A Survey on Creating, Investing, Vulnerabilities & Countermeasures of Cryptocurrencies

Revanth Yenugudhati
Msc. Computer Science
Lakehead Univesity
ThunderBay, Canada
ryenugud@lakeheadu.ca

***Abstract*—Cryptocurrency is a recent and significant in the financial industry. The goal is to offer a currency that is not tied, created or backed by a government. Cryptocurrency use the BlockChain technology as the financial platform.This paper aims to address the development of the crypto currencies over a period of time. The value of the currencies and the position of the currencies in the market. Generation of the bitcoins and the shared of the code for generation of new currencies This paper also discuss the " what the factors or on which bases the users choose the cryptocurrency".The paper also discusses the vulnerabilities faced by crypto currencies and its prevention steps for a safe and secure transaction or value of the cryptocurrency. These properties include Short form, current value in market, currency's market capitalization, programming language of implementation, its year of release, founder of cryptocurrency, block time, all time high, all time low, market rank of the currency, its type of proof and algorithm used in currency and the most influencing factors that would influence the values and the investors in investing the crpto industry and also including the vulnerabilities and its prevention steps .**

***Index Terms*—Cryptocurrencies, Bitcoin,Altcoin, Blockchain**

I. Introduction

In the earlier times the people used to trade items by hand.Once there is a boom in the online industry the trading system has also entered online. With respect to the trading the money has also taken many different form overtime. The most used currencies in the form of electronic money and virtual currencies. Electronic money represents the traditional money followed by each government while virtual currencies have their own currency units [1].One of the most important aspects of our world that has been greatly influenced by the internet is the global economy in which trading between people in different countries can be carried out online. Money has been taking many different forms overtime, starting from commodities to commodities-backed currency then to fiat currency and recently to the internet-based forms which are electronic money and virtual currencies. Cryptocurrency is the new generation of virtual currency. This can be bought using the real and other virtual currencies and also be sold for real and other currencies according to specific knowledge. The evolution of the cryptocurrencies are based on the Blockchain technology.While Bitcoin is widely seen as a pioneer in the world of cryptocurrencies.There are more than 4,000 cryptocurrencies in existence as of January 2021 such as Bitcoin,Litecoin,Dogecoin etc. While many of these cryptos have little to no following or trading volume, some enjoy immense popularity among dedicated communities of backers and investors. Beyond that, the field of cryptocurrencies is always expanding, and the next great digital token may be released tomorrow.It is considered as an innovation in the virtual currency and the financial industry as well. Cryptocurrency is intended to substitute the exiting printed currency to provide a peer to peer medium of exchange. Cryptocurrency industry has grown dramatically .The market value fluctuates due to high level of volatality. The industry's market value is larger than some major technology companies as well as some world economies.

In this survey we discuss about the development of the cryptocurrencies in the period of time , the unbound values of the cryptocurrencies which used to change time to time,discuss the standing positions of the cryptocurrencies. How bitcoins are generated and the source code of the cryptocurrencies shared to generate a new type of cryptocurrencies,finally discuss the factors the would influence the users in investing in the cryptocurrencies and we discuss the vulnerabilities and countermeasures for vulnerabilities.

II. Terminology

Key terms used in this paper include the following:

Block Chain: Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

Mining: a required verification step for a Cryptocurrency transaction and for adding transaction records to the public ledger. Mining also introduces new Cryptocurrency units in the system.

Block: a data structure containing transaction data.

Hash: a one-way function [2] that takes data of any size as input and produces a fixed length output. Hash computation should be fast and easy, while reversing the process should be expensive and difficult. Reversal should require a brute force algorithm. Any change in the input should propagate through the entire output, so that outputs for similar input have no predictable similarity.

Bitcoin: The first ever crypto currency introduces in 2008. It has the highest value compared to other Altcoins

Altcoin: The coins other than Bitcoin come under the Alternative coins category.

