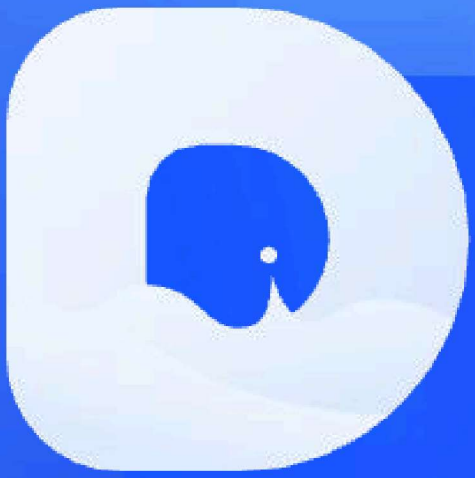


DO Network

DO Whitepaper(v2024.12)

DO Whitepaper(v2024.12)

DO Network

1.Introduction

Since the birth of Bitcoin, public blockchains, as the underlying infrastructure that supports the decentralized nature of blockchain and its development, have been undergoing continuous iteration and evolution. Over the past decade, various public blockchains have emerged like mushrooms after a rainstorm. Some have developed through market cycles, both bull and bear, while others have gradually faded from view. Meanwhile, the market has conducted its own validation through the rise and fall of these public blockchains.

Throughout this process, the ups and downs of the market have prompted blockchain developers and builders to ask themselves: What kind of public blockchain do we need? What kind of public blockchain will be recognized by the market and users, and truly embody the essence of "blockchain"?

Different people will give different answers to this question. And DO Network is one of those answers—deeply considered, carefully designed, and practically advancing.

What is DO Network?

What is DO? Ultimately, DO stands for Decentralized Organization.

DO Network is a highly decentralized, ultra-high-performance public blockchain. Through its unique Wave Consensus, DO Network delivers excellent TPS and gas experiences, while adhering to the principles of decentralization, offering an extremely low-barrier, convenient participation experience for both node construction and network involvement.

DO believes that the spirit of blockchain is about sharing and broad participation. Public blockchains need to make breakthroughs in performance and scalability while ensuring a high degree of decentralization. Improving blockchain performance and scalability aims to provide users with a better and more accessible network experience, thereby attracting more users to participate in the network, further enhancing the network's decentralization.

Therefore, "decentralization" remains the core characteristic of blockchain networks. Public blockchains should, within the constraints of current technological conditions, achieve a dynamic balance under the "impossible triangle" limitation, based on decentralization.

DO also stands for Distributed Ownership, Dynamic Open, Data Optimization, and Digital Operation.

Target and features of DO

DO is dedicated to building a blockchain network where everyone can participate, easily participate, and is willing to participate. DO believes that decentralization in technology is only one part of the equation, and reducing the barriers to user participation is also a crucial aspect of decentralization. Based on this, DO has incorporated several key features in its network design to ensure that all users can participate conveniently:

- Ultra-high performance
  Block time is less than 0.1 seconds, with TPS exceeding 1000.
- Ultra-low gas fees
  $1 can complete over 10,000 transactions.
- Extremely low participation threshold
  2000 DO is enough to run a node, and 200 DO is enough to stake and earn rewards.
- Innovative technology
  Unique Wave Consensus, which is EVM-compatible.

Target and features of DO

Decentralization is the foundational characteristic of blockchain networks, and decentralization is a multi-layered concept that can be explained from different perspectives. Regarding decentralization, Ethereum founder Vitalik Buterin once provided a classic explanation. He argued that decentralization should be defined from three angles: architecture, governance, and logic.

- Architectural decentralization refers to how many node failures the system can tolerate while still continuing to function.
- Governance decentralization refers to how many individuals or organizations are needed to ultimately control the system.
- Logical decentralization refers to whether the system’ s interfaces and data present themselves as a single, unified whole.

Building upon Vitalik's discussion and various other perspectives on decentralization, DO has constructed its own decentralized system through the following directions:

Layer One of Decentralization: Device Decentralization

Device decentralization means more than just having blockchain network devices geographically distributed across different locations worldwide. It also implies that anyone can own and operate the devices required to run the blockchain network.

If the requirements for running the network demand highly specialized or expensive equipment, many individuals would not meet the criteria, leaving only a few capable of running the network. This would not represent true decentralization.

Device decentralization should enable everyone to easily acquire and operate their own device to run the blockchain network at an affordable cost, ensuring inclusivity and accessibility for all.

Layer Two of Decentralization: Token Decentralization

Tokens are the carriers of value in a blockchain network and a core component of its ecosystem. Token decentralization refers to the widespread distribution of token ownership, ensuring that no single entity or individual can independently exert significant influence over the tokens.

While Bitcoin's technology is relatively easy to replicate today, its decentralized token distribution remains unparalleled and a critical aspect of its decentralization.

When discussing token decentralization, it’ s important to evaluate actual controllers rather than just addresses. If tokens are distributed across multiple addresses but are effectively controlled by the same person or organization, this does not qualify as sufficient decentralization.

Layer Three of Decentralization: Information Decentralization

How can we determine whether a blockchain is truly decentralized? Developers can verify this by reviewing the code, but ordinary users often lack the ability to read or understand it. As a result, they must rely on developers to convey this information. However, if the developers are directly tied to the blockchain itself, their claims may not be fully trustworthy.

To achieve decentralization at the information level, information must be open, clear, and effectively communicated. This includes providing ordinary users with straightforward ways to access and verify information, allowing independent developers with different perspectives to question and validate the system, and even enabling users to participate in technical activities without coding skills (e.g., no-code token issuance).

Layer Four of Decentralization: Structural Decentralization

This layer means that regardless of large-scale failures in hardware, nodes, users, or network spaces, the blockchain network should remain operational.

For example, if a global internet outage occurs and half the planet loses connectivity, the blockchain network must still be able to function. If the nodes of a blockchain are all concentrated in geographically localized regions, such an event could lead to a total shutdown.

While the likelihood of such extreme scenarios is very low, structural decentralization becomes highly significant for blockchains that are widely used by people across the globe. Though this aspect may not be apparent during normal operations, it could prove critical during extraordinary circumstances.

Target and features of DO

DO is an established public blockchain. Since its inception in 2018, it has undergone long-term technical development and testnet operations. DO's mainnet went live in Q2 2021, followed by several mainnet and hard fork upgrades. Over the years, DO has accumulated more than 100,000 users and reached a peak FDV of $2 billion. After experiencing market cycles, DO has continued to adhere to its decentralization principles, maintain stable progress, and align with the development trends of the blockchain world, achieving new growth and accomplishments.

2.Technique

Brief Introduction

DO Network aims to build a high-performance, resilient public blockchain infrastructure that supports distributed applications across various use cases. Anyone or any organization can innovate, build, and contribute to creating a decentralized and secure blockchain ecosystem on it.

To meet these needs, DO focuses on the following core concepts:

- Speed: DO is written in C/C++, which offers high efficiency and portability. Transactions on DO are processed extremely quickly, with full network consensus achieved on-chain in as little as 1 second.
- Security: DO incorporates a range of technologies at the consensus layer, including Verifiable Random Functions (VRF), Byzantine Fault Tolerance (BFT) algorithms, Ed25519 elliptic curve signatures, and a self-developed consensus protocol. These technologies ensure both speed and security, maintaining equal rights and status for each node. Even if a single or a small number of nodes experience issues, it will not significantly affect transaction processing or the network's overall operation.
- Scalability: DO uses a Directed Acyclic Graph (DAG) blockchain structure to offer higher bandwidth processing capability and allows transactions to carry custom data.
- High Customization: Business chains can operate independently based on different transaction types or business entities. DO's application scope is also virtually limitless.
- Immutability: As a highly decentralized distributed ledger, DO makes it nearly impossible to tamper with transaction data.
- Public and Transparent Transactions: While all nodes on the public chain join the network anonymously, any node can view the account balances and transaction activities of other nodes. Validation nodes are distributed globally, and everyone collectively participates in maintaining the blockchain and recording all transaction data.
- Smart Contract Support: DO currently supports the Ethereum Virtual Machine (EVM), allowing most Ethereum-based smart contracts to run on DO with little or no modification.

