MERKLE NETWORK WHITEPAPER

Web 3.0 Protocol For
Interoperable Oracles

Table of Contents

01

Introduction

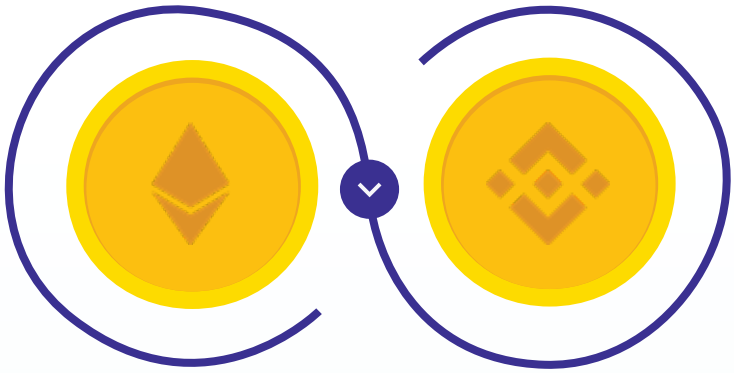
Blockchains are gaining popularity as a technology that can improve the transparency and security of the value chain. Distributed ledgers offer a plethora of use cases to reduce the inefficiencies in the current systems; however, there are still roadblocks in the path to mass adoption of the use of blockchain technology in scalable systems.

The growth of the distributed ledger space has led to the emergence of multiple blockchains which do not communicate with each other and are operating in isolation. These blockchains are gaining popularity because of features they offer to the applications like network effects, speed, transaction cost, security, consensus algorithms etc. However, these blockchains are operating in silos and are running their ecosystems in isolation from the ecosystems operating on other blockchains. Even worse, the current solutions which are only limited to providing cross-chain bridges are highly centralised and susceptible to counterparty & security risks.

There is a pressing need for interoperability between the current blockchains in use. The current growth of the blockchain ecosystem is not being limited by the capabilities of blockchains but by a lack of reliable solutions to connect them. A protocol to allow blockchains to interact with each other will enable decentralised applications to tap into the capabilities of multiple blockchains. Moreover, opening communication across blockchains will usher a new wave of technological advancements in the interoperable defi applications where money markets can operate across chains.

Merkle Network solves the interoperability problem between multiple smart chains using a secure oracle network for inter-chain communication. Merkle Network facilitates the transfer of information between blockchains allowing applications to both tap into the information from other blockchains and update the information on the other blockchains. This 2-way interchain communication opens up the applications to build innumerable use cases and capabilities in decentralised applications.

02



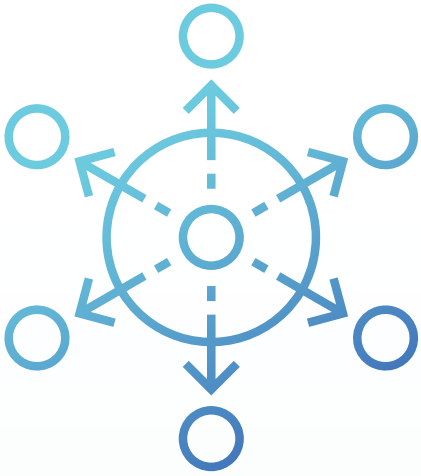
Understanding Interoperability

Interoperability is the ability of an application to exchange information between different ecosystems. Interoperability is not just a desired characteristic but a much-needed feature to enable the blockchain ecosystems to operate to their full potential. It is imperative for commercial applications to have an option to work with a flexible technology stack for a mass scale adoption.

For example, Alice wants to swap her Token A on Ethereum blockchain to Bob's Token B on Binance smart chain. Since these 2 tokens are on different blockchains, both Alice and Bob will need to deposit their tokens on a centralized exchange to swap token A with token B. The reliance on a centralized exchange makes them both susceptible to counterparty risk. Such dependence on a centralised party can be avoided with a decentralised exchange that can operate on both chains using interoperability. Since these 2 blockchains operate in isolation from each other, the interoperability between chains can only happen when they can share data and communicate.