III. Related works

In the related works we will be discussing the previous works done by various people who worked on similar topics in this area. As crypto currency is the latest topic to debate many people invested their time in investigating about cryptocurrencies.

Cybercriminal attacks using Cryptocurrencies take many forms. "High yield investment programs" (HYIP) is one of the popular examples of the scams that cybercriminals carry out. HYIP is a scam in which investors are promised a high-interest rate, e.g., more than 1-2% per day [3].Ransomware is a denial-of-access attack in which a malicious piece of software locks and encrypts a victim's device data until a sum of money is paid.

Fatemah presented a signature-based ransomware identification method based on graphic mining. The study concluded they had 96.6% rate of successful detection [4].

Daniel Dimov has discussed about the vulnerabilities that will be occurred during the exchange of the cryptocurrencies. He have discussed like phishing, missing wallet protections, transaction malleability and software vulnerabilities. Such things will be creating a unsafe environment and gives an easy way to hackers [1].

Amna Al Shehhi along with few other members of Masdar institute of technology have discussed about the user who invest and the factors behind the user selecting a cryptocurrency. Sazeed and Tugrul have given there study on the adoption rate of the users investing in the bitcoin and the generation of the bitcoin.

According to Kshetri and Voas, the denial of services and productivity losses due to ransom attacks are in billions of USD.Amin et al. developed a new approach for identification and analysis of crypto-ransomware. With this approach the encryption method and characteristic behavior features used by the crypto-ransomware infecting the victim's system are defined [5].Boldt [6] proposed a viable method for crypto-ransomware detection and analysis. The biggest deficiency of this approach is that there is no case study to test the applicability of the method and the programs used in the approach cannot be used free of charge.

Based on the above readings, I have found few shortcomings in the previous readings there are more issues with the hackers and the ransomware attacks. Resulting in the huge loss of the cryptocurrencies from the wallets of the users. To the best of our knowledge, this is the first survey that discusses and highlights the impact of existing as well as possible future security and privacy threats to cryptocurrencies and its associated technologies. The second survey will be on the factors or the decision need to be taken while choosing a cryptocurrency exchange network as exchange is the major part of your wealth, where we will be getting money or trying to invest in the Crypto.There might few fraudulant cases where there would be pishing attacks and as the volatile nature of crypto we need to take while investing in the cryptocurrencies exchanges.

IV. Overview of Cryptocurrencies

A cryptocurrency is a digital currency that does not exist in form of coins or bills, only as book money. Cryptocurrencies differ in their characteristics and by the projects behind them. Since this year at the very latest, they are experiencing a breakthrough in the financial world. By now, even professional investors are active in this sector because of its high growth rates and yield opportunities.In 2008, a programmer (or perhaps a group of program- mers) using the name Satoshi Nakamoto published a paper describing digital currencies and the following year launched the Bitcoin network [7].

In 2009, the Bitcoin software was made public and thus began mining – the process by which new Bitcoins are created, and transactions are recorded and verified. A year later, on 22 May, a guy named Laszlo Hanyecz made history by trading Bitcoin for the first time. He agreed to pay 10,000 BTC for two pizzas in Florida. Admittedly, a day he'll forever regret. Up until then, Bitcoin had no assigned value [7].

Unlike government currencies, there is no central bank backing Bitcoin and anyone with a computer or an Application-Specific Integrated Circuit (ASIC), which is a dedicated machine specifically created for the purpose, can create a Bitcoin by a process called mining. The first altcoins appeared in 2011 as Bitcoin increased in popularity primarily due to the idea of a decentralised currency that was not controlled or regulated by any government. Despite being the original cryptocurrency, Bitcoin has lagged concerning usability and is not a transactional crypto. Bitcoin is more of a store of value or even a commodity. At the same time, ETN continues to prove it is transactional and, therefore, usable.It is relatively fast, cheap and easy to do since in Bitcoin, each participant theoretically has equal power. There are no banks, therefore no bankers, so everyone stores their own Bitcoin in a virtual account called a wallet. The user controls their own money and users can even send micropayments as small as what is called one Satoshi or 0.00000001BTC, (a Bitcoin to eight decimal places) or about $0.000005 today. The value of a Bitcoin, like any other currency, is dependent on what the buyer is willing to pay. If nobody used Bitcoin it would have no value but Bitcoin can have any price, and volatility is common, making and losing fortunes for many people in the process