These features collectively ensure that DO Network can provide a secure, efficient, and scalable platform for a wide range of decentralized applications.

Wave Consensus

Given that current mainstream consensus mechanisms cannot effectively balance efficiency and decentralization, DO utilizes its self-developed Wave Consensus at the consensus layer. Compared to traditional Proof of Work (PoW), it is more efficient and eliminates the need for computational power competition. Each node in the network has a unique node ID, and nodes are selected for validation in the mainnet through discrete random numbers.

The Wave Consensus used by DO performs data validation through multi-linear broadcasting by randomly selecting validation nodes from the verification pool using a discrete random number algorithm. The final legitimacy of the block is determined through a signature verification process that ensures the block’ s validity.

The wave protocol of Do network is a special consensus algorithm, which is driven by local consensus to reach an agreement across the network, just like the wave driving gradually covers the entire sea area, so we call it the wave consensus protocol.

We hope that the consensus process is safe, simple and efficient, which is designed to improve the overall performance of the network.

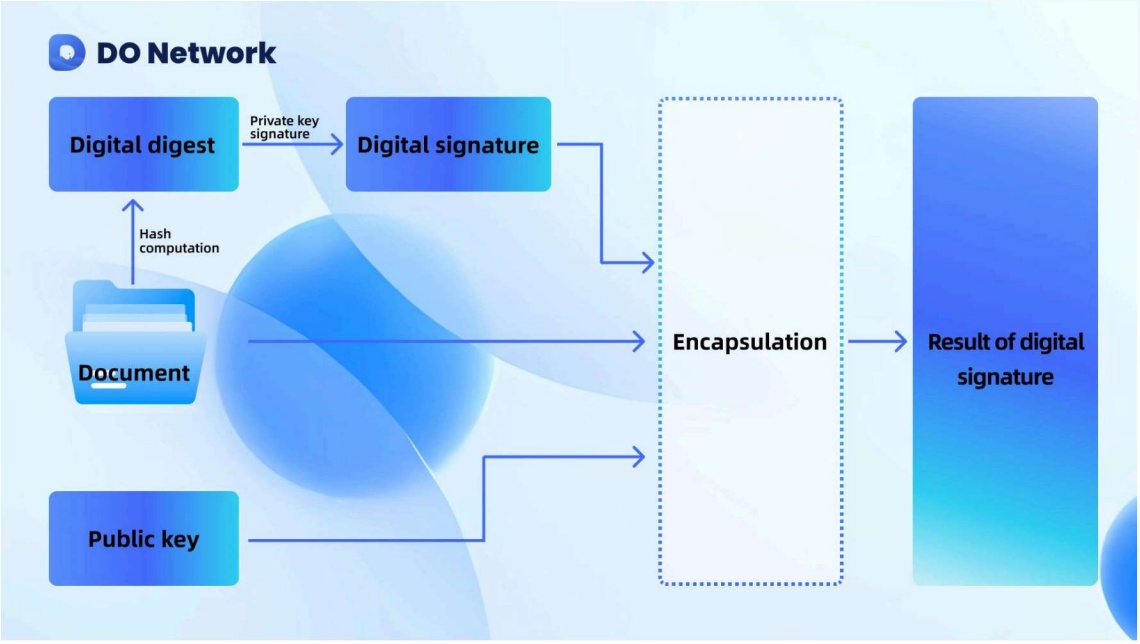
The generated random number and the time axis combine to form a smooth and unpredictable trajectory by adopting the dual VRF random algorithm. Do Network will elect a candidate from the legal verification nodes of the whole network. The consensus of 2/3 nodes of the whole network can be completed only after the candidate and verifiers of different groups reach an agreement on the transaction.

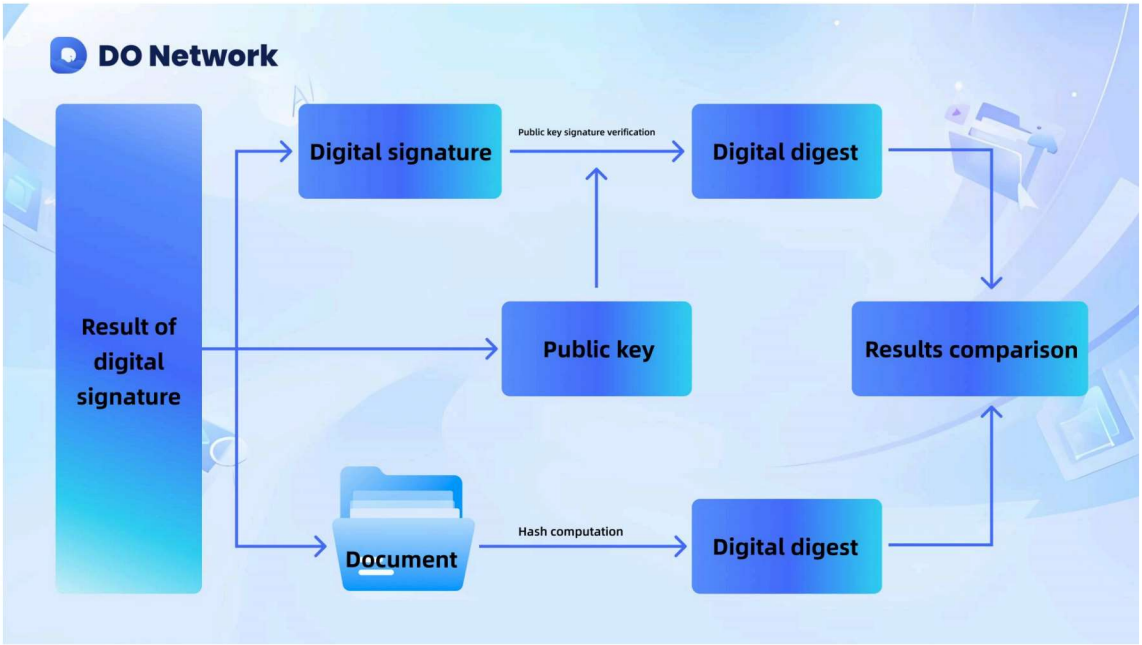
Consensus Process

In the DO Network, there are four types of node roles. However, node roles are not permanent identities; they refer to the specific role a node plays during a particular transaction process. These roles are as follows:

1. Initiator Node: The node that initiates the transaction. It organizes the transaction and sends it to the packaging node.
2. Packaging Node (Delegate Node): Responsible for forwarding the transaction and packaging it into a block. Once the transaction is packaged into a block, the packaging node sends the block to the validation nodes. After the block passes validation, it is broadcasted to the entire network.
3. Validation Node (Candidate Delegate Node): The node responsible for validating the block sent by the packaging node. If the block is validated successfully, the validation node notifies the packaging node.
4. Other Nodes: These are nodes that do not participate in the transaction process but are responsible for storing the blocks broadcasted to the network in their databases.

In DO, every node has the potential to assume one of the above roles during a transaction. A single node can play all four roles simultaneously in different transactions, depending on the situation. This flexibility ensures a dynamic and efficient consensus process within the network.



