Research Inventy: International Journal of Engineering And Science
Vol.11, Issue 2 (February 2021), PP 31 - 37
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

An Analysis of Bit Coin Crypto Currency and Block Chain Technology

Tapan Golakiya[1], Ruchita Golakiya[2]
[1] *Software Development Engineer, Brillio LLC, Canton, MI, USA*
[2] *Department of Computer Science, Wayne State University, Detroit, MI, USA*
Corresponding Author: golakiyatapan@gmail.com

Abstract: *To make Online money transfer secure and less costly without going through any trusted third party, in 2008, one researcher called himself as 'Satoshi Nakamoto' invented cryptocurrency known as 'Bitcoin'. Satoshi Nakamoto suggested that Online money transactions can be done directly peer-to-peer without including any trusted third party and with more security and anonymity of source and destination. In this paper, we described an analysis of Satoshi Nakamoto's Bitcoin currency, proof of work, Bitcoin mining, challenges, and weaknesses of Bitcoin, and how revolutionized the Bitcoin cryptocurrency will be in future. We also de- scribed different types of possible attacks on Bitcoin Network.*
Keywords: *bitcoin, cryptocurrency, block chain, ledger.*

Date of Submission: 20-02-2021 Date of Acceptance: 10-03-2021

1. INTRODUCTION

Since a long time, humankind has keep developing the medium and form of currency. [8] Long before, all countries were using different form of money like gold, bronze, silver, jewellery, etc. After that, financial authority was taken over by government and they started making coins using various metals. After some years, paper bills came in use that made it easy to carry money. In 21st century, technology kept developing and banks came in picture. People started using credit cards and debit cards in form of currency. Nowadays, ease of Electronic Payments is reached at the different level. It takes only minutes to transfer money from one place to anywhere in the world.

[1] For all these Online methods, there is a need of financial institutions who serve as third parties to process these electronic payments. Still, they cannot provide surety that mediating disputes will be fully avoided. The cost of mediation increases the transaction costs. Even, completely non-reversible transaction as not possible. There was no communication channel existed which is secure and without any trusted party. To reduce the cost of electronic payments, [1] researcher who called himself 'Satoshi Nakamoto', introduced cryptographic proof for electronic payments, that allows any two parties to do transactions directly without any need of trusted party, with security and with guarantee of making it non-reversible. Computationally impractical to reverse the transaction makes it non-reversible. The currency introduced for this Cryptographic payment known as 'Bitcoin'. This paper describes that, how bitcoin transaction works, what is the proof-of-work behind block chain and mining process, etc.

This paper discusses about the peer-to-peer network solutions for double-spending problem. Peer-to-peer network means, Nodes which are part of network are aware of all transaction going through the whole network. [6] Transactions are secure as they are verified by all the nodes of the network and afterwards it gets reported in public ledger commonly known as block chain. [8] Cryptocurrency relies on the process of solving complex math problems to create unique digital codes, known as hashes.

We have shown, how anonymity of nodes works in block chain, and as per some re- searchers' analysis, how attackers can perform different type of attacks on bitcoin network, that can risk the anonymity of nodes. Bitcoin cryptocurrencies have some strengths, weaknesses, and Threats, which are elaborated in this paper.

2. BITCOIN TRANSACTIONS

[4] Bitcoin Transaction defines movement of bitcoin from source addresses to destination ad- dresses. Source address can be multiple as well as destination addresses. Indirectly, Bitcoin is chain of digital signatures. Below is the

Bitcoin transaction structure simply described in Fig. 2.1 by Satoshi Nakamoto in The White Paper [1]. As shown, Owner signs the hash of the previous transaction using its own private key and the end of the coin is updated by the public key of immediate owner. Next owner can verify the signature to get the previous owner.

In this kind of transaction, there appears the problem of double spending. Which means, Payee cannot verify that, previous owner did not use this coin for multiple time. For example, if we make a copy of regular currency and spend both original and duplicate copies, that means we double spend the same money bill. Same thing can be happened to Bitcoin transactions. One solution to solve the double spending problem in bitcoin transactions is to create the central trusted authority. So, after every transaction, bitcoin will go to trusted authority and it will create the new bitcoin signed by itself, that says that bitcoin is trusted and not double spent. This solution solves the problem, but it does not satisfy one of the purposes of Cryptographic currency, which is no use of any trusted third party that can increase the cost of transaction.

