Queensland University of Technology

School of Information Systems
Faculty of Science and Engineering

Security and Privacy Aspects of Bitcoin

Submitted By

Student Name: Abhishek Paleli George, Nancy Rathi

Student ID: n10724389,n10820701

Abstract

Cryptocurrencies are a tricky pit to fall into if you are not aware of the whole working as well as the market share that they hold. Crypto currencies are often values so much, higher than any countries currency value because of the demand and the volume present. The most unique characteristic of bitcoin, another cryptocurrency is that it is decentralized, which means it is not controlled by anyone and cannot be demonetized or devalued by a ruling authority. They can be used to make a lot of transactions over the internet and are used by many people. Due to heavy encryption, many locations have also banned the use of bitcoins all together because of the sinister intentions of many people. Bitcoins cannot be traced back to a source because of encryption, the question arises whether it is a good thing or a bad.

Contents

1 Introduction

The report is on the currently very hot topic crypto currency. The most popular crypto as if today is bit coin. The most known crypto is bit coin. Crypto currency is basic an electronic currency that is been used to trade goods and services. It is a kind of encrypted code which is been circulated with its key to the receiver. It uses a kind of encoding system that has limited resources and the resources is been transferred from the sender to receiver. This report is going to discuss in details about the crypto currencies and also includes the knowledge about the crypto mining and how crypto is ledged and the accounting of the crypto currencies and security concerns that are been associated with the crypto currency. This report is going to discuss method to get the crypto and methods to earn the crypto currency. The main motive of this report is to discuss the security threats and risks that are been associated with the crypto currency. This report is going to include the description of crypto currency and discussion about the techniques that is been used to generate crypto currency and secure the crypto currency. The particular crypto that this report is going to consider is bit coin that is a hot topic as if today. Bit coin is the file that is been stored in the digital bank or wallet. That is been stored in a register or ledge known as block chain. It could be used to trade goods and services. The sender and receiver have an encrypted address of bit coin that could be sent feather to complete the transaction.

2 Description

The crypto that is been discussed in this report is bit coin that is the most popular and known crypto currency. Bit coin is a virtual or digital currency. Bit coin is the currency that could be used to exchange in return to any good or services but not all the goods or services are been offered in exchange of bit coin and some countries had also banned the currency exchange as it is not controlled or traced by any government and it is the exchange as a files that are been stored in a e wallet. The bit coin could be exchanged and sender can send the bit coin to the receiver. Each and every transaction of bit coin is been stored in a ledge known as block chain and this ledge is been distributed to all the block chain in the entire world. This register of transaction help in preventing the duplication of bit coin and spend the bit coin that is not been owned by the spender or double transmission of same bit coin (Conti et al., 2018).

Bit coin can be collected by three means which are either spend the real money to buy the bit coin then other ways is to provide the goods or services in exchange of bit coin and the last way to get the bit coin is by creating the bit coin using the computer. Bit coin can be created by granting the computer to make the transaction of bit coin and some time the computer owned used to transfer the funds or bit coin can be rewarded by bit coin. This creation of bit coin is known as bit coin mining. The computer that is been used for the transaction of bit coin has to perform very complex and difficult sum. As the number of transactions are increasing the complexity of the sum or difficulty to stop production of bit coins in large quantity is also increasing for which good quality system with great computation power are been required. It became profession to mine the bit coin (White et al., 2020).

Bit coin is been valued so much because it could be exchange to get goods and services and it act like any other currency that is been circulated by the authorities that could be used to get goods or service in exchange and it is so high valued because some people are willing to exchange the good or services in less bit coin and its value is increasing because of its popularity and the fact that crypto currency is not been monitored by any government and bank. It is perfect currency to invest in to hide the money from the authorities so it is so popular and many threats are also associated to the bit coin that are been discussed in the further part of this report. Then the bit coin can be used to store the resources that are un traceable and hidden. The bit coin could also be used to shop goods and services anonymously without leaving any money trail. It could be used to hide the money from the government and authorities and no one could link any individual with bit coin ownership and every bit coin can be distributed in different parts with different addresses that is very difficult to trace and locate to trace the owner of the bit coin.

