INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898

Volume: 05 Issue: 05 | May 2023

Blockchain Merkle Tree

Absalamova Go'zal Bo'riboyevna

Assistant, Department of Software Engineering, Faculty of Intellectual Systems and Computer Technologies, Samarkand State University named after Sharof Rashidov

----------***----------

Abstract: In this research, the Blockchain Merkle Tree, which plays a decisive role in ensuring the integrity and security of data in the blockchain network, is analyzed. The Merkle Tree, also known as a hash tree, is a fundamental concept in blockchain technology. Named after Ralph Merkle, the Merkle Tree is a hierarchical data structure composed of cryptographic hash functions. The Merkle Tree provides several benefits in a blockchain context. First and foremost, it allows for efficient verification of data integrity. Instead of needing to validate each and every transaction in a block, a participant can simply verify the Merkle root and a small number of other hashes in the tree to ensure that the data hasn't been tampered with.

Keywords: Blockchain, data structure, Hash Tree, Ralph Merkle, **Binary Merkle Tree, block header.**.

INTRODUCTION

Merkle tree is a fundamental part of blockchain technology. It is a mathematical **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as **Hash Tree [1]**.

At its core, the Merkle Tree takes a collection of data (such as transactions in a blockchain) and combines them through a process called hashing. Each transaction or data element is individually hashed, and then pairs of hashes are combined and hashed together until a single root hash, known as the Merkle root, is obtained. This root hash represents the entire set of data in a concise and verifiable manner. Additionally, the Merkle Tree enables efficient synchronization and pruning of blockchain data. As new transactions are added, the tree structure allows for quick identification of differences and updates, making data synchronization faster and more efficient. Similarly, old or redundant data can be pruned by removing branches or leaves of the tree without affecting the overall integrity of the Merkle root. The Merkle Tree also contributes to the security of blockchain networks. In a decentralized system where multiple participants hold copies of the blockchain, the Merkle Tree provides a cryptographic proof of the validity of the data. By comparing hashes and verifying the Merkle root, participants can detect any attempts to modify or manipulate the data [2].

The concept of Merkle Tree is named after **Ralph Merkle**, who patented the idea in **1979**.

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES
https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 05 Issue: 05 | May 2023

Fundamentally, it is a data structure tree in which every **leaf node** labelled with the hash of a data block, and the **non-leaf node** labelled with the cryptographic hash of the labels of its child nodes. The leaf nodes are the lowest node in the tree [3] .

Merkle trees work

A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not.

Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. The Merkle Trees are constructed in a bottom-up approach [4,5].

Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes. Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd number of transactions, the last hash will be duplicated once to create an even number of leaf nodes [6,7].

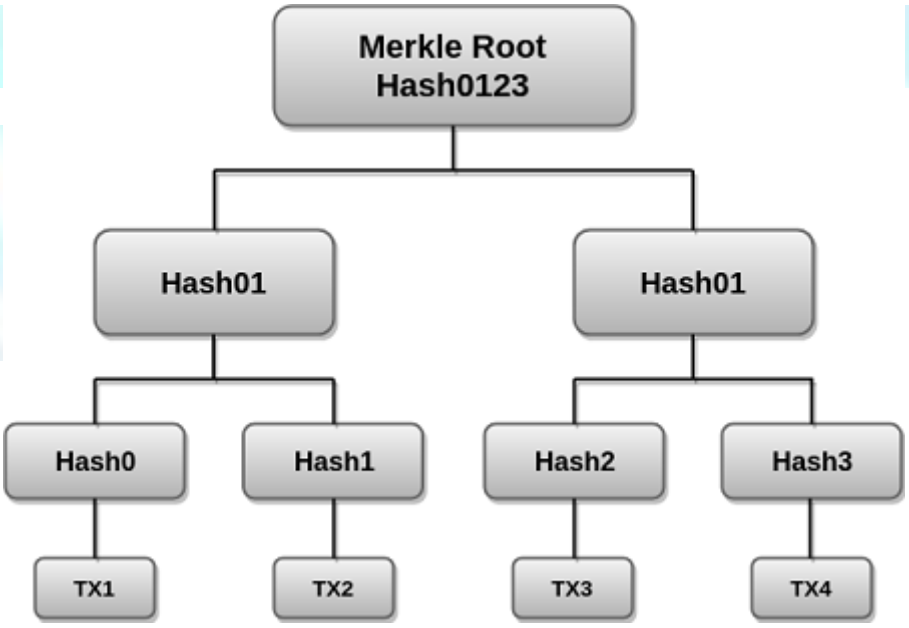

Figure 1. Merkle tree.

