Marq's Consensus Protocol

Abstract

Smart contract platforms and cryptocurrencies have captured mass attention but still have not been able to achieve mass adoption due to scalability and user experience issues. Even on Ethereum, which is the most widely used smart contracts platform, there have not been many examples of DApps which have seen mass adoption. There have been a few cases where one or the other particular application temporarily succeeded in achieving a significant user base, but it led to crippling of the entire network during the high network load times. Essentially, this means that even the most advanced and widely used platforms are not ready for mass adoption yet.

Adding to the challenges, the sheer number of blockchains available presents another obstacle to the mass adoption of blockchain technology. With so many options, users may find it difficult to adopt all of them, leading to a fragmentation of the ecosystem. This fragmentation can hinder the growth of the blockchain industry as a whole and may slow down the development of new, innovative solutions. Therefore, it is essential to find ways to bridge different blockchain networks and promote interoperability, allowing users to take advantage of the benefits offered by various blockchains without having to adopt them all.

Marq recognizes the challenges facing smart contract platforms and cryptocurrencies, particularly the issues of scalability, user experience, and the difficulty of achieving mass adoption. To address these issues, Marq has developed its proprietary solution, which is the hyper chain that sits in the middle of all blockchain networks and provides a two-way bridge to existing blockchains, allowing for seamless interoperability.

By leveraging the existing developer community, Marq aims to provide a powerful and versatile solution for building Web3 applications. Hyper Layer allows users to take advantage of the benefits offered by various blockchains without having to adopt them all, thereby addressing the problem of too many blockchains. By bridging different blockchain networks, Marq hopes to create a more seamless and user-friendly experience for developers and end-users, while also ensuring speed, security and scalability.

Introduction

Marq's Consensus Protocol is an innovative approach to achieving distributed consensus in blockchain networks. The protocol is designed to provide fast, secure, and reliable transaction processing, making it an attractive option for a wide range of blockchain applications.

At the heart of Marq's Consensus Protocol is a unique approach to achieving consensus that combines multiple layers of verification to ensure the accuracy and integrity of the blockchain ledger. This approach leverages the strengths of multiple consensus mechanisms to achieve fast and reliable transaction finality, while also optimizing for efficiency and scalability.

One of the key features of Marq's Consensus Protocol is its dynamic verification process that adjusts based on network conditions and the behavior of network participants. This process encourages honest behavior among nodes and adapts to changing network conditions to ensure optimal performance.

Another important aspect of Marq's Consensus Protocol is its focus on user privacy and data protection. The protocol is designed to provide robust security features that protect user data from theft, hacking, and other forms of malicious activity. This makes it an ideal solution for use cases that require high levels of security and privacy, such as finance, healthcare, and supply chain management.

Marq's Consensus Protocol is a breakthrough technology, offering a unique approach to distributed consensus, scalability, and security. Its innovative strategies ensure efficiency and effectiveness, making it an attractive solution for various blockchain applications.

The Network

Marq's network is a highly secure and reliable platform for Web3 applications, providing permanent storage of transaction data through parallel processing across multiple nodes. This ensures the integrity and accuracy of the data, making it tamper-proof and resistant to any changes or modifications.

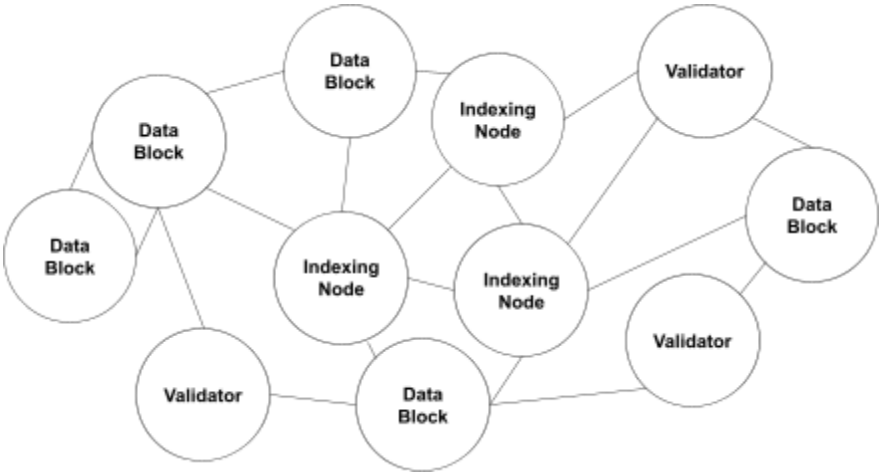
The network's architecture is designed to enable parallel processing of transaction data, enabling multiple nodes to work together to verify and process transactions simultaneously. This results in faster execution speeds, making it ideal for applications that require high transaction volumes.

