Blockchain Technology Over Cryptocurrency: A Decentralized Ledger

Manisha Kanwar [1], Anil Dhankar[2]
[1]Dept of MCA
[2] Assoc. Professor,Dept of MCA
[1, 2]RIET Jaipur

Abstract- *This Research Paper is about Decentralized Cryptocurrency (known as Bitcoins) where the transaction can be done by broadcasting the Block. This type of broadcasting intends to transact to volunteer "miners" around the world. These miners then compete to create a cryptographic signature that proves the transaction (and others) is valid and was initiated by an authorized party. This signature and the transactions are then permanently committed to history on the blockchain. This Research Paper presentation describes what is blockchain? what cryptography money is? How cryptography money is related to blockchain and how transactions can be securely done through blockchain technology without the need of any middlemen or any trusted third party to handle the transactions.*

Keywords- Bitcoins, Cryptographic Signature, Tokenize Payment, p2p networking .

I. INTRODUCTION

Blockchain is a chain of blocks and each block contains some data or information. This technique was originally described in 1991 in a research paper by a group of researchers. The was originally intended is to timestamp the digital documents so that no one can perform backdate them or tamper with them. It was unused until it was adapted by Satoshi backdate them or to tamper with them. It was unused until it was adapted by Satoshi Nakamoto in 2009 to create a digital cryptocurrency bitcoins. Blockchain is a decentralized ledger of all the transactions across a peer-to-peer network. Peer to peer network is the network in which all the nodes or computers in that network are connected directly with each other. As Blockchain Technology works on peer-to-peer networking so there is no central node that can handle the ledger of all the transactions. However, in it, every network a set of blocks or chain of blocks is created and each block contains information's about transactions or ledgers and that blockchain is transparent in nature so that everyone can access it that's why it is distributed among all the nodes across the network and that's the main reason of decentralized ledger.

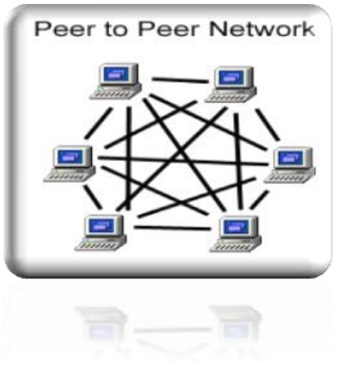


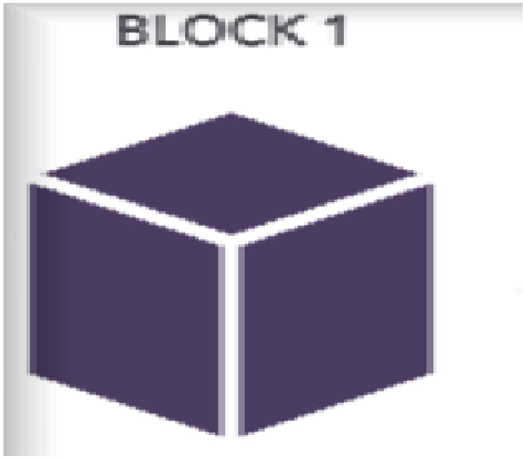
Fig 1:- Peer to Peer Networking (also known as Mash Topology)

Using this technology any one can perform their transaction without need of any trusted third party or central certifying authority.

II. LITERATURE SURVEY

Block chain is collection of bitcoin blocks in which each bitcoin block contain all the information related to transaction and ledger of transaction in the form of data, hash value and the previous hash value. That previous has value is used to link the previous block with the new one. With that data, Bitcoin block contains Block Header too.

First block of blockchain is called as Generis Block whose previous hash value (which is used to link the blocks with each other) and Timestamp is 0.



Hash value: 6u992
Previous Hash: 00000
Timestamp: 0

Fig2 :- Generis Block

In above figure generis block is shown as its previous hash value and timestamp is zero. Now hash value of that generis block is used as previous hash value in next block.

So every newly generated block contain new Hash Value (which is again used in next block as previous hash value), Previous Hash Value (which is the hash value of previous block connected with it) and a new timestamp value.