03

Merkle Network Approach



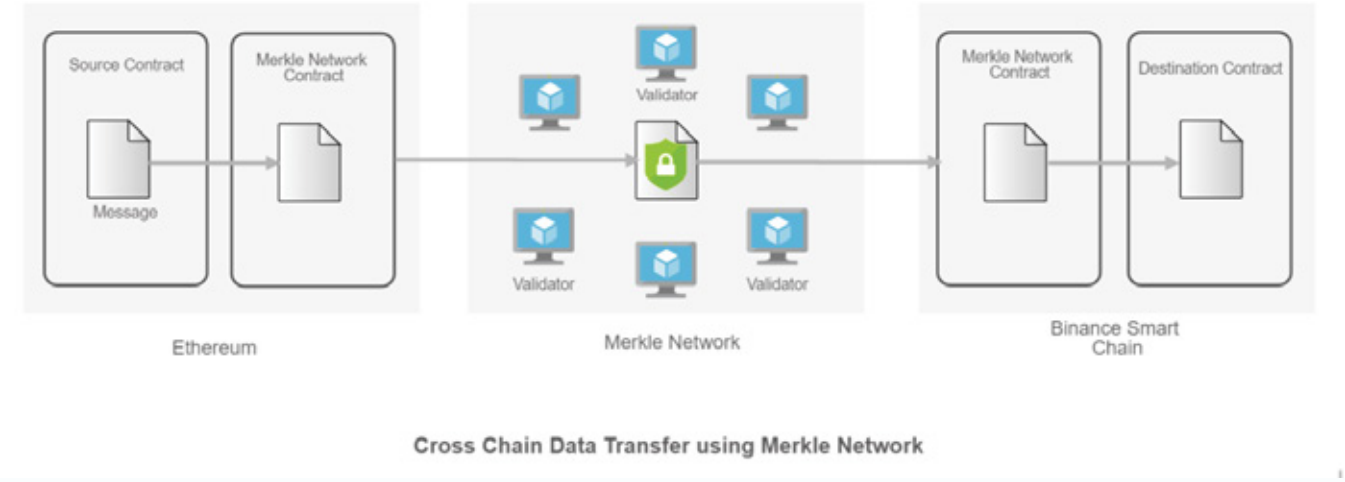
Merkle Network's main functionality is to connect multiple blockchains and bridge the gap between the decentralised ecosystem flourishing in these blockchains. Merkle network leverages the use of interoperable oracles to transfer data between blockchains. Just as oracles have successfully connected blockchains with the outside data, Merkle network's interoperable oracles will connect the blockchains by allowing the flow of information between the chains.

Merkle network is built to be secure and trustworthy through a range of incentives and penalties for the node operators. Merkle Network is being built to support multiple blockchains including but not limited to Ethereum, Binance Smart chain MATIC, Tron etc. Merkle Network includes two approaches to achieve interoperability to cover a wide spectrum of use cases to be built using this feature. As per the Merkle Network approach the data transmission request can originate from either source blockchain or the destination blockchain.

3.1 Cross Chain Data Transfer Using Merkle Network

When data transmission requests originate from the source blockchain, to send a data packet from the source chain to the destination chain the message passes through Merkle Network which is secured with a network of validator nodes. The below diagram illustrates the high-level details of the transfer of information between Ethereum and Binance smart chain. Both source and destination blockchains have Merkle Network's Interoperability contract. The message is sent to Merkle Network Contract which acts as the information source for the oracle. The message from the Merkle Network contract on Ethereum is sent to the Merkle Network where it is processed for the destination blockchain. The validator network validates the message

