exchange in Canada had been hacked and the attackers stole all their funds which were immediately withdrawn. Without any further noticed to customers or investors, they decided to shut the website down because of the attacks. That made people more suspicious of their action because they

closed everything including social media and would not be able to refund all customers. Since MapleChange did not communicate with them, people suspected that it was a inside job but not a hacker that took all the funds (Daria, 2018).

An article that was published in 2019 by Wired Website discussed how QuadrigaCX, the CEO Canadian company Cotton was the only one who knew how to access the Cold Wallets had died in India and took that Cold Wallets of people's money with him to his grave. They mentioned that Cotten planned his own death and that it was an exit scam to pretend his death. They were six cold Wallets that Cotton knew about. And he had access to all but five of them, the rest having been emptied completely by Cotten. Even though, it was still unclear with the whole situation of Cotton death, the widow wife was able to reimburse an amount of $ 9 million assets (Stokel-Walker, 2019).

An article that was published in 2019 by Coin telegraph mentioned that Cryptopia company suffered from security breach because users were having hard time accessing their accounts. Because of the issues going on, they found out that there was no customers data on their systems meaning usernames and email addresses. Unfortunately, users who lost funds in the company would not be able to get refunded because they were not enough details on them to know if they were already in their systems (Kuznetsov, 2019).

An article that was published in 2019 discussed how Coinmama based in Israel, suffered a major brokerage from hackers that stole users' accounts' details and information; these accounts allowed users to buy and sell Bitcoin and Ethereum by

using their credit Card to purchase them. They were no cryptocurrency Wallets stolen from Coinmama (Huillet, 2019a).

An article that was published in 2019 by Cointelegraph discussed about Bithumb, a South Korean Cryptocurrency exchanges that had been hacked by someone who worked for the company. That employee completely withdrew an amount that was more than $3 million. They still did not find the person until then (Zuckerman, 2019).

An article that was published in 2019 by Cointelegraph noted how DragonEX, a Singapore based Cryptocurrency exchange had been hacked by the North Korean Lazarus group who mentioned they were responsible for this. They basically created some fake company by convincing the employees at DragonEX to download some malware in which they were supposed to check to make sure they were not malicious malware or viruses. DragonEX had to take full responsibility to refunds users who lost their funds during these attacks (Huillet, 2019b).

An article that was published in 2019 by CNBC website discussed the number of bitcoins stolen by hackers from a majority Cryptocurrency exchange Binance. Hackers had some ways to send malicious scam and viruses to hack into Binance, and they eventually stole customers' data. Binance would cover users who had been affected by hackers (Kharpal, 2019).

An article that was published in 2019 by Cointelegraph mentioned that GateHub, which was a UK and Slovenia based Cryptocurrency exchange had been hacked. They are still some investigations going on as to how hackers got access to user's funds. The great thing was that GateHub were able to recover the stolen funds (Alexandre, 2019).

An article that was published in 2019 by CoinDesk discussed how Bitrue, that was part of Singapore based Cryptocurrency exchange got hacked. Since the company only had few users that were affected, Bitrue agreed to refund them all (Palmer, 2019).

An article that was published in 2019 by Cointelegraph discussed how Bitpoint, a Japanese Cryptocurrency exchanges had experienced a tremendous loss of amount because their security breach was not secure at all. Hackers were able to steal an amount of $32 million, and unfortunately, Bitpoint was able to recover only $2.3 million to give to the affected users that got hacked (Wood, 2019).

An article by Yousaf, “Vietnam-Based Crypto Exchange VinDAX Loses at Least $500K to Hack” that was published in 2019 explained VinDAX, a Vietnam based Cryptocurrency exchange that got hacked by attackers and stole assets of customers. VinDAX conducted Token’s sales for unknown blockchain projects. They asked the blockchain projects for help on funds if they can be able to provide that to them (Yousaf, 2019).

An article that was published in 2019 highlighted Upbit which is a South Korea Cryptocurrency exchange that had been hacked and moved to the cold wallet. Unfortunately, the funds stolen by hackers had been on the move. Upbit were able to update their security breach (Huillet, 2019d).

An article that was published in 2020 by Security Affairs explained Altsbit, an Italian Cryptocurrency exchange that had been around for few months but had been hacked by a Lulzec group who mentioned they were responsible for that. Unfortunately, they had to close Allsbit by May 2020 (Paganini, 2020).

An article that was published in 2018 spoke about Binance, which was one of the world's largest cryptocurrencies by exchange volume. They tried to hint the hackers after stealing the contents of the company bitcoin Hot wallet. Although, it was mentioned that this form of crime had cost companies and governments $11.3 billion in illegitimate transactions and lost tax revenue (Bischoping, 2018).

Since hackers were able to hack in one of the largest crypto exchanges in the global market, they need to find a way to minimize this incident to prevent it from happening and facilitates the recovery to be more structured and apparent. They also need internal insurance funds to compensate users to make sure this incident will not arise. The next chapter in this paper will aim to discuss the literature review related in the methodology section.

Literature Related to the Methodology

This chapter discusses the different methodologies that are used to evaluate security and privacy in cryptocurrency wallets from academia, and industry. This includes the security of App-based Wallet, Web-based Wallet, Hardware Cryptocurrency Wallets and Paper Wallet.

Since OWASP Top 10 Internet of Things has been part of the industry, it will evaluate the security features related to different types of wallets. OWASP stands for Open Web Application Security Project which provides threats known to devices and applications. This OWASP has top ten latest list of Internet of Things (IoT) vulnerabilities (Lampe, 2014).

Figure 2 focuses on the Internet of Things (IoT) top 10 items that has been designed for hardware devices, web based and app based related to security (Lampe, 2014).

Figure 2

OWASP IoT Top Ten and Applicability of Existing Security (Jariwala, 2020)

OWASP IoT Top Ten	Maturity	Builds on Existing Knowledge of	
List Item	of List Item	Application Security	Network Security
I1 - Insecure Web Interface	Mature	Yes	Some
I2 - Insufficient Authentication/Authorization	Mature	Yes	Yes
I3 - Insecure Network Services	Mature	Some	Yes
I4 - Lack of Transport Encryption	Mature	Yes	Yes
I5 - Privacy Concerns	Emerging	Some	Some
I6 - Insecure Cloud Interface	Mature	Yes	Some
I7 - Insecure Mobile Interface	Emerging	No	Yes
I8 - Insufficient Security Configurability	Mature	Yes	Yes
I9 - Insecure Software/Firmware	Mature	Some	Some
I10 - Poor Physical Security	Emerging	No	Some

App based wallet has been part of the best products and tools used by investors for easier access and have safer transaction as well as management of their funds and sensitive data. There are seven important Bitcoin wallets in Figures 3 listed below in which investors trust by using these wallets to protect their investments (Rosenberg, 2019). These seven important Bitcoin wallets will be discussed in detail in this chapter by explaining the use of these Bitcoin wallets.

Coinbase is one of the easiest wallets that users or investors can buy, sell, and hold your cryptocurrencies in; with this Coinbase, you connect to any bank account which make it easier to transfer money in and out of the wallet. You can buy or sell your cryptocurrencies by using these dollars (Rosenberg, 2019).

Trezor is a physical device that you can connect to your computers where you can store your bitcoin and access it. It is not like Coinbase where you can buy or sell. This wallet provides some protections in cases if you lose your devices, or your passwords. The most important feature of this device is that it keeps hackers away from stealing your bitcoin (Rosenberg, 2019).

Electrum is a software wallet in which your Bitcoin is stored in an encrypted file on your computers or laptop. The big advantage with this wallet is that you can quickly get active, and successively and store your Bitcoin on your personal computer. In case, if you are having issues with your computer, issues such freezing, crashes, hacks, and breaches of security, it could significantly cost you, and you could lose your coins. This software wallet does support a recovery process by allowing you to create a cold storage with a printed or handwritten set of keys (Rosenberg, 2019).

Blockchain wallet is a technology that allows others digital currencies and bitcoin to exist; It is like Coinbase in which you can buy and sell through the platform in different Countries but with a small fee of charge. To protect this wallet, you are required to answer three specific security keys in your account for instance email verification, two-factor authentication ,and a backup security phrase (Rosenberg, 2019).

Robinhood is a wallet and exchange like Coinbase. It is a free stocking that supports users with their investments which includes cryptocurrencies like Bitcoin. Unfortunately, you cannot transfer Coins to and from Robinhood to another wallet. But, it is secure enough for your stocks and coins (Rosenberg, 2019).

Exodus is a software wallet very easy to use like Electrum. You can store coins directly through the app. There is no need to set an account because your wallet and currency belongs to you personally. It contains a private keys encryption and important security tools to use. This wallet is good for people who have an investment background and would like to increase their knowledge on digital currency (Rosenberg, 2019).

Mycelium is another mobile-only Bitcoin wallet, precisely focusing on Android and iPhone. It is a bit more complicated to use than some other Bitcoin wallets. It also allows for secrecy and keeps your Bitcoin in your pocket everywhere you go (Rosenberg, 2019).

The way to know that you are using the proper web-based wallets is to make sure that you have an installation of Windows 10 along with a range of web browsers like Mozilla Firefox and Google Chrome (Konash, 2019). The following web-based cryptocurrency wallets that we will discussed in this chapter while using OWASP Top ten IoT guidelines are:

- Metamask
- Blockchain.info
- MEW (MyEtherWallet)
- StrongCoin
- Jaxx
- coin Wallet
- Green Address

They are some tools for instance SSL labs and Security headers which are used to check websites for their levels of security; the type of technology they use for securing the website and each site also gives details on what is not secure and what solutions can be put in place to increase the security level of the website.

Companies from different Countries have supplied hardware wallets, explaining the aims and objectives of these wallets. There are some reasons why users or investors are recommended to use these types of hardware wallets because of the degrees of security and privacy. The purpose of these Hardware Wallet is to promote a safe way of storing and sending bitcoin (Costea, 2019). These are the five Hardware Wallets listed which are Trezor T, Ledger Nano X, KeepKey, Bitbox, and Coldcard Wallet.

Figure 3

Paper Wallets (Ameer, 2017)

Paper wallet is another way of storing cryptocurrency which creates an image that contains the private and public keys to a new wallet address along with QR codes. This is depicted in Figure 3 above, which you can see the printed, sealed, and stored securely in a safe or another secure place (Benton, 2019).

An article that was published in 2020 by SpringerLink “understanding the creation of trust in cryptocurrencies: the case of bitcoin” discussed about Cryptocurrencies providing trust through technology by identifying functionality, reliability, and helpfulness in which users evaluate trust in technology and in bitcoin (Marella et al., 2020).

While looking at the solutions provided by the researchers, they are similar to what would be proposed during the methodology part which are : managing your own private keys and not shared with anyone; making sure that you save these recovery phrase provided by your hardware wallet; these private keys are a minimum of twenty four words recovery phrase which are important to remember and to save in a secure area; creating a password with a maximum of ten characters containing letters, symbols, and numbers, and also used a complicated password instead; setting up multiple questions that must be answered before information can be retrieved or approved as well as two-factor authentication .These solutions will be discussed in detail in the following chapter.

