IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12440

BLOCKCHAIN TECHNOLOGY

Sujata Gawade[1], Pournima Kamble[2]

Lecturer, Computer Technology, BVIT, Navi Mumbai, India[1]

Lecturer, Computer Technology, BVIT, Navi Mumbai, India[2]

Abstract: Blockchain is a secure, distributed, peer-to-peer, and open ledger. Blockchain is a chain of blocks that contains transaction information. It is meta-technology as it affects other technology. Blockchain is a digital decentralized digital ledger made up of blocks that record data across a peer to peer networks. It is used for the secure transfer of items like money, property, contracts, etc.

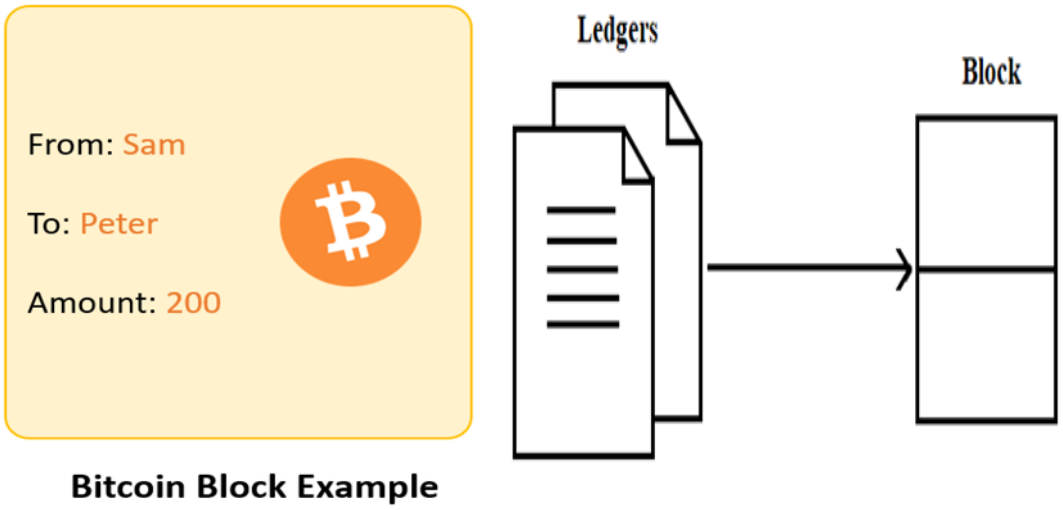
Keywords: Peer-to-peer, decentralized, distributed.

I. INTRODUCTION

W. Scott Stornetta and Stuart Haber was the founder of blockchain technology. It consists of records related to transactions. Blocks are linked together via cryptographic hashes. In blockchain consensus, cryptographic algorithms are used for the validation of new transaction blocks.

Blockchain uses a computationally practical key for time-stamping digital documents so that there is higher security. Blockchain resolves the double records problem. Blockchain consist of software applications, databases, and some connected computers, etc.

II. BLOCKCHAIN ARCHITECTURE



Bitcoin Block Example

- **Block**- Block contains transaction information that have taken place within 10 minutes such as money transfer, house transfer, gadget transfer, etc.
- For Example: Bitcoin block contain information about sender, receiver and number of coin transferred.
- **Each block consists multiple ledgers.**
- **Ledger** is database that stores transaction information.
- Ledger is a blockchain diary.