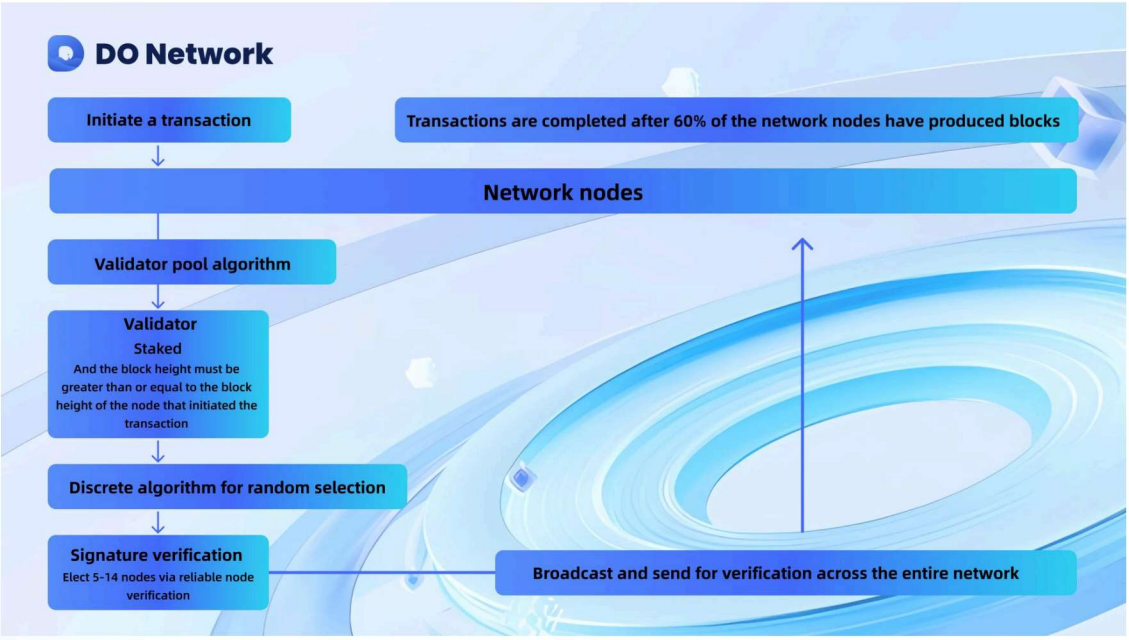


The transaction process is as following:

The transaction process in DO Network involves the selection of several nodes across the entire network. All node selections follow the principles of fairness and randomness, utilizing Verifiable Random Functions (VRF) for selection and validation. The process is as follows:

1. Initiating Node (A): The initiating node (A) selects a packaging node using VRF based on the block information, then sends the transaction to the packaging node (B).
2. Packaging Node (B): The packaging node (B) verifies using VRF that it was selected by the initiating node (A). Afterward, it selects several nodes from the network to forward the transaction to them.
3. Transaction Validation: The nodes that receive the transaction verify the transaction and the VRF. If validation is successful, they notify the packaging node (B).
4. Consensus Confirmation: Once the packaging node (B) receives notifications from a sufficient number of nodes to reach consensus, it places the transaction into a cache. At regular intervals, the packaging node (B) will package all the transactions in the cache into a block.
5. Selecting Validation Nodes: The packaging node (B) uses VRF to select several nodes as validation nodes and sends the block to them.
6. Block Validation: The validation nodes verify both the block and the VRF. If successful, they notify the packaging node (B).
7. Final Consensus: Once the packaging node (B) receives notifications from enough validation nodes to reach consensus, it broadcasts the block to the entire network.
8. Broadcast Validation: Other nodes, upon receiving the broadcast, perform VRF validation to ensure that the packaging node (B) (the broadcast initiator) is indeed the node selected by the initiating node (A).

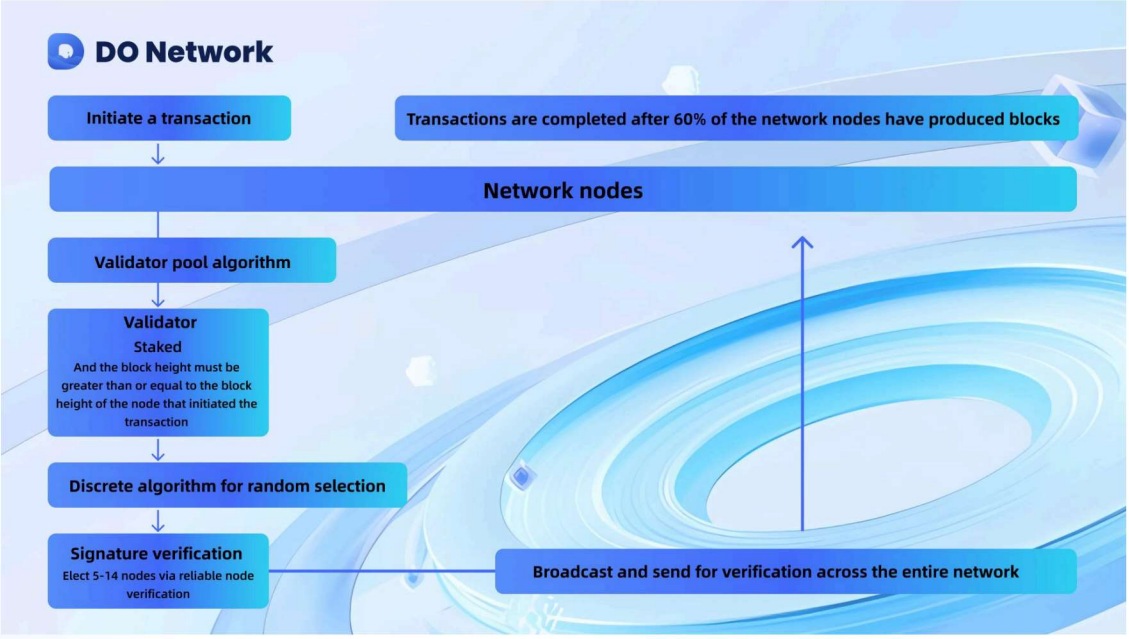
This process ensures both fairness and security, with multiple layers of validation and consensus, leading to an efficient and decentralized transaction



In traditional blockchains, the slow block generation speed and block size limitations lead to slow on-chain speeds. However, on DO, a single block can contain an unlimited number of transactions.

1. Initiating Node (A): The initiating node (A) selects a packaging node using VRF based on the block information, then sends the transaction to the packaging node (B).
2. Packaging Node (B): The packaging node (B) verifies using VRF that it was selected by the initiating node (A). Afterward, it selects several nodes from the network to forward the transaction to them.
3. Transaction Validation: The nodes that receive the transaction verify the transaction and the VRF. If validation is successful, they notify the packaging node (B).
4. Consensus Confirmation: Once the packaging node (B) receives notifications from a sufficient number of nodes to reach consensus, it places the transaction into a cache. At regular intervals, the packaging node (B) will package all the transactions in the cache into a block.
5. Selecting Validation Nodes: The packaging node (B) uses VRF to select several nodes as validation nodes and sends the block to them.
6. Block Validation: The validation nodes verify both the block and the VRF. If successful, they notify the packaging node (B).
7. Final Consensus: Once the packaging node (B) receives notifications from enough validation nodes to reach consensus, it broadcasts the block to the entire network.
8. Broadcast Validation: Other nodes, upon receiving the broadcast, perform VRF validation to ensure that the packaging node (B) (the broadcast initiator) is indeed the node selected by the initiating node (A).

This process ensures both fairness and security, with multiple layers of validation and consensus, leading to an efficient and decentralized transaction process within the DO Network.



In traditional blockchains, the slow block generation speed and block size limitations lead to slow on-chain speeds. However, on DO, a single block can contain an unlimited number of transactions.

With data security and decentralization guaranteed, the on-chain speed on DO can reach as fast as 0.1 seconds. The network acceptance threshold is set to 75%, which is the optimal speed and success rate ratio verified and practiced. If the broadcast fails to meet the network’ s acceptance threshold, nodes that have already added blocks will validate and roll back the failed transaction blocks during the synchronization process.

Cryptographic Algorithms and Security

To protect the security of on-chain assets, DO employs widely-used and extensively tested security algorithms. These mainly include ED25519 elliptic curve signature algorithm and Verifiable Random Function (VRF). At the same time, DO also uses digital signatures to verify information.

- **ED25519 Curve**

ED25519 is an EdDSA signature scheme based on SHA-512 and Curve25519. Its name is derived from the combination of the first part of EdDSA and the latter part of Curve25519. EdDSA (Edwards-curve Digital Signature Algorithm) is a type of signature algorithm based on twisted Edwards curves, and Curve25519 is a specific twisted Edwards curve.