The banking system today is stagnant and runs on an obsolete infrastructure which takes days or weeks to send money around the world. Bitcoin is a new financial system, designed by the people, for the people and theoretically everyone has equal power. People control their own money and the rules of the Bitcoin system are enforced on everyone by each other through mutual distrust [8]. Nobody can tamper with or influence the system except in one unlikely scenario of controlling 51

A. Value

Originally, Cryptocurrencies was not of interest to the general public, since mainly cryptographers, hackers, and mathematicians understood its purpose and use. It is generated by an algorithm, it is impossible to counterfeit, it is more or less anonymous, and since it is a peer-to-peer network there are no additional fees from middlemen such as banks. In fact, these are the virtues of a currency uniquely suited to our modern digital economy. However, although the value of Bitcoin lies is a combination of speculation on future value and genuine, undeniable usefulness, the wild swings in price Bitcoin has been experiencing are a natural reaction to the massive global interest in a pool of money that is relatively tiny compared to its government-backed peers.

Virtual currencies exhibit network externalities, the more people use them, the more valuable they are. Because Bitcoin was the first digital currency to market gives it a tremendous advantage. Bitcoin gets the most publicity and has more people and merchants supporting it, and also has the most users invested in it. As long as Bitcoin continues serving the needs of users, it has the potential of remaining the most important digital currency indefinitely. And although there are many proposed improvements to Bitcoin that are theoretically interesting, none appear to be able to induce users to switch in large numbers [9].

If we go into the values of each crptocurrencies, I have considered top ten cryptocurrencies and Bitcoin stands in the first place with a value of $38,851 as of today (14/06/2021).the second place is occupied by Yearn Finance with a value of $38,421.The next place goes to ethereum with a values of $2,471.

The values of the currencies subject to change everyday. These currencies does not have a fixed value. These are decentralised currencies so the there would be no third party between transactions. There are many other cryptocurrencies in race but trying to over come the competition. No person, institution or government guarantees Bitcoin, since nobody owns the network. This means that there is no guarantee that a Bitcoin will have a stable relationship to any conventional currency. The Bitcoin floats against conventional currencies and has been less than a dollar in 2011 to more than $1,200 in 2013 to presently about $38,812.

B. How does Cryptocurrency work

A user creates a transaction. The transaction is broadcasted into the Peer to Peer network consisting of nodes. A node is computer responsible for creating blocks. The network of nodes validates the transactions. A few transactions create a new block. The block contains information of the transactions like date, time and the amount of money. And finally block chain participants who allocated processing power to validate a transaction will receive a award in the form of a cryptocurrency [24].

In Bitcoin mining, thousands of competitors race to solve a mathematically complex repetitive problem. If a person solves the problem then they are rewarded with the ability to add a block to the Bitcoin global transaction register and get 25 Bitcoins as a reward [24]. However, because it takes so much computing power the more popular way is to join a mining pool of thousands of users each contributing their computing power to solving this problem and being rewarded with a share of the profits from the solving of the problem.Originally it was thought that Bitcoin would be the "people's currency" and that computing power would be decentralized and everyone would have an equal chance of solving the Bitcoin problem called a hash function [8]. However, it has evolved that this hash function can be solved more efficiently by dedicated equipment built specifically for this purpose. What has happened is that instead of the average computer user trying to mine Bitcoin with their PC, it has now become the realm of people or groups of people investing hundreds of thousands of dollars into dedicated machinery which only has one function and that is to solve the hash function

Bitcoin is open source therefore anyone can take the source code, make minor modifications and then create a similar network to Bitcoin thereby creating their own currency. However, the core Bitcoin protocol is extremely difficult to change because of the decentralization of the network, therefore if someone believes they have an idea for a better virtual currency, it is much easier to start their own currency that to convince Bitcoin users to change the currency so that they can compete with the bitcoin [8].