As the record of each and every transaction of every bit coin is been recorded and is been maintained properly no bit coin can have duplicity or has multiple owner at the same time. As the bit coin is not been link to any individual and if the bit coin address of the wallet in which the bit coin is been stored is been forgotten or lost the bit coin will also be lost forever and there is no way to retrieve it which is a total loss condition (Ghimire and Selvaraj, 2018).

The average time to mine one bit coin is around 10 minutes and it consumes around 72000 GW in power to mine one bit coin. It can be mined using the ASIC miner. Bit coin mining requires the bit coin mining rig and a bit coin wallet to store the bit coin. Then the miner has to join the mining pool for bit coin mining and has to run program to mine the bit coin on the computer that is going to be utilized to mine bit coin and transfer the bit coin through the computer.

And the miner could be rewarded or gain bit coin in exchange.

Bit coin transaction is secure but the record that is been maintained in the ledge should also be secure. The record is main component to link or trace the fake bit coin or duplicate bit coin. If the record is been compromised and the new record is been updated to the whole network then it is impossible to trace back the original bot coin and the duplicate one. So the security of the ledge also known as block chain is very important and delicate to secure the bit coin and prevent the circulation of the fake bit coins (Miraz and Ali, 2018).

Then the transaction must be secure as it has the high values and leaves no money trail so the transaction must be neat and secure so that the send could not fraud the receiver or the receive could not deny the transaction completion. Then the transaction must be carried safely without any interference with other factor and the transaction should not be manipulated or been tracked by any one as the one tracing or manipulating the transaction can commit the fraud and can claim the bit coin that is been transferred and is been stored in the digital wallet.

The security measures that are been associated with the bit coin transaction or ledge that is been recorded to maintain the record of the transactions and the bit coin that are been mined till now includes the Paper wallets can be utilized to keep bit coins disconnected from the internet and the attackers, which essentially diminishes the odds of the crypto currency being taken by programmers or PC malware. bit coin is a very secure and private protocol engrossing millions of users worldwide is because of the encryption and the implementation of it inside the block chain. SHA-256 is an encryption algorithm that is really effective when it comes to privacy. Like passwords, SHA-256 algorithm creates unique and irreversible keys so that the privacy of the block chain remains intact. It is a mathematical algorithm that receives input as the details of the block chain and the transactions inside them to create a 256-bit unique number that keeps the information safe (Sai et al., 2019).

Bit coin mining is the process of keeping and creating these records, an i.e., block, for which the participant receives a reward or a fee, this fees is the actual bit coin value that is mined. Usually, there is always a group of people that mine a single block and that is accepted, so the reward is often distributed among the participants and it should be secured to secure the crypto currency such as bit coin (He et al., 2020).

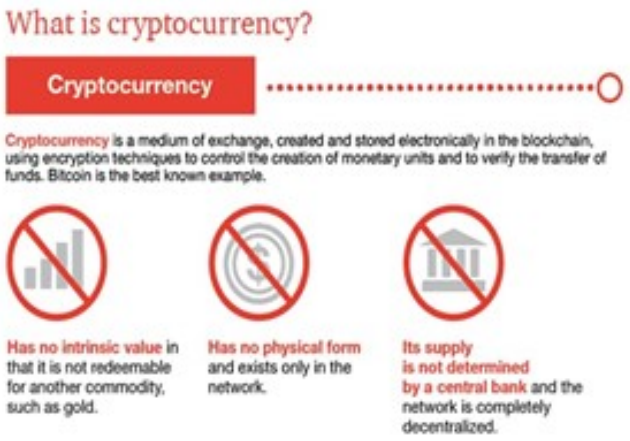

Figure 1: Cryptocurrency concept (Fintech, 2021)