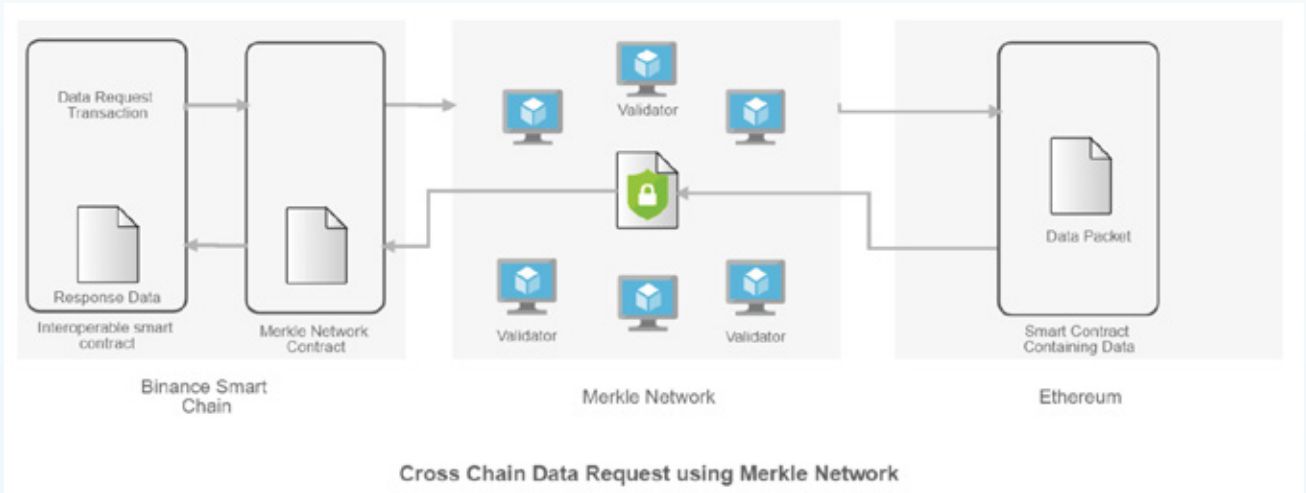
transaction before sending it to the Merkle Network contract on the Binance Smart chain. The information updated on the destination contract acts as the information oracle for the destination contract.



Cross Chain Data Transfer using Merkle Network

3.2 Cross Chain Data Request Using Merkle Network

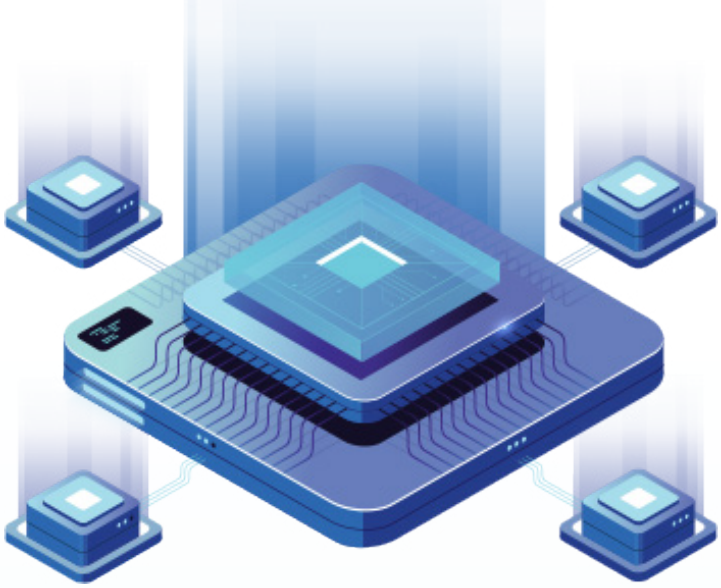
In a cross-chain data request, the data request is generated by a contract on the destination contract which also consumes that data for interoperable applications. To request a data packet from another blockchain, a data request transaction is sent from the contract on the destination chain (Binance Smart Chain in the below diagram) to the Merkle Network via Merkle Network contract on the destination chain. Merkle Network nodes process this request and source the information requested from the source blockchain (Ethereum in the below diagram). This data is then converted into data



Cross Chain Data Request using Merkle Network

04

Architecture



Merkle Network consists of a network of nodes as the base layer of the protocol which are connected to multiple blockchains. These nodes can independently harvest the data from the blockchains and process them into destination blockchain readable format. The messages from the node operators are aggregated via Merkle Network's consensus mechanism before sending them to the destination blockchain.