C. Factors behind Investing in a Cryptocurrency

”I ended up making back pretty much everything I lost in a single trade. The feeling was one of absolute euphoria [10].”

Many studies were taken on ”how people choose to invest on the bitcoin?” As bitcoin or cryptocurrencies are not stable in value, it is hard to predict on which crypto currency to choose. Many people without knowledge have invested into the cryptocurrencies and went into loss.Economists have never had to consider a system such as Bitcoin until it was developed and now they are just beginning to imagine the ramifications. Some economist believe that Bitcoin will fail because the price of producing a Bitcoin clone is zero but it is also possible that Bitcoin will disrupt the entire monetary system. Money should serve as both a reliable medium of exchange and a stable storage of value. It is this storage of value that causes most economists problems since money that is a reliable store of value is usually backed by a government or some central authority or it has inherent value, such as gold or silver. If there is no backing and no intrinsic value people will not trust it over time.

There are many factors to be considered while investing in a crypto currency .The authors have tried to observe the increased adoption level through time by examining the market capitalization , estimated number of users and the daily volume. The number of cryptocurrency exchange sites users is the most accurate indicator of the most cryptocurrency users. The factors influencing users to the adoption decision fall into four main categories like technical, economical,social and person.

Technical factors are like Control over the system, Anonymity, Fast transfer, Blockchain technology, system security, the team behind it [11]. There are few other factors that effect the users in investing in the crypto currencies like Investment oppurtunities, Low transaction cost, Alternative banking system, supply limit, Incredible demand of altcoins [12]. There are even social factors that influence the people in the world in investing in such types of currencies. They are like social norms, Global attention etc.

D. Chosing a platform for crypto exchange

There are few factors need to be taken into mind before choosing a platform for cryptocurrency exchange. I have listed few things that need to be taken care while choosing a cryptocurrency exchange, They are like:

1) Authenticity and security: It is imperative to do research and guarantee you are choosing a legitimate and secure platform.One of the biggest issues in the cryptocurrency industry today centers on pump-and-dump schemes. Exchanges are responsible for preventing this fraud.

2) Method of purchase: If you do not have any cryptocurrency before joining an exchange, it is essential that you choose a platform that accepts fiat currency so that you may enter the market. It is also important to note how long purchases take to complete. Some platforms process transactions nearly instantly while others can take days or weeks.

3) User interface and user experience: User experience is subjective and different people will enjoy different interfaces.Whether you are a seasoned cryptocurrency trader or buying bitcoin for the first time, an intuitive interface and good user experience aids user actions on the exchange to be more informed and more efficient.he exchanges with the "best" user experiences will see the largest growth in transaction volume in the coming years.s

4) Supported tokens: Most exchanges support Bitcoin and Ethereum, but investors in cryptocurrency know that is just the tip of the iceberg. There is a significant variation in supported cryptocurrencies across different exchanges; some platforms, like Binance, trade a long list of altcoins, whereas Coinbase trades only four major cryptocurrencies.

5) Trading platform, P2P exchange: There are three main types of cryptocurrency exchanges, so you need to know what they are before choosing a cryptocurrency exchange.Trading platforms are the most common and include Binance and Coinbase.P2P exchanges help mitigate network congestion and maintain a secure, trustless system for the exchange of cryptocurrencies.

6) Fee Structure: ransaction fees and fee structures differ across various exchanges, which is critical when choosing a cryptocurrency exchange. Some exchanges offer discounted fees. This occurs when an exchanges own token is used to complete transactions. Also, it can relates to how many tokens are held. Others only charge a transaction fee on sales, permitting purchases free of fee.