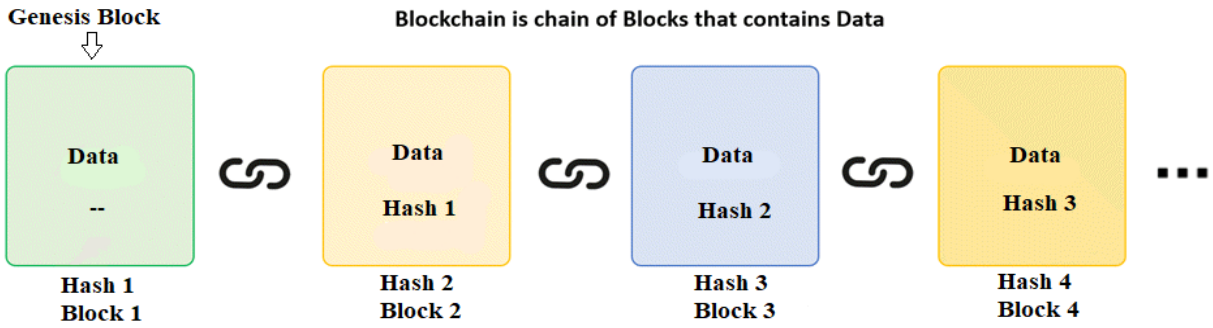
Each block has its capacity: once block is full, then new block is created and that is connected to previous block with Hash values.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12440



How data stored in block?

In Bitcoin there is a window of 10 minutes. Whatever transaction executed in 10 minutes are stored into block and after every 10 minutes a new block is created and each new block is chained (connected) with previous block using Hash value.

The first block of chain is called as Genesis block.

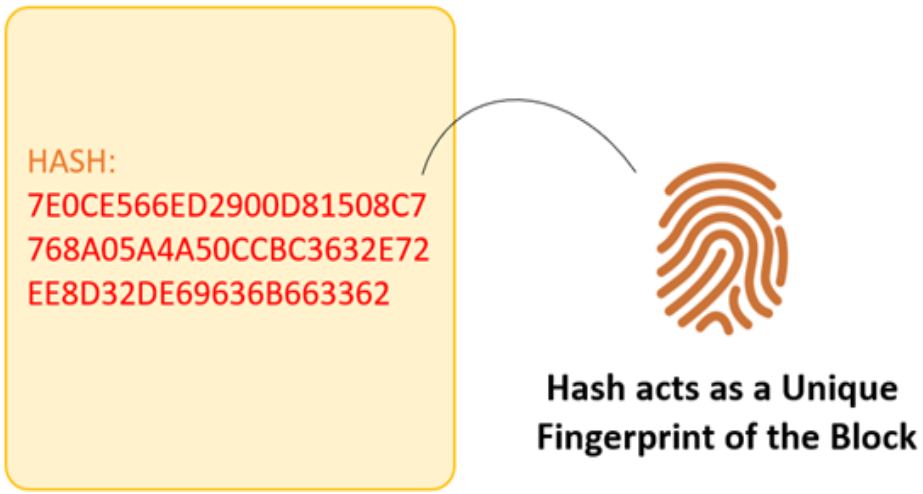
What is Hash?

Each person fingerprint is unique similarly each block hash value is unique. Hash is used to uniquely identify block and its contents in a block chain.

How to find Hash value?

The hash value of 1st block is calculated by taking all data of 1st block and applying hashing algorithm(such as SHA-3 or SHA-56) on first block data , then Hash value of 1st block is stored into 2nd block.

Similarly, Hash value of 2nd block is calculated by taking all data of 2nd block. Hash value 1st block and applying hashing algorithm on second block and so on.

