DOMI CHAIN

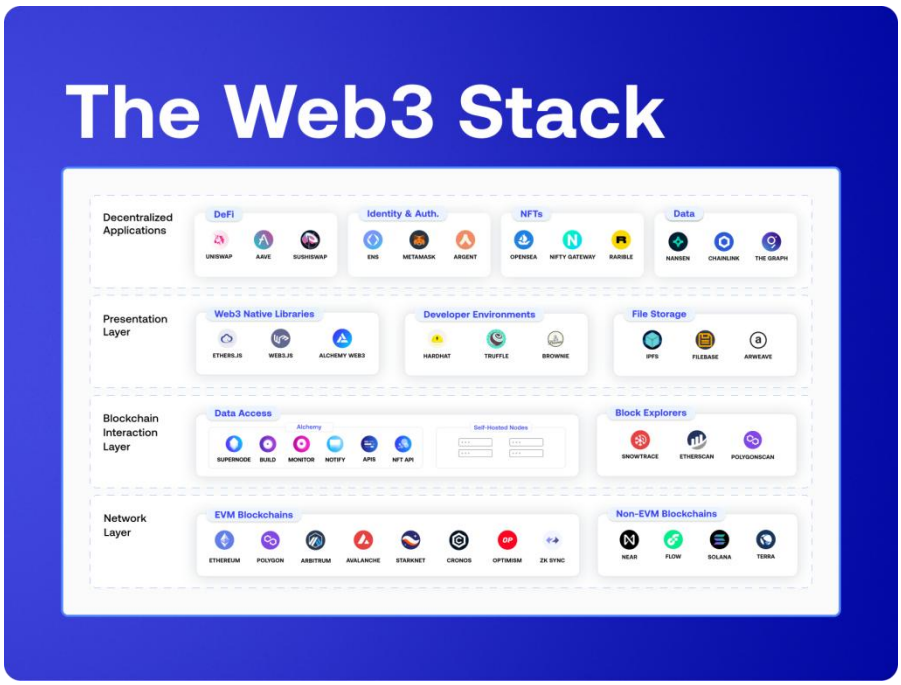
REDEFINING A NEW GENERATION OF HIGH-PERFORMANCE PUBLIC CHAINS

Web3 Overview

The emergence of the Web3 industry signifies a new era for the internet. It is not just a technological breakthrough but a significant transformation in social and economic paradigms. At the core of Web3 is the idea of creating a decentralized internet ecosystem, allowing users better control and ownership of their data, identity, and assets.

The rise of the Web3 industry represents a reevaluation of the traditional internet. During the Web2 era, tech giants accumulated vast amounts of user data, leading to users losing control over their data and privacy. Web3 aims to disrupt this scenario by establishing a user-centric internet where data and value can flow in a decentralized manner, free from the control of centralized entities. The realization of this vision requires robust infrastructure support.

In the Web3 ecosystem, public chains play a crucial role as foundational infrastructure. A public chain is a decentralized distributed ledger that records data for all transactions and smart contracts. This data forms the basis of Web3 applications, including decentralized finance (DeFi), non-fungible tokens (NFTs), decentralized applications (DApps), and more. Public chains provide a secure, reliable, and tamper-resistant ledger, ensuring the smooth operation of the Web3 ecosystem.



The importance of a public blockchain lies not only in the storage and transmission of data but also in its decentralized nature. In traditional internet systems, data and transactions are controlled by centralized entities, making them vulnerable to manipulation and misuse. The decentralization feature of a public blockchain means that no single entity can control the entire network, ensuring the security of data and user privacy.

CONTENT

TABLE OF CONTENTS

CONTENT

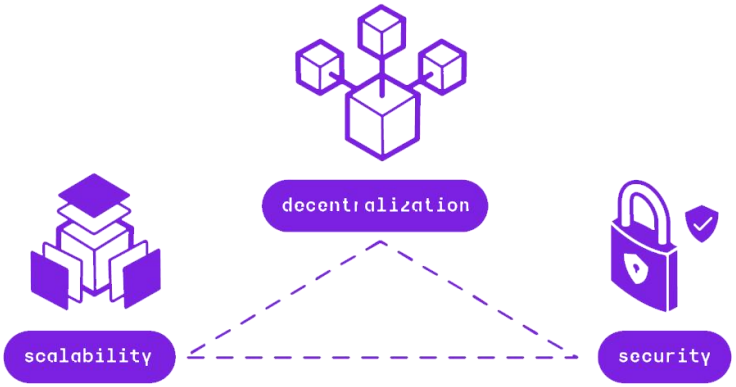
TABLE OF CONTENTS

1.1 The Trilemma Of Blockchain

Despite proving its outstanding practicality in various industries from finance to art, blockchain technology's underlying infrastructure in decentralized networks faces unique challenges compared to centralized networks. As early as the 1980s, computer scientists developed the so-called CAP theorem to elucidate what might be the most significant challenge among these. According to the CAP theorem, decentralized data storage — of which blockchain is an iteration — can only simultaneously provide two out of three guarantees: consistency, availability, and partition tolerance (CAP). In the context of modern distributed networks, this theorem has evolved into the Blockchain Trilemma. It is widely believed that public blockchains must sacrifice the security of their infrastructure, decentralization, or scalability.