V. VULNERABILITIES AND COUNTER MEASURES

In this section I have surveyed few vulnerabilities and its counter measures so that one can follow it while creating a cryptocurrency and helps to answer my research question what steps can be taken to prevent the attacks on cryptocurrency? Hackers and thieves find cryptocurrency system an easy way to fraud the transactions. In this section, we discuss existing security threats and their countermeasures for Bitcoin and its underlying technologies. We provide a detailed discussion of potential vulnerabilities that can be found in Cryptocurrencies. Apart from double spending, which is and will always be possible, the attack space includes a range of wallet attacks , network attacks and mining attacks.

A. Types of Attacks

1) Double spending: A client in the Bitcoin network achieves a double spend (i.e., send two conflicting transactions in rapid succession) if she can simultaneously spend the same set of bitcoins in two different transactions [13].In Cryptocurrency, a network of miners verify and process all the transactions, and they ensure that only the unspent coins that are specified in previous transaction outputs can be used as input for a follow-up transaction. This rule is enforced dynamically at run-time to protect against the possible double spending in the network. The distributed time-stamping and PoW-based consensus protocol is used for orderly storage of the transactions in the blockchain.A form of double spending called Finney attack [**?**], in which a dishonest client pre-mines a block that contains the transaction. To avoid the Finney attack, the vendor should wait for multiple confirmations before releasing the product to the client. The waiting for multiple confirmations will only make the double spend for the attacker harder, but the possibility of the double spend remains.

2) Client side security checks: Each Crptocurrency user posses a set of private-public keys to access its account or wallet. Hence, it is desirable to have the key management techniques that are secure, yet usable. This is because unlike many other applications of cryptography if the keys of a client are lost or compromised, the client will suffer immediate and irrevocable monetary losses.The authors in [15] found that the primary vectors of attack on Bitcoin involve collisions on the main hash or attacking the signature scheme, which directly enables coin stealing. However, a break of the address hash has minimal impact, as addresses do not meaningfully protect the privacy of a user.Bitcoin relies on public key cryptography. This raises the issues of the secure storage and management of the user keys. Over the years, various type of wallet implementations is researched to obtain secure storage of the user keys. It includes software, online or hosted, hardware or offline, paper and brain wallets.To avoid the risks mentioned above such as managing cryptographic keys [17], lost or stolen devices, equipment failure, Bitcoin-specific malware, to name a few, that are associated while storing the bitcoins in a wallet, many users might prefer to keep their coins with online exchanges. However, storing the holdings with an exchange makes the users vulnerable to the exchange systems.Although, the vulnerability of an exchange system to the disastrous losses can never be fully avoided or mitigated. Therefore the authors in [17] presents Provisions, which is a privacy-preserving proof of solvency for Bitcoin exchanges.

3) Networking issues: We will start our discussion with the most common networking attack called Distributed Denial-of-Service (DDoS) which targets Bitcoin currency ex- changes, mining pools, eWallets, and other financial services in Bitcoin. Due to the distributed nature of Bitcoin network and its consensus protocol, launching a DoS attack has no or minimal adverse effect on network functionalities. Hence attackers have to lunch a powerful DDoS to disturb the networking tasks. Unlike DoS attack, in which a single attacker carried out the attack, in DDoS, multiple attackers launch the attack simultaneously. DDoS attacks are inexpensive to carry out, yet quite disruptive.As stated above that DDoS attack take various forms, one of which is to discourage a miner so that it will withdraw itself from the mining process. For instance, if an attacker displays to a colleague miner that it is more powerful, it can snatch the reward of mining, and it is the apparent winner of the mining process, then honest miner backoff since its chances of winning is less.by using a Malleability attack an adversary clogs the transaction queue [18]. This queue consists of all the pending transactions which are about to be serviced in the network. Meanwhile, an adversary puts in bogus transactions with the high priority depicting itself to be highest incentive payer for the miners. When the miners try to verify these transactions, they will find that these are the false transaction, and but by this time they have already spent a considerable amount of time in verifying these false transactions. This attack wastes time and resources of the miners and the network [19].