Summary

In conclusion, there are myriads of different types of cryptocurrency wallets; these elements will be used to evaluate Web based Wallet, App based Wallet, hardware wallet and Paper Wallet. As mentioned earlier, OWASP for IoT guidelines are industry

standard tests which will help evaluate the IoT security. The results of these screenshots will be charted and evaluated by providing solutions on securing the cryptocurrency wallets in the next chapter.

Chapter III: Methodology

Introduction

This chapter of methodology will provide solutions and methods on how to secure the Cryptocurrency Wallets by identifying the necessary security features to protect Cryptocurrency Wallets from hackers and quantifying by providing tools and techniques that can help protect users' funds.

Design of the Study

Step 1: Identification: Identify the necessary security privacy features for users to interact safely; In this step, security, and privacy features necessary to protect cryptocurrency wallets will be investigated and explored from different research papers and industry standards.

Step 2: Quantification: provide users with a tool that can help them to evaluate the degree of protection that every cryptocurrency wallet has. This will enable cryptocurrency users to make well informed decision when they choose a wallet.

Data Collection

This section will focus on the data collection description from the popular online Bitcoin environment. Then, we will elaborate on the methodological approach and techniques of the data. The objective of the data collection is to comprehend how Bitcoin or cryptocurrency wallets have generated trust among its users despite being unidentified. In this framework, discussion forums have played a critical role in the growth of Bitcoin. This online forum was started by Satoshi Nakamoto for the purpose of communicating with other developers and investors. As of September 2019, Bitcoin

Forum has estimated 2.6 million members posting 52 million posts on 1.21 million topics (Marella et al., 2020).

Figure 4

General Statistics of Bitcoin Talk Forum (Marella et al., 2020)

General statistics of Bitcointalk forum	
Total Members	2663701
Total Posts	52398770
Total Topics	1216200
Total page views	4795109378
Average registrations per day	398.21
Average posts per day:	7310.46
Average topics per day	294.41
Average online per day	168.12
Male to Female Ratio of members	4.7:1
Average page views per day	1336429.59

In addition to that, they provided several online forums that focuses on cryptocurrency Wallets. They compared different data sources such as online discussion, interactions which can be accessed on an unparalleled scale. It allows us to gather the technological features related to trust in Bitcoin from the users' own perspectives of things.

Figure 5

Comparisons of Various Online Forums (Marella et al., 2020)

Measure	BitcoinTalk Forum	Cryptocurrency Talk	Bitcoin Garden Forum	Bitcoin Stack Exchange Forum
Total Number of Members	2,663,701	90,098	26,033	67,212
Total Number of Posts	52,398,770	456,113	429,913	NA
Total Number of Topics	1,216,200	111,779	55,147	22,922

Tools and Techniques

There are a few tools and techniques that will be used on this project; The first tool is the MCDM (Multiple Criteria Decision making) refers to making decisions in the presence of multiple, usually conflicting criteria (Xu et al., 2001). It consists of two techniques that will be discussed which are the weighted method and AHP (Analytic Hierarchy Processing).

Providing weights to criteria has been an important part that needs to be reconsidered. It has been one of the major factors while facing Multi-Criteria Decision Making. The weighted method primarily focuses on two such criteria those being, the qualitative and quantitative analysis of the data to be able to form the more accurate decision making (Xu et al., 2001).

Although, this Analytic Hierarchy Processing method is one of the most applied methods based on pairwise comparisons, the actual number of comparisons is calculated by:

$$cp = \frac{n(n-1)}{2}$$

Where cp = the number of comparisons and n = number of criteria.

Security Assessment for Crypto Currency Wallet a =

$$\sum_{feature\ 1}^{Feature\ n} Feature\ i\ Score * Feature\ i\ Weight$$

Hardware and Software Environment

This part shows the different types of hardware and software environment which will be discussed later by providing the tests results, and by evaluating most precisely on all the hardware wallet, mobile, online, web-based, and paper wallets.

Online or Web-based Wallets:

1. Metamask
2. Blockchain.info
3. MEW(MyEtherWallet)
4. StrongCoin
5. Jaxx
6. coin Wallet
7. Green Address

Hardware Wallets:

1. Trezor T
2. Ledger Nano X
3. Keepkey
4. Bitbox
5. ColdCard

Mobile or App-based Wallets:

1. Coinbase
2. Electrum
3. Blockchain

4. Robinhood
5. Exodus
6. Mycelium
7. CashApp

Paper Wallets

Summary

To conclude the methodology part, I will be identifying and quantifying the necessary security privacy features for users to interact safely and provide users with a tool that can help them to evaluate the degree of protection that every cryptocurrency wallet has.

This complete set of guidelines will be the structure used to test all the different types of cryptocurrency wallets. These four well known elements are to be used to test online, web based, app based, hardware, and paper wallets. The results of these extensive testing's, along with screenshots of the wallets and statistical data that will be evaluated in the next chapter.

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, results of the testing will be logged and evaluated; the following websites, apps, and hardware wallets were tested using the OWASP Top 10 Iot testing device guidelines and were described in the previous chapter as follows: web-based, hardware, app-based, and paper wallets.

Data Presentation

This section shows tables containing test results from all the web-based, hardware wallets, and app-based wallets cryptocurrency wallets for the starred paper. The following shows a summary of findings for each device, smartphones, paper wallets and website which I tested below.

Online or Web-based Wallets

They are a type of electronic card which is used for transactions made online; Its utility is the same as a credit or debit card, it primarily has two components, the first is software, and the second is information. The software component stores personal information and provides security and encryption of the data, whereas the information component is a database of details provided by the user which includes their name, home address, payment method, amount to be paid, credit or debit card details, etc. These wallets are vulnerable, and it is recommended not to leave a large amount of crypto token to this wallet. It does have some advantages and disadvantages:

Advantages:

- The transactions are completed in short period of time.

- It is recommended to store a small amount of cryptocurrency or token into your wallet.
- Some of these digital wallets are suitable for storing several different cryptocurrencies and making transfer between them.
- They require you to input your PIN to authorize payment or any transactions. For devices with biometrics, a payment would require your fingerprint to authorize it
- It can be very convenient for travelers. If your electronic wallet accepts your payment card and you are traveling abroad, the country you are visiting most likely will be able to use your electronic wallet as payment information too.
- Possibility of using TOR network for more privacy.

Disadvantages:

- The full control of digital wallet is in the hand of the third party, and it is not available worldwide.
- It is recommended to use a personal computer when using a digital wallet and it is important to have security software installed.
- It does not eliminate the security risks because of the Lack of knowledge in information technologies that leads users to the risk of various online frauds.

Each of these seven web-based wallets were tested while using the OWASP Top 10 Iot devices framework as a guideline.

1. **Metamask.** It is a tool that users need to access and connect to new types of applications; It is a wallet that keeps the valuable data and safe and secure, it is a shield that protects against hackers and data collectors. It is a very safe a secure way to connect to blockchain-based applications. The users are in control when interacting on the new decentralized web, and they control their own identity. No more new passwords when you visit the site, because what the Metamask does is that it can generate passwords and keys on the device so the users can only have access to their account and data (Salvo, 2020).

Users are free to choose what they want to share and what they want to keep private. Metamask has a secret phrase with twelve words that controls your account. The secret phrase is uses for the login, and the password is the proof of your ownership all included in one. It is very important to keep the secret password in an extremely safe place as you easily access it, and it would be safer there. This wallet operates over myriads of browsers such as Google Chrome, Mozilla Firefox, Brave, and Opera browsers. The example is shown on Figure 6 below:

Figure 6

Metamask Secret Phrase (Senishin, 2019)

Identification:

- The new version 8 of Metamask wallet allows users to decide what each site has access to.
- This new feature enables you to easily switch between accounts, so you can control which accounts interacts with different sites across the decentralized web.
- It allows websites to encrypt and decrypt messages intended for web 3 users.
- LavaMoat was built into the new wallet which is a set of tools to prevent cyber-attacks.

Quantification:

- Using a private key
- Modify the user model; sign a precise piece of data generated by our back end.
- Back-end will consider you of that public address.
- Signing based authentication mechanism with a user public address as their identifier
- Available plugin on Metamask Chrome extension or Firefox add-on
- It serves as Ethereum wallets, you will get access to a unique Ethereum public address which you can send and receive Ether or tokens.
- New encryption feature for developers and boosted the app’s security with its new LavaMoat tool.

2. Blockchain.info. The most popular crypto wallet where you can only have control over your crypto and your private key is blockchain. With this blockchain, you can buy, sell, send, receive, exchange, store, and switch between cryptocurrencies without leaving the security of your own wallet. Based on this blockchain security, there are a few steps that need to be taken into consideration; these steps can be that you only have access to your private keys and your crypto; or that you can set up a four-digit PIN number wherein you have a backup and recovery with your unique twelve-word backup phrase. Finally, you could choose to avoid security breaches with the advanced two-factor authentication system.

Identification:

- It is easy to use. It is just like any other software or a wallet that you use for your day-to-day transactions.
- It is very secure, and it is just a matter of securing your private key.
- It Allows instant transaction across geographies; There are low transactions fees; the cost of transferring funds is much lower than with a traditional bank.
- It allows transactions across multiple cryptocurrencies. This will help on an easy currency conversion.

Quantification:

- Software wallets and hardware wallets which you plug into a USB drive.
- Paper based wallets in which you print your public and private key on a piece of paper to keep it in a secure area.
- They are two types of Blockchain which are hot and cold wallets.

- Hot wallet which Cryptocurrency can be transferred quickly; private keys are stored in the Cloud for fast transfer.
- It has an easy access but has a risk of unrecoverable theft when hacked.
- It does have a Cold wallet where the transaction is signed offline and later disclosed online; private keys are stored in a hardware.
- This transaction helps in protecting the wallets from authorized access and other vulnerabilities.

3. **MEW(MyEtherWallet).** MEW is a free client-side wallet that is used to interact with the Ethereum blockchain while you control your own keys and funds. It allows you to generate wallets, interact with smart contract. It is not a bank or an exchange app. You are the one who is in control or in charge of it. You are the one who holds the keys, funds, and personal information. It means that MEW cannot have access to the accounts, your recovery keys, your reset passwords, or any transaction. For security purpose, it is important that every user write their keys and passwords down and save it in a secure area. Do not store your key's information on a computer or phone.

Identification:

- It is a process which begins with the generation of your Crypto Wallet key
- This key offers complete and permanent access to your account and all the funds involved.
- Your private key is extremely valuable, so it is encrypted with a master key.

- For security purpose, this encrypted key is encrypted again with a key generated from the Android of your device or a secure area if you are using and IOS device.

Quantification:

- MEW Wallet offers a PIN Code and a Biometric signature like a Face ID or a fingerprint
- It uses another software called “Aave” with the MEW wallet app.
- MEW wallet utilizes multi-layer encryption and isolation to keep your keys safely stored away locally in your device.
- No one has access to these keys except you.
- The MEW Wallet app offers a 24- word recovery phrase to back up and restore your wallet.
- This phrase acts the same as private key, so it is very important to write down on a piece of paper and stored it in a different area.