There are three types of nodes in the network: validating nodes, data blocks, and indexing nodes:

Validating Node
A validation node is a type of node in the network that is responsible for validating transactions and blocks on the network.The validation node performs several critical functions, including validating transactions and participating in the consensus process to reach agreement on the state of the network.

Indexing Node
An indexing node is a type of node within the Marq network that is responsible for creating and maintaining the multi-level tree structure that enables efficient and secure storage of transaction data. This node plays a critical role in optimizing transaction processing speed by indexing the latency and capacity of validating nodes, ensuring that blocks are validated quickly and efficiently. In addition, the indexing node is responsible for linking data blocks via an address location, allowing one node to refer to another with the leaf node at the lowest level. This approach provides several benefits, including faster transaction processing and improved data integrity. The indexing node also acts as a key component of Marq's network architecture, enabling the network to handle high volumes of transactions with efficiency and speed.

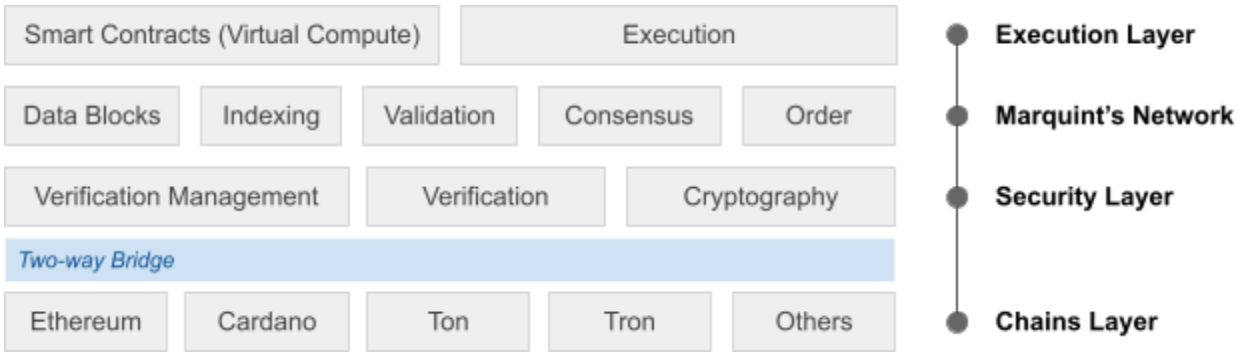
Data Block (node)
Data blocks in the Marq network serve as a repository for transaction data. Each data block contains a fixed-size amount of information and is linked to other data blocks through the network's multi-level tree structure. The data blocks are stored across multiple nodes in the network, ensuring redundancy and security. With advanced caching mechanisms, data access after retrieval is efficient and fast. The data blocks provide a permanent and tamper-proof record of transactions, ensuring the integrity and accuracy of the data stored on the Marq network.



Marq's network uses advanced indexing technology, encryption, consensus, cryptography, and distributed principles to create a secure and transparent network that can handle high volumes of transactions with efficiency and speed. By leveraging these core features, Marq's network offers a powerful solution for building decentralized applications that can run on the Web3 infrastructure. These applications can be used for a wide range of use cases, from finance and healthcare to supply chain management and gaming.