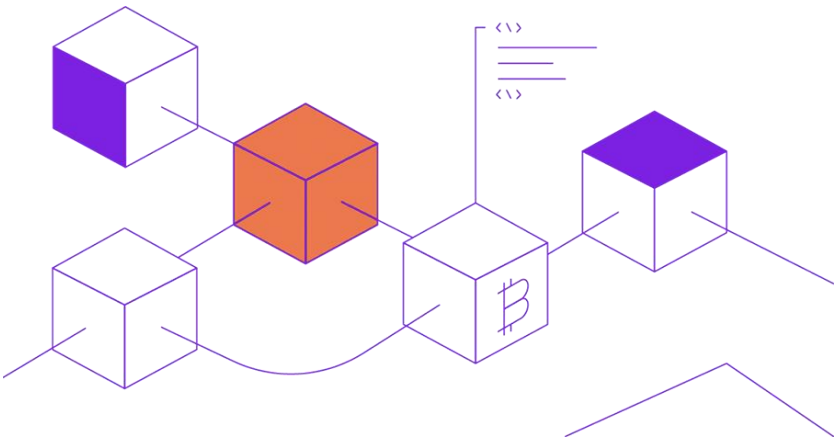
Unlike the client-server relationships dominating central network infrastructures (such as VISA or the Internet), public blockchain networks leverage decentralized consensus mechanisms. This means managing a widely distributed node network to achieve data consensus on infrastructure capable of resisting external attacks while maintaining transparency and open, fair access. This is a challenge! For example, while Bitcoin is decentralized and secure, it can only process approximately seven transactions per second (TPS). Enterprise blockchains, like Hyperledger Fabric, are secure and can handle high transaction throughput but are centralized on a very limited number of nodes reaching consensus. Fast, decentralized but insecure blockchains are susceptible to sustained hacking attacks.

Therefore, achieving a secure network on a widely distributed network while managing transaction throughput at the scale of the Internet is the Holy Grail of blockchain technology. A global community composed of enterprises, startups, and technologists is fervently developing first-layer and second-layer solutions to address the Blockchain Trilemma. The first layer refers to blockchain networks built for speed, security, and growth. The second layer refers to technical optimizations and products that can be used in conjunction with existing blockchain networks to enhance their scalability. Striking the right balance between the two layers could become an explosive catalyst for the adoption and evolution of blockchain technology and decentralized networks.



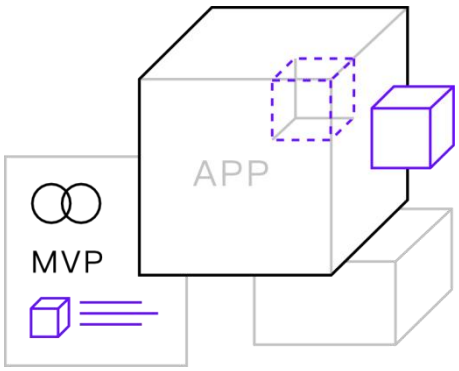
What is decentralization?

Decentralization is the core philosophy of blockchain technology, driving projects across the entire ecosystem. The application of decentralized processes and technologies can eliminate the role of intermediaries across industries and manifest in various ways. For example, by removing banking institutions from financial instruments, decentralized finance (DeFi) platforms can allocate profits and governance to users and the broader community, rather than intermediaries. At a more foundational level, decentralized networks employ consensus through crowdsourcing, meaning no single entity can control or audit the data transacted through it. However, achieving optimal decentralization often comes at the cost of reduced network throughput. As more miners contribute to consensus securing the network, transaction speeds decrease—this is considered a widely adopted obstacle.