4. StrongCoin. It is a hybrid wallet that allows you to send and receive bitcoins just like any other wallet. The bitcoin private key which requires you to send money is encrypted in the user browser before reaching out to their servers. Therefore, their servers only hold encrypted private keys and you are the only one that can spend your bitcoins. Even non hybrid wallets are not safe; It would only take a hacker or an employee to have access to your keys and all your bitcoins will vanish forever. Nevertheless, experienced bitcoins users can lose their coins because they can

mistakenly delete their wallet file on their computer. So, StrongCoin can take care of offsite secure backup so you do not have to worry as much.

Table 2

Pros and Cons on StrongCoin Table

Pros	Cons
Been in the industry since 2011	Only supports bitcoin
Over 130,000 users	No support for fiat currencies
Data is encrypted in the user's browser and only unlocked with a password the user supplies	Small community
Available on several number of devices	Concerns raised by the cryptocurrency community
	1% fee charged for outgoing transactions

Identification:

- Offline paper backup like USB flask disks.
- Keroku security to ensure transparency in its security promise and a reputable cloud perform known to perform regular security audits.
- StrongCoin built-in escrow service helps protect your trading engagements when buying and selling.
- Private keys are what allow users to gain access to their cryptocurrency funds, meaning that they should be kept secure from others.
- Buy Bitcoin directly

Quantification:

- You have a public key that you can send and receive money.
- You have control of your private keys.

- It works on multiple devices like desktops, tablets, mobile devices (Android and IO's)
- It only offers hybrid wallet.

5. Jaxx. It is another cross-platform blockchain wallet which managed bitcoin, Ethereum and many cryptocurrencies. It is a simple process to send and receive many cryptocurrencies in your wallet; one can view their balance, any transaction, and detailed coin information. Furthermore, It does connect easily to third-party trading services. The third-party trading is mostly Changelly and Shapeshift that can have access to your wallet. You can buy and sell any supported digital assets which includes bitcoin, Ethereum and Litecoin. As for the security purpose, you are the one owning the keys which means that it is a twelve-word phrase mnemonic, generated by using a standard BIP 39 libraries. To further secure your Jaxx wallet, you will need a longer password combing numbers, special characters, upper- and lower-case letters. To protect the data, you must take extra security measures by encrypting core wallet data using a bank grade encryption after setting up a password.

Below are the steps on how to download Jaxx though your desktop, Chrome Extension, or mobile devices IO's and Android (Yasin, 2018).

Figure 7

Downloading Jaxx (Yasin, 2018)

Figure 8

Creating a Checksum for Every Download (Yasin, 2018)

Figure 9

Latest Features on the Application (Yasin, 2018)

Figure 10

Create a New Wallet or Restore an Older One (Yasin, 2018)

Figure 11

Two Options: Express or Custom on Jaxx (Yasin, 2018)

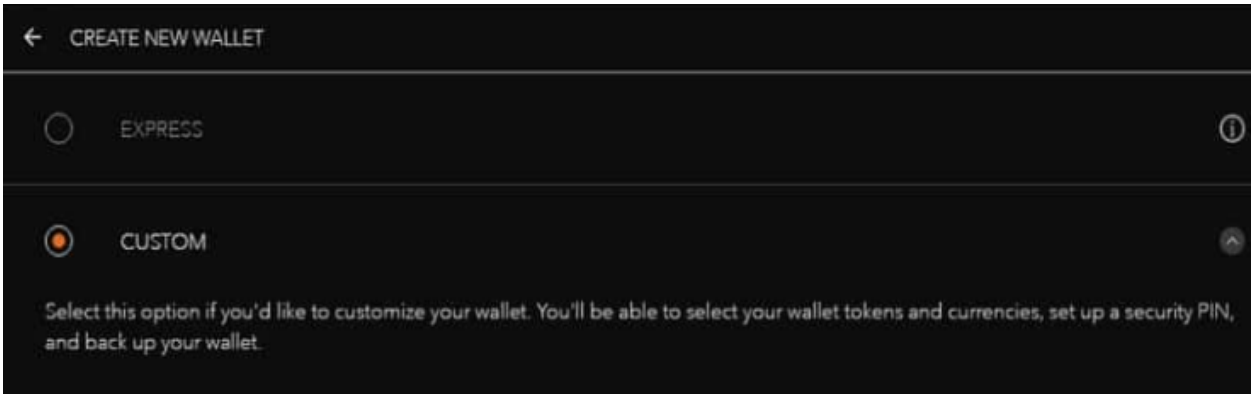


Figure 12

Selection of Cryptocurrencies on Jaxx (Yasin, 2018)

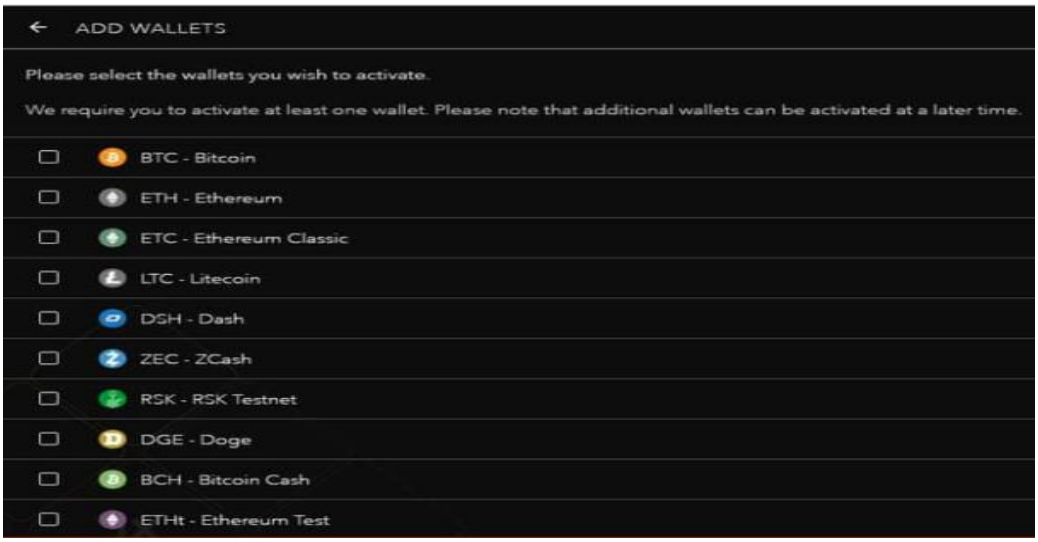


Figure 13

Fiat Currency on Jaxx (Yasin, 2018)

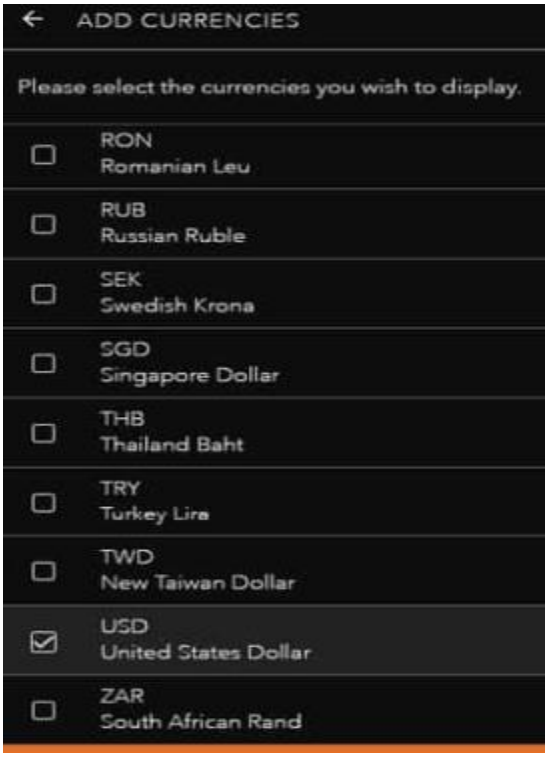


Figure 14

Backup Phrase of Jaxx (Yasin, 2018)

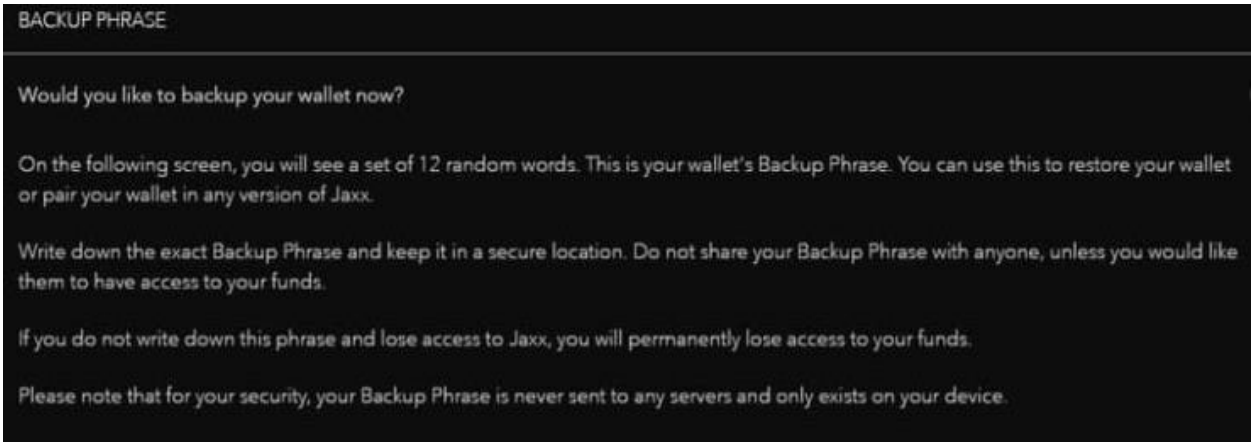
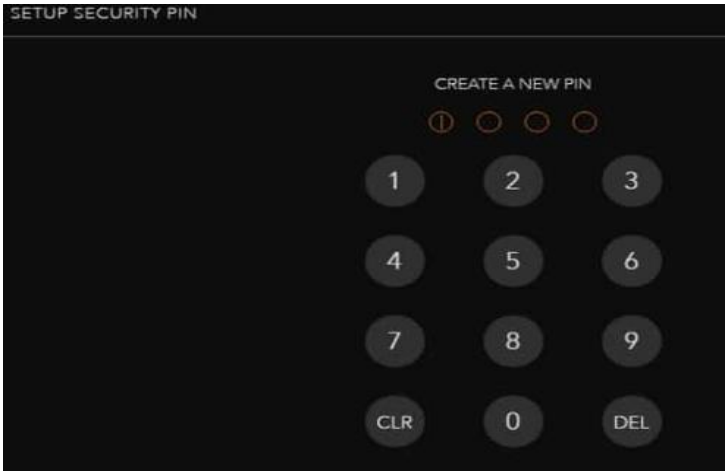


Figure 15

Set Up 4-digit Security Pin (Yasin, 2018)



Identification:

- Jaxx has both password and PIN protection.
- Jaxx never has access to that phrase or your private keys, they are always securely on your own personal device.
- There is an improved new security model that protects your sensitive information with a strong password, while using an AES-256 encryption enhanced by 5000 rounds of PBKDF2 password hashing.
- It has anonymous tracking, recovery seed, Password protection, automated updates.
- A hierarchical deterministic wallet is a wallet whose design allows to create different unplanned addresses for different transactions. It indicates that every time you transact with the Jaxx wallet, it will generate a random public key.