The Architecture

The Marq network architecture consists of four abstract layers that work together to create a secure, efficient, and decentralized platform for Web3 applications. At the core of this architecture is the chain layer, which supports various blockchain chains such as Ethereum, Bitcoin, and others. The chain layer interacts with the security layer through a two-way bridge, allowing for secure and efficient data transfer between the two layers.



The security layer serves as the gateway to the Marq network, providing access control and authorization mechanisms to ensure the integrity and confidentiality of the network. It is responsible for managing authentication, encryption, consensus, and other security-related tasks.

The network layer is where the distributed nature of the Marq network is realized. It consists of multiple nodes working together to provide parallel processing of transaction data, enabling fast and efficient execution of transactions. The network layer also incorporates advanced indexing technology to create a multi-level tree structure for the efficient and secure storage of transaction data.

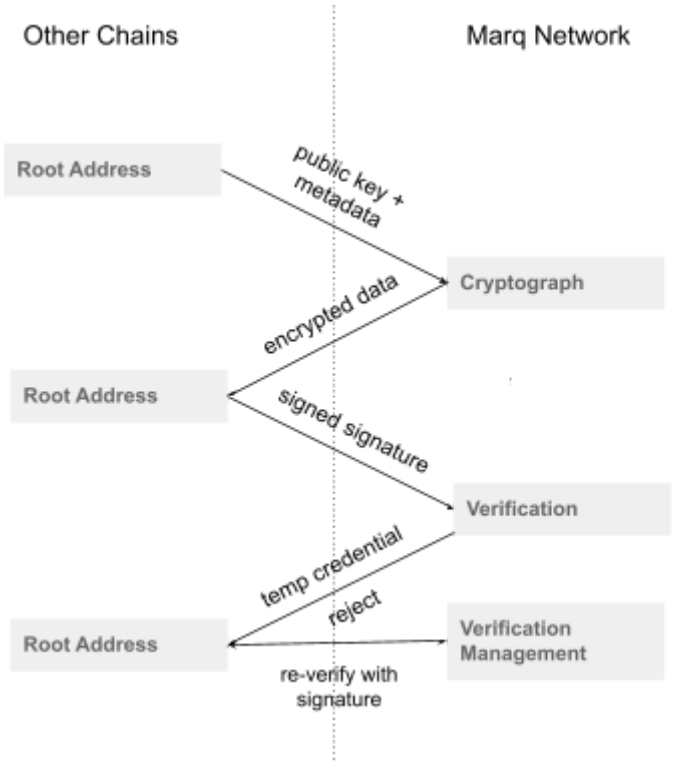
The execution layer comprises the smart contract execution and transaction execution mechanisms. This layer provides the computational power necessary for the execution of complex smart contracts and the processing of transactions on the Marq network.

Interoperability

The two-way bridge in Marq's network plays a crucial role in facilitating secure and efficient communication between the chain layer and the network. When a wallet intends to interact with the Marq network, it transmits its public address and metadata, such as chain information and wallet details, via the two-way bridge to the security layer.

Subsequently, the Cryptographer, who is responsible for encrypting and decrypting messages, responds with an encrypted message that requires the wallet's signature for verification. The wallet signs the encrypted message with its private key and returns the signature hash to the security layer.

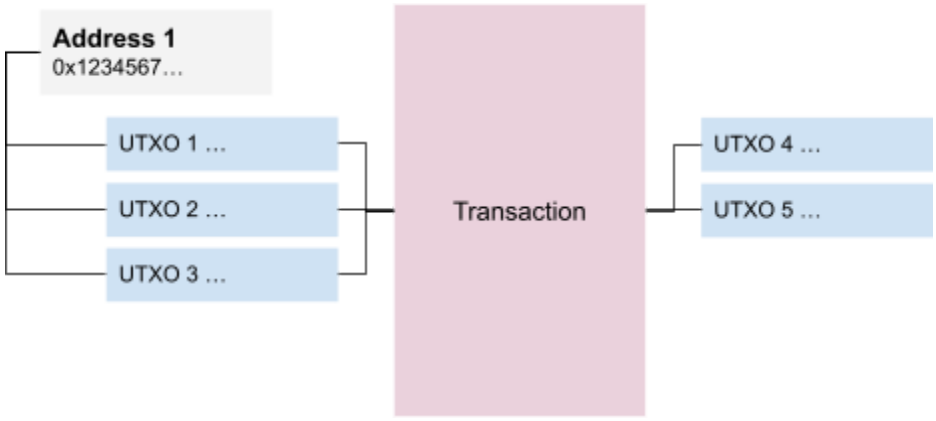
The validator in the security layer then verifies both the signature and the message. If the information is validated, the security layer issues a temporary credential to the wallet, enabling the user to interact with the Marq network securely. This process ensures the network's security and integrity, safeguarding the users' assets.