As mentioned in the earlier VRF process, ED25519 is involved in both the creation and verification of VRF. During the VRF creation process, the transaction or block hash is encrypted using ED25519 along with the SHA-256 hash of the private key. During the verification process, the signature result is validated using ED25519.

The security of the ED25519 elliptic curve has been widely recognized from both mathematical and practical perspectives. It also offers extremely fast key generation and verification speeds, improving transaction verification efficiency while ensuring security.

- **VRF Random Verification Algorithm**

In the DO blockchain, randomization is heavily used during the transaction flow to ensure fairness. However, ordinary random methods cannot prevent malicious behavior resulting from source code modifications. Therefore, DO introduces the Verifiable Random Function (VRF) to validate the randomness results.

A Verifiable Random Function (VRF) is a cryptographic scheme that maps inputs to a verifiable pseudo-random output. It ensures that the random output is both unpredictable and verifiable, providing a guarantee of fairness.

The VRF random verification algorithm is essential to DO's entire consensus protocol and is used in scenarios that require random node selection. Whether in transaction flow or block flow, VRF is involved. During VRF creation, the current node's private key and the transaction or block hash are used as input parameters. The hash string itself is hashed using SHA-256, and the resulting encrypted value, along with the private key, is used as the VRF signature (proof). The signature

(proof) is then hashed again using SHA-256, and the resulting output is the final VRF creation output.

When validating the VRF, the process is reversed. The signature result and the current block or transaction hash are input parameters, and the validation result is compared with the SHA-256 hash of the private key. If they match, the VRF validation is considered successful.

- **Digital Signature**

The fundamental properties of a digital signature are non-repudiation, immutability, and message integrity.

A digital signature (also known as public key digital signature or electronic seal) is different from a physical signature on paper. It uses public key cryptography techniques and is a method for authenticating digital information. A digital signature is typically defined by two complementary operations: one for signing and one for verification. A digital signature is a string of numbers that can only be generated by the sender of the message and cannot be forged by others. This string also serves as valid proof of the authenticity of the message sent by the sender.

Digital signatures are an application of asymmetric encryption and hashing technologies. The signing process involves encryption, and the verification process is a decryption process.

DO uses digital signatures because of their non-repudiation property—since no one can forge the sender’ s private key signature. The sender encrypts the message with their private key, and only the sender’ s public key can decrypt it. Digital signatures also ensure message integrity. When a digital signature is applied, it uses a specific hash function, meaning the hash value generated for different files will always be distinct.

- **Hash function**

A hash function, also known as a hashing function, is not designed for data encryption and decryption. Its main purpose is to verify data integrity.

By using a hash function, a "digital fingerprint" (hash value or message digest) can be created for data. The hash value is typically a short, random string of letters and numbers. The parties communicating agree on a specific hash algorithm before the communication begins, and this algorithm is publicly known. If the message is tampered with during transmission, the message will no longer match the previously obtained digital fingerprint.

Hash functions are widely used for verifying information integrity and are a core technology in digital signatures. Common algorithms include MD (Message Digest Algorithm), SHA (Secure Hash Algorithm), and MAC (Message Authentication Code Algorithm). To ensure both speed and security, DO uses the SHA-256 algorithm as its preferred hashing method.

In summary, in DO's consensus protocol, a discrete random number algorithm is used to randomly select validation nodes from the verification pool. The data validation process involves multi-linear broadcasting and signature verification, which ultimately determines the block’ s legitimacy.

DO's Wave Consensus avoids the issues of power concentration and the "winner-takes-all" problem that arise from free competition for the right to record transactions in traditional POW systems. It achieves a balance between fairness and competitiveness to some extent. In the DO network, as the number of validator nodes increases, the network’ s capacity will scale accordingly. When the number of nodes reaches a certain scale, the low-energy consumption of nodes and the increasing availability of future validator nodes will significantly control transaction costs. The consensus protocol executes computations using CPUs, which significantly reduces costs compared to using GPUs, ASICs, and other hardware.

What’ s more, based on Wave Consensus, DO has built the "Wave Value" system, a quantitative evaluation system that measures the contribution of nodes within the Wave Consensus framework. The higher the Wave Value of a node, the higher its contribution, similar to how higher hash power in the BTC network results in greater rewards.

Network and Communication

Distributed Network and Node Communication

DO employs a fully connected, decentralized, and distributed P2P network structure.

DO connects to the blockchain network through a P2P (peer-to-peer) model. In this blockchain network, all full nodes are equal, acting both as clients and servers.

All nodes in DO are equal and have the following characteristics:

- Archival Nodes: These nodes store the historical state of all blocks. The world state corresponding to any block in history is preserved on these nodes.
- Validation Nodes: These nodes are capable of directly validating the validity of transaction data locally.
- Broadcasting Nodes: These nodes participate fully in the broadcasting of block and transaction information across the entire network.
- Heartbeat: This function checks the connection status in the network.
- Interface: DO provides an open query interface, offering accurate and up-to-date information about the current network state.
- Synchronization Nodes: When a new node joins the network, these nodes detect the new node, establish a connection, and broadcast the updated information to other nodes.

This decentralized and distributed approach ensures that all nodes in DO have the ability to fully participate in the blockchain's operations, contributing to its security, reliability, and scalability.

Through the node list, each validator node is assigned a unique ID to ensure its authenticity in the network. By verifying the node list data, validator nodes that meet the conditions are gathered into the validator pool. A discrete random function is then used for the random selection of block validators, ensuring smoothness and fairness in node selection. This approach helps avoid unfairness that could arise from continuous functions due to network speed and other factors. The core objective of this approach is to ensure the randomness and security of validator selection and block production, and to establish a tolerance range for malicious nodes. Nodes that participate in validating the legitimacy of blocks can earn corresponding rewards.

DO is designed with a fully connected architecture, offering high throughput, reliability, and low latency. To maintain these advantages, DO performs best in environments with 500 to 1000 nodes, ensuring both performance and security. Based on its unique mechanism, the network is designed to handle computational tasks at the single-node level. If a node reaches its performance bottleneck due to excessive pressure and can no longer participate in transactions, it will temporarily be unavailable. Because node participation in the network is highly fluid, the usability of the DO network layer remains stable over the long term.

Network Communication Process

DO employs a stable TCP peer-to-peer (P2P) communication protocol. In this system, when a message is received, it is first stored in a cache, then distributed by a transaction dispatcher, and finally processed by the appropriate functions.

In a typical P2P network, each node stores information about other nodes. When requesting a specific node, the system needs to iterate through all the nodes until it finds the requested one. However, a common issue faced by some blockchain projects is that as the number of network nodes expands, it becomes infeasible to store information about every other node on each individual node. As the number of nodes increases, the layers also grow, and with higher layers come more stored information. This makes data retrieval increasingly difficult and reduces the timeliness of network data.

To address this problem, DO sacrifices some level of node quantity at the application layer to increase the efficiency of node communication. In the service layer, DO can quickly complete communication across the entire network. If the node count exceeds a threshold, transaction speeds may slow down, and DO will remove a portion of the un-staked nodes to resolve this issue.

Process for Handling Node Requests

When node A receives a request message, the information of the sender, node B, is used to update its node list. The specific steps are as follows:

1. Record Information: Node A records the IP address, block height, and other relevant information of node B.
2. Update Existing Node: If node B already exists in node A’ s list, update the information of node B in A’ s list.
3. Add New Node: If node B is not already in node A’ s list, add node B’ s information to A’ s list.
4. Broadcast Node Information: Node A then broadcasts node B’ s information to other nodes.

The node list contains information recorded by node A about its peers, including details such as IP address, name, and identification. This information is used to determine how nodes communicate (either directly or via forwarding) and to serve as a routing mechanism. Each node saves the information of all connected nodes.

This peerlist and communication structure ensures efficient, decentralized, and reliable information sharing across the network.

TCP Registration Steps

1. Registration Request: The registering node sends a registration request to the node to be registered. If the two nodes are not yet connected, a connection attempt will be made first. If the connection fails, the registration process will be retried.
2. Registration Response: The registered node processes the registration request and returns specific node information.
3. Processing Registration: The registering node processes the registration response from the registered node and records the relevant node information.

