A STUDY ON BLOCKCHAIN AND CRYPTOGRAPHY

[1]Ritik Banger, [2]Risheek Mittal, [3]Ronit Khowal and [4]Anurika Mehta

[1]B. Tech. Student, [2]B. Tech. Student,[3]B. Tech. Student,[4]Associate Professor,

Poornima Institute of Engineering & Technology, Jaipur, India

Abstract : This study has been undertaken toall the segments and functioning of BlockChain and Cryptocurrency. They have become one of the hottest topics in the tech and finance world. This technology directly affects the financial world. It is safe, secure and fast and expanding with a predicted rate of 42.8% by 2020. The immense potential this technology holds for future growth give rise to the concept of BitCoin, Ethereum etc. There are more than 2000 startups based on BlockChain Technology with a high market inclination.

***IndexTerms* - BlockChain, Cryptocurrency, BitCoin, Mining, Block Generation.**

I. INTRODUCTION

The BlockChain is the invention that allows digitally generated information to be allocated without being copied. BlockChain Technology is the heart of the new internet i.e. digital currency, BitCoin and any other online transaction. Tech experts found a big potential in this technology. “BlockChain is an incorruptible digital ledger of economic transaction that can be programmed to record not just financial transactions but virtually everything of value.”[1].

In plain layout, the data is not owned by any single computer but by a chain of computers so that the blocks of data are secured and bound to each other using chain, that technology is known as BlockChain technology. There is no transaction cost due to BlockChain, in Layman language BlockChain is a process to pass information or data from A to B in a safe and automated manner.

Cryptocurrency works on the principle of BlockChain Technology, that is why, BlockChain is the most trending item of current era, due to it’s secure nature cryptocurrency is widely accepted. It’s value is increasing day by day. Many oil industries, IBM Technologies, Mercedes Benz, Swiss Bank, Samsung, and even Google is planning to launch their own cryptocurrency in 2019 for safe and secure transactions.

Now, this technology is disrupting almost every marketshare due to its popularity and demand in the world.

Satoshi Nakamoto introduced the concept of BlockChain in 2008 in the form of cryptocurrency BitCoin. It’s function is to allow users to secure and control their monetary values so that no third party like government or banks would be able to access or control it. It is a process to carry everyone to the highest grade of liability.

Three technologies work behind the BlockChain Technology-

- Private Key Cryptography
- Peer 2 Peer Network
- BlockChain’s Protocol Program

II. BLOCKCHAIN AND ITS ARCHITECTURE

The internet of information is brought by the first generation of internet revolution while the blockchain technology is mechanized by the second, result in delivering us the internet of value to transmute the business world and alter the old form of human interest to become better (as shown in table 1) blockchain technology is a vast, universal distributer ledger or database running on million of gadgets and open to everyone, where not just information but anything of value-capital, but also characters, headlines, actions, even votes-can be moved, stored and managed securely and privately. The well-established trust is due to the clever mechanism of blockchain and the blocks used in its codes.

2.1 KEY ATTRIBUTES OF BLOCKCHAIN

- Decentralization. Each transaction on the cryptographic channel needs to be validated through a trusted media.
- Persistency. Transactions are completed quickly and failed transactions are not admitted by good miners.
- Anonymity. The real identity of the user is not given while him interacting with the generated BlockChain address.
- Auditability. BlockChain also keeps the unspent transactions while also keeping the spent ones in the fields. [2]-[3]

2.2 Block Generation and Mining

Blocks are the transaction data that is permanently recoded in files. Those blocks are organized into a linear sequence over time. The chain is built up by new blocks that are being processed by minors. As blocks are added at the end of BlockChain it become harder and harder to change and give rise to BitCoin's irreversible transaction.

The process of mining is the process of competing to be the next to find the answer that solves the unique mathematical complication of the current block.

BlockChain Mining generally involves mining of BitCoins and requires a high configured system to be able to mine them as several complex mathematical complications need to be solved in due time. The purproof of stacke of mining is not about creating new BitCoins but it is a mechanism that allows the BlockChain to be a decentralized security.

2.3 The Working of BlockChain

The working of Blockchain is shown in fig 1:

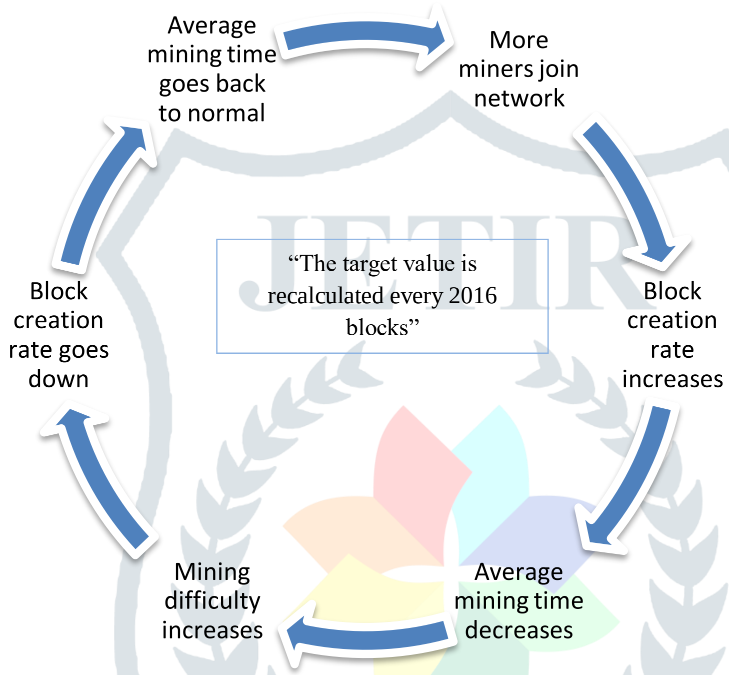
Average mining time goes back to normal
More miners join network
"The target value is recalculated every 2016 blocks"
Block creation rate goes down
Block creation rate increases
Mining difficulty increases
Average mining time decreases

Fig 1 The Blockchain working

2.4 Challenges to BlockChain

Inspite the large scope of Blockchain, it faces many challenges that restricts the use of BlockChain. [4] Some big challenges are given as follows (Fig 2):

Privacy Leakage:

1. Mixing [5].
2. Anonymous[6].

Scalability:

1. Storage optimization of blockchain. [7].
2. Redesigning blockchain[8].

Selfish Mining

Privacy Leakage
Scalability
Selfish Mining

Fig 2. Different challenges to blockchain mining

Table 1. Different generations of blockchain technology

Generations	Names	Features	Popularity	Cost in market (15march)
First	BitCoin	Full Validation, Better Privacy, A Better UI, Supports the Network	Exceedingly High	$3849.78
Second	Ethereum	Decentralized, Automatic, Open, Security, Reliability, Unstoppable Apps, No need for intermediaries	Very High	$131.62
Third	Cardano	High Scalability, Interoperability, Privacy, Governance	Unseemingly Less	$0.0459
Fourth	Multiversum	Relational Database, Divisible Chains, Interoperability with Other BlockChains, Multiversum Main Net, Smart Contract	Not Released Yet	0.0025476 (expected)

The cryptocurrency is a decade-long arrival in research industry but the decentralized cryptocurrencies like BitCoin changed the finance and technological world completely. Out from being a transactional process on the Internet, the BlockChain Technology has proclaimed a mechanism to store and deal all the varieties from values to money. [9]

III. Cryptography

Cryptography is a word that is derived from the Greek letters "Kryptos" means hidden or secret and "graphein" means to comproof of stacke. The science or process of secret coding especially cipher system or codes. A vital role is played by Cryptography for ensuring secure communication between different entities. The hash function of cryptography is given in fig. 3[10-11]

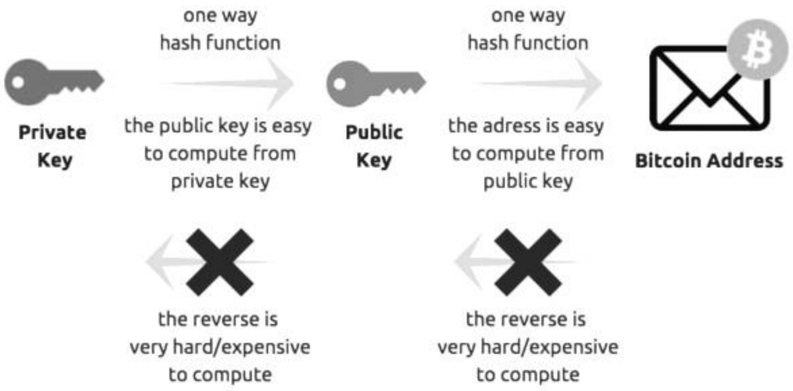
Private Key
one way hash function
the public key is easy to compute from private key
Public Key
one way hash function
the adress is easy to compute from public key
Bitcoin Address
the reverse is very hard/expensive to compute
the reverse is very hard/expensive to compute

Fig 3 Cryptography hash function

3.1 Bitcoin

BitCoin is a widely accepted virtual currency that is growing day by day. It works on the principle of cryptography i.e. it is secure, anonymous, fully validated and gives high privacy to the user.

3.1.1 Mining of BitCoin

"BitCoin Mining is the system of adding transaction records to BitCoin's public ledger of past transactions or BlockChain. The BlockChain serves to confirm transactions to the rest of the network as having taken place."[12]

3.1.2 BitCoin Miners

The hash function is cryptographically secured and the sole means to find an answer to that complication by trying all the feasible sequences. The person who will fix the prior complication earliest the most of the time is the one who has access to a huge amount of ciphering proof of worker. All those people are referred to as miners.