There are few more vulnerabilities like that the vulnerabilities that exist in the refund policies of the current Bitcoin payment protocol, a malicious user can perform the so-called Refund attacks.Yet another attack on the Bitcoin networks is called Time jacking attack [20].

B. Counter Measures

For Double spending type of attack, there are counter measures that can stop it doing. These measure stops the fraudulent transactions happening the crypto network.This is achieved by enforcing a simple rule that only unspent outputs from the previous transaction may be used in the input of a next transaction, and the order of transactions is specified by their chronological order in the blockchain which is enforced using robust cryptography techniques. This boils down to a distributed consensus algorithm and time-stamping.The most effective yet simple way to prevent a double spend is to wait for multiple numbers of confirmations before delivering goods or services to the payee.

Client side securities includes securing client side amenities so that the hacker could not connect the wallet and the coins in the wallet will be safe. For this, authors have developed a cold wallet kind of thing in which there will two systems. In which once system will not be connected to internet, the other systems will be connected to the internet. When the system is not connected to the internet then hacker would not be able to do an attack on the clients machine.This would be securing the wallet.

For the Network issues such a DDoS attacks which are simple and more prone to the attacks of the system.Authors propose Proof-of-Activity (PoA) protocol, which is robust against a DDoS attack that could be launched by broadcasting a large number of invalid blocks in the network. In PoA, each block header is stored with a crypt value and the user that stores the first transaction places this value.ny subsequent storage of transactions in this block is done if there are valid stakeholders associated with the block. Storage of crypt value is random and more transactions are stored, only if more stake users are associated with the chain. If the length of the chain is more, then the trustworthiness among other peers increases and more miners get attracted towards the chain. Hence, an adversary cannot place a malicious block or transaction since all the nodes in the network are governed by stakeholders.

VI. Conclusion

In this paper, I have covered the topic of the development of the cryptocurrency and the ways the cryptocurrencies are generated and distributed around the world. Next I have discussed the ranking of the currencies in which Bitcoin stands first in the race as it is the initial crypto currency introduced into the world. I have also discusses the problems or vulnerabilities that will be occurring in the transactions and the prevention measures to get rid of bad things and be successful in crypto trading and creation.There would be no competition to it as of now as it follows its standards and next in the paper there are the ways how cryptocurrencies are generated and how the code can be shared as it is open source. This would help in creating the new cryptocurrencies.The paper has also given the ways to investigate several factors behind choosing a cryptocurrency to mine and/or use through conducting an online survey directed at people who are currently using and/or mining such currencies. Such techniques would help the users to understand the trends in the cryptocurrency and the factors that need to be taken care before investing in the crypto market.

Cryptocurrency's future outlook is still very much in question. Proponents see limitless potential, while critics see nothing but risk.While the number of merchants who accept cryptocurrencies has steadily increased, they are still very much in the minority. For cryptocurrencies to become more widely used, they have to first gain widespread acceptance among consumers.

VII. Acknowledgement

I express my sincere gratitude to our faculty Trevor Tommesh for his able guidance throughout my survey. The information provided in the survey paper is true and best of knwoledge got referring different papers in the didifferent areas of the Cryptocurrency.All the papers or the websites mentioned

in the references are used for collection of information and most of them are cited.

REFERENCES

[1] https://resources.infosecinstitute.com/topic/the-decline-of-ransomware-and-the-rise-of-cryptocurrency-mining-malware/

[2] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014

[3] K. Toyoda, P. Takis Mathiopoulos, and T. Ohtsuki, “A novel methodology for HYIP Operators’ bitcoin addresses identifcation,” IEEE Access, vol. 7, pp. 7483574848, 2019.