Quantification:

- Backup wallet where you can find your unique 12-word backup phrase and pairing code and have the option to back up your wallet by verifying the backup phrase.
- Display private keys by viewing and exporting and public address.
- Pair devices from another device with your backup phrase or pairing code
- You can Transfer paper wallet, Setting up the security PIN.
- Reset Jaxx cache by clearing cached data and BTC mining fees.

6. CoinWallet. It is one of the easiest wallets, similar like Coinbase to buy, sell and hold cryptocurrencies. You can connect to many banks to transfer money in and out of the wallet. You can even use that money to buy bitcoin and any further cryptocurrency. All your digital assets such as tokens and collectibles are stored in one place on your own device. For security purposes, your keys are protected with secure enclave and biometric authentication technology. You will need a password and an email account to be able to access and send message from that email address. Wallets have what is called a private key that is needed to send funds from a digital wallet. You are the one managing your private keys most of the time, securing your funds with a password, device confirmation, and 2-factor authentication. They will then utilize this secure cold storage technology to protect customers' funds.

Identification:

- The 2-step verification feature can also be enabled in our account's settings while using biometric fingerprints.

- You are recommended to enable a security passcode in the app's security settings.
- It is important to secure your email and your Coin Wallet / Coinbase account
- Security keys and Time-based One Time Password (TOTP) can both be enabled in your account's settings.
- Keep your devices clean and updated by utilizing anti-virus protection and scan your device regularly.
- Protect your cloud storage accounts while utilizing the address book and whitelisting features.
- Whitelisting is a security feature in the address book that allows Crypto withdrawals to only go to addresses already designated in your address book.

Quantification:

- Use a strong, long, random, and unique password for your account.
- Utilize the strongest form of 2- step verification for all cryptocurrency transactions.
- Recurring transactions are an interesting function.
- It provides simple way to buy and sell the most popular Cryptocurrencies such as Bitcoin, Ethereum and Litecoin
- You can purchase Cryptocurrency via credit or debit card, a wire or bank transfer.
- Setting up an account is a quick and easy process, it requires your full name, address, bank details and proof of ID.

7. Green Address. It is a handy wallet with multi-signature, enhancing security feature, and privacy; this wallet enables users to access, store, send or receive bitcoin alone. But users can access their wallet through their mobile phone or the web. It does have good security features to ensure the safety of the users' funds. It does support twelve languages, and the wallet app is available for download in specific app stores such as Android and IOs stores. For security measures, your keys are not directly sent to you, not even the servers and encrypted form contain them. However, logging in the app will require you to input your mnemonic phrase and password. Eventually, you will need to access the app with a PIN number. With this feature, you can check your wallet balance anytime, or conduct any transactions without full access to the wallet. The article on "Review Green address Bitcoin wallet" mentioned that the Green Address has some advantages and disadvantages that users should be aware which are listed below (Ryan, 2018).

Advantages:

- Several security tools availability with four different options on the two factors authentication
- Multi-signature of wallets
- API tools availability to use.
- Mobile platforms availabilities
- Four fee programs availabilities

Disadvantages:

- Recovery phrase and PIN code are created by the server.

- Only Bitcoins are supported by the platform.

Identification:

- Provide pre-signed transaction which means that each time your wallet has updates we will forward to you by unlocking funds at a date in the future of your choice.
- Offering a second signature that provides extra security with two factor authentications for transacting, transaction limit, and instant payments with double protection.

Quantification:

- PIN login to your wallet from any of your devices without using passphrase.
- Generated recovery passphrase and PIN codes and setting up the two-factor authentication through your phone number.
- The two factors have four options which are google authenticator, phone call, email, and SMS.
- They are very organized properly, all the buttons are visible, and the navigation through the wallet is extremely convenient for beginners in the Crypto industry.

Hardware Wallets

1. **Trezor T.** It is a hardware wallet that allows you to send, receive, and store a wide range of cryptocurrencies; It is also much safer than any traditional software wallets in which your private keys are held on the physical device instead of a desktop or a smartphone. It is never connected to an internet server, meaning that hackers

cannot have access to your funds. It is one of the multi-currency wallets in which one can store a plethora of cryptocurrencies. It does have some advantages and disadvantages which are listed below.

Table 3

Trezor T Wallet Advantages and Disadvantages

Advantages	**Disadvantages**
It is the safest way to store your cryptocurrency	You will need to buy an amount of money if you want to buy a Trezor wallet
Your private key is always kept offline	Consideration on how often you plan on using the Trezor hardware wallet to make transactions
Whether is to send/ receive coins or check your balance, you will need your personal PIN number	When planning to send funds you will need to plug the wallet to your desktop device then logging with your PIN which is not convenient way to access your cryptocurrencies.
You have a backup passphrase which must be writing down	When it comes to user friendliness, Trezor can be a little bit tricky for starters, especially if they have not used a similar device before.
It is impossible for hacker to attack the Trezor wallet	

For security overview, the wallet has something called “limited USB Connection” which means that even if the computer device is infected, your cryptocurrency would still be safe. The Trezor team has designed another way for the PIN number like every time you enter a number, the setup of the numbers changes automatically. That is the way to avoid your PIN getting compromised by hackers. The article titled “An in-Depth look at the Trezor Model T hardware wallet “ stated how to set up or install the device with specific instruction to follow while going to Trezor website to initiate the wallet or

the firmware, creating a new wallet, backing up the seed, adding a PIN and naming the wallet (Redman, 2019).

Figure 16

Initiate the Firmware, Create a New Wallet and Backing Up the Seed (Redman, 2019)

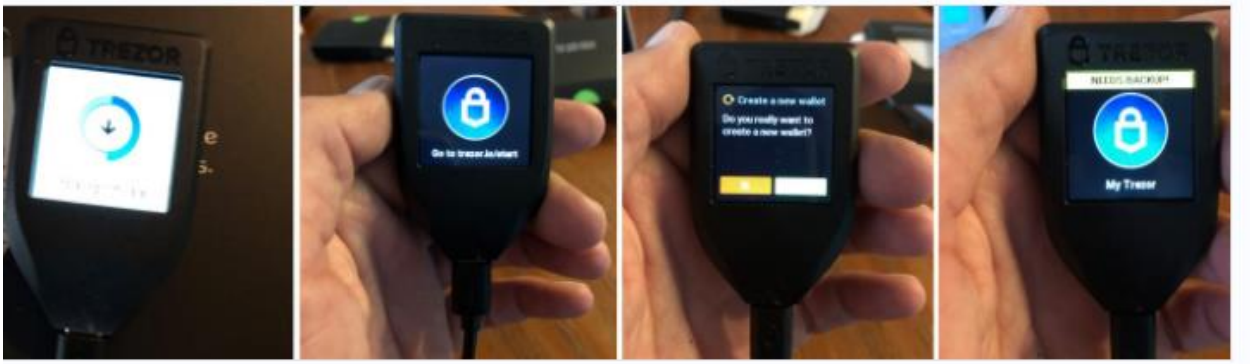
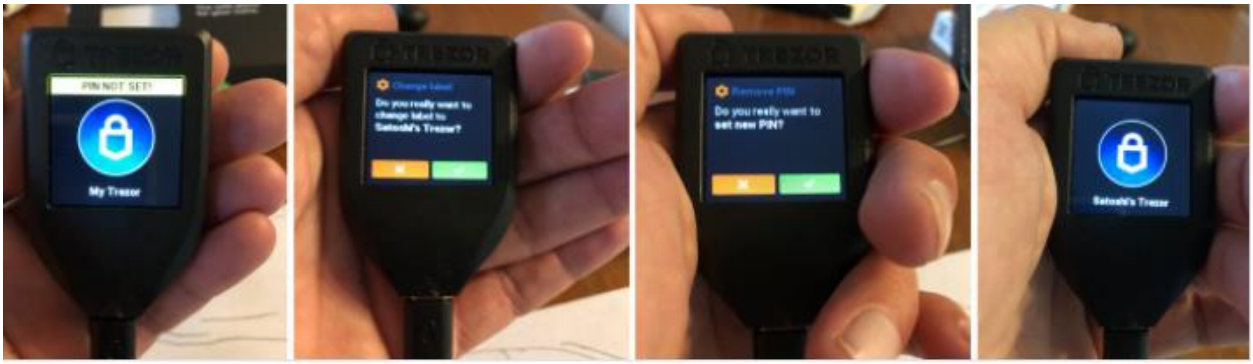


Figure 17

Setting Up the PIN and Naming the Device (Redman, 2019)



Identification:

- PIN is a powerful tool to keep your coins safe.
- Passwords on the device are individually locked with Trezor password managers employ a user's digital keys.
- Creating the standard recovery seed which enables users to recover the entire wallet with the help of a twelve-word recovery seed.

- Contains a passphrase to generate a new wallet; users will be required to enter the passphrase in addition to their security PIN.

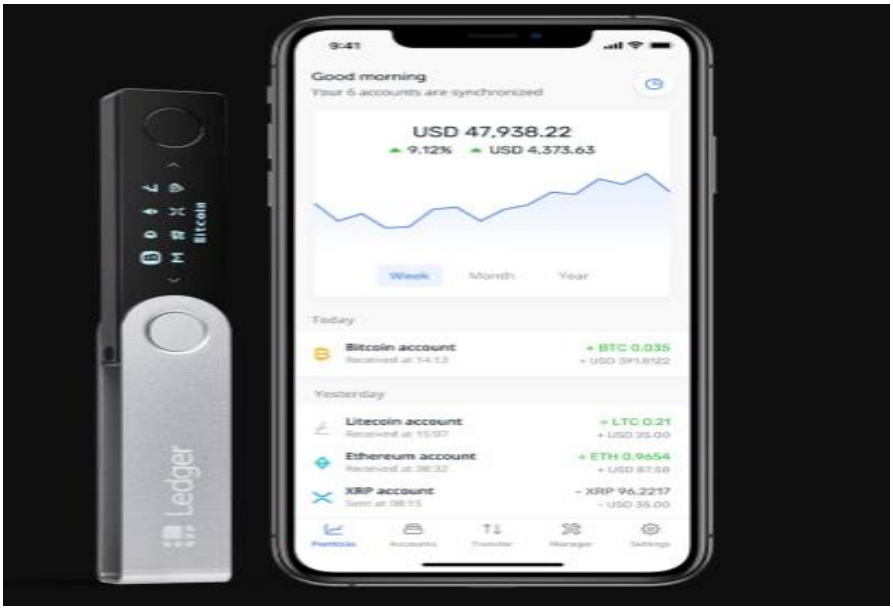
Quantification:

- It is protected by a PIN code which can be up to nine digits long.
- You Keep your recovery seed safe.
- You can reinforce your accounts with U2F hardware.
- It is compatible with both computers and smartphones software's such as windows 10. MAC operating systems, Linux, and Android Operating systems

2. **Ledger Nano X.** It is another hardware wallet that allows you to buy and securely manage your crypto in one single-app, everywhere you go. You connect your device to the ledger live mobile app with Bluetooth and safely manage your crypto from your smartphone. For security measures, when owning crypto, you only get your private key. You need to secure it to secure your funds. It does offer the best level of protection in which your keys will remains protected in a certified secure chip. It does support 1500+ crypto assets, helping you in managing any transaction (Figure 18, shown below).