Heartbeat Mechanism

If a node goes offline and fails to reconnect within a specified time, its heartbeat count becomes zero, and the node is removed.

Heartbeat Process:

1. Ping Request: Each node reduces the heartbeat count of all known nodes by 1 and sends a ping request to them.
2. Pong Response: When the receiving node successfully receives the ping request, it resets the sending node's heartbeat count and sends a pong response back.
3. Heartbeat Reset: When the sending node successfully receives the pong request, it resets the receiving node's heartbeat count and updates the corresponding node's information.

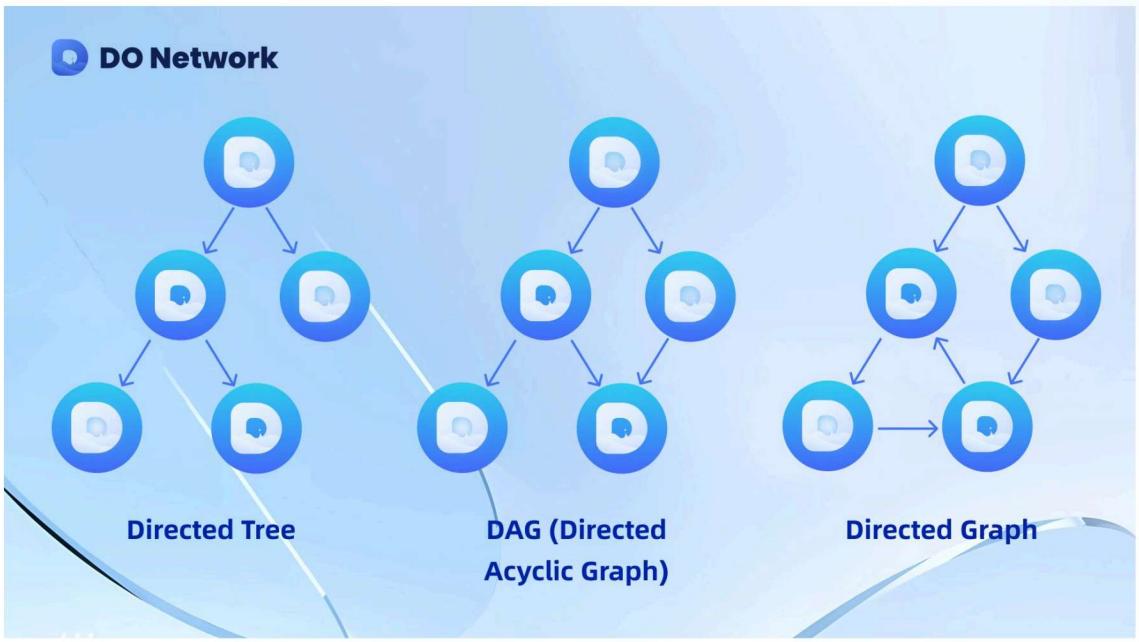
Block Height Change Notification

Process:

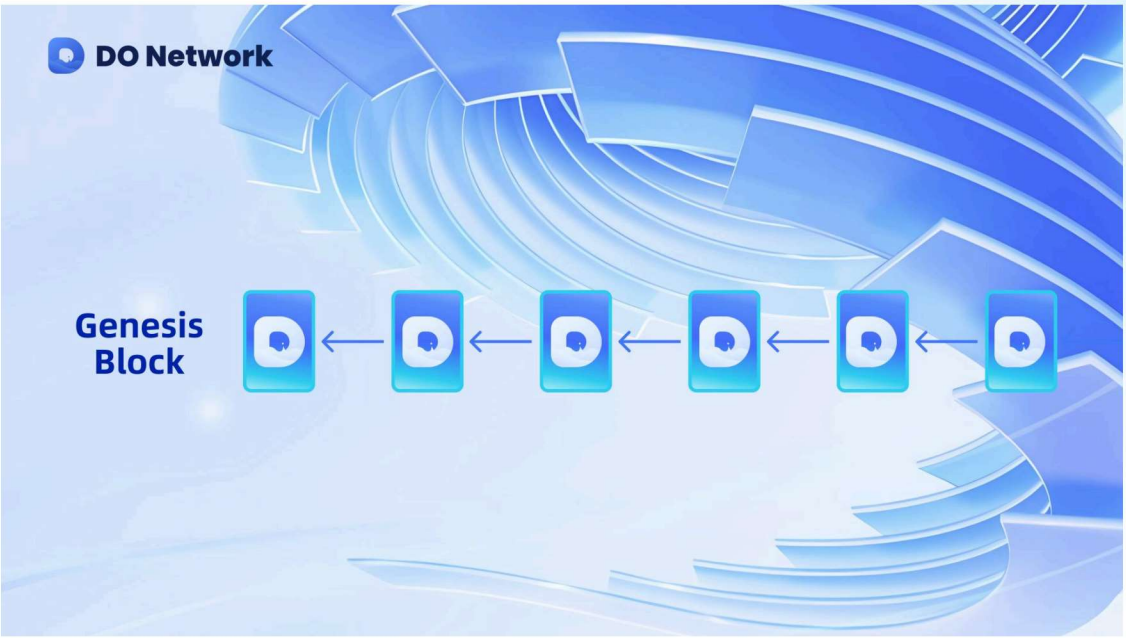
When a node's block height changes, it sends its updated block height to the nodes it is connected to. The receiving node processes the block height change request and updates its own block height accordingly.

This ensures that all nodes in the network stay synchronized and are aware of changes in the blockchain’ s state.

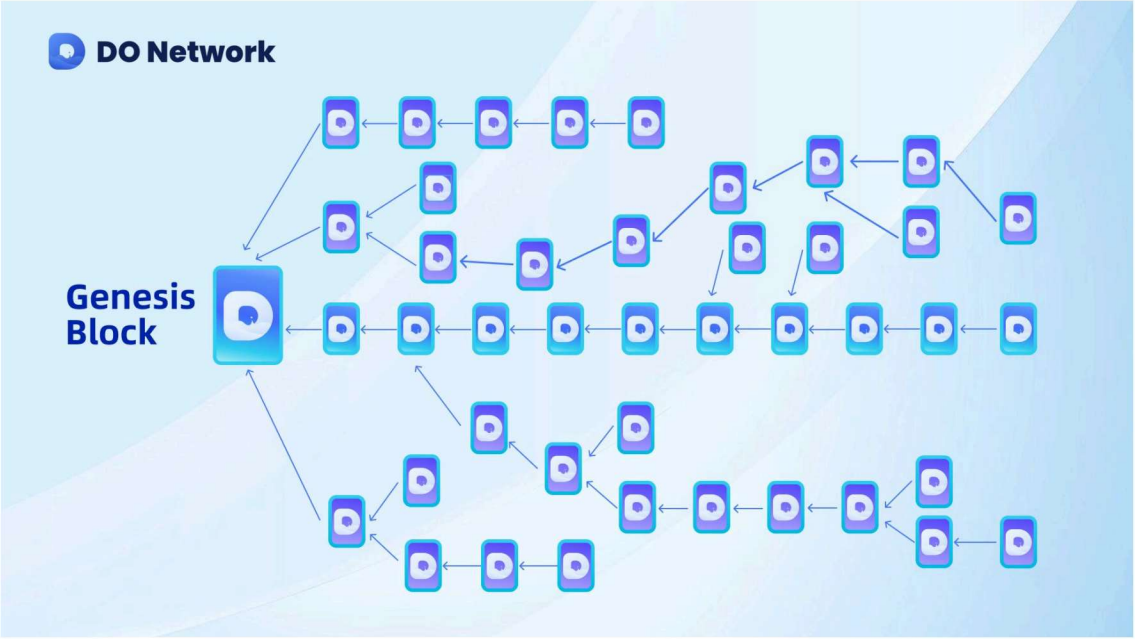
Data Structures



DAG (Directed Acyclic Graph) is a new underlying ledger structure. "Directed" means there is a direction, and "Acyclic" means there are no cycles. Compared to a Merkle tree, which is a directed tree structure where each vertex can only point to one previous vertex, and the data flows in a clear direction, a DAG structure allows each vertex to point to multiple previous vertices, while still maintaining a clear flow of data.