Other solution to double spending problem is that all nodes are aware of all transactions going in whole network. That means, all nodes have the same copy of history of transactions. So, at the time of transaction nodes can verify that whether it is first time received or second time. [2] To determine the order of the transactions, transactions are grouped into blocks, which server to timestamp the transaction that [2] Blocks are connected into a chain, with each referencing to the previous one, this creates block chain.

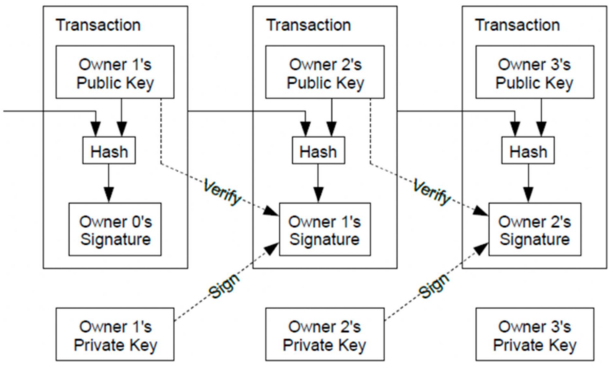

Fig 2.1 Bitcoin Transaction [1]

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
e631567f352f...:1	3.02887912	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402201700305a3d79a[....]2b985b15daa0ab9c50cd61449ca037dc9f0
c284ec1d325f...:0	3.04042789	1GY84QPLfM9d4KqTjTtbHsb9BX9FFIkYQx	Address	3045022100e7240041f2d3[....]91d95b56ad29f817f3e3259daffbd72f2e98
0fbcc1d29b8c...:0	2.99934316	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402200f6c9b4281cb0[....]2b985b15daa0ab9c50cd61449ca037dc9f0
232715b3c51a...:1	3.00515088	17ALqzZFPb5qXz9aQhzgK6ts9tdZfV8Mwu	Address	304402207311495478c1d[....]8d4656bf7613d47dd4e6a5b062d9fb6a34

Outputs

Index	Amount	To address	Type	ScriptPubKey
0	0.51682435	1LUHXNTsHPUGVJjeefPdh2rpdxtWoHrcKv	Address	OP_DUP OP_HASH160 d5936a017766c48be2ada9a77153ecc6db80b8 OP_EQUALVERIFY OP_CHECKSIG
1	11.5569767	1HzAb4E1kZH4pDKoxML4KXBLPfyUocrw4s	Address	OP_DUP OP_HASH160 ba51b9ece7595c72a2cbc1d4e3e90e356f77804 OP_EQUALVERIFY OP_CHECKSIG

Fig 2.2 [4] Bitcoin Transaction Example. Four input addresses and two output addresses.

Above Fig. 2.2 is the example of bitcoin transaction. [4] Input addresses in transaction are the source address and output addresses are destination addresses. Here, total amount of the output addresses must be less than the total amount of output addresses. Given that, the bitcoin protocol requires that the input addresses in a transaction must fully spend the exact amount of a previous transaction that they received. This is the reason why input address has the index value of a previous received transaction. The public ledger in the system cannot be modified. So, before a transaction can be accepted by the receiving node, it must verify that there are no previous transactions in the ledger that have used the same input address with the same index as the input addresses in the transaction being validated. This solves the double spending problem.

[4] The below Fig. 2.3 shows the interesting fact about bitcoin transaction, which is input addresses in a transaction must fully spend the exact amount of a previous transaction that they received.