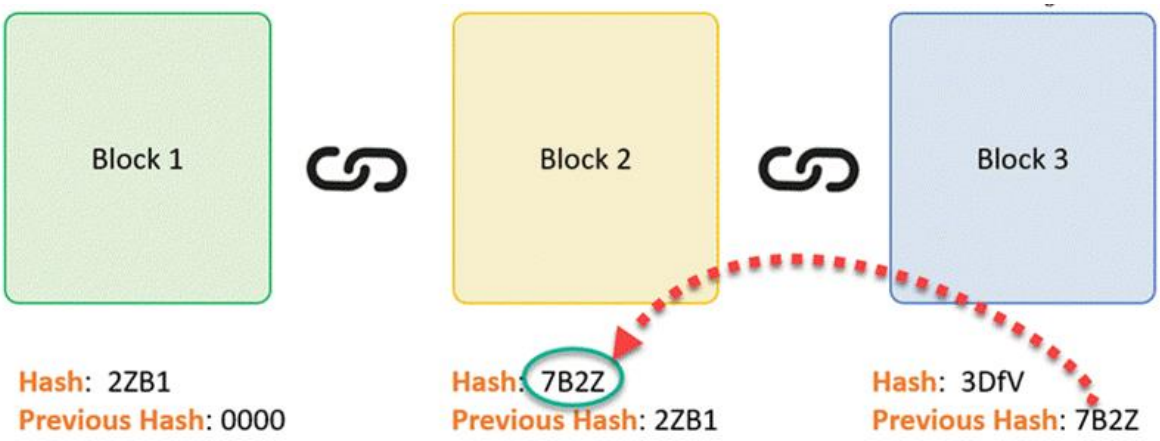


IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12440



Who is Responsible for adding block into Blockchain?

Miner is full node that verifies all transaction and add block into blockchain and gets some rewards. For example: In Bitcoin network , Bitcoin miner will get $10 for adding block in Blockchain.In Blockchain network there will be multiple miners. Everyone wants to add block in Blockchain and get rewards. So to get reward, miner need to solve puzzle.The node that solves puzzle first will get chance to add block in Blockchain and earn reward.

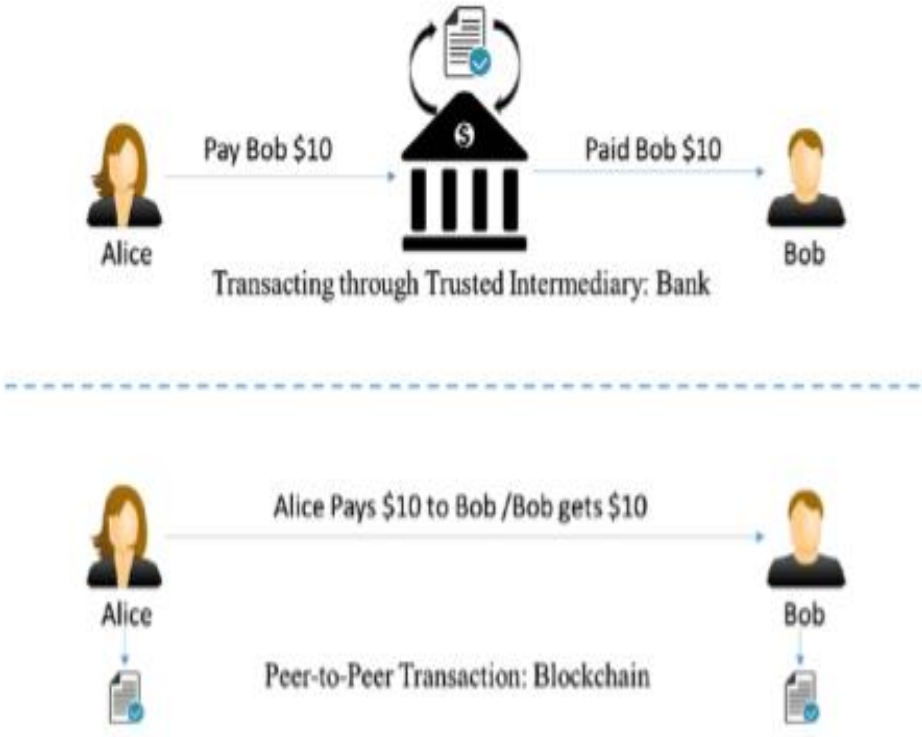


Figure 1-1. Transaction through an intermediary vs. peer-to-peer transaction

This ledger database is an append-only database and cannot be changed or altered. There is no need for trusted third parties to serve as intermediaries to verify, secure, and settle the transactions. Blockchain technology was designed to enable true decentralization. Every node on the blockchain network has an identical copy of the blockchain