It is broadly fruitful primarily due to its following characteristics:

1.A given complication is very difficult to decipher.
2. Whenever determining a key to a given complication, it is effortless to authenticate if it is legit or not.

When a miner mines a new block he gets honoured with some bounty and therefore are encouraged to keep mining. Miners are inspired not to cheat due to the limited quantity of ciphering proof of worker.

3.1.3 BitCoin Security

BitCoin miners comforts in keeping the BitCoin structure shielded by accepting agreements. Mining is a crucial and intrinsic unit of BitCoin that guarantees decency by preserving the BitCoin structure safe, stable and secure.

The proof of work Concept: “A hash function is any function that can be used to map data of arbitrary size to data of fixed size. If a hash function is secure it’s output is indistinguishable from random.”[13]

A proof of work or “proof of work” is a segment of evidence which is crucial to generate & is valuable with the passing time, so as to fascinate certain requirements. Generating a proof of work can be unspecified measure with low feasibility, so that considerable trial and error is necessary on average before an authentic proof of work is generated.

The proof of stack Concept: The architect of a fresh block is picked in a regulated manner i.e. contingent on its wealth, also defined as stack.

The proof of stack or proof of stack withdraws the energy and computational proof of worker necessity of proof of work and changes it with stake. Stake is mentioned as an amount of currency that a person is ready to lock up for a particular amount of time. In exchange, the person get a chance proportional to his stake to be the next person who leads and select the next block.

There are distinct existing coins that use pure proof of stack.

3.2 Crime and Economics

With the implementation of cryptocurrency, the crime rates in virtual banking has decreased the system of BitCoin design has encouraged other applications too and are understandable by the civic. “BlockChain is considered as a type of payment rail. Private BlockChains have been prospective for business use.” [14]

Global businesses like Whatsapp, Alphabet, Amazon etc are working on their own private cryptocurrency to reduce online fraudlent and crimes. The BitCoin not only cuts down on fraud, such as double spending or spams but also impact the economy of any nation as it will remove the middleman cost by transferring funds simply, fastly and safely.

3.3 Applications

- BlockChain IOT
- BlockChain Healthcare
- Supply Chain Sensors
- Public Value
- BlockChain Identity
- Personal Identification (Better than UIDAI, India)
- BlockChain Business
- Ensuring a secure Internet

IV. Conclusion

To sum up, the BlockChain is the most proof of workerful tech of future and with its wide applications it will change the society by its block generation process and with advancement in cryptography, people can use it in their day to day life to decrease the cybercrime rates and revolutionize the public value by its proof of work and proof of stack concepts. The economy of any nation is also affected by the use of this technology. It is emerging as one of the most trending weapon of today that can remove the commission by third parties and can save a lot of money. The potential of cryptocurrency is also increasing every second. Many miners are already gaining benefits from cryptocurrency by mining BitCoins. The fully validated and secured nature of Cryptocurrency make it one of the most trusted currency globally. The downfall of cryptocurrency for now is that if once the virtual money is stolen or if the wallet is hacked, the stolen currency cannot be redeemed back as the intake of cryptocurrency is anonymous and the path is encrypted.

REFERENCES

[1] Don and Alex Tapscott, authors BlockChain Revolution(2016).

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Zibin Zheng, Shaoan Xien, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data

[4] Jonathan Hassel ,https://www.cio.com/article/3055847/what-is-blockchain-and-how-does-it-work.html

[5] M. Moser, "Anonymity of bitcoin transactions: An analysis of mixing ¨ services," in Proceedings of Munster Bitcoin Conference ¨ , Munster, ¨ Germany, 2013, pp. 17–18.

[6] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in Proceedings of IEEE Symproof of stackium Security and Privacy (SP), Berkeley, CA, USA, 2013, pp. 397–411.

[7] J. Bruce, "The mini-blockchain scheme," July 2014. [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf

[8] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoinng: A scalable blockchain protocol," in Proceedings of 13th USENIX Symproof of stackium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59

[9] Arvind Narayanan and Andrew Miller, Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts.

[10] Faiqa Maqsood, Cryptography: A Comparative Analysis for Modern Techniques, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[11] C. Narasimham and J. Pradhan, "Evaluation of Performance Characteristics of Cryptosystem Using Text Files.," J. Theor. Appl. Inf. Technol., vol. 4, no. 1, 2008.

[12] [Online]. Available: https://www.BitcoinMining.com

[13] [Online]. Available: https://en.wikipedia.org/wiki/Hash_function

[14] "Blockchain may finally disrupt payments from Micropayments to credit cards to SWIFT"[Online]. Available: *dailyfintech.com. 2018-02-10.* Retrieved 2018-11-18.