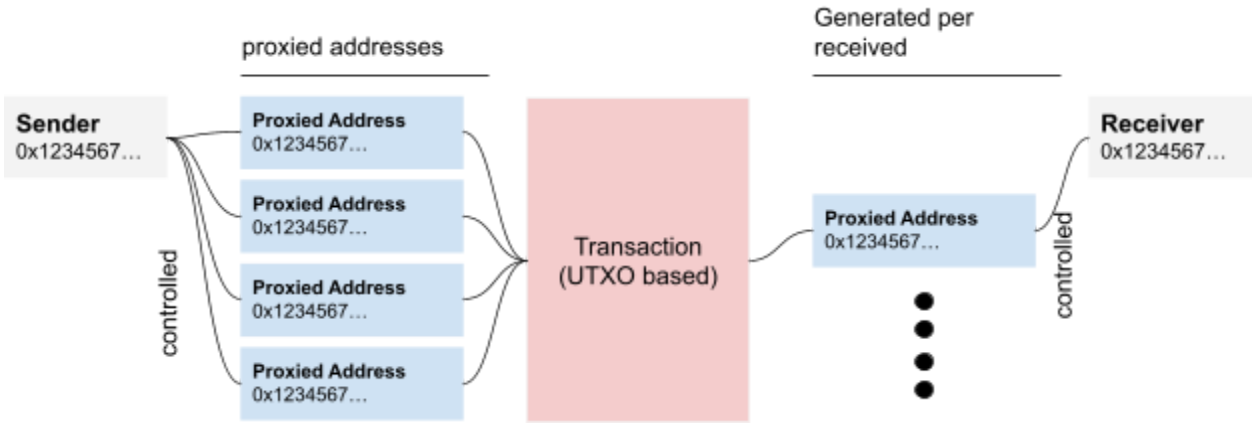
Privacy-Focused: Ensuring Confidentiality and Security in Data Handling

Marq's consensus protocol is designed to ensure the ultimate privacy and security of transactions on the network. To achieve this, the protocol utilizes the Proxied Unspent Transaction Output (PUTXO) model.

The traditional Unspent Transaction Output (UTXO) model allows each transaction output to be spent only once, with any leftover value returned to the wallet as a new unspent transaction output. This approach enables more efficient use of network resources and faster transaction processing times. However, the UTXO model has limitations that can compromise the privacy of users, as each transaction output is linked to a specific address on the blockchain, enabling the tracking of funds between addresses.



PUTXO is a new approach to transaction privacy that combines the benefits of the traditional UTXO model with the added privacy provided by proxied addresses. PUTXO uses a unique one-time proxied address for each transaction output. The proxied address acts as a proxy for the real address, obscuring it from view and making it much more difficult to track the movement of funds between addresses.



PUTXO prioritizes user privacy and security while enabling traceability of funds on the network. By using unique one-time proxied addresses that can be linked to real addresses on the blockchain, transactions involving PUTXO remain auditable and verifiable. This feature enhances privacy without sacrificing the ability to trace the flow of funds, ensuring that transactions are secure and transparent.