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
073a12d29e11....:0	0.706	1NYB35emL1yQunpExWhRM6CHBAzbJVx9Sd	Address	304402205d2b1[....]0a9b96e22abb02da6e3a03c1aa8c

Outputs

Index	Amount	To address	Type	ScriptPubKey
0	0.4	13osnkmwyYaER5tBPp5f9zWjWhpHwNgD66	Address	OP_DUP OP_HASH160 1ecdc8400fe4360569c1b18f9927ee1a7ee46443 OP_EQUALVERIFY OP_CHECKSIG
1	0.3059	1ATkLdK5icinT2c5F2NWoJYs8QWs4y5NUg	Address	OP_DUP OP_HASH160 67c81fc63d214d19696f25d1fd1fe360dabdf371 OP_EQUALVERIFY OP_CHECKSIG<

Fig 2.3 [4] Interesting Fact about Bitcoin Transaction

From above figure, if sender wants to send 0.4 bitcoin to receiver and last received transaction for sender was 0.706 bitcoin, then sender must spend 0.706 bitcoin. For this, sender will set two output addresses, one of receiver for 0.4 bitcoin and other one which points to sender itself for the remaining change of 0.3059 bitcoin. That's how this satisfies the transaction protocols.

3. PROOF-OF-WORK AND BLOCK CHAIN MINING

[9] Transactions need to be verified and confirmed by the network so everyone can agree on that. To do this, bitcoin transactions are grouped together in blocks. Every block possesses the cryptographic hash of the previous unit and its own cryptographic hash that serves as a unique identifier. The Fig. 3.1 shows the simple example of that.

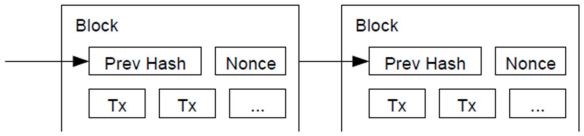

Fig. 3.1 [1] Block Chain

So, [3] block chain is made up of logs all transaction that ever occurred since creation of bitcoin. Block chain keeps growing as new transaction occurs and new blocks extend it by pointing the processor block. As, bitcoin network is decentralized, and as we have seen that all nodes in the bitcoin gets the same copy of history of transactions which is called block chain. Every time a block is created, it will be appended to the existing block chain by connecting to the predecessor block. Block creation in the network is uncoordinated because there are so many nodes in the network. Thus, blocks which are created almost at the same time by different nodes may extend the same parent block. Such blocks contain a different version of the transaction logs and contain conflicting transactions. So, the question is, how to get rid of this fork (branch) in the chain? The rule is Adopt the Longest Chain, when nodes come to know about conflicting blocks that make up the longest chain from both branches, they adopt the longer one and abandon blocks in their shorter version of fork. The time between each block creation is helpful enough to make conflicts rare. Because after block creation it will be propagated to all nodes in the network before the next block is created. Average block creation time in the network is 10 minutes.

[4] Mining process is adding the new block into the block. This information will be transmitted through the distributed network to all nodes (bitcoin users). The bitcoin network is dynamically created and maintained by users who perform a process called mining, which involves using specific software to solve complex mathematical problems. This process, known as the proof-of-work system, was first proposed by Adam Back and is called "Hashcash." The proof-of-work requires computational power to find a hash of the new block with value lower than nonce which is already defined target. An important thing about hash function is that, even a change of one bit in the input string completely changes the output hash value. For example, if the target is to get 50 zeros as the 50 most significant bits in the output, then this computationally hard problem can be solved by brute force method only. Miners perform a lot of computational power to create the valid block with valid hash. When a miner successfully solves the complex mathematical problem required to create a new block on the bitcoin network, that block is added to the top of the blockchain, a decentralized and public ledger that records all bitcoin transactions. Once the block has been added to the blockchain, all other miners will discard the work they were doing to create that block and move on to collecting and verifying new transactions for the next block.

4. HOW MINERS GET REWARDED

[4] Blocks mining is a hardworking task in the bitcoin system, which requires a lot of computation efforts from miner. In exchange of miners' efforts, these two mechanisms help miners in getting the rewards, first mechanism is in form of newly created bitcoins. After block creation, there is one special transaction on the top of block called 'Generation Transaction' which has no input address but has output address as a miner's address who created the block. This is how miners' get rewarded with bitcoin. The second mechanism is in form miner is paid for each transaction. Calculation of charges are done by finding the difference between input amount and output amount. All fees collected will be included in generation transaction.

