Pros and Cons of Merkle Tree

Remya Chandran

St. Joseph's College Devagiri

Corresponding author: Remya Chandran, Email: nivedika@gmail.com

The Merkle trees are a type of structure that provides for the efficient and secure authentication of vast amounts of data and is a key component of blockchain technology. This is used in distribution systems to ensure that data is authenticated effectively. This technology is used by Ethereum and Bitcoin. It is incredibly efficient because it uses hashes instead than whole files. The Merkle tree is an essential component of blockchain technology. It's an arithmetic data structure made up of hashes of various data blocks that serves as a summary of all transactions in a block. It also enables well-organized and secure content verification in large amounts of data. It also aids in validating the data's consistency and content. Merkle Trees are used by Bitcoin and Ethereum.

Keywords: Authentication, Keyless signatures, Merkle Signature.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 649–653. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-61

1 Introduction

The Merkle trees are a crucial aspect of block chains that support their functioning. With Merkle trees, enormous data structures may be validated safely and effectively, and in blockchains, virtually endless data can be expected. Prior to Merkle Trees, every blockchain transaction had its own unique transaction ID. Blockchains are made up of hundreds of thousands of blocks, each of which can hold many transactions. Memory space and computational power become evident issues. As a result, when handing out and validating transactions, it is advantageous to utilise as little data as feasible. It decreases CPU processing times while maintaining a high level of security. Merkle Trees is a company that specialises in this type of work. Merkle Trees essentially take a large number of transaction IDs and run them through a mathematical process that yields a single 64-character code known as a Merkle Root. The Merkle Root is critical because it allows any computer to quickly and reliably verify that a certain transaction occurred on a block. The merkle tree provides users with a hash-based architecture to ensure data veracity as well as a simple mechanism to validate data integrity[1][2].

A Merkle tree summarises all of the transactions in a block by generating a digital fingerprint of the complete collection of transactions, allowing a user to check whether or not a transaction is included in the block. Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains (the Merkle Root). They're built from the ground up, using hashes from individual transactions. Each non-leaf node is a hash of its previous hashes, while each leaf node is a hash of transactional data. Merkle trees are binary, hence an even number of leaf nodes is required. The last hash will be duplicated once if the number of transactions is odd[3][4][8].

If the number of transactions is odd, the last hash will be copied once in each transaction to ensure an even number of leaf nodes.

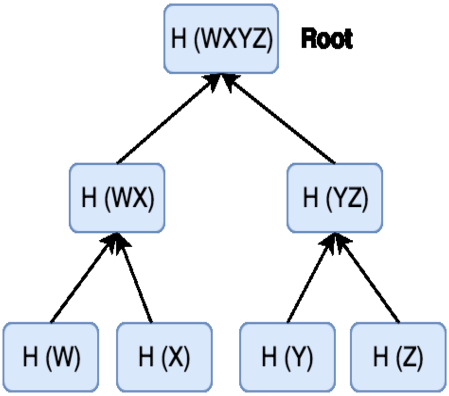

Fig 1.1

For example the above figure 1.1 shows four transactions in a single block. The leaf-node corresponds to the parents of these leaves, which are hashes of the concatenation; the leaf-node contains hashes of a file's data [5][1][6].

2. Data Authentication

Merkle trees is used for data authentication[7]. The steps of data authentication is as follows.

1. Data is being downloaded from an untrustworthy network.
2. The server will be tasked with proving that the piece is in the tree.
3. The relevant hashes will be returned by the server.
4. Using this information, the user can calculate the root hash, compare it to the root hash, and access the file.

For example, the user must check if the chunk (Y) is there in the original file . The server responds with the information H (Z) and H (WX) based on the request.