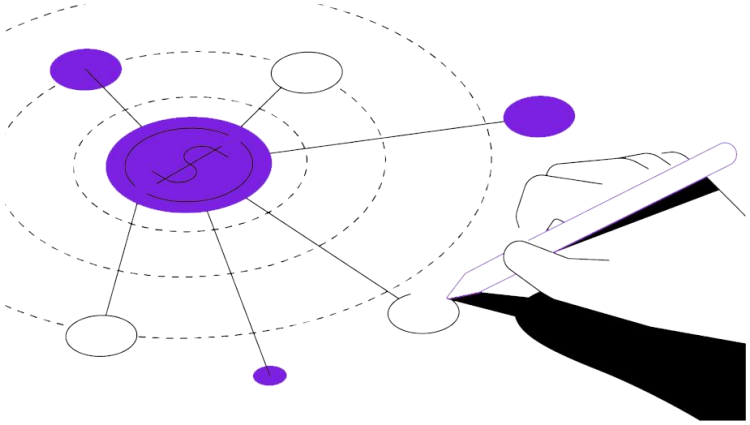
What is blockchain security?

In order to increase network throughput on the blockchain, there is a motivation to reduce the distribution of blockchain nodes geographically, in terms of quantity, or both. However, this shift towards greater centralization can compromise the security of Proof of Work (PoW) networks. When achieving consensus on an open network with limited node distribution, 51% attacks are more likely to occur, as hackers can more easily accumulate hashing power. By overwhelming the network, hackers can hijack it and manipulate transactions for economic gain. For example, in August 2020, the Ethereum Classic (ETC) blockchain – unrelated to Ethereum itself – suffered three 51% attacks, reorganizing over 4,000 blocks, allowing criminals to manipulate data and double–spend their ETC currency, resulting in losses worth millions of dollars to the network. Blockchain security is a crucial aspect of the network that cannot be compromised.



What is scalability?

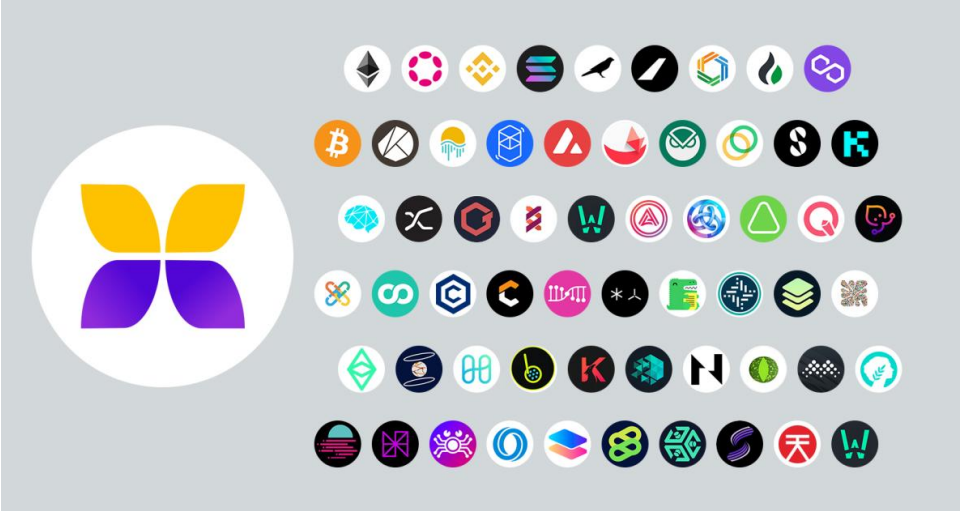
The scalability of a blockchain protocol refers to its ability to support high transaction throughput and accommodate future growth. This means that as use cases expand and blockchain technology sees accelerated adoption, the performance of a scalable blockchain should not be compromised. It is said that blockchains that perform poorly as adoption increases lack scalability. The blockchain trilemma informs us that achieving greater scalability is possible, but it may come at the cost of security, decentralization, or both. Scalability is the only way for blockchain networks to reasonably compete with traditional centralized platforms, which often have superior network settlement times and availability. Despite many blockchain platforms having established decentralization and security, achieving scalability remains a primary challenge for leading decentralized networks today.



Although the blockchain trilemma poses significant challenges to the adoption of blockchain technology, solutions are emerging to effectively and synchronously balance network security, decentralization, and scalability.

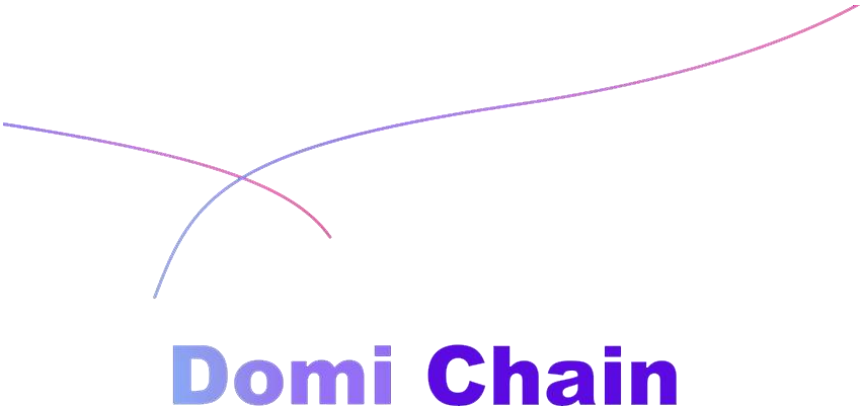
1.2 The Competition Landscape Of Public Blockchains