3 Security and Privacy Aspect of Bit coin

Bit coin is so far the best crypto currency. In any case, very much like other cryptographic forms of money, Bit coin has experienced a drop significantly for as long as a couple of months. Value instability stays quite possibly the main difficulties confronting all cryptographic forms of money, as they attempt to explore a complex system towards being perceived as an actual monetary item by the entire world. Digital currencies also have a lot of risks attached to their benefits. These risks are mostly concerned with the security and privacy of the digital wallets, transaction, and exchange of currency, vulnerability to certain types of digital attacks through a cracker, and people who abandon pools and are en route to individual mining for their own benefits. Some of these issues are also very negative in nature, such that they affect bit coin in a very bad way (Tripwire, 2018).

3.1 Security of bit coin

Bit coin should be kept secure and safe no matter how much of the currency someone has. Since the market value of this currency is so high, even a single bit coin is worth protecting and keeping safe.

3.1.1 paper Wallet

Despite the fact that bit coin is an absolutely a virtual monetary item, it very well may be kept secure in a simple structure such as a physical form. Paper wallets can be utilized to keep bit coins disconnected from the internet and the attackers, which essentially diminishes the odds of the crypto currency being taken by programmers or PC malware. Printing the substance of a wallet, essentially the private keys and their relating public keys - makes an actual record that,

obviously, should be kept safe and locked up.

3.1.2 Regular backups

Ordinary reinforcements of a bit coin wallet are fundamental to secure against PC malfunctions, digital attacks, and common mistakes, yet never store them on the web, particularly if the reinforcement isn't scrambled or using any kind of latest encryption. At last, consistently utilize the most recent variant of bit coin programming, and the utilization of a secret key that is containing a strong combination of numbers, symbols, and capital and lowercase characters so that a brute force attack cannot overtake the system (Cobb, 2018).

3.2 Privacy of bit coin

Bit coin is very advanced yet simply designed around the cryptography protocol. The cryptography bit is the most important aspect of the currency since it provides anonymity and privacy and a decentralized currency.

3.2.1 Sha-256 encryption

Bit coin uses SHA-256 encryption for both its Proof-of-Work (PoW) system and transaction verification. The reason that bit coin is a very secure and private protocol engrossing millions of users worldwide is because of the encryption and the implementation of it inside the block chain. SHA-256 is an encryption algorithm that is really effective when it comes to privacy. Like passwords, SHA-256 algorithm creates unique and irreversible keys so that the privacy of the block chain remains intact. It is a mathematical algorithm that receives input as the details of the block chain and the transactions inside them to create a 256-bit unique number that keeps the information safe. The unique part is that even changing a single character inside the inputs

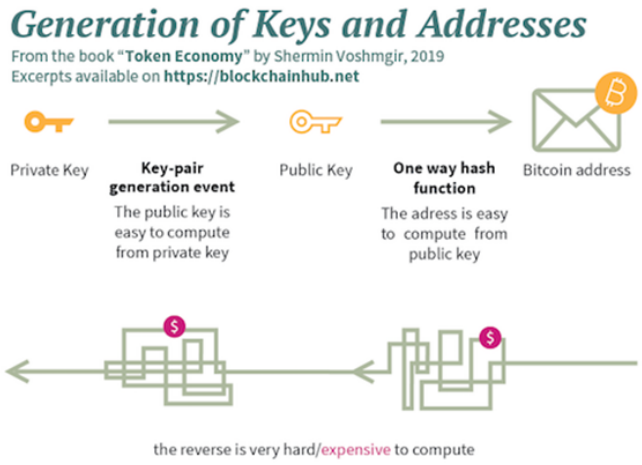

Figure 2: Hash computation (Vosmgir, 2018)

affects the output massively. It means that if a number 1 will be switched to 2 in the input, the

entire output will be completely different. It is used for bit coin transaction records; bit coin mining, where people look for the compatible hashes similarly. It is also used for storage and other related structures and systems. SHA-256 is actually quite popular and used for other security systems as well (Khaliq, 2021). The manner in which mining works is at one time a mining hub has bundled information for exchange, it is at that point where it needs to utilize computational processing ability to attempt arbitrary varieties as quick as conceivable to add onto that information so that the returning output coordinates with the SHA-256 hash. In reality, the mining is really difficult but it is smartly managed so that the reward for the mining is distributed and acquired easily without much problem and deduction (Luno, 2019). Even though