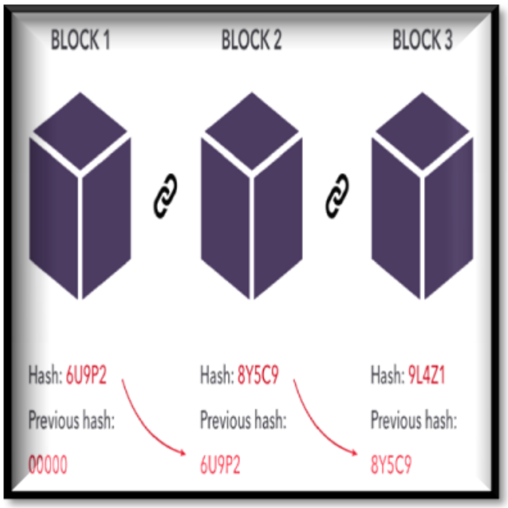


Fig3:- Structure of Blockchain

In above figure, Hash value of BLOCK1 is used as Previous Hash value of BLOCK2, BLOCK2 has a unique Hash Value assign to it which is used in BLOCK3 as Previous Hash Value and so on, so every new block is added by using the previous hash value or hash value of previous block.

Each block contain some data and Block Header. Data is information or ledger about all the Transaction performed at that block.

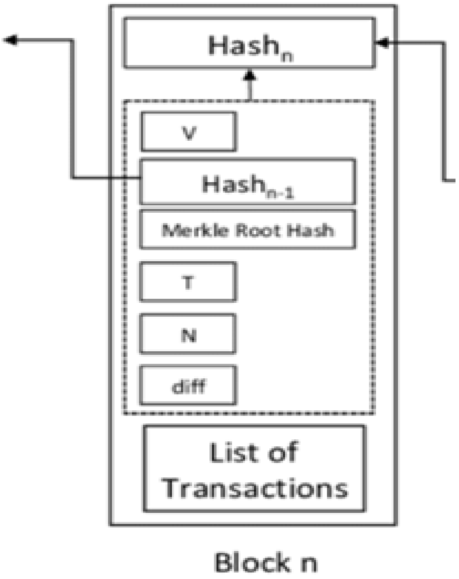


Fig4 :- Brief structure of a block

Block Header consists of a unique value or cryptographic certificate is assigned to each block called as Hash value ($Hash_n$), Version (V), Timestamp (T), Markle Root Hash, Hash value of Previous block ($Hash_{n-1}$) and Proof of work and List of Transactions.

Proof of work consist of Nounce (N) and Target Difficulty algorithm (diff) which is cryptography algorithm used to perform secure transaction.

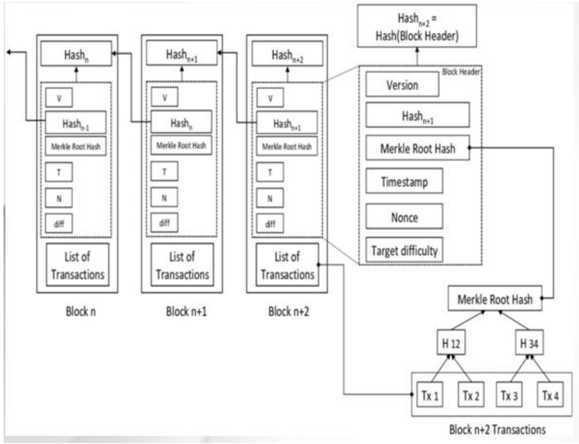


Fig5 :- Brief structure of a blockchain

Working of Blockchain Technology

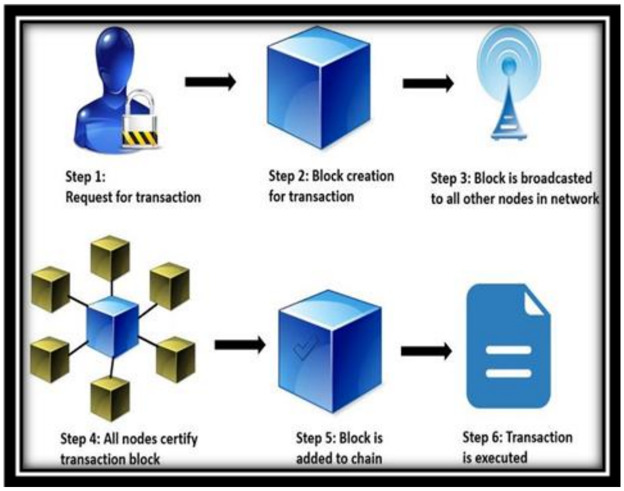

Step 1:
Request for transaction
Step 2: Block creation for transaction
Step 3: Block is broadcasted to all other nodes in network
Step 4: All nodes certify transaction block
Step 5: Block is added to chain
Step 6: Transaction is executed

Fig6 :- Flow Diagram to show how a block is added in Blockchain

To add each block in the blockchain

i) A request is generated by a node for transaction.
ii) Then on the basis of that request a block is created for transaction.
iii) That newly generated block is broadcasted to all other nodes in network.
iv) All nodes verify an certify that transaction block.
v) Now newly generated block is added to the chain
vi) Transaction is executed.