Since there is ample number of bitcoin miners and winner for block creation is the only one who gets credit (reward) for block creation. This decreases the possibility to get rewards for individual miner. Because of this reason, "mining pools" came into picture. Mining pool is group of individual miners that agrees to share any rewards received with all the miners in the pool, in proportion to each miner's contribution to the computing power. The amount of shared reward will be low but the possibility to get rewards for individual miners will increase.

5. STRENGTHS OF BITCOIN CRYPTOCURRENCY

[8] Since starting, maximum number of bitcoins is fixed, which is 21 million bitcoins. The speed at which bitcoins are getting mined is decreasing during time, as number of users in bitcoin network is increasing. Whenever in future, mined bitcoins will reach at the count of 21 million, network will stop issuing new bitcoins. Because of this reason, network will never become inflated from and overabundance of bitcoins. As bitcoin is totally new currency, it also has its own value, which. In 2015, when demand of bitcoin currency was at highest peak, it became the best performing currency throughout the year 2015.This concludes that bitcoin one of the highest value currencies by the starting of 2017. "Bitpay", which is the largest bitcoin processor in the world for mining, has declared in 2016 that, bitcoin transaction rate grown 110% in just 12 months. They also studied the transaction volume growth in different region of the world.

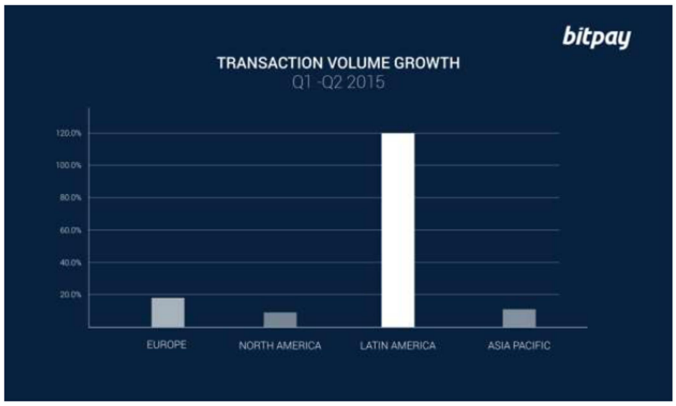

Fig 5.1 [8] Bitcoin Transaction Volume Growth

As we saw in above Fig. 5.1 that, Latin American countries have seen a huge increase in bitcoin transactions. In Argentina, bitcoin transactions increased 510% from 2014 to 2015. There were certain reasons after that. One of the reasons was that government put some restrictions on converting currency to US Dollars. Therefore, black market for converting currency to USD and bitcoin adoption arisen. Other reason is that most people in Argentina are unbanked. But they had quick access to mobile, which was very easy medium to access bitcoin network because of many applications like "Bitpay".

[8] Other most important reason of increasing bitcoin transaction is that currency should be locally accepted. For example, If an American wants to exchange USD for Chinese Yuan and use that to purchase things. They would have to visit Currency exchange. After getting exchanged USD to Chinese Yuan, they will not be able to use Yuan to purchase anything from market, as Yuan is not accepted as a currency in USA. This is not the situation with Bitcoin, because it is accepted worldwide.

To buy the bitcoin, one only need to create online account with online exchange, can make the request to buy bitcoins. If there is an increase in the use of bitcoin as a currency, it will likely encourage merchants and vendors to accept it as payment, and conversely, if more merchants and vendors accept bitcoin as payment, it may lead to an increase in its use as a currency.

6. WEEKNESSES OF BITCOIN CRYPTOCURRENCY

[3] Bitcoin has few weaknesses that are part of its design.

Whenever the fork happens in the block chain, and there are two choices to choose the single chain whichever is longest, then longest chain rule will be applied, and network will converge to a single choice. If there are two conflicting blocks exist in the system, network is partitioned to nodes that can accept only one version of chain from two. Once, the new block is created by anyone, and one of the possible choices of chain become longer. Network will adopt the longer version of chain and will discard the other version.

An Attacker can use this situation to reverse the transaction in block chain. For example, an attacker has some transaction in the block chain, and wants to reverse that transaction. It can try to create the fork in the block chain just before the block containing its own transaction. Then, attacker tries to extend this fork until it is longer than the current chain. Once this fork becomes longer than the current chain, network will adopt the fork branch and abandon the original version of chain. But to create the situation like this, an attacker must create enough number of blocks in his fork to overtake the original version of chain. Since block creation is computationally hard, he must produce blocks at the rate higher than the rest of the network combined.