Merkle Network is designed as a two-way communication protocol that allows both requesting data from other blockchains and pushing data to other blockchains. This approach provides Merkle Network with the complete flexibility to operate as a messaging protocol connecting multiple blockchains. Moreover, this architecture allows Merkle Network to support a wide spectrum of interoperable use cases to be built using the protocol.

Merkle Network is designed to be blockchain agnostic with support for multiple blockchains.

4.1 Merkle Network Transport Layer

The base layer of Merkle Network is the decentralized oracle network that consists of Merkle Nodes, a consensus protocol for aggregating messages and relayers to send transactions on the blockchain.

4.2 Merkle Network Protocol Layer

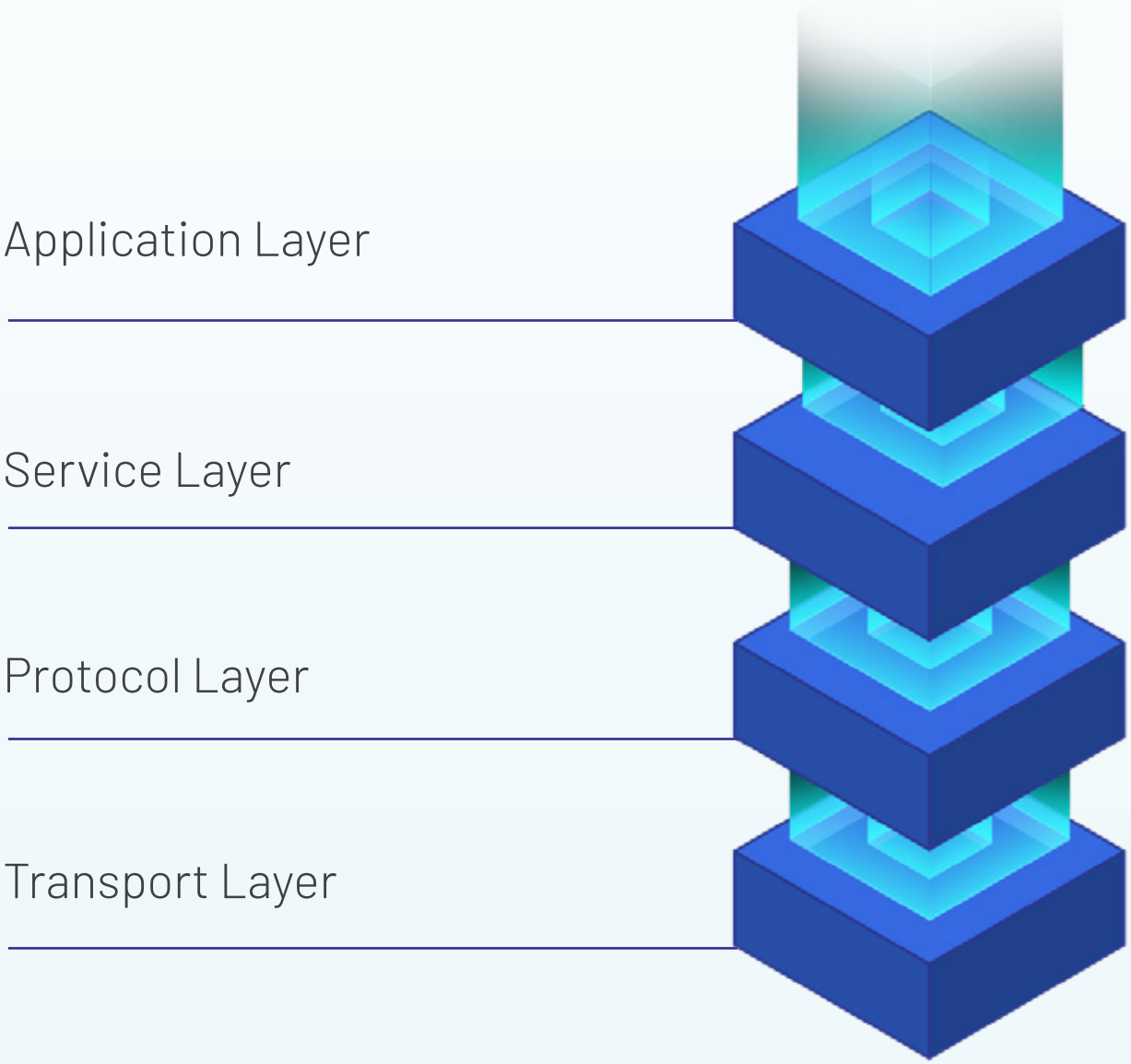
Merkle Network Protocol layer consists of Merkle smart contracts, staking contracts and data transfer and request standards for sending and receiving messages. All the services built on Merkle Network interact with this layer and smart contracts can directly request or send data using the protocol layer.