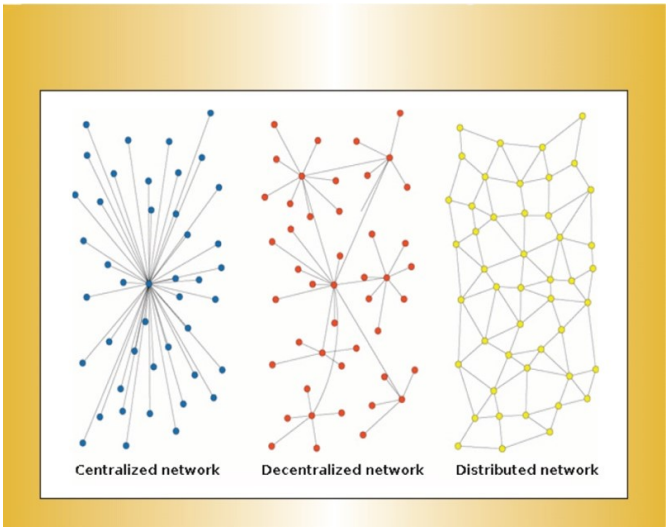

Figure 3: Network layout (Murray, 2018)

it is very complex and time consuming to match the hash with the compatible SHA-256 hash, it is equally rewarding. So from everyone in the crypto currency community it is heavily recommended that people do their own research before getting into it.

4 Block chain and its features

A block chain is in its entirety, is a ledger or a record of transaction regarding that particular crypto currency. So, a bit coin block chain consists of all the list of transactions that keep taking place over the world. A block chain is preferred because it is very robust and secure when it comes to attacking and hacking the system. The architecture makes it very hard and difficult to cheat the block chain. A bit coin block chain is basically a computerized ledger of bit coin exchanges and transactions that is copied and dispersed across the whole organization of system frameworks on the block chain. Every 'block' in the chain contains various exchanges, and each time another transaction happens on the block chain, a record of that exchange is added to each member's

ledger. The decentralized information base oversaw by various members is known as Distributed Ledger Technology (DLT). This is where mining comes in, bit coin mining is the process of keeping and creating these records, an i.e. block, for which the participant receives a reward or a fees, this fees is the actual bit coin value that is mined. Usually, there is always a group of people that mine a single block and that is accepted, so the reward is often distributed among the participants. This method is preferred since the mining requires a heavy processing unit so when the resources are pooled together by various participants it becomes easier. Each user gets the reward according to its contribution (Euromoney, 2020).

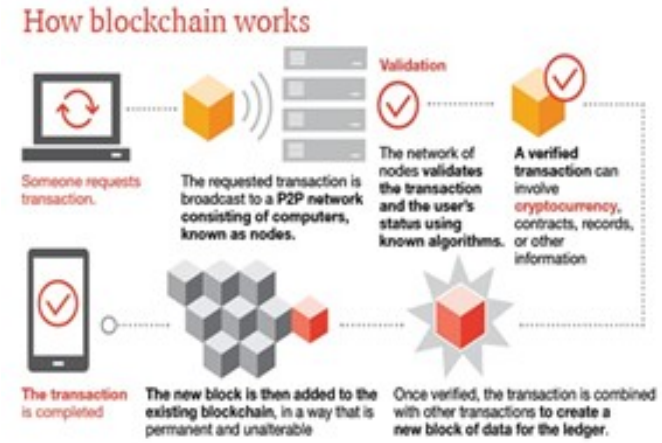

Figure 4: Block chain working (Fintech, 2021)