[4] D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware

[5] https://websitem.karatekin.edu.tr/ilkerkara/paylasimlar/dosya/0f7a100dcf5c42d2

[6] M. Boldt, andB. Carlsson.2006 Analysing privacy-invasive software using computer forensic methods. ICSEA, Papeetee.

[7] https://www.investopedia.com/terms/b/bitcoin.asp

[8] Lee, T. (2013) The Washington Post. Dogecoins and Litecoins and Peercoins oh my: What you need to know about Bitcoin alternatives. Retrieved 12/28/2013 from http://www.washingtonpost.com/blogs/theswitch/wp/2013/12/26/ dogecoins -and-litecoins-and-peercoins-oh-my-what- you-need-to-know-aboutbitcoin- alternatives/

[9] Popper, b. (2013) The Verge. Bitcoin is too cheap for its own good. Retrieved 1/3/2014 from http://www.theverge.com/2013/12/9/5192054/bitcoin-boom-bust-bubble-currency-technology

[10] https://www.bbc.com/news/uk-scotland-57268024

[11] Saeed Alzharni, Analysis of the cryptocurrency adoption decision,2019

[12] Seema Rawat. ”Proposed noval security system based on passive infrared sensor.” In 2016 International Conference on Information Technology (InCITe)-The Next Generation IT Summit on the Theme-Internet of Things: Connect your Worlds, pp. 44-47. IEEE, 2016.

[13] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bitcoin,” in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917

[14] H. Finney, “Best practice for fast transaction acceptancehow high is the risk?” Available: https:// bitcointalk.org/ index.php?topic=3441. msg48384#msg48384, 2011

[15] . Giechaskiel, C. Cremers, and K. B. Rasmussen, “On bitcoin security in the presence of broken cryptographic primitives,” in Computer Security – ESORICS 2016.

[16] P. Litke and J. Stewart, “Cryptocurrency-stealing malware landscape,” 2014

[17] G. G. Dagher, B. B unz, J. Bonneau, J. Clark, and D. Boneh, “Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges,” in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’15. ACM, 2015, pp. 720731

[18] Malleability attack a nuisance but bitcoin not broken, pundits say,” Available: http:// www.financemagnates.com/ cryptocurrency/ news/ malleability-attack-a-nuisance-but-bitcoin-not-broken-pundits-say/

[19] The bitcoin malleability attack how can it undermine the blockchains credibility?” Available: http:// www.coinwrite.org/ , 2017

[20] corbixgwelt, “Timejacking and bitcoin,” Available: http:// culubas. blogspot.de/ 2011/ 05/ timejacking-bitcoin 802.html, Mar. 2011

[21] D. Folkinshteyn and M. Lennon, ”Braving Bitcoin: A technology acceptance model (TAM) analysis”, Journal of Information Technology Case and Application Research, vol. 18, no. 4, pp. 220-249, Oct. 2016

[22] CoinReport. (2014). What are the Advantages and Disadvantages of Bitcoin? [Online]. Available: https://coinreport.net/coin-101/advantages-anddisadvantages- of-bitcoin

[23] https://www.nasdaq.com/articles/6-things-to-consider-when-choosing-a-cryptocurrency-exchange-2018-02-21

[24] https://hackernoon.com/how-to-create-your-own-cryptocurrency-tips-to-get-started-947ba92f79f9

[25] B. Carson. (2014, May, 4). Such Dogecoin. Much Validity. How one altcoin may have turned into cryptocurrency’s best marketing tool [Online]. Available: https://gigaom.com/2014/05/04/suchdogecoin- much-validity-how-one-altcoin-may-haveturned- into-cryptocurrencys-best-marketing-tool

[26] http://bitcoinmagazine.com/12342/bringing-bitcoin-to-the-middle- east-cointalks-dubai

[27] https://www.researchgate.net/topic/Cryptocurrency