Figure 18

Ledger Nano X (Phillips & Phillips, 2020)



It does come inside a small package that includes the device itself, a USB cable, one keychain, a kay ring, and multiple recovery sheets to write down your seed phrase provided.

Identification:

- You can set up the PIN protection that the end user must enter correctly before accessing all services provided by Ledger Nano X
- Ledger Nano X does not keep backup of your recovery phrase.
- Make sure you are the one holding your 24 words recovery phrase.

Quantification:

- You can Set up a PIN code on your device with 8 digits for optimal security.
- Set up a password with 4 numbers to prevent unauthorized access ledger data on your phone.

- You can set up the software on your IO's, Android and computer
- It does support most languages and you can select the one you prefer.

3. **Keepkey.** It is a hardware wallet making the bitcoin security even more simple for users; It does provide users or investors with a secure environment to store their cryptocurrency wallets such as Bitcoin, Ethereum, Litecoin, Name Coin, and Dash. As for security, keepkey stores your private keys in a separate offline environment. In addition, the keepkey can be protected by using the PIN code and backed up with an eighteen to twenty-four-word recovery seeds. It does have several randomizations to prevent hackers from stealing your digital assets with malware.

Identification:

- The private key is stored directly on Keepkey and it does not leave the device.
- Your PIN code prevents any hackers from having access or viewing any transactions or your balances.
- The keepkey wallet is entirely backed up with a 12-word recovery sentence that is generated on setup. It can also be used to recover in case if you lose your wallet or it gets stolen.
- You can have the convenience of accessing and trading cryptocurrency directly from your wallet.

Quantification:

- The keepkey is very flexible and it can be used in different types of operating systems devices such as Windows, MAC OS, Linux, Android, and Chrome extension
- All private and public keys must be secured with an authorized PIN Code which you will have access every time.

The keepkey wallet does have some advantages and disadvantages that needs to be taken into consideration.

Advantages:

- The level of security of the Keepkey wallet is very high because the hardware wallets are impossible to get hack or concede.
- The wallet has a built-in exchange with other cryptocurrencies wallets for further ease of use and functionality for investors.
- The Keepkey wallet can manage multiple cryptocurrencies.
- You will need a randomized PIN number to unlock the wallet.

Disadvantages:

- If you leave your device or computer without you being in front and someone else have access to your device, you can lose all your information on your device.
- The keepkey wallet is very expensive to purchase because of the quality of the wallet.

4. **Bitbox.** It is a simple minimalist hardware wallet which secure your digital assets and manages them easily. Moreover, it does support Bitcoin, Ethereum, and Litecoin. For security purpose, it does have a private key stored on an ultra-secure tamper-proof chip: the password is encrypted; malware proof meaning private keys never touch the internet or external device; easy backup and recovery; unified accounts; full node support; encryption communication and open- source auditability.

Identification:

- It has an easy backup thanks to a microSD card and can display your 24 recovery words.
- It is important to securely verify your transactions by receiving addresses and other data while entering your password directly on the OS device instead of the app itself.
- A secure chip is important to avoid any brute force attacks by using your password which will make such attacks even more difficult to access it

Quantification:

- You will need to set up a name and password for the wallet.
- Each device's password encrypts the backup of the wallet and is generated with the password; if in case you change your password in the future, the device password will no longer be recognized or will no corresponds to the recovery passwords of older backups.
- You will need to set up your password which consists at least four characters.

5. **ColdCard.** it is an easy wallet to use, extra secure, open source and very affordable hardware wallet. It is easy to backup with an encrypted microSD card. You have full control over your bitcoins, meaning that no third party can freeze, or have access to your funds. You are responsible for securing and backing up your wallet. Your private keys are stored in a dedicated security chip. They used the software called Micro Python to make changes. For security purposes, the wallet is loaded from a secure specialized environment provided by the device. It does provide a very strong protection against computer vulnerabilities and malware.

Identification:

- It only supports Bitcoin and Litecoin cryptocurrencies.
- Verification of the device serial number to ensure that it matches the serial number on the package.
- You are only recommended 4 to 6 digits while entering the prefix PIN to protect against hackers.
- You will need to enter the rest of your preferrable PIN with only 4 to 6 digits.
- It supports a passphrase of 24-word seed in which you will access to a new wallet for any passphrase.

Quantification:

- The PIN code for Coldcard can be from 4 to 12 digits long which can be divided into two parts: the prefix and the rest PIN.
- The Coldcard can store the private key in a secure element that will encrypt the data SHA 256 hashing and a true random number generator.

- You can also import the existing wallet by providing 12-to-24-word seed for the Coldcard.
- It also uses a microchip to store important information.

App-based Wallets

1. Coinbase. The number one mobile app, crypto wallet app, and web3 Dapp browser. It makes it easy for users to send, receive, and store bitcoin, Ethereum, Litecoin and Bitcoin Cash. It allows users to interact with the web3 decentralized application powered by Ethereum. The capabilities of Coinbase are:

- Security of the user-controlled crypto wallet, meaning sending, receiving, securing, and storing; you are in control of your private keys which are stored only on your devices using secure element technology. You only have access to your funds, nobody else.
- You can send cryptocurrency payment to anyone all over the world. It does have a backup private key to the cloud, meaning you backup your wallet and private keys to Google drive to prevent yourself from losing your funds, your device, or misplacing your recovery phrase.

Coinbase is very safe and has been used in more than 30 States in the United States and many countries in which you can send and receive funds, can store users' digital assets in an offline storage, and the cryptocurrency is stored on the user's servers with protection.

Identification and Quantification:

- You can manage your portfolio by buying and selling digital currencies, keeping track of all of them.
- You can invest in cryptocurrency by scheduling a day you want to buy if it is daily, weekly, or monthly.
- You can use the Coinbase app on Android and IOS.
- In addition to the verification on all accounts, you will need a username, password while entering a code provided by the mobile phone and adding more security to the account.
- You can add security by storing your funds in a vault even if it shows any delayed withdrawals.
- It is beginner friendly and easy to use with clear tools, great information and details on different cryptocurrencies wallets.
- It accepts a variety of payment methods and fiat when it comes to the money to buy Crypto through bank transfers like debit/ credit card.
- You will need a strong password very long, must be random and unique.
- To protect your mobile devices, you should use anti-virus protection and a scanner for your device.
- To prevent any threat, you can ensure that your digital assets are in a safe place by stopping the most advanced malware, scammers, and ransomware.
- Be very aware of phishing so that they will not have access to your information (debit card, credit card, and password).

- Coinbase is a very safe application that ensure that your account and cryptocurrency are in a safe place.

2. Electrum. It is a fast, secure, and easy to use wallet and furthermore, it is one of the most popular bitcoin wallets on the market. It does split the permission to spend your bitcoin between several wallets. It also supports hardware wallets like Ledger, Trezor and Keepkey. It has various user interfaces which can be used on mobile, and desktop. It is a free software; it is decentralized, and anyone can run an electrum server.

They are two factor authentication which are being safe from malware, using two factor authentications by electrum and trusted coin, which you can only verify. It does have a private encryption key using a seed containing twelve to twenty-four words, with a strength between 128 bits and 256 bits, making it difficult to crack. A seed phrase is also a recovery tool in which if you forgot your password, the seed phrase is the only way to bring your wallet back (Bogdan, 2018).

Identification:

- You will need to trust the Electrum lead developer since it was created in 2011.
- You can connect to a trusted server by letting Electrum decide which server to use the option to take.
- You will receive a 12 words of generations seed which will allow you to recover your wallet in case your computer crashes.

- You can create a password with a maximum of 6 to 8 characters to encrypt your wallet's keys.
- All the investor's funds are swept from a paper wallet or transferred into the Electrum wallet while importing the private keys.
- Electrum's seed allows you to rebuild all of your wallet 's addresses and private keys.
- Backups of Electrum are very easy to first create, secondly, manage and thirdly provide great security.

Quantification:

- It uses a remote server that can perform the most complicated tasks and allows you to restore your wallet easily and your passwords.
- It does have a private key with a 128-bit base value, meaning that investors do not need any backups.

The fact that Electrum does support a few cryptocurrency wallets like Bitcoin cash, Litecoin and DASH, however, it does have some advantages and disadvantages that should be considered:

Advantages:

- The operation speed of the Electrum is very important.
- It is very simple to use the app.
- It has a very safe systems which provides investors with control over their funds.

Disadvantage:

- There is an inability to generate the Nested Setwig addresses due to insufficient compatibility with every services.

3. Blockchain. It is a very safe, easy to use and supports a wide range of currencies. It uses a twelve words backup phrase to protect your wallet; acting as a backup to ensure access to your funds. Your wallet private keys never leave your possession, and you only have access to your wallet. You can backup when you needed too while blockchain creates a server-side backup by using a strong encryption. For security feature, you include a PIN protection, paper wallets import as well as submitting the wallet code for security audits.

Identification:

- Blockchain security feature contains records of transactions of any digital assets between two different parties.
- Security aspects can be very critical while focusing on transparency, confidentiality and protection against hackers and fraudsters.
- Blockchain offer confidentiality by enabling investors with a ledger to see only the authorized transaction.
- It also helps prevent malicious attacks.
- Investors have their own private and public keys most precisely for the transactions they make and their account for their personal signature.
- The public key blockchain uses computers to connect to the public internet in which any computers can obtain access and join.

- As for the private key blockchain, only members who have their own identity registered can join.

Quantification:

- Solidity is used to build and deploy smart contracts on any blockchain and Ethereum based applications.
- Geth is a program which acts as a support of the Ethereum blockchain and allows investor to transfer tokens between addresses, create, and execute smart contract through the Ethereum virtual machine, and explore block history on blockchain.
- Remix does support deployment, testing and debugging of smart contracts that connect to the blockchain while using MetaMask.
- “My Ether wallet”, the safest way to store Cryptocurrency is by using a paper wallet that has two ways of storing; namely hot and cold storage; hot storage makes it easy to spend Crypto as it is connected to the internet but can be vulnerable to hackers; cold storage which stored the cryptocurrencies offline is very difficult to spend but is very safe from attackers.

The benefits of Blockchain are as follows:

- It has a great transparency with blockchain technology.
- It enhances security better than any other record keeping systems.
- It eliminates error through real- time tracking of transactions.
- It improves traceability.
- It increases efficiency and velocity, but reduces on- cost, and material cost.

4. Robinhood. Robinhood did not start as a crypto wallet but is a free-trading app that lets investors trade stocks, options, exchange-traded funds, and cryptocurrency without paying commissions or fees. It does offers both web and mobile trading, but the platforms are purposely bare-boned, and some investors may find the range of tradable securities and account options lacking. The positive aspects of Robinhood are that you can trade and exchange cryptocurrencies in an easy manner. Its target audience are first time traders and cryptocurrency investors to whom they charge annual fees and account fees.