In a DAG, there is no concept of blocks; the basic unit is individual transactions. Each unit records a single user’ s transaction, which eliminates the need for block packaging time. The validation method relies on the subsequent transaction validating the previous one. This validation approach enables asynchronous and concurrent writing of many transactions, ultimately forming a tree-like topological structure that greatly enhances scalability.



While blockchains, under the premise of decentralization and security, cannot significantly improve scalability, leading to difficulties in commercial applications, DAGs, theoretically, are decentralized. If the network is strong enough, security can be ensured, and more importantly, scalability can be significantly improved. Distributed databases using DAG technology can drastically increase transaction throughput while reducing transaction fees to extremely low levels.

DO uses a DAG structure to avoid the concurrency limitations of traditional blockchain block packaging. By changing the chain-like structure of blocks into a DAG topology, blocks can be written concurrently. Under the same block packing time, the network can parallelize the creation of N blocks, which increases the transaction throughput by a factor of N. The combination of DAG and blockchain addresses efficiency issues. When a transaction is initiated, it is broadcasted to the network for immediate confirmation. From a graph-theory perspective, this shift from a single chain to a tree-like or mesh topology, from block granularity to transaction granularity, and from single-point jumps to concurrent writing, has significantly improved the efficiency of the DO network.

Synchronization

In cryptocurrency systems, due to the replicability of data, there is a possibility that the same digital asset could be used more than once. This is known as a double spend attack or double spending. It is because of this phenomenon that DO Network uses error correction and synchronization mechanisms to resolve some of the issues related to double spending.

Synchronization of DO introduction

Synchronization is the process of ensuring that transactions on the blockchain reach all nodes as quickly as possible, providing the foundation for consensus to bundle transactions into blocks. Fast and reliable synchronization is essential for DO's ability to achieve ultra-high throughput. Synchronization involves blocks containing multiple transactions, and completing such efficient and high-quality synchronization requires solid technical support, such as reliable node discovery, fork management, and UTXO validation.

In DO, block creation is a passive process that only occurs when transactions are generated, unlike the regular block creation mechanism in other blockchains. Any user can synchronize all the data blocks on the main network, but before synchronizing blocks, they need to have a reliable node connected to the mainnet.

When running, blockchain nodes periodically broadcast their highest block height to other nodes. Upon receiving block height broadcasts from other nodes, a node compares its own block height with the received height. If the node's height is behind, it triggers the block download process.

The block download is completed via a "request/response" method. The node entering the download process randomly selects nodes that meet the criteria and sends a request for a specific block height range. The receiving node responds with the corresponding block data based on the request.

DO's synchronization guarantees data consistency across the network, providing a secure foundation for consensus and ensuring the security and robustness of the DO network.

In DO, synchronization is done in rounds, based on a set time interval. The node calculates the network-wide height (the height with the largest proportion) based on the height received from other nodes and compares it with its own height. If the node's height is lower than the network-wide height, it begins synchronization by first obtaining blocks from several staked nodes. It then retrieves the block header hashes, validates them, and requests the actual block data. If the height difference is within a certain range, the blocks will be validated.

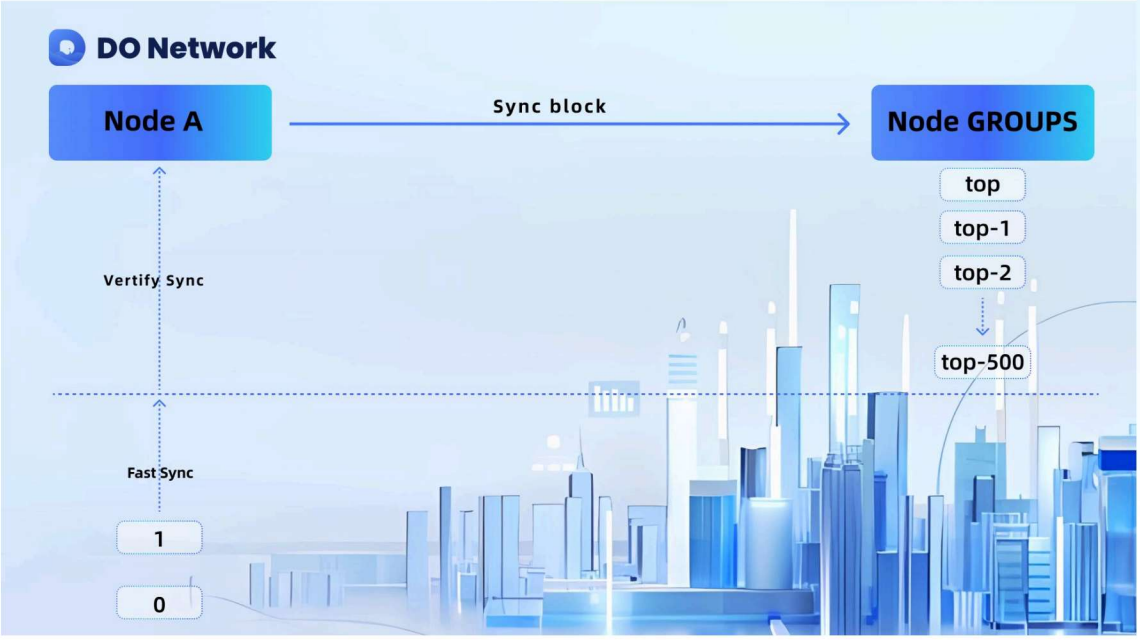
The core mechanism of DO's chain synchronization is designed based on a Byzantine Fault Tolerance (BFT) model. Synchronization requests are sent to several randomly selected nodes that meet specific conditions, and the responses are analyzed through Byzantine Fault Tolerance. A secure and valid data range is then extracted, and the node requests the block data from these nodes.

Verification Synchronization

Verification synchronization is the main method for synchronizing data blocks on the DO blockchain, as well as the primary means for correcting erroneous blocks. When a node fails to reach consensus with the majority of nodes on the network due to factors like network issues, performance problems, forks, or other unforeseen events, and if the difference in block height between the node and the network is less than 100, the node will initiate a verification synchronization process. The workflow for verification synchronization is as follows:

1. The synchronizing node will request data from specific block heights across the network using Byzantine consensus mechanisms.
2. The requested data is verified upon receipt. If the requested block is not found locally, the node will initiate the block recovery logic.
3. Once the data is verified, it is written to the node’ s cache.
4. If a block exists locally that should not be there, the extra block is added to the rollback cache.
5. During the subsequent rollback process, erroneous blocks are eliminated.
6. Whether the issue is a missing block or an erroneous block, the repair process will update the local database accordingly.

This synchronization ensures that the network resolves discrepancies in block height or invalid blocks, ensuring data integrity and preventing issues like double spending.



Block Recovery Synchronization

Block recovery synchronization is an extension of the previous mechanism. When a node's block height diverges significantly from the network, and the local database is missing data, the node will use block recovery synchronization to quickly pull in missing blocks and add them to the local database. The process involves fetching hash data at a certain block height, comparing it with the local data. If the verification is successful, the missing blocks are added to the cache and then eventually to the database. If there is a mismatch between the fetched hash data and the local data, the node will perform another Byzantine synchronization to fetch the blocks. If the Byzantine synchronization fails again, the node will perform another verification synchronization at the current block height.

Fast Synchronization

Fast synchronization occurs when a block's predecessor hash is missing during block storage. In this case, fast synchronization is used to quickly locate the missing block hash and add the current block hash to the database. Fast synchronization also serves as a logical supplement to the other two synchronization methods.