Proxied Address

A proxied address is created by a user to act as a proxy for their primary address, enabling them to interact with the blockchain using a separate address while maintaining control over their assets. It is secured and linked with the primary address using the highly secure ChronoSecure Algorithm developed by Marq. When creating a proxied address, the public key and encrypted code are broadcasted to the network, facilitating transaction authenticity verification and privacy preservation of the user's primary address. To ensure secure access to their assets, the user can retrieve the private key using the ChronoSecure Algorithm with their signature and encrypted code.

The ChronoSecure Algorithm is a highly secure encryption and decryption algorithm developed by Marq. It utilizes a unique combination of the cryptographic content, a signature of the content, and a timestamp to encrypt and decrypt data. When encrypting the cryptographic content, the algorithm takes the content and its signature as inputs. The algorithm generates an encrypted code that can only be decrypted using an object that contains the encrypted code, a timestamp hash generated using the encrypted code, and a signature that is signed with a private key. This time-based approach to encryption and decryption adds an additional layer of security, as the decryption process is only valid for a limited period of time.

PUTXO Safety Check and Verification Process

When a user produces a PUTXO transaction, the transaction is first broadcast to the network to check if the proxied address exists. This is done by checking the signature of the proxied address in the past block. If the signature is valid and the address exists, the PUTXO transaction is added to the mempool.

However, if the proxied address does not exist or the signature is invalid, the PUTXO transaction is rejected by the network and not added to the mempool. This prevents the scenario where funds are sent to a non-existent proxied address and ensures that only valid transactions are processed.

In addition, each PUTXO transaction has a unique identifier that prevents double-spending. This identifier is generated by combining the transaction inputs, outputs, and a timestamp, and then taking a cryptographic hash of the result. Any attempt to spend the same output twice will result in a different transaction identifier, which will be rejected by the network.

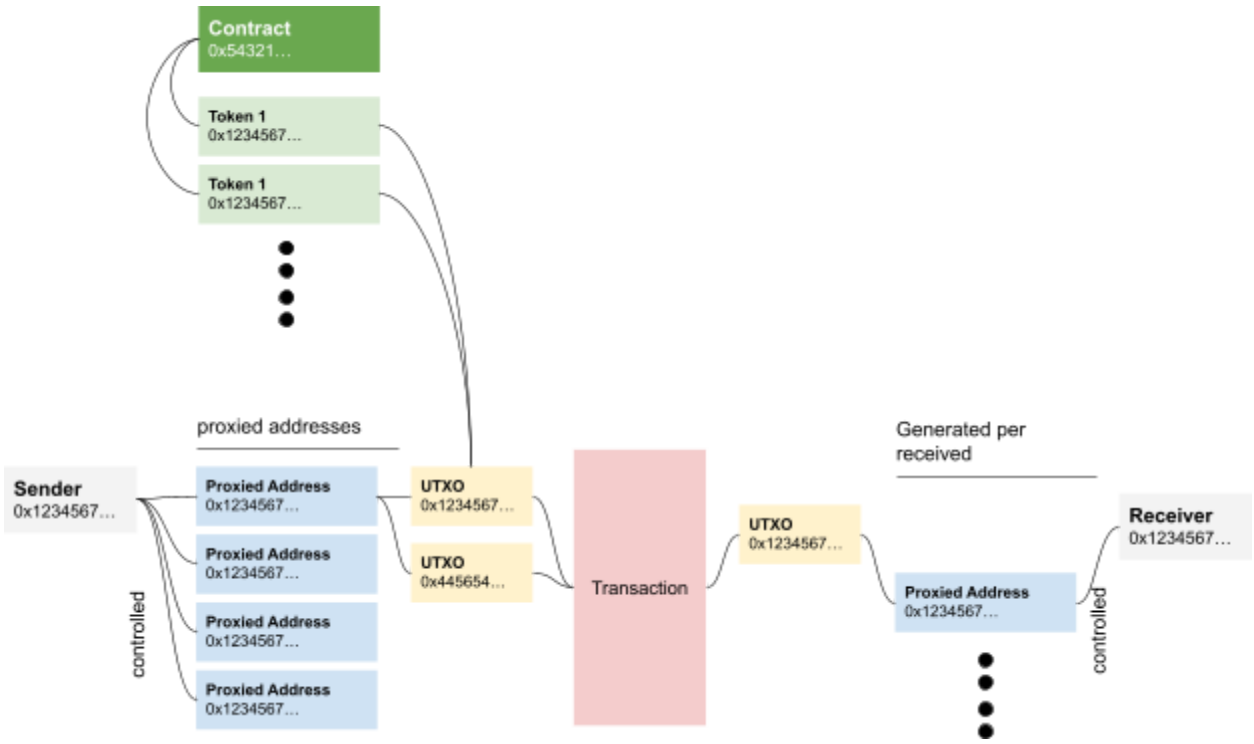
By using these safety checks, the Marq network is able to ensure the integrity of PUTXO transactions and prevent malicious behavior such as double-spending or sending funds to non-existent proxied addresses. This improves the security and reliability of the network, which is essential for a decentralized financial system.