III. REASON WHY BLOCKCHAIN IS BECOME A MAINSTREAM TODAY:

- The future is Cash Free.
- Increase Digital Processing Power.
- Rapid growth in cybercrimes.
- Raise of Bitcoins and Cryptocurrency.
- Availability of Data.
- Security of Data.

IV. FEATURES

- Digital identity of Physical assets.
- Integration with RFID and IOT Sensors.
- Tokenize Payments.
- Smart Contacts.
- Proof of supply with Scanned Image.
- Barcode and QR Code integration.

V. ADVANTAGES OF BLOCKCHAIN IN CRYPTOCURRENCY DOMAIN

- Process Integrity.
- Trustlessness (No need of any trusted third party.)
- Improved Traceability
- Provide better Security.
- Faster processing
- Increased Efficiency
- Provide Transparency.

VI. DISADVANTAGES OF BLOCKCHAIN IN CRYPTOCURRENCY DOMAIN

- Complexity.

The blockchain is not simple as non-techies or old generation people can’t understand this technology easily.

- Size of Blockchain.

Bitcoins in Blockchain is of 200 GB but, every day when new transactions happen data are recorded to the blockchain then the size of blockchain is increase with each transaction.

- Human Errors:

As Blockchain is immutable therefore it need 100% correct information while creating block, if any mistake occur with data or at the time of transaction then that mistake cannot be correct easily. It can only be corrected by changing all the blocks of that blockchain and that process is time consuming

VII. CONCLUSION

Through this Research paper I tried to demonstrate the working of blockchain technology in cryptocurrency.

Features of Blockchain are not just use in currency and payment or to contracts , property and all financial market transaction but it is also used in some other areas also like government, health, science, publishing, economic development, art and culture.

REFERENCES

[1] Message from the Blockchain 2019 General Chairs. (2019). 2019 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain.2019.00007.

[2] Message from the Blockchain 2019 Program Chairs. (2019). 2019 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain.2019.00008.

[3] Blockchain 2019 Organizing and Program Committees. (2019). 2019 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain.2019.00009.

[4] Message from the Blockchain 2020 General Chairs. (2020). 2020 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain50366.2020.00006.

[5] Message from the Blockchain 2020 Program Chairs. (2020). 2020 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain50366.2020.00007.

[6] Blockchain 2020 Organizing Committee. (2020). 2020 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain50366.2020.00008.

[7] Message from the Blockchain 2020 Steering Chairs. (2020). 2020 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain50366.2020.00005.

[8] Seres, I. A. (2020). On Blockchain Metatransactions. 2020 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain50366.2020.00029.

[9] Faria, C., & Correia, M. (2019). BlockSim: Blockchain Simulator. 2019 IEEE International Conference on Blockchain (Blockchain). doi:10.1109/blockchain.2019.00067.

[10] Treiblmaier, H. (2019). Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. Frontiers in Blockchain, 2. doi:10.3389/fbloc.2019.00003.

[11] Blockchain and economic transactions. (2020). Cryptocurrency and Blockchain Technology, 9-22. doi:10.1515/9783110660807-002.

[12] Senthuran, G., & Halgamuge, M. N. (2019). Prediction of Cryptocurrency Market Price Using Deep Learning and Blockchain Information. Essentials of Blockchain Technology,349-364. doi:10.1201/9780429674457-15.

[13] Financial characteristics of cryptocurrencies. (2020). Cryptocurrency and Blockchain Technology, 55-76. doi:10.1515/9783110660807-004.

[14] Blockchain and Distributed Ledger Technology (DLT) [Working Title]. (2019). doi:10.5772/intechopen.82803.

[15] ICBC 2019 Final Program. (2019). 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). doi:10.1109/bloc.2019.8751438