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12440

Decentralized Blockchain System

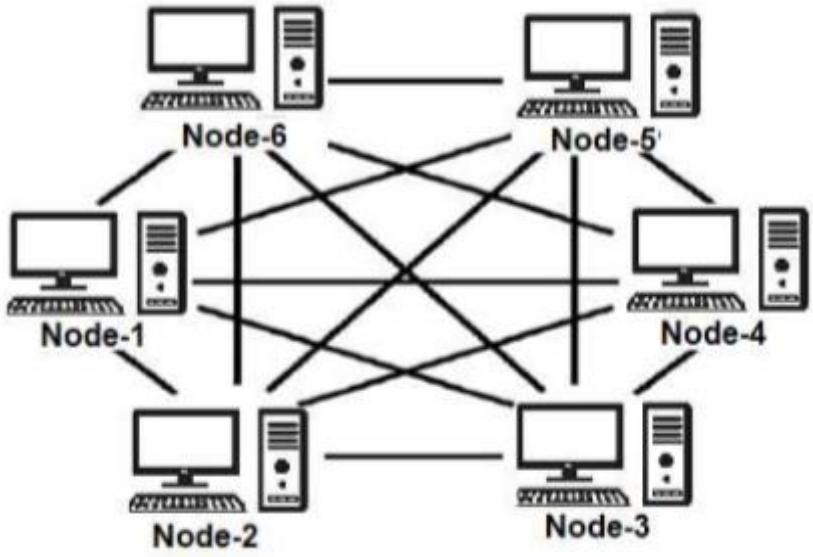


Fig.3.3 A decentralized and peer-to-peer system

All nodes in decentralized system are connected with each other in peer to peer network. Decentralized systems are **difficult to design, maintain, govern, or impose trust.**

Layers of Blockchain

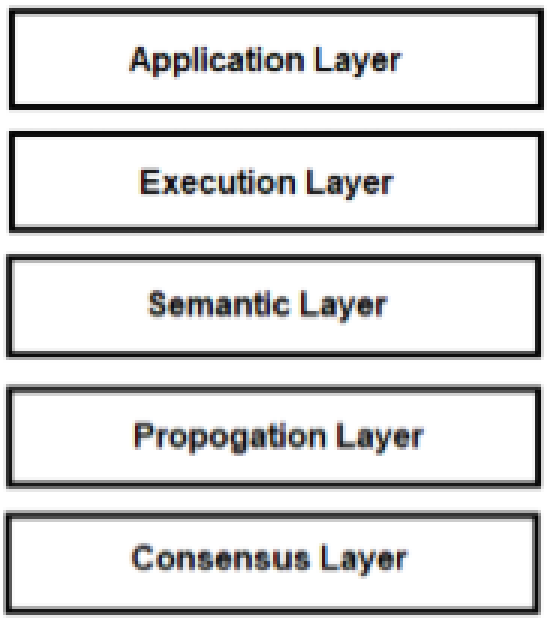


Fig.3.5 Layers of Blockchain

1. **Application Layer:**
It is made **up** of smart contracts and decentralized applications DApps). This layer acts as the front end of the blockchain through which users interact with the blockchain network.

2. Execution Layer:
The Execution Layer executes the instructions of application on all the nodes in a blockchain network.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12440

3. Semantic Layer:
Semantic Layer also called as logical layer and it deals with the validation of the transactions done in the blockchain network

When a transaction is initiated by a node, the set of instruction are executed on the execution layer and validated by the semantic layer.

4. **Propagation Layer (Network Layer):**
This layer facilitates communication between the different nodes within the blockchain network. When new transaction is done, then it's broadcasted to all other nodes in the network by propagation Layer

III. CONCLUSION

Blockchain technology is a distributed, decentralized, and open ledger. In Blockchain technology, a third party is not required for any transactions. It is a secure, demanding and trusted technology.

REFERENCES

[1] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world:Income tax considerations of the bitcoin economy," 2013. [Online]. (Available: https://ssrn.com/abstract=2394738
[2] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
[3] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
[4] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning," arXiv preprint arXiv:1601.01405, 2016.
[5] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
[6] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
[7] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
[8] NRI, "Survey on blockchain technologies and related services," Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf
[9] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed.Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170
[10] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, 2014.
[11] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digitalsignature algorithm (ecdsa)," International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.