5 Recommendations

There are a lot of key points that should be kept in mind while trying to play around or dive into bit coin, or any other crypto currency for that matter. There are a lot of issues surrounding and concerned with the mining as well as investment of bit coin. Bit coin allows you to trade the currency and execute transactions in an unexpected manner in comparison to you typically do. Bit coin should be kept secure and safe no matter how much of the currency someone has. Since the market value of this currency is so high, even a single bit coin is worth protecting and keeping safe. All things considered; you should set aside effort to educate yourself prior to utilizing Bit coin for any genuine exchange. Bit coin ought to be treated with a similar consideration as your standard wallet, or significantly more sometimes. The same goes for the various investments related to the stocks of bit coin. If a trader wants to set ahead and invest in bit coin or other similar currencies then the knowledge and experience should be present. It is always recommended to start off small and read and learn about the working as well as the functionality of the architecture before going at it from a professional perspective (Bit coin, 2021).

6 Conclusion

In this report, the various aspects of the crypto currency know as bit coins were discussed along with their features and the architecture of the block chain. The recommendations of using and dealing with bit coins were also focused on as well as the security and privacy features were discussed. Growing in popularity bit coin really grabbed everyone's attention and stunned everybody with the initial performance back in 2015. Now, at a stable but still a high enough price, it is maintained and created many more crypto currencies based off of its architecture. This relates to all the currencies that when the price of bit coin dips, other currencies also suffer so e fluctuation. This report includes the discussion in details about the crypto currencies and also includes the knowledge about the crypto mining and how crypto is ledged and the accounting of the crypto currencies and security concerns that are been associated with the crypto currency. This report is going to discuss method to get the crypto and methods to earn the crypto currency. The main motive of this report is to discuss the security threats and risks that are been associated with the crypto currency. This report is going to include the description of crypto currency and discussion about the techniques that is been used to generate crypto currency and secure the crypto currency.

7 References

Bitcoin. (2021). Some things you need to know, https://bitcoin.org/en/you-need-to-know

Cobb, M. (2018). How to secure bitcoin: What are the best ways to keep it safe? https://searchsecurity.techtarget.com/answer/Is-Bitcoin-safe-The-truth-about-Bitcoin-security-and-crypto-currency

Conti, M., Kumar, E. S., Lal, C., Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys Tutorials, 20(4), 3416-3452.

Euromoney. (2020). What is blockchain? https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

Fintech. (2021). Making sense of bitcoin, cryptocurrency and blockchain. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

Ghimire, S., Selvaraj, H. (2018, December). A survey on bitcoin cryptocurrency and its mining. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE.

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. IEEE Network, 34(6), 114-119.

Khaliq, A. (2021). The Good, The Bad And The Ugly of Bitcoin Security, https://www.hongkiat.com/blog/bitcoin-security/

Luno. (2019). SHA (256) Rule - keeping your crypto encrypted, https://www.luno.com/blog/en/post/sha-256-rule

Miraz, M. H., Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. arXiv preprint arXiv:1801.03528.

Murray. J. (2018). The Coming World of Blockchain. The CPA journal, 2018(6).

Sai, A. R., Buckley, J., Le Gear, A. (2019, March). Privacy and security analysis of cryptocurrency mobile applications. In 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ) (pp. 1-6). IEEE.

Tripwire. (2018). Security Concerns and Risks Related To Bitcoin, https://www.tripwire.com/state-of-security/security-awareness/security-concerns-risks-related-bitcoin/

Voshmgir, S. (2019). Token Security: Cryptography – Part 2. https://blockchainhub.net/blog/blog/cryptography-blockchain-bitcoin/

White, R., Marinakis, Y., Islam, N., Walsh, S. (2020). Is Bitcoin a currency, a technology-based

product, or something else?. Technological Forecasting and Social Change, 151, 119877.