The above example is the most common and simple form of a Merkle tree, i.e., **Binary Merkle Tree**. There are four transactions in a block: **TX1**, **TX2**, **TX3**, and **TX4**. Here you can see, there is a top hash which is the hash of the entire tree, known as the **Root Hash**, or the **Merkle Root**. Each of these is repeatedly hashed, and stored in each leaf node, resulting in Hash 0, 1, 2, and 3. Consecutive pairs of leaf nodes are then summarized in a parent node by hashing **Hash0** and **Hash1**, resulting in **Hash01**, and separately hashing **Hash2** and **Hash3**,

INTERNATIONAL JOURNAL OF HUMAN COMPUTING STUDIES
https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 05 Issue: 05 | May 2023

resulting in **Hash23**. The two hashes (**Hash01** and **Hash23**) are then hashed again to produce the Root Hash or the Merkle Root [8,9].

Merkle Root is stored in the **block header**. The block header is the part of the bitcoin block which gets hash in the process of mining. It contains the hash of the last block, a Nonce, and the Root Hash of all the transactions in the current block in a Merkle Tree. So having the Merkle root in block header makes the transaction **tamper-proof**. As this Root Hash includes the hashes of all the transactions within the block, these transactions may result in saving the disk space.

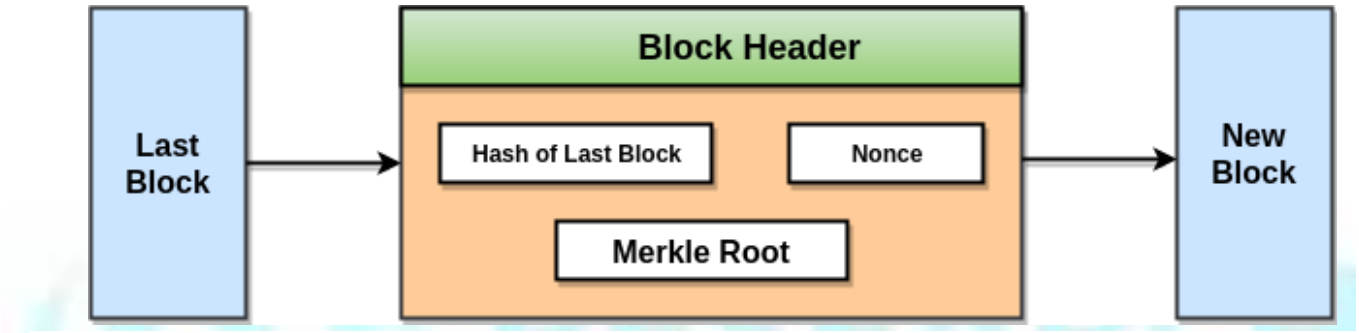

Figure 2. Block Header.

- It provides a means to maintain the integrity and validity of data.
- It helps in saving the memory or disk space as the proofs, computationally easy and fast.
- Their proofs and management require tiny amounts of information to be transmitted across networks [10].

Conclusion

Overall, the Merkle Tree is a vital component in blockchain technology, enhancing data integrity, efficiency, and security. Its hierarchical structure and cryptographic properties make it an essential tool for ensuring the trustworthiness and immutability of blockchain-based systems.

References

1. Hwang, M.S.; Lin, I.C. Introduction to Information and Network Security (in Chinese); Mcgraw Hill: Taipei,Taiwan, 2011.
2. Kumar, C.; Singh, A.K.; Kumar, P. A recent survey on image watermarking techniques and its applicationin e-governance. Multimed. Tools Appl. 2018, 77, 3597–3622. [CrossRef]
3. Cox, I.J.; Miller, M.L.; Bloom, J.A. Watermarking applications and their properties. In Proceedings ofthe International Conference on Information Technology: Coding and Computing (Cat. No. PR00540),Las Vegas, NV, USA, 27–29 March 2000; pp. 6–10.
4. Joshi, M.A. Digital Image Processing: An Algorithmic Approach; PHI Learning Pvt. Ltd.: Delhi, India, 2018.
5. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. IJ Netw. Secur. 2017, 19, 653–659.

https://journals.researchparks.org/index.php/IJHCS e-ISSN: 2615-8159 | p-ISSN: 2615-1898
Volume: 05 Issue: 05 | May 2023

6. Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
7. Hughes, L.; Dwivedi, Y.K.; Misra, S.K.; Rana, N.P.; Raghavan, V.; Akella, V. Blockchain research, practiceand policy: Applications, benefits, limitations, emerging research themes and research agenda. Int. J.Inf. Manag. 2019, 49, 114–129. [CrossRef]
8. Benet, J. Ipfs-content addressed, versioned, p2p file system. arXiv 2014, arXiv:1407.3561.
9. Mougayar, W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology; JohnWiley & Sons: Hoboken, NJ, USA, 2016.
10. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. Int. J.Web Grid Serv. 2018, 14, 352–375. [CrossRef]