[8] Even, bitcoin has received questionable reputation through time. Silk Road was an online marketplace, which allowed millions of customers and thousands of drug dealers to make drug deals. They used the bitcoin as a primary means of transaction. Due to some reasons, it ran for 3 years and profited nearly one billion USD. Here, bitcoin anonymity seems negative perspective. Because there is not positive marketing towards cryptocurrencies, the general people will think bitcoin as a currency used by criminals only.

Cryptocurrencies also developed questionable security. Mt Gox was the world's first bitcoin exchange until it went bankrupt. It was robbed by hackers in 2011. The reason behind this was that main programmer of this was not using version control and security issues were not getting fixed in time. People sold their bitcoin being afraid of it getting stolen.

Nowadays, bitcoin network has started being stabilize, and because of competition in mining the bitcoin, immediate returns of investment is not guaranteed. This is called "halving event". This makes less likely to enter new individual miners into bitcoin network.

7. BITCOIN ANONYMITY

[4] Bitcoin Anonymity is one of the reasons of success of bitcoin cryptocurrency. Bitcoin users in the network can create any number of anonymous bitcoin addresses that can be use in their transactions. Although, all the transactions are publicly announced through public ledger to all the nodes in the network, nodes can only know the address of the source and destination address of transaction. But the real identity if source and destination address is still anonymous as public ledger does not have the information that who is the owner of this specific address. We can also call it as a semi-anonymity. There are many papers published to prove the threat on bitcoin anonymity by performing different methods of analysis on bitcoin network.

A. Blockchain Analysis

This is the direct approach to analyze the anonymity of users in bitcoin network, which is to analyse the data contained in the blockchain. The main goal of analysis is to cluster all addresses in the blockchain that belong to the same user address. There are multiple techniques introduced to carry out such analysis and clustering.

[4] Based on blockchain information, authors of this study constructed the transaction network and the user network. This looks like the directed graph in which each vertex represents a transaction, and each edge represents whether there is an input or output address that is linked to this transaction. The user network constructed by

clustering address of the same user assuming that, all input addresses of a transaction belong to the same user. Furthermore, the activity of known users can be observed in detail.

[4] Other study took one more step into clustering. In this, all input addresses of the given transaction are clustered together and examining the output addresses as well. They studied that; many Bitcoin transactions involve only two output addresses. In such cases, if one of the two addresses has already been identified in the blockchain, the other address can be considered a "shadow" address. This shadow address can be directly linked to the input addresses for the transaction, providing a way to trace the movement of Bitcoin within the network. By analyzing shadow addresses in this way, researchers can gain a better understanding of the anonymity of Bitcoin users. Authors, studied that, by performing behavior-based clustering, K-means and Hierarchical Agglomerative Clustering techniques, 40% bitcoin users' profiles can be identified.

Many researchers provided different studies to unveil the anonymity of bitcoin users, and the key to all studies was to perform clustering technique on bitcoin network to get the cluster of addresses belonging to the same user.

B. Traffic Analysis

Bitcoin transactions are transmitted through a peer-to-peer (P2P) network, which utilizes the Transmission Control Protocol/Internet Protocol (TCP/IP) to communicate between devices. However, this network can potentially compromise the anonymity of Bitcoin users, as the TCP/IP information can be used to identify the parties involved in a transaction. One study was performed on real time bitcoin transactions data which was collected for 5 months. For almost 5 million transactions, the IP address information was collected by them from where the transaction has been received. Only single input transactions are considered in this study. To associate a Bitcoin address with an IP address, some users have proposed using the link between the two. This would be accomplished by examining the first transaction from a particular IP address, which would contain the Bitcoin address. By linking the IP address with the Bitcoin address in this way, it may be possible to trace the identity of a user who is attempting to remain anonymous. Traffic analysis did not get much attention of researchers because network data must be gathered.