It is very beneficial for those are constantly trading their crypto Coins. In other words, the Robinhood wallet will suit short-term traders the best to perform trades very quickly and effectively, while avoiding the possibility of missing out on a potential deal. A key benefit that one will notice is that Robinhood's crypto wallets support all sort of main cryptocurrencies like Bitcoin, Bitcoin Cash, Ethereum classic, Litecoin, and Dogecoin. It is super easy to use, beginner friendly when it comes to cryptocurrency choices, and its usability aspects (Carey, 2020).

As for the advanced security features with online wallets, especially those that are based in exchanges have a hard time when it comes to persuading the user that their crypto coins are secure while being in the wallet in- question.

When it comes to discussing Robinhood's Crypto wallets with respect to security, you'd have the ability to turn on two-factor authentication, while also being able to add some custom PIN codes in order to ensure even better standards of protection.

The negative aspects when it comes to using Robinhood's Crypto wallets is that it does come with a lot of issues on the security side of things; It does have a potentially unsecure cryptocurrency wallet when it comes to online, software(app), hardware, and paper wallet in the order of the least secure to the safest one. Robinhood crypto wallet is an online based exchange platform because it is always connected to the internet in which can always be hacked or stolen during a cyberattack. It does not have any retirement account, no mutual funds or bonds, and has limited customer support.

Identification:

- You have a sensitive details and information present there, for instance your Social Security Number which is encrypted before they are stored on the app.
- Your account password is not stored on the plaintext but hashed while using the BCrypt hashing algorithm.
- Your mobile phone and the web application communicate with the servers while using the Transport Layer security.
- It does not have any access to your banking verification after it is processed; they do however use trusties third party to access the investor's information on their bank account such as your account balance.
- You can secure your mobile app by using a Face ID, a PIN code with a four-digit number, and touch ID.

Quantification:

- It offers market news where you can browse to see news articles on financial posts, Reuters, New York Times, and MarketWatch.

- It provides top movers which shows which stocks are moving the most.
- You can create a customized list of stocks you would like to follow.
- You can use analyst ratings to help you decide on what you need to buy, hold, or sell.
- The candlesticks chart helps you to analyze trends in a stock performance.
- Margin trading allows investors to control their buying power.
- The stock screeners which scan the whole market by providing averages on the price, trading volume, charting patterns and allows investors to compare different options.

5. Exodus. It is a secure, wonderful desktop bitcoin and cryptocurrency wallet. What makes it different from other wallets is that it focuses on user experience; it provides information on your crypto assets and makes it easy to trade cryptocurrencies. It does provide the information you need and makes it easy to find what you are exactly looking for. It does not have a hosted centralized server. You are in control of your cryptocurrencies meaning your own security guard; you keep your private keys on your computer. It is also available on Android and IOs devices and supports twelve words seed phrase.

Identification:

- Setting up a password on Exodus wallet is important and must be a unique password with at least 16 characters long to prevent hackers from gaining access or using malware.
- They used hardware wallets to enhance security while pairing it with Trezor.

- In case of funds lost in the Exodus Wallet, you are required to send the remaining funds to a different wallet, and a wallet Safe report.
- It is important to protect your secret twelve words recovery phase.
- It is important that you do not download any suspicious sites or pirates' sources.

Quantification:

- You can use the Exodus Wallet on multiple devices such as Android, IOS, and computers if each app is on the latest version.
- After downloading the Exodus wallet app on the current computer, you will need to find the 12-word secret phrase and restore it into your new computer device.

6. Mycelium. It is one of the oldest and most popular bitcoin wallets available. It is accessible, you can send and receive bitcoin anywhere in the world and at any time. You can even pay for goods and services, receive funds from others quickly and easily with the QR code embedded right on the front page of the wallet. It allows you to change settings to your preferences.

As for security feature, Mycelium wallet has the expected PIN protection for opening the wallet, sending funds, and exporting private keys. It does have a backup seed phrase of twelve random words when you generate your wallet. The seed phrase can be used to restore your wallet on a different device if needed.

Identification:

- Blockchain application is one of the main security considerations for this wallet.
- it has a PIN protection for having access to the wallet, sending funds, and exporting the private keys.
- you get a backup seed of twelve random words which can be used to restore another wallet if needed.
- you can monitor your funds or balances without exposing your private keys to anyone.
- Mycelium does a great job on maintaining the security of your Bitcoin when it comes to the smartphone app.

Quantification:

- it is one of the oldest Bitcoin wallets used on Android and iOS devices.
- Mycelium wallet is very accessible meaning you can send and receive Bitcoin anywhere.

7. CashApp. It is a mobile payment service created by Square. Inc., very easy to download on devices such as iOS and an Android and allows users to send or receive money from another user using the mobile App as well. It allows you to request, and transfer money to another cash account which runs like a virtual bank platform. You can withdraw the money with their ATM card called the Cash Card, which is a black customizable Card, which makes investing in Cryptocurrency even more convenient.

Identification:

- It does have security features such as PIN entry, Touch ID, or Face ID verification protected payments.
- It does have limited Cryptocurrency Wallets and your Bitcoins are securely stored in an offline system.
- You will receive an account notification alert on your email.
- They protect all your data by using the PCI-DSS level 1 certification.
- You have protection on unauthorized charges.

Quantification:

- It is used on smartphone devices devices using both Android and iOS operating systems.
- They will help you create a unique username called a “$” cashtag which allows users to transfer and request money from one-another after entering this username.
- It does not charge monthly fees.
- You can invest or buy stocks in specific companies with few restrictions on the scale of purchase.
- There are fees while using Credit or Debit Cards from elsewhere, CashApp will charge of 3% of those transactions in order to complete.

Paper Wallets

The safest way to store any cryptocurrency is by using a paper wallet. It is an offline cold storage method of saving cryptocurrency. It includes printing out your public

and private keys on a piece of paper which you store and save in a secure place. The keys are printed in the form of QR codes which you can scan in the future for all your transactions.

The reason why it is so safe is that it gives complete control to the user. You do not need to worry about the well-being of a piece of hardware, nor do you have to worry about hackers or any piece of malware. This makes you the master of your investment, and if following the instructions are followed properly, there is a little chance of your private keys falling into someone else's hands; of course, this means that keeping a record of them is even more important. Losing private keys means you will lose the entire contents of your paper wallet.

Data Analysis

A data analysis is a set comprised of information that uses qualitative and quantitative data to analyze as well as to evaluate and compare different types of cryptocurrency's wallets but mostly be focused on three cryptocurrency wallets that I am currently using on my device which are Robinhood, CashApp and Coinbase. Below is the procedure used to analyze the data.

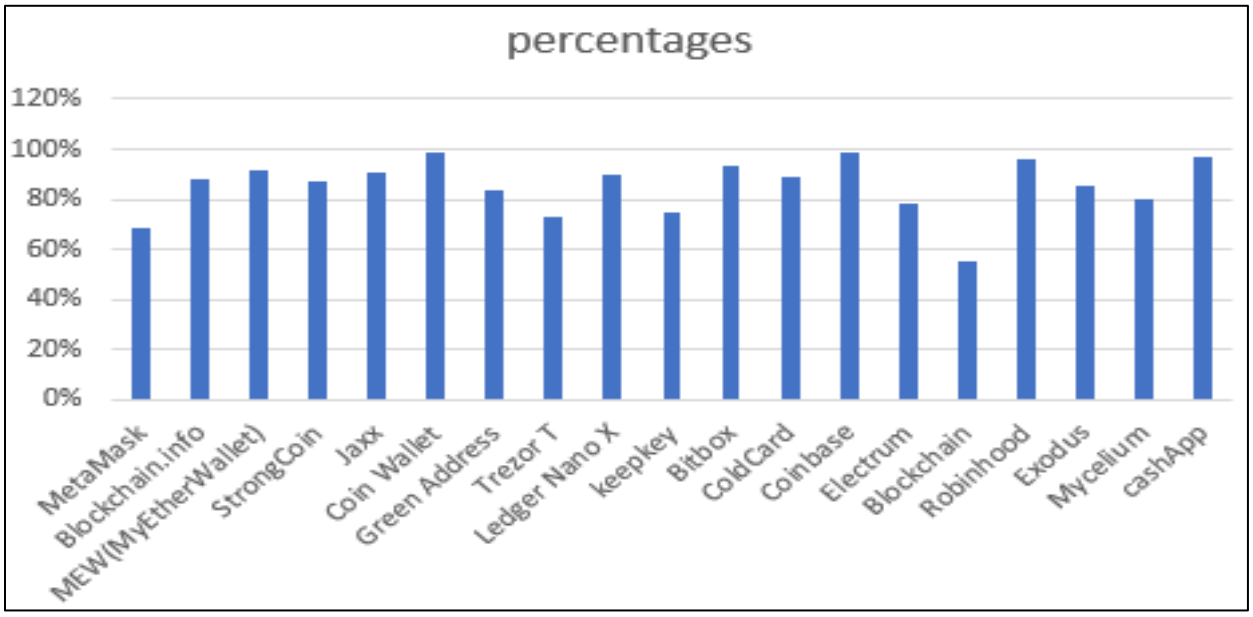
Figure 19

Data Analysis of Different Cryptocurrency Wallets

	wallet type	web interface	mobile app	desktop client	independent wallet	privacy	security	percentages
MetaMask	Hot wallet	yes	yes	yes	yes	moderate	weak	69%
Blockchain.info	Hot wallet	yes	yes	no	no	weak	good	88%
MEW(MyEtherWallet)	Hot wallet	yes	no	yes	yes	good	good	92%
StrongCoin	Cold and Hot wallet	yes	yes	yes	yes	variable	good	87%
Jaxx	Hot wallet	no	yes	yes	yes	good	good	91%
Coin Wallet	Software, Hot wallet	yes	yes	no	no	good	good	99%
Green Address	Hot wallet	yes	yes	yes	yes	moderate	good	84%
Trezor T	Hardware wallet	yes	no	no	yes	variable	good	73%
Ledger Nano X	Hardware wallet	yes	yes	no	yes	variable	good	90%
keepkey	Hardware wallet	yes	no	yes, USB HID- class	no	variable	good	75%
Bitbox	Hardware wallet	yes	yes	yes, USB	yes	good	good	93%
ColdCard	Hardware wallet	yes	no	yes, USB	yes	variable	good	89%
Coinbase	Software, Hot wallet	yes	yes	no	no	good	good	99%
Electrum	Hot wallet	no	no	yes	yes	good	moderate	78%
Blockchain	Hot wallet	yes	yes	no	no	weak	good	55%
Robinhood	Hot wallet	yes	yes	yes	yes	moderate	good	96%
Exodus	Hot wallet	no	no	yes	yes	good	good	85%
Mycelium	Hot wallet	no	yes	no	yes	good	good	80%
cashApp	Hot wallet	yes	yes	yes	no	good	good	97%

Figure 20

Percentages *of Different Cryptocurrency Wallets*



According to the statistics, the three most popular platforms that I am currently using, and most traders and individuals are using nowadays are, Rohinhood, Coinbase Wallet, and CashApp; when comparing the three cryptocurrency wallets, they are very easy to use but have some slightly differences. Robinhood is a free trading application that allows traders or investors to trade free stocks, options, cryptocurrencies, exchange trading funds without paying any fees. It does offer web, individual taxable accounts, margin accounts, cryptocurrency, and mobile trading.