4.3 Merkle Network Service Layer

Merkle Network's Service Layer consists of the interoperable services built using Merkle Network. These services include but are not limited to decentralised token bridges, decentralised NFT bridges, interoperable wallets, interoperable exchanges and other services that can facilitate the applications to run smoothly across multiple blockchains.

4.4 Interoperable Application Layer

The application layer consists of all the applications that may use Merkle Network directly or using one of the services built on Merkle Network protocol. These applications can be built effortlessly without getting into the intrinsic details of the complexities involved with cross-chain communication.



05

Security

Security is at the core of Merkle Network's Decentralised Interoperable Oracle Network and the services built on the Merkle Network Protocol layer will be able to choose from a range of consensus mechanisms to fit their use case and security needs.

5.1 PoS Validation

Under the Proof of Stake validation, the contract owner will be able to select the validators from the validator pool and choose the consensus threshold. The contract owner will also have the authority to update the validators including adding & removing validators and consensus threshold as per the changing requirements.

The validators will be required to stake tokens to the staking pool to join Merkle Network's consensus. The validation reward for the validators will depend on the number of staked tokens and the token amount will also be factored in to determine the weight of the votes. Once the consensus is reached the relayer will aggregate the signed messages to be sent to the oracle feed.

5.2 Custom Validation

Merkle Network is designed to be an open protocol that is flexible to meet the needs of the projects. Merkle Network operates as legos for development for adding interoperability using oracles. Under the custom/self-validation, the contract owner may run their own validators and choose the consensus rules

to meet their requirements. This discretionary approach would require utmost security from the contract operator but this also opens up opportunities for new innovations to be built using Merkle Network as the messaging layer to meet the ever-changing needs of the industry. Custom Validation opens up the network for a plethora of innovations in the consensus mechanisms.

5.3 Hybrid Validation

Under Hybrid Validation, the contract owner can use a combination of Merkle Network's PoS validation and custom validation to manage consensus. A consensus is reached when PoS validators AND custom validator(s) are in agreement. This adds an extra layer of security and confidence for the contract owner to operate decentralised interoperable features to the applications.