C. Mixing

[4] To improve the bitcoin anonymity property of the bitcoin system, few authors proposed the idea of using mix services. As the name suggests, this procedure mixes the information to break the relation between input and output address. A mixing service allows Bitcoin users to send their Bitcoin to the service, which then mixes it with Bitcoin from other users and sends it to the intended recipient. This process helps to obscure the connection between the input and output addresses, making it more difficult to trace the origin of the Bitcoin. This mix service should be some trusted central party that is able to link all input and output addresses. It should also satisfy the most important property, 'non-reversibility' of bitcoin network. To make any transaction the valid one, all the users should sign who are participating in mixing service. Mixing services work by mixing the Bitcoin from different users, making it more difficult to trace the origin of any Bitcoin transaction.

8. BITCOIN FAILURE OPPRTUNITIES

[4] As a pioneer in potentially transformative technology, Bitcoin holds a special place among financial technologies. Its peer-to-peer network allows it to address the shortcomings of traditional banking and facilitate transactions in a way that is not possible with traditional methods. As such, it has the potential to solve many of the problems currently facing the financial industry. Cryptocurrencies helped to solve the problems of unbanked customers. Some countries in south America have more than 50% of population that have no access to bank. But most of the population have access to phones. That makes it very easy to access the bitcoin network and make transactions using bitcoin only. Bitcoin network also has opportunities for IT Developers, who can increase the reliability through mobile applications and better user interface.

More businesses have started doing international transactions using cryptocurrencies, which makes it secure and reliable as bitcoin is almost accepted world-wide. Even, most of the countries have already passed regarding taxation on cryptocurrencies.

9. CONCLUSION

When bitcoin cryptocurrency first introduced online by Satoshi Nakamoto. And because, it was not presented in any conference, it did not get that much attention by world. After that, some researchers moved to this subject to get into. Even, some big business started accepting bitcoins for international transactions. As, it became easy to use, more people started using and more businesses started accepting bitcoin. Although bitcoin is introduced and structured for secure and anonymous transaction, it got attention of attackers. Researchers proved by different ways that, how is it possible to attack bitcoin network. As we have seen, some of those attacks are possible only in theory, not practically. We also discussed, as like everything, bitcoin also has some strengths and some weaknesses. Bitcoin was strong enough that, it gained a lot of attention in some Latin American countries and some other parts of the world. People, who wanted to earn some money through bitcoin, started doing more mining. And that kept making bitcoin network stronger. Many researchers have researched on cryptocurrency in past, and a lot of going on in present. So, current situation stats that, cryptocurrencies like bitcoin have a very bright future, in tomorrow's financial world.

REFERENCES

[1] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", N.P.. Web, 30 Jan 2014.

[2] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage, "A fistfull of Bitcoins: Characterizing Payments Among Men with No Names," IMC'13, Barcelona, Spain, October 23-25, 2013.

[3] Aviv Zohar, "Bitcoin: Under the Hood", Communications of the ACM, vol. 58, No. 9, September 2015.

[4] Jordi Herrera-Joancomarti, "Research and Challenges on Bitcoin Anonymity", Conference Paper – Sepetember 2014, DOI:10.1007/978-3-319-17016-9_1

[5] Pilkington, Marc, Blockchain Technology: Principles and Applications (September 18, 2015). Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. Available at SSRN: https://ssrn.com/abstract=2662660

[6] Alex Kroeger, Advisor-Tim Fuerst, "Essays on Bitcoin".

[7] Jonathan Chiu, Thorsten Koeppl, "The Economics of Cryptocurrencies: Bitcoin and beyond", April 2017.

[8] Peter D. DeVries, "An Analysis of Cryptocurrency, Bitcoin, and the Future", Article- October 2016.

[9] Corin Faife (November 2, 2018), The Bitcoin White Paper Explained, Retrieved from https://breakermag.com/the-bitcoin-white-paper-explained/

[10] Cryptovest, " bitcoin and blockchain: what math puzzle do miners actually solve? Example with real transactions", Retrived from https://steemit.com/bitcoin/@cryptovest/bitcoin-and-blockchain-what-math-puzzle-do-miners-actually-solve

[11] Sava Gerov (2018) , "Bitcoin White paper explained", Retrieved from https://medium.com/coinmonks/bitcoin-white-paper-explained-part-1-4-16cba783146a?