The mobile trading platforms offers customizable alerts, candlesticks charts, news, and ability to listen to live to earning calls. Robinhood also puts limits on orders on all transactions of the traders so they do not perform if the market moves against them after an order is placed. It makes transactions quite a lot easier by showing a trading price without fees. Unfortunately, having no fees causes a huge mark-up in which other orders and trade prices are not showed. Robinhood only offers a limited range of 7 stocks for trading. If you plan on using the US Dollar for your trading, Robinhood is the best choice for you.

If you want to use your funds with bitcoin or buy bitcoin and transfer it to a private controlled wallet or a different trading platform, Coinbase wallet would work best for you as It has both a convenient layout and software with online wallets which gives access to a wide spectrum of decentralized innovation in which allows users to store their own Crypto. You do not really need to create a Coinbase account to use the Coinbase Wallet app. It helps users to manage their own private keys by storing their Crypto assets on their devices. There is also a fee schedule posted on their website depending

on how much you trade, which can be difficult to calculate the net trading price. Coinbase offers more than17 stocks for trading as well. If you are looking to only invest in the future of currency, which is digital Coinbase remains the easiest place to buy, sell, and manage your digital currency.

The last one is CashApp, owned by Squares. Inc., it is a financial technology industry leader and one of the largest payments transfer application wherein users can send and receive money. But the App is also used to invest in stocks, as well as to buy and sell Bitcoin; it has been increasing immensely in popularity since the year of 2020 due to the pandemic or COVID-19 pandemic situation with the percentage of 127% in the quarterly revenue, and a 361% increase year-on-year.

Furthermore, it functions very similar to a bank account, giving users a debit card called “cash card” to make purchases using their funds in their cash app account even easier. CashApp does not charge any fees when sending and receiving money. However, if you are using a credit card, there is a fee of 3% on the transaction to send money. But to avoid being charged, it would be better to link your bank account and deposit the money in the next 2 or 3 days maximum. CashApp does have a limited stock and can start as a little as a one-dollar purchase, however, they do allow you to invest in partial shares which is a good way to build a portfolio with a small amount of cash.

Summary

After identifying, quantifying, analyzing, and evaluating the Cryptocurrencies wallets such as web-based wallets, App- based wallets, hardware wallets, we conclude

that they do possess different types of security features and privacy that are very important. To secure the cryptocurrencies wallets, you can either convert to paper wallet by following their instructions on bitcoinpaperwallet.com or using a cold storage for a safe place. The last chapter would be focus on the results, the conclusions, and the future work on how to evaluate security in Cryptocurrency wallets.

Chapter V: Results, Conclusion, and Recommendations

Introduction

The final chapter will call upon the generalization of the paper; it will then look at the process, testing framework, results, or conclusions before providing any recommendations in the field of research.

Results

Earlier in this paper, in Chapter III, methodology aims, and objectives were set out; this chapter will look at the solutions and methods on how to secure the Cryptocurrency wallets by identifying their security features to protect them from hackers and quantifying by providing tools and techniques that can help protect a user's funds.

The main objectives at the start of the paper were to answer each of the following questions.

- The security measures needed to protect users of online Cryptocurrency trading platforms.

The security measures needed to protect users of online Cryptocurrency are: to use the physical wallets to store the majority of users Cryptocurrency while keeping a minimum amount of currency in the online wallets instead of the online wallets because it attracts the attention of hackers; it is important to use two strong and unique passwords; get an understanding of the Cryptocurrency wallets you want to buy or sell; protecting yourself from mobile phishing and it is crucial to use hot wallets that are more convenient for traders or investors.

- Find out if these Cryptocurrency wallets can be stolen by hackers.

Yes, the Cryptocurrency wallets can be stolen by hackers even if it has a hyper security. It would be phenomenal if we can create an unshakable exchange, however, that is not the case; hackers do have multiple methods such as phishing viruses with which they obtain users API keys, two-factor authentication codes, and other information to execute their plan.

- The different types of Cryptocurrency wallets.

Any types of Cryptocurrencies wallets are combined with private and public keys which can be classified as follows: Desktop, mobile, hardware, paper, web, or online wallets.

- To evaluate security in Cryptocurrency wallets.

To evaluate security in Cryptocurrency wallets, you will need to add new but critical features like PSBT (Partially Signed Bitcoin Transaction) in the hardware wallets products and respond to bug statements and the vulnerabilities. It is also important to make sure your device is using the updated software, setting up extra layers of security meaning two-factor authentication in which a confirmation code will be sent to your mobile phone before accessing it.

Conclusion

To conclude, I would say that the objective of the study was to enable users to evaluate the security and privacy of the Cryptocurrency wallets. The main aim was to improve the security in Cryptocurrency trading by searching for relevant articles on Cryptocurrency wallets attacks to gain a strong understanding of Cryptocurrency

wallets. It will be analyzed in a literature review and this review will be utilized to create a testing framework.

A detailed literature review of attacks on the types of Cryptocurrency wallets are described on Chapter II along with weaknesses and testing methods provided. It was found relevant to the main topic and academic as well. The academic resources incorporated on this paper are Science Direct, Coin telegraph, Research gate, IEEE Explore describing the main topic on evaluation of the Cryptocurrency wallets and the importance of security technology on these Cryptocurrency wallets.

Chapter II literature review was covered by the Cryptocurrency wallets attack types, hardware attacks, and human attacks. The attack types in this chapter enabled the design of a testing framework to test different types of wallets which was then analyzed in Chapter IV where testing was carried out using some criteria from the OWASP Top 10 for IoT devices. The final reports were presented in Chapter IV data presentation and analysis where outcomes, and findings on different types of Cryptocurrency wallets were discussed. After analyzing numerous sources, several articles, this paper was able to gain a detailed understanding of the topic. The essay began with the introduction by giving the readers a history and background on the topic about Cryptocurrency Wallet security.

After reviewing these articles related to the topic, this essay was able to identify and quantify the different types of Cryptocurrencies Wallets. As for the testing framework, the OWASP guidelines for IoT devices were chosen because it allowed the user to understand how to evaluate security in Cryptocurrency wallets. Furthermore, a

table for each wallet category such as App-based, Web based, Desktop wallet, Mobile wallet, and Hardware wallet was created, and it was described and tested in Chapter IV. After evaluating the different types of Cryptocurrencies wallets, this essay concludes that paper wallets are the most secure form to hold your Cryptocurrency in.

Future Work

While working on this paper with the support provided by my advisor, I was able to finally conclude my Starred Paper by utilizing well known research databases such as Google Scholar, IEEE Explore, ResearchGate to find relevant and up-to-date articles related to the main topic which is evaluating security in Cryptocurrency Wallets. As we know, technology has been moving at a phenomenally fast pace with new devices on the market which provide security features in Cryptocurrency wallets. As mentioned earlier on in Chapter UV about the different types of Cryptocurrency wallets, the most popular platform currently in use by investors, traders and even myself are Robinhood, Coinbase and CashApp; the fact that I am also using all these three platforms helped me realized that they all need some more security features for protection against hackers. They are specific ways to keep and secure your Cryptocurrency wallets which are: having two strong key passwords; working with reputable Cryptocurrency Wallets on mobile apps; protecting yourself from mobile hacking or phishing; being aware of how your wallet is used in transactions like Robinhood, Coinbase and CashApp; avoiding sharing your secret key with anyone; hot wallets are more convenient for investors or traders. But they are two platforms that I will recommend everyone to join, and which are the more secure the two software’s being Coinbase and Robinhood

because they are more convenient, they facilitate ease of access, provide the ability to trade and buy Cryptocurrency wallets, can work with reputable Cryptocurrency wallets and mobile apps.

References

Alexandre, A. (2019, June 6). *Report: Nearly $10 million in XRP stolen in GateHub hack*. Cointelegraph. https://cointelegraph.com/news/report-nearly-10-million-in-xrp-stolen-in-gatehub-hack

Ameer, R. (2017, July 12). *Paper wallet guide: How to protect your cryptocurrency*. Blockgeeks. https://blockgeeks.com/guides/paper-wallet-guide/

Baldwin, C. (2016, August 3). *Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong—Reuters*. https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP

Benton, O. (2019, July 12). *Paper wallets—A relic of the past*. Medium. https://blog.trezor.io/paper-wallets-a-relic-of-the-past-1f711ba82b8c

Bischoping, G. (2018). Prosecuting cryptocurrency theft with the Defend Trade Secrets Act of 2016. *University of Pennsylvania Law Review*, *167*(1), 239-259.

Bogdan, K. (2018, June 26). *Electrum: An Analysis of a Veteran Bitcoin Wallet | Finance Magnates*. Finance Magnates | Financial and Business News. https://www.financemagnates.com/cryptocurrency/education-centre/electrum-analysis-tried-true-bitcoin-wallet/

Browne, R. (2017, December 7). *More than $60 million worth of bitcoin potentially stolen after hack on cryptocurrency site*. CNBC. https://www.cnbc.com/2017/12/07/bitcoin-stolen-in-hack-on-nicehash-cryptocurrency-mining-marketplace.html

Buchholz, K. (2020, August 10). *Infographic: How common is crypto?* Statista Infographics. https://www.statista.com/chart/18345/crypto-currency-adoption/

Carey, T. W. (2020, October 26). *Robinhood kicks cybersecurity month off by getting hacked*. Investopedia. https://www.investopedia.com/robinhood-kicks-cybersecurity-month-off-by-getting-hacked-5082845

Coinsutra. (2019, August 6). Explaining hash rate or hash power in cryptocurrencies. *CoinSutra - Bitcoin Community*. https://coinsutra.com/hash-rate-or-hash-power/

Conti, M., E, Kumar, S. K., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452. https://doi.org/10.1109/COMST.2018.2842460

Costea, V. (2019, November 12). *Best hardware wallet on the market review Part 2 page sep sitename*. Bitcoin Magazine. https://bitcoinmagazine.com/articles/bitcoin-wallet-reviews-whats-the-best-hardware-wallet-on-the-market-part-2

Daria, R. (2018, October 29). *Canadian crypto exchange Maplechange gets hacked, all the funds gone*. Coinspeaker. https://www.coinspeaker.com/canadian-crypto-exchange-maplechange-gets-hacked-all-the-funds-gone/

Demartino, I. (2015, February 17). Chinese exchange KipCoin has been hacked. *Coinjournal*. https://coinjournal.net/chinese-exchange-kipcoin-hacked/

Fredrik, V. (2019, January). *Local bitcoins hacked, 8 bitcoins stolen*. https://cryptonews.com/news/localbitcoins-hacked-8-bitcoins-stolen-3273.htm