The Smart Contract

In the Marq Consensus Protocol, smart contracts play a pivotal role in enabling diverse transactions on the network. Unlike other blockchain networks, where users have unrestricted access to deploy smart contracts, the Marq Consensus Protocol enforces strict governance through the Marq Committee and third-party experts to ensure that smart contract standards are secure and stable. This rigorous approach guarantees that only approved smart contract standards are allowed on the Marq network, providing users with a higher level of security and trust. Additionally, the use of approved standards promotes interoperability and compatibility among smart contracts, streamlining the development of decentralized applications on the Marq platform.

Extended PUTXO

Marq Consensus Protocol has extended the PUTXO model to support the execution of complex smart contracts through the use of ePUTXO.



The ePUTXO model expands on the traditional concept of addresses by using a lock-and-key analogy. Unlike in traditional UTXO models where locks are restricted to public keys and keys to signatures, ePUTXO addresses can contain arbitrary logic in the form of scripts. When a transaction is validated by a node, the node checks whether the transaction can use a particular output as an input by executing the script provided by the output's address. This flexibility allows scripts to carry state information, making them more powerful.

In addition, ePUTXO outputs can carry arbitrary data in addition to an address and value, further enhancing the capabilities of the scripts. By generalizing the concept of addresses, the ePUTXO model allows for greater flexibility in designing complex smart contracts and enables more sophisticated use cases on the Marq network.

One key advantage of the ePUTXO model is its ability to precisely predict the fees required for a valid transaction before it is posted. This is a notable difference from account-based models like Ethereum, which are indeterministic and cannot guarantee the effects of a transaction on-chain. With account-based models, there is a risk of monetary loss, unexpectedly high fees, and potential for adversarial behavior due to the uncertainty of the system. By contrast, the deterministic nature of the ePUTXO model allows for more reliable fee estimation and a lower risk of unintended financial consequences.

In summary, the ePUTXO model provides enhanced security and privacy, as well as predictable smart contract execution costs. Additionally, the model enables more powerful parallelization, which is optimized for efficient network resource utilization.

Extended Proxied Address

The Extended Proxied Address is a unique feature of the Marq Consensus Protocol that allows for complex smart contract execution. It is created through a smart contract and acts as an agent or middleman that executes the conditions of the smart contract when they are met. Unlike traditional smart contract addresses, the Extended Proxied Address contains additional logic in the form of scripts that can be executed to carry out specific tasks.

For example, the Extended Proxied Address can be used to distribute tokens to all NFT holders in a smart contract. When a certain condition is met, such as the end of a crowdfunding campaign, the Extended Proxied Address can receive the tokens and execute a script that distributes them to all NFT holders according to a predetermined algorithm.

One of the key benefits of the Extended Proxied Address is that it allows for more precise and efficient use of resources. Instead of executing the same script multiple times for each user or address, the script can be executed once by the Extended Proxied Address and the results can be distributed accordingly. This reduces the amount of computational power and transaction fees required to execute complex smart contracts.