Byzantine Synchronization

Both verification synchronization and block recovery synchronization use the Byzantine method. The Byzantine process for verification synchronization involves three phases:

1. Phase One: The node asks 25 nodes across the network for data. If the response matches the local data, the synchronization proceeds to the next phase. If unsuccessful, the node proceeds to the next phase of Byzantine synchronization.
2. Phase Two: The node asks 250 nodes across the network. Again, if the data matches, the synchronization moves forward; if not, it goes to the final phase of Byzantine synchronization.
3. Phase Three: This phase involves asking the entire network for node data. After fetching the data, different strategies are applied depending on the synchronization method.

For block recovery synchronization, the Byzantine method involves querying the entire network. Verification synchronization will roll back incorrect blocks and add missing blocks, while block recovery synchronization adds the last retrieved data as the final source and writes it to the local database.

Additionally, because the last phase of Byzantine synchronization queries the entire network, it is nearly impossible for malicious nodes to cause harm. This significantly increases the cost and difficulty of malicious attacks, making it a highly secure method. Therefore, DO' s unique Byzantine process ensures that DO Network is a highly secure and reliable blockchain.

DO Smart Contract

Introduction

A smart contract is a computer protocol designed to digitally propagate, verify, or execute contract terms. Smart contracts allow for trustworthy transactions to take place without the need for a third party, and these transactions are traceable and irreversible.

The purpose of smart contracts, through the use of consensus mechanisms and immutable ledger technology, is to effectively prevent transaction data from being tampered with, ensuring the integrity of the transaction process and the irreversibility of the results. Compared to traditional contracts, smart contracts implement contract terms through programming code and automatically execute related actions when specific conditions are met, without requiring manual intervention. This helps establish trust between different parties and reduces transaction costs that may arise from distrust.

Additionally, the DO project is fully integrated with the Ethereum Virtual Machine (EVM), enabling the execution of smart contracts and the implementation of application logic. Currently, the DO Virtual Machine supports most of the popular contract standards in the market (such as ERC-20, ERC-721, ERC-1155, etc.).

DO uses Solidity as its smart contract programming language. Solidity is an object-oriented high-level programming language. The EVM used by DO supports most of the features of the

Solidity standard and compared to Ethereum, DO's contract execution fees are lower, and the block processing speed is faster.

However, due to its unique architectural model, DO differs slightly from the standard Solidity implementation. These differences include:

- The basic unit of DO token transfers within contracts is 1e-8 DO.
- The details of contracts supporting the block variable differ.
- DO account addresses can include multiple smart contract addresses.

Contract Deployment and Execution

DO currently supports the deployment and execution of smart contracts on nodes. To deploy a contract, you need an active, transaction-enabled node and an account with a sufficient balance of DO tokens to cover the deployment fees.

The binary code of the smart contract in Remix IDE is represented as BYTECODE.object or Calldata, and it is displayed as a string of hexadecimal numbers.

Similar to contract deployment, contract execution is also currently limited to being carried out on nodes. In addition, executing a contract requires knowledge of the account that deployed the contract and the transaction hash of the deployment transaction.

Contract Deployment Steps:

1. Create a new blank text file named contract.txt and paste the contract's binary code into the file.
2. Copy the file "contact" in the /contact directory file to the directory where the DO node is located.
3. Run the node.
4. Select the menu option **8. Deploy contract**.
5. Choose the type of virtual machine to run the contract.
6. If the contract constructor requires parameters, enter the binary code for the deployment parameters (if the file "contact" in the /contact directory contains Calldata, you can skip this step); otherwise, enter 0 to skip.

Contract Deployment Steps:

1. Run the menu option **9. Call contract**.
2. Enter the contract deployer's account address.
3. Enter the transaction hash of all transactions during the contract deployment.
4. Enter the required input for executing the contract to complete the execution.

Additionally, since DO uses a DAG network structure while Ethereum uses a single-chain structure, and their consensus mechanisms are not fully identical, certain Solidity instructions have been adjusted in the EVM virtual machine. The specific differences are as follows:

- block.basefee: 1
- block.chainid: 518
- block.coinbase: Block producer
- block.prevrandao: Random number generated by concatenating and summing the UTXO hash used in the transaction
- block.gaslimit (uint): 9223372036854776028
- block.number: Block height
- block.timestamp: The block timestamp in the TxInfo blockTimestamp field, usually accurate to the second, but with possible errors of a few seconds
- gasleft(): Remaining gas
- tx.gasprice: 1
- tx.origin: The originator of the transaction
- blockhash: Returns 0 due to the different semantics of block.number

3.Tokenomics

DO is the native token of the DO Network, representing the value and rights within the DO network and deeply integrated with the DO ecosystem economy.
Holding DO grants the following rights:

Staking

DO holders can stake their tokens to earn stable and attractive annual percentage yields (APY) as a reward for their contribution to the DO network. A minimum of 199 DO is required to participate in staking, ensuring that every DO holder can enjoy APY, which fully reflects the decentralized nature of DO.

Governance

DO holders can participate in the governance of the DO network by submitting proposals, voting on proposals, and engaging in the decision-making process within the DO ecosystem.

Ecosystem Participation

DO tokens serve as the entry point for engaging with various projects in the DO ecosystem. Within these ecosystem projects, DO can be used for paying gas fees, staking, trading, holding, and other purposes. As DO holders participate in ecosystem projects, they can also earn rewards through various methods.

Currently, DO has achieved an impressive price increase of approximately 2000%.

Initial token distribution

The total supply of DO is 200 million, with the initial distribution as follows:

- DO Node Incentives: 55%, totaling 110 million, with 48% remaining.
- DO Initial Circulation: 35%, totaling 70 million.
- DO Operational Expenses: 5%, totaling 10 million.
- DO Ecosystem Foundation: 2.5%, totaling 5 million.
- DO Developer Community: 2.5%, totaling 5 million.

Token staking

Currently, more than 50 million DO are staked, accounting for over 50% of the current circulation of approximately 100 million DO. The high staking rate is driven by attractive staking rewards and an extremely low staking threshold.

- **The staking reward calculation is as follows:**

Reward Rate (ER) = IR (Annual Inflation Rate) / SR (Staking Rate)

- **Where:**

SR = (Total Staked Amount in the Network - Amount Staked on the Day) / (Total Circulating Supply in the Network - Amount Issued on the Day)

- **The value of IR is determined by SR, and the relationship between the two is as follows:**

Year	SR	IR (Caclulation)	IR (Results)
2023	0.25	0.085	0.085
	0.26	0.085(1-0.015)	0.083725
	0.27	0.085(1-0.015*2)	0.08245
	.....	.....	.....
2024	0.25	0.085(1-0.1)	0.0765
	0.26	0.085(1-0.1-0.015)	0.075225
	0.27	0.085(1-0.1-0.015*2)	0.07395
	.....	.....	.....
2025	0.25	0.085(1-0.1*2)	0.068
	0.26	0.085(1-0.1*2-0.015)	0.066725
	0.27	0.085(1-0.1*2-0.015*2)	0.06545
	.....	.....	.....
.....	Calculating as above(IR minimum 0.015)		

- **Note:**

- The value of SR is capped at 0.90. If SR exceeds 0.90, it is calculated as 0.90.
- The minimum value of SR is 0.25. If SR is less than 0.25, it is calculated as 0.25.
- The minimum value of IR is 0.015. If IR is less than 0.015, it is calculated as 0.015.

• After calculating the Reward Rate (ER), we can determine the amount of reward (S) a single user can receive:

S = (Personal Total Staked Amount - Personal Staked Amount on the Day) * ER (Reward Rate) / 365

• Note:

- The SR result is retained with two decimal places (no rounding).
- The ER result is retained with eight decimal places (no rounding).

Token burn mechanism

Token burn refers to the act of transferring tokens to an address that can never be accessed, also known as a burn address. By burning tokens, digital assets are permanently locked, effectively preventing them from circulating. Burning tokens can lead to an increase in the price of the remaining circulating tokens, as the asset's price is often determined by supply and demand. When the available assets are fewer than the demand, the price tends to rise. Conversely, if there is an excess of assets that cannot meet the demand, the price will fall. By reducing the supply of tokens, burning them creates an imbalance in supply and demand, and the scarcity of the asset typically drives up the price.