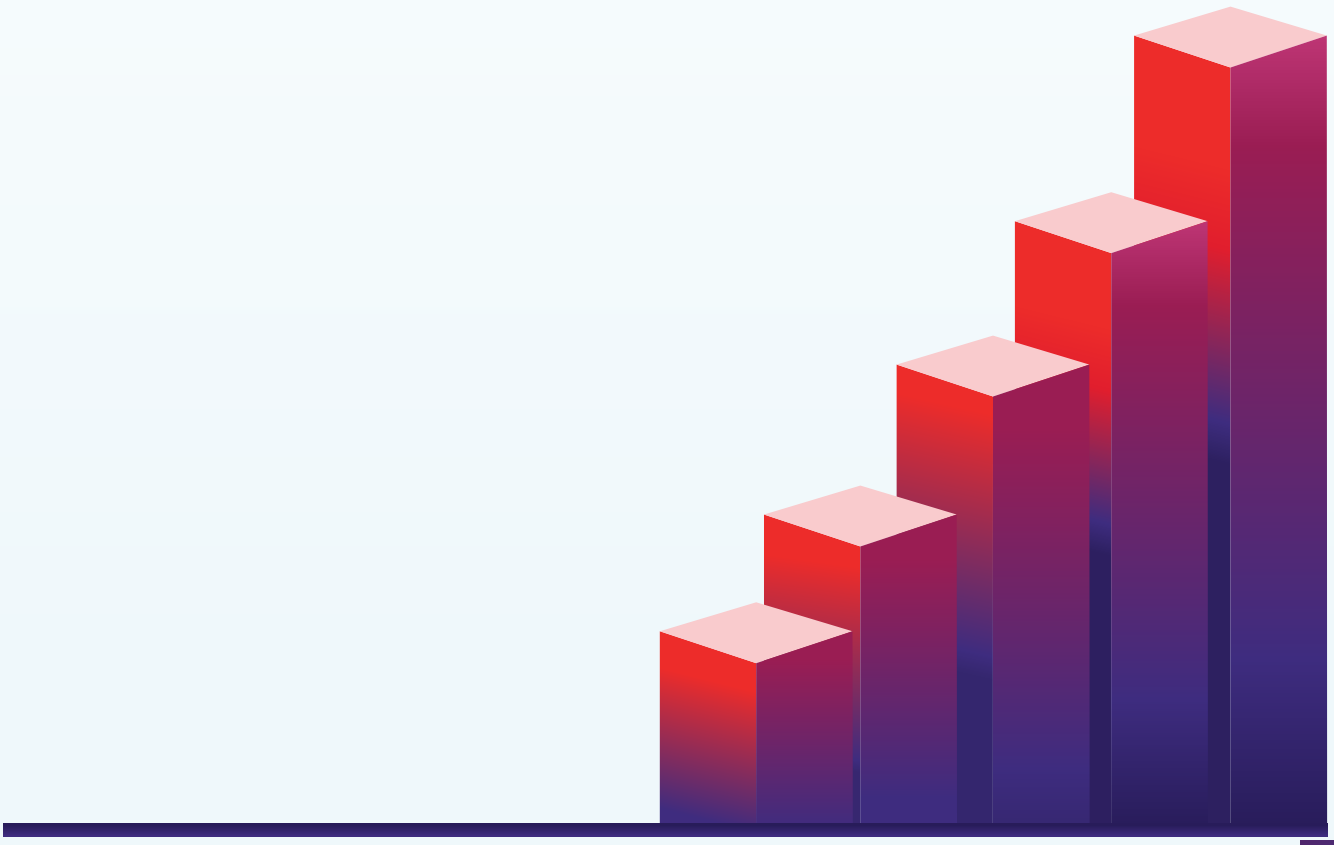
Hybrid Validation truly demonstrates the flexibility of Merkle Network to act as a framework for adding interoperability and adapt to the changing requirements.

06

Scaling

Merkle Network is designed to be scalable to meet current and future demand for interoperability services. Merkle Network is built to scale both horizontally and vertically to minimise latency and achieve the desired throughput to keep up with the growth of high throughput blockchains.

The current blockchains in use are rampant with slow speeds and high transaction costs which is leading to the emergence of various high throughput blockchains that can take the computing and storage load of the existing blockchains. Merkle Network can be viewed as a decentralised layer-2 network that can be used by multiple blockchains to communicate with each other. Merkle Network is scalable to meet the throughput demands for both source and destination blockchains, only limited by the transaction limitations of source and destination blockchains.



07

Market Opportunity

The market opportunity for interoperability is immense as almost every decentralized application would use interoperability to add scalability and resilience to the application. One of the prominent projects in this space is Polkadot which has already joined the ranks of the top projects in the blockchain space before the launch. Chain link has already demonstrated the utility of oracles in bringing the outside data to blockchain applications and nearly all major DeFi projects now use oracles.