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). *On the security and performance of proof of work blockchains* (No. 555). http://eprint.iacr.org/2016/555

Geuss, M. (2012, August 12). *Bitcoinica users sue for $460k in lost bitcoins*. Ars Technica. https://arstechnica.com/tech-policy/2012/08/bitcoinica-users-sue-for-460k-in-lost-bitcoins/

Gobry, P.-E. (2013, January 8). All money is fiat money. *Forbes*. https://www.forbes.com/sites/pascalemmanuelgobry/2013/01/08/all-money-is-fiat-money/

Greenfield, R. (2012, September 5). *A bitcoin heist and the upside of government regulation*. The Atlantic. https://www.theatlantic.com/technology/archive/2012/09/bitcoin-heist-and-upside-government-regulation/323969/

Hartnett, K. (2019, April 2). *How the EverCrypt library creates hacker- proof cryptogaphy.* https://www.quantamagazine.org/how-the-evercrypt-library-creates-hacker-proof-cryptography-20190402/

Huillet, M. (2019a, February 16). *Major crypto brokerage Coinmama reports 450,000 users affected by data breach*. Cointelegraph. https://cointelegraph.com/news/major-crypto-brokerage-coinmama-reports-450-000-users-affected-by-data-breach

Huillet, M. (2019b, March 26). *Singapore: Crypto exchange DragonEx reports hack of both platform, user assets*. Cointelegraph. https://cointelegraph.com/news/singapore-crypto-exchange-dragonex-reports-hack-of-both-platform-user-assets

Huillet, M. (2019c, June 17). *Report: Record-breaking coincheck hack perpetrated by virus tied to Russian hackers*. Cointelegraph. https://cointelegraph.com/news/report-record-breaking-coincheck-hack-perpetrated-by-virus-tied-to-russian-hackers

Huillet, M. (2019d, December 3). *Upbit hack: Stolen ETH worth millions on the move to unknown wallets*. Cointelegraph. https://cointelegraph.com/news/upbit-hack-stolen-eth-worth-millions-on-the-move-to-unknown-wallets

IT, P. (2020, January 6). What is cryptocurrency mining? *IT PRO*. https://www.itpro.co.uk/digital-currency/30249/what-is-cryptocurrency-mining

Jariwala, C. (2020, July 18). OWASP Top 10 overview and vulnerabilities. *Penetration Testing and CyberSecurity Solution - SecureLayer7*. https://blog.securelayer7.net/owasp-top-10-overview-and-vulnerabilities/

Kharif, O. (2019, September 5). *Fewer people are sending bitcoin to largest crypto exchanges—Bloomberg* [News]. Fewer People Are Sending Bitcoin to Largest Crypto Exchanges. https://www.bloomberg.com/news/articles/2019-09-05/fewer-people-are-sending-bitcoin-to-largest-crypto-exchanges

Kharpal, A. (2019, May 8). *Hackers steal over $40 million worth of bitcoin from one of the world's largest cryptocurrency exchanges*. CNBC. https://www.cnbc.com/2019/05/08/binance-bitcoin-hack-over-40-million-of-cryptocurrency-stolen.html

Konash, M. (2019, September 30). *Top 10 web crypto wallets of 2019*. Coinspeaker. https://www.coinspeaker.com/top-10-web-crypto-wallets-of-2019/

Kumar, M. (2019, May 8). *Binance hacked—Hackers stole over $40 million worth of bitcoin*. The Hacker News. https://thehackernews.com/2019/05/binance-cryptocurrency-hacked.html

Kuznetsov, N. (2019, May 30). *The cryptopia nightmare drags on as liquidators struggle to reimburse hacked users*. Cointelegraph. https://cointelegraph.com/news/the-cryptopia-nightmare-drags-on-as-liquidators-struggle-to-reimburse-hacked-users

Lampe, J. (2014, November 10). *How to test the security of IoT smart devices*. Infosec Resources. https://resources.infosecinstitute.com/test-security-iot-smart-devices/

Lansky, J. (2018). Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, *9*(1), 19–31. https://doi.org/10.20470/jsi.v9i1.335

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of bitcoin. *Electronic Markets*. https://doi.org/10.1007/s12525-019-00392-5

Mearian, L. (2019, April 17). *What's a crypto wallet (and how does it manage digital currency)?* Computerworld. https://www.computerworld.com/article/3389678/whats-a-crypto-wallet-and-does-it-manage-digital-currency.html

Mizrahi, A. (2016, May 15). *Gatecoin lost $2m worth of bitcoin and ethereum in hot wallet cyber hack* | *finance magnates*. Finance Magnates | Financial and Business News. https://www.financemagnates.com/cryptocurrency/exchange/gatecoin-lost-2m-worth-bitcoin-ethereum-hot-wallet-cyber-hack/

Mohit, K. (2013, November). *Bitcash.cz Bitcoin Exchange hacked; Money from 4000 Bitcoin wallets stolen*. The Hacker News. https://thehackernews.com/2013/11/bitcashcz-bitcoin-exchange-hacked-money.html

O'Neal, S. (2018, June 27). *From coincheck to bithumb: 2018's largest security breaches so far*. Cointelegraph. https://cointelegraph.com/news/from-coincheck-to-bithumb-2018-s-largest-security-breaches-so-far

Paganini, P. (2020, February 11). *The Altsbit exchange will exit in May following a hack*. Security Affairs. https://securityaffairs.co/wordpress/97622/cyber-crime/altsbit-exchange-hacked-exit.html

Palmer, D. (2019, June 27). *Singapore exchange bitrue hacked for over $4 million in crypto*. CoinDesk. https://www.coindesk.com/singapore-exchange-bitrue-hacked-for-over-4-million-in-crypto

Phillips, D. / D., & Phillips, D. / D. (2020, January 12). *Ledger Nano X review: An expensive step in the right direction*. Decrypt. https://decrypt.co/16035/ledger-nano-x-review-an-expensive-step-in-the-right-direction

Redman, J. (2019, January 26). An in-depth look at the trezor model t hardware wallet | Reviews Bitcoin News. *Bitcoin News*. https://news.bitcoin.com/an-in-depth-look-at-the-trezor-model-t-hardware-wallet/

Rizzo, P. (2014, March 5). *Poloniex loses 12.3% of its bitcoins in latest bitcoin exchange hack*. CoinDesk. https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack

Rosenberg, E. (2019, October 20). Best bitcoin wallets. *The Balance.* https://www.thebalance.com/best-bitcoin-wallets-4160642

Ryan, J. (2018, April 23). What is greenaddress and how to use this bitcoin wallet. *BitcoinBestBuy*. https://bitcoinbestbuy.com/wallets/greenaddress-bitcoin-wallet/

Salvo, D. / M. D. (2020, July 2). *MetaMask unveils new Ethereum wallet, updates privacy features*. Decrypt. https://decrypt.co/34463/metamask-unveils-new-ethereum-wallet-updates-privacy-features

Sam, T. (2018, May 26). Cryptocurrency trading app Taylor loses 2,500 ETH in $1.5M hack. *CryptoSlate*. https://cryptoslate.com/cryptocurrency-trading-app-taylor-loses-2500-eth-in-1-5m-hack/

Samman, G. (2015, February 15). *BTER gets hacked for 1.75 million in bitcoin*. Cointelegraph. https://cointelegraph.com/news/bter-gets-hacked-for-175-million-in-bitcoin

Schwarz, M. (2018, April 3). *7 of the biggest recent hacks on crypto exchanges*. CSO Online. https://www.csoonline.com/article/3505512/7-of-the-biggest-recent-hacks-on-crypto-exchanges.html

Sead, F. (2019, December 11). *ShapeShift denies claims by Kraken that KeepKey can be hacked in 15 minutes*. https://cryptonews.com/news/shapeshift-denies-claims-by-kraken-that-keepkey-can-be-hacke-5277.htm

Seang, S., & Torre, D. (2018). *Proof of work and proof of stake consensus protocols: A blockchain application for local complementary currencies*, p. 21.

Senishin, R. (2019, January 14). *How to create a wallet in MetaMask?* Medium. https://medium.com/dappband/how-to-create-a-wallet-in-metamask-c45819225b6f

Sharma, R. (2018, May 30). *Bitcoin gold hack shows 51% attack is real*. Investopedia. https://www.investopedia.com/news/bitcoin-gold-hack-shows-51-attack-real/

Song, J. (2017, August 12). *Mt. Gox hack technical explanation*. Medium. https://medium.com/@jimmysong/mt-gox-hack-technical-explanation-37ea5549f715

Stan, H. (2015, July 1). *Details of $5 million Bitstamp hack revealed*. CoinDesk. https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange

Stokel-Walker, C. (2019, March 4). The QuadrigaCX crypto mystery deepens as wallets turn up empty. *Wired UK*. https://www.wired.co.uk/article/quadriga-ceo-died-crypto-cold-wallets-empty

Usman W, C. (2018). *The problems of cryptocurrency thefts and exchange shutdowns*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131702&download=yes

Wolfie, Z. (2018a, June 11). *Coinrail exchange hacked, loses possibly $40 million in cryptos*. CoinDesk. https://www.coindesk.com/coinrail-exchange-hacked-loses-possibly-40-million-in-cryptos

Wolfie, Z. (2018b, September 20). *Crypto exchange Zaif hacked in $60 million bitcoin Theft*. CoinDesk. https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft

Wood, A. (2019, July 14). *Hacked bitpoint exchange finds $2.3m in stolen crypto*. Cointelegraph. https://cointelegraph.com/news/hacked-bitpoint-exchange-finds-23m-in-stolen-crypto

Xu, L., Yang, J.-B., & Manchester School of Management (University of Manchester. Institute of Science & Technology). (2001). *Introduction to multi-criteria decision making and the evidential reasoning approach*. Manchester School of Managment, University of Manchester Institute of Science and Technology.

Yasin, D. (2018, March 10). Jaxx wallet beginner's guide. *CryptoPotato*. https://cryptopotato.com/jaxx-wallet-beginners-guide/

Yoshifumi, T., & Sophie, K. (2014, February 28). Mt. Gox files for bankruptcy, hit with lawsuit. *Reuters*. https://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228

Young, J. (2019, June 18). *Round-up of crypto exchange hacks so far in 2019—how can they be stopped?* Cointelegraph. https://cointelegraph.com/news/round-up-of-crypto-exchanges-hack-so-far-in-2019-how-can-it-be-stopped

Yousaf, R. (2019, November 11). Vietnam-based crypto exchange VinDAX loses at least $500K to hack. *AllStocks Network*. https://all-stocks.net/vietnam-based-crypto-exchange-vindax-loses-at-least-500k-to-hack/

Yuji, N., & Sam, K. (2017, September 11). *North Korea Is dodging sanctions with a secret bitcoin stash—Bloomberg*. https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ArXiv:1903.07602 [Cs]*. http://arxiv.org/abs/1903.07602

Zuckerman, M. J. (2019, March 30). *Crypto exchange bithumb reportedly hacked of almost $19 mln in EOS, XRP*. Cointelegraph. https://cointelegraph.com/news/crypto-exchange-bithumb-reportedly-hacked