• Token will be burned for the purpose of following:

1. Deflation: Burning tokens can reduce the actual circulation of the supply so the token will be in deflation and has a good performance of price. Sometimes, cryptocurrency projects burn tokens in a manner similar to stock buybacks, absorbing circulating tokens and returning value to investors by increasing the price of the remaining assets. By reducing the number of circulating tokens, this process aims to enhance the value of the remaining tokens.
2. Stablecoin Mechanism: Some algorithmic stablecoins use token burns to anchor the asset price at a target level. When the asset price falls below the target price, burning tokens reduces supply and better aligns with demand, helping to push the price back up.
3. Preventing Malicious Behavior: Some users or miners may engage in "self-trading" to earn rewards, which is meaningless for the blockchain ecosystem. This behavior slows down the network and increases transaction times. A small amount of token burn can be used to prevent this behavior. Since the amount of tokens burned is minimal, the impact on individuals is insignificant, but it can effectively deter malicious actions.

DO Burn Mechanism

A burn address is a digital wallet that cannot be accessed because it has no private key, like a lock for which no one has ever made a key. Sending tokens to a burn address effectively removes them from the overall supply, locking them in a place where no one can access them, thus preventing them from being traded again. In the case of DO, the token burn mechanism is primarily used to address malicious transactions performed by users who control a large number of nodes in order to earn gas fees. By implementing this burn mechanism, DO can reduce malicious behavior and ensure the network operates efficiently.

4.Ecology and Governance

Introduction of DO Ecology

After years of developing, DO has a great foundation of ecology. DO's ecosystem development and advantages can be divided into three main parts:

- Community
  After years of development, DO has built a community of over 100,000 members across various social platforms both domestically and internationally. A significant proportion of the community members have followed DO through both bullish and bearish market cycles, resulting in very high loyalty.
- Ecosystem Partners
  DO has established partnerships with over 100 projects across various sectors, bringing them into the DO ecosystem to promote the growth and development of the network together.
- Ecosystem Applications
  Currently, DO's ecosystem has seen the emergence of various projects including wallets, cross-chain bridges, DEXs, games, bots, NFTs, memecoins, and more, attracting a large number of community users.

The members of DO Network can get involved in the ecology through various kinds of ways:

- Developers set up and operate DO nodes.
- Developers participate in project incubation contests, hackathons, and other events.
- Earn rewards through node staking.
- Engage with ecosystem projects.
- Join community activities.
- Mint tokens and add liquidity pools with no coding required.

To encourage developers to build the ecology, DO has developed a huge grant program to help the developers with the problems they face and support them. The grant program is promoted by DO foundation, and the program includes:

- Support in DO tokens.
- $25,000 worth of Amazon Cloud resources.
- Technical assistance.
- Promotion, community engagement, and event support.
- Design support and more.

Thus, DO is keeping building the ecology so that DO ecology can be:

- **Distributed Ownership**

That means everyone can be the owner of the ecology, and everyone can benefit from the ecology. DO makes it easy to build and run a node, the technique issues are easy with no threshold, no verification, or requirement. DO allows more and more people to join in, and let everyone have Distributed Ownership.

- **Dynamic Open**

DO Network is an open public ecology, allowing anyone to join by staking DO, running a node, or delegating. DO's wave consensus enables flexible TPS (transactions per second) scaling to meet demand. The busier the network, the higher the TPS, ensuring smooth operation even with high transaction loads. That makes DO ecology Dynamic Open.

- **Data Optimization**

DO ecology wants the data to be well managed on the chain so that users can enjoy stable and high performance together with decentralization. With wave consensus, the ecology can optimize the data record, the data package, and the data broadcast. So in DO ecology, the data on the network can be well optimized and well managed.

- **Digital Operation**

DO is building a Digital Operation ecology on the blockchain network, as people all over the world are gradually turning their assets into tokens on the blockchain, such an ecology based on digital operation has been more needed, And DO ecology is friendly and convenient for everyone, looking forward to being involved to be part of people's digital life.

Governance

Governance is one of the key elements of decentralization in a blockchain public network. The governance system allows participants in the network to be involved in decision-making processes and defines the network's technical updates and resource allocation.
To ensure decentralization, governance should take place on-chain, meaning decisions are explicitly made by holders of the protocol's key resources (e.g., token holders) through an online voting mechanism. This approach provides clarity and execution in the decision-making process, maximizing the decentralization of the network's structure.

DO's governance follows these principles:

- Usability: The governance process should be clear and easy to understand. The mechanisms for participation and voting should be simple and straightforward, enabling governance to be efficient and practically executable.
- Scalability: As the number of governance participants and the complexity of governance grow, the governance system should ensure its smooth operation.
- Decentralization: Governance should allow all stakeholders of the platform to participate and have enough influence, but it must prevent any one group from controlling the platform over time.
- Effective Participation: The governance system should ensure that participants have given enough thought before voting and make decisions based on their own will, without external influence, and in line with their own interests. Voting should not be random, such as simply voting for the most popular option. The governance system should also encourage participants to express their specific views on proposals beyond voting.

DO is in the process of building its governance system and will launch it soon.

5.Summary

Introduction of DO Ecology

A public chain is the foundation of the blockchain world, serving as the long-term development cornerstone and guarantee for the blockchain industry. DO believes that the development of a public chain project requires a steadfast goal, with long-term construction and development centered around that goal. DO has always positioned “high decentralization” as the core of its development, adhering to the objective of “everyone can participate, everyone can easily participate, and everyone is willing to participate.” DO also hopes that the entire blockchain industry will flourish, ushering in the Web3 era for the digital world.

As of 2024, cryptocurrencies have become an integral part of global life. However, the adoption of public blockchains, compared to the widespread ownership of cryptocurrencies, still remains relatively niche. Due to the constraints of the "impossible triangle," the development of public blockchains is essentially a process of seeking a balance between decentralization, performance, and scalability, while achieving technical breakthroughs. In this context, the various public blockchains that have emerged today each have different positioning and directions.

DO, among them, has chosen a strategy rooted in decentralization and, based on this foundation, has achieved good performance and scalability. DO firmly believes that decentralization is the fundamental key to blockchain's ability to change the world. In order to achieve the aforementioned goal of "everyone can participate, everyone can easily participate, and everyone is willing to participate," DO will focus on the following areas of construction and progress based on its current foundation:

- **Building More Nodes**

To further enhance the decentralization of DO, the project plans to significantly increase the number of nodes globally. As mentioned earlier, the ultra-low threshold for running DO nodes will make this plan highly feasible. With the continued growth of DO nodes, not only will DO become more decentralized, but it will also make significant progress in terms of network stability, performance limits, and other aspects.

- **Developing the Ecosystem**

DO will support more ecosystem developers through grants, fostering the creation of more applications across different sectors in the DO ecosystem. This will lead to the

emergence of high-quality, high-quantity applications, and potentially some breakout applications. This move will not only increase user activity within the DO ecosystem but also attract more new users, further supporting the development and construction of the DO network itself.

Continuous Community Building

A large portion of DO's community members have been part of the DO network for several years, demonstrating high quality and loyalty. On this foundation, DO plans to further expand and strengthen the community by attracting new members. Additionally, DO will introduce community governance voting, allowing members to have a stronger sense of participation and become more involved in the construction of the DO network.

Strengthening Asset Liquidity

DO will enhance asset liquidity within the DO ecosystem and between assets from other public blockchains through various DeFi applications and tools, such as DEX, cross-chain bridges, and cross-chain applications. DO will adopt a more open approach to interoperate with other public chains, enabling asset and interaction exchanges, further improving the operability of the entire blockchain industry and network. This will lower the operational barriers and facilitate smoother transitions for Web2 users into the Web3 world.

If you are interested in DO and wanna build the blockchain world together with us, you can contact us to know more about us, joining the network or achieve business cooperation:

- Official website:https://www.donetwork.io/#/pc/Index
- Twitter:https://x.com/Donetwork_club
- Discord:https://discord.gg/donetwork
- Telegram:https://t.me/DoNetworkclub