Merkle Network is diving into a blue ocean of markets with immense opportunities and possibilities to help applications leverage interoperability to build on a scalable infrastructure. Although the integration possibilities are endless, there are some of the major use cases that are in dire need of interoperability. Tokens will be able to move freely across blockchains without the need for a centralised custodian or gateways. Decentralised exchanges can operate on multiple blockchains using interoperability and enable the flow of liquidity between the chains. Decentralised applications will be able to support multiple blockchains without getting stuck on a single chain. Enterprise-grade applications will be able to move on blockchains with added flexibility to the right technology stack to build the applications.

08

Use Cases

Merkle Network opens up floodgates for a vast spectrum of existing applications and new & innovative applications to be built using interoperability. Some of the use cases and applications that Merkle Network will revolutionise include

- Cross-Chain Decentralized Applications
- Decentralised Token Bridges
- Interoperable DeFi Markets
- Multichain Interoperable Exchanges
- Lending & Borrowing Platforms
- Yield Optimisation and Distribution
- Multichain Token Standards
- Solving Fragmentation of Assets Across Chains
- Flexible Smart Contracts
- Computing & Storage Arbitrage

09

$MERKLE Token Utility

Merkle Network uses MERKLE token to reward Merkle Node operators for transferring the data from the source blockchain to the destination blockchain while maintaining the integrity & readability of the data and uptime guarantee of the node operators. Users and smart contracts looking to use the Merkle network to transfer data between the chains pay the Node operators in Merkle tokens.

Furthermore, MERKLE tokens will also strengthen the node network through staking tokens to operate nodes. The staking will bring the vested interest in the network for node operators and act as a deterrent for bad actors to enter the ecosystem. There will be a need for a consensus of node operators to maintain the network and the addition of nodes will need additional token lockups as the network grows.

9.1 Transaction/Gas Fees

MERKLE token is used to pay transaction fees to the Merkle Network node operators for the retrieval of data from the source blockchain, converting it into destination blockchain readable format, off-chain computing, uptime guarantees and paying the gas fees on the destination blockchain.

9.2 Staking

MERKLE tokens will be used to secure consensus nodes on the network's PoS consensus. The validators will be required to stake tokens to the staking pool to join Merkle Network's consensus. MERKLE tokens will also act as a reward to maintain the uptime and integrity of the system.

9.3 Rewards

MERKLE tokens will be rewarded to the validator nodes, relayers and staking holders. The validation reward for the validators will be directly proportional to the number of staked tokens. Users can also stake & delegate their tokens to the nodes to earn rewards.

9.4 Token Burns

Token burns will be an integral part of the Merkle Network where a proportion of the fees will be burned making the supply deflationary with the growth and adoption of the protocol.