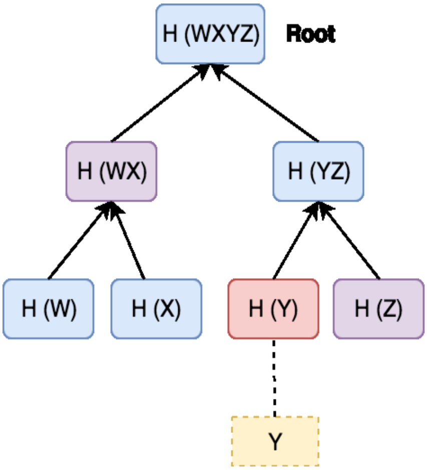

Fig. 1.2

How does the user calculate:

- H (YZ) from H (Y) that the user already has and H (Z) that the trustworthy server provided.
- H (WXYZ) from the user's H (YZ) calculation and H (WX) from the trustworthy server.
- The original root hash H (WXYZ) that compares and calculates can now be used to locate the file on an untrusted network. To ensure that the chunk is still on the tree and hasn't been tampered with or damaged, the hashes should be compared.

2 Advantages

- It has a specified internal structure and is useful for verifying block headers. Return proof of existence can be sent in variable format. Lookup can be kept in Merkle tree.
- It can be perform updates in a specific order and to calculate root hash predictably.
- It will helps to block header preparation as well as header verification.
- It saves a lot of space by only using space for shared sub trees once.
- It aids in memory or disc space conservation as proven, and it is computationally simple and quick.
- Their proofs and management require the transmission of modest amounts of data across networks.
- Simplified Payment Verification is a way to validate transactions in a block without having to download the complete block.

3 Disadvantages

- The merkle does not yield absence since the position of an element in the tree is unknown.
- When used in the Ethereum network, it has two major drawbacks:
  - ➢ It necessitates a huge computer capacity, which increases electricity costs as well as system maintenance costs; and
  - ➢ It slows down the system, making it time consuming.

4. Conclusion

Merkle trees are an important part of blockchains. Blockchains are used for effective and secure validation of huge data structures, particularly in possibly infinite data sets. This is for successful large-scale data mapping; it will assist in identifying tiny data changes and pinpointing the specific spot where the changes occurred. It served as the full data's fingerprint. On a blockchain, Merkle Trees benefit both consumers and miners. Users can validate individual blocks and test transactions using hashes from other Merkle Tree branches. Miners can continuously compute hashes as they receive transactions from their peers. The "irreversible" and encrypted data blocks of the blockchain can also aid in the fight against cybercrime, as any attempts by a hacker to change data will be recognised immediately. Companies and governments are joining up as blockchain uses for cyber security emerge.

5. Future Work

The blockchain protocol level, which is characterised by recursive interactions between human agents and the blockchain protocol, requires the most attention and research work in the future.

References

[1] Youngjoo Shin (2018), ―Improving Security And Reliability In Merkle Tree-Based Online Data

[2] Francesco Restuccia,Salil S. Kanhere &Salvatore D'oro (2018), ― Block Chain For The Internet Of Things: Present And Future: Ieee Internet Of Things Journal, Vol. 1, No. 1.

[3] Kaufman (2002), "Network Security: Private Communication In A Public World", Upper Saddle River, Nj, Us, Prentice Hall Press, 2002.

[4] R. C. Merkle (1988), &Quot;A Digital Signature Based On A Conventional Encryption Function,&Quot; In Advances In Cryptology—Crypto'87", Pp. 369-378.

[5] Buldas, A., Laanoja, R. (2013), ―Security Proofs For Hash Tree Time-Stamping Using Hash 17 Functions With Small Output Size In: Boyd, C.,Simpson, L. (Eds.): Acisp 2013‖, Lncs 7959, Pp.235–250, 2013, Springer, Heidelberg (2013).

[6] An Image Authentication Scheme Using Merkle Tree Mechanisms,Yi-Cheng Chen,Yueh-Peng Chou And Yung-Chen Chou July 2019.

[7] Enhancing The Security Through The Usage Of Merkle Tree And Timestamp In Peerto Peer Messaging,Katyayani Sharma And Dr. Vairamuthus,International Journal Of Pure And Applied Mathematics Volume 119 No. 7 2018.

[8] Improving Security And Reliability In Merkle Tree-Based Online Data Authentication With Leakage Resilience,Dongyoung Koo,Youngjoo Shin, Joobeom Yun, And Junbeom Hur Mdpi, December 2018.