10

Tokenomics

Total supply

60,000,000

Seed & Private round

12,000,000

Token Swaps & IDO

16,000,000

Liquidity Provisioning

2,000,000

Marketing

6,000,000

Reserve

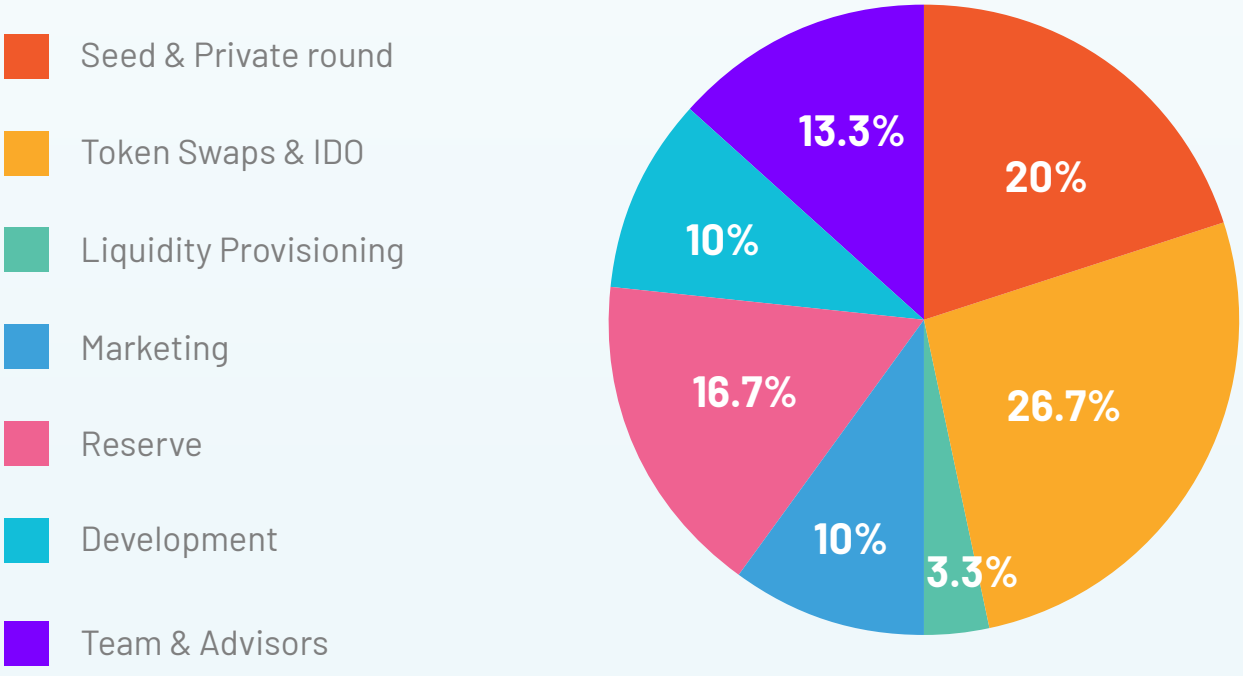
10,000,000

Development

6,000,000

Team & Advisors

8,000,000



Vesting Schedule

Seed & Private round
0% at TGE, Then 1% released each day

Token Swaps & IDO
20% at TGE, Then 1% released each day

Team, Advisors & Reserve
0% at TGE, 2 years vesting

Marketing & Development
0% at TGE, 1 year vesting

Seed & Private Round

The allocation pool for Seed and Private Round is reserve for funds and strategic investors who will assist with the growth and adoption of Merkle Network's interoperability protocol.

Public and private round

This allocation pool will provide MERKLE tokens to all circulating ETHV tokens holders with 1:1 token swaps. The remaining tokens will be sold on IDO platforms.

Marketing & Partnerships

This allocation pool will be used for ongoing marketing and growth-oriented/ strategic partnerships to bring awareness and adoption for Merkle Network across geographies and blockchains.

Team & Advisors

The allocation for team and advisors is vested for 2 years. This allocation fund will enable Merkle Network to onboard and retain innovators on Merkle Network.

Liquidity Provisioning

The liquidity will be added to multiple liquidity pools across chains to provide accessibility of MERKLE tokens across these chains.

Reserve

Reserve tokens are allocated for meeting token requirements outside the scope of the above allocations to fuel the growth of the Merkle ecosystem. This token pool will be used for any future liquidity provisioning, liquidity mining/ rewards program and bootstrapping growth initiatives for the protocol.

Development

This is a long term token reserve kept aside to meet any future development needs of the protocol.

11

Roadmap

Q4 2020

Idea Conceptualisation

Q1 2021

Development commences

Q3 2021

POC successfully tested

Q4 2021

Whitepaper Release

Q4 2021

Token Launch

Q4 2021

Testnet launch

Q4 2021

Mainnet launch on multiple chains

Q1 2022

Development commences on services architectures

Q1 2022

Additional blockchains support

Q1 2022

Cross-chain token transfer protocol launch

Q1 2022

Cross-chain NFT transfer protocol launch

Q2 2022

New consensus algorithms

Q2 2022

Defi integration SDK launch

Q3 2022

Interoperable token standard launch

Q3 2022

Updated roadmap launch for future development

Join us on Telegram

Follow us on Twitter & Medium

www.merkle.network