As the blockchain ecosystem continues to grow, a single public blockchain is no longer sufficient to meet the ever-increasing demands. Consequently, multi-chain technology is gradually gaining prominence, with public blockchains like Domi Chain, BSC, Solana, Avalanche, and others emerging one after another. They aim to attract users and developers by enhancing performance and offering better scalability.



Competitors in the public blockchain space strive to continuously improve technology, enhance performance, security, and scalability to meet the growing demands. Technological innovations such as smart contracts, sidechains, sharding, and decentralized identity have driven the evolution of the competitive landscape. These innovations provide public blockchains with additional functionalities like NFTs, DeFi, and DApps, attracting more developers and users.

In addition to technological innovation, the construction of an application ecosystem is also a key factor in the competitive landscape. The success of a public blockchain depends not only on its technical capabilities but also on its attractiveness and usability. Examples of successful cases include Ethereum's DeFi ecosystem and NFT market, Polkadot's cross-chain applications, and Solana's high-performance DeFi applications. Establishing a robust application ecosystem is crucial for attracting more users and developers.



The competitive landscape of public blockchains is an area full of opportunities and challenges. Projects like Domi Chain are striving to establish a leading position globally, offering developers and users a wider array of choices.

2.1 Introduction To The Public Chain

Domi Chain has created a scalable, secure, decentralized, and permissionless platform that supports faster and higher throughput transactions and applications, providing better infrastructure for the DeFi and Web 3.0 ecosystems. Without compromising on security, it can process 100,000 transactions per second, without relying on second-layer solutions or sharding technology.

Domi Chain truly addresses the trilemma of blockchain, attracting significant attention and participation from a large user and developer base. The ecosystem is growing, encompassing various sectors such as NFTs, DeFi, GameFi, infrastructure, DAOs, cross-chain bridges, and more. The prosperity of the ecosystem significantly enhances the scalability and composability of the Domi Chain ecosystem, paving the way for the development and construction of more innovative projects on the platform.

Domi Chain employs the following methods to tackle the seemingly insurmountable trilemma and create a scalable, secure, decentralized, and permissionless blockchain.

1) Domi Chain generates a cryptographic hash sequence for all received transactions. The transaction order is no longer determined by block producers; instead, it is determined by a cryptographic hash algorithm and persistently stored on the blockchain. We refer to this as Proof of Time (PoT). Conceptually, this is similar to Solana's Proof of History (PoH, see reference 1), but there are significant differences in architecture and implementation.

2) Domi Chain uses a special Proof of Stake (PoS) algorithm called Fast Byzantine Agreement (FBA, see reference 2) as the consensus for block production and validation, enabling transactions to be completed within 3.5 seconds.

3) Domi Chain introduces a hybrid validation model to enhance security while maintaining unrestricted participation and decentralization of power. We introduce a new decentralized firewall composed of mobile devices and laptops worldwide to support transactions and monitor block production and validation. Any device can join the network to perform these functions and receive rewards. Transaction endorsements are achieved by sampling random nodes and obtaining sufficient collateral. This process significantly reduces the number of erroneous transactions. An unlimited number of nodes (referred to as monitoring nodes or distributed firewalls) can execute this function. Block production and validation are carried out by a set of high–bandwidth, high–performance, commercial–grade servers (referred to as core nodes) distributed globally. Monitoring nodes are only involved in monitoring the blockchain and endorsing transactions; they do not produce blocks. By separating blockchain monitoring from block production/validation, we achieve unlimited decentralization, widespread participation, and enhanced security. Any mobile device and computer can join the network without permission and hardware restrictions.

4) Introducing a new consensus algorithm (Domino Consensus) that can quickly identify fraudulent nodes from a large number of monitoring nodes.

5) Introducing decentralized storage as part of the blockchain to offload large or old data. This is particularly useful for storing high–resolution NFT image data.

2.2 Investment Institutions

Amazon Web Services (AWS) has invested up to $170,000 in Domi Chain, demonstrating not only AWS's confidence in Domi Chain but also providing robust support for its future development. As a leading global provider of cloud computing services, AWS's investment goes beyond financial support, serving as recognition of the platform's technology and ecosystem.

AWS's support will further solidify Domi Chain's position in the Web3 ecosystem, offering better tools and resources for users and developers.

Virtual Geo is a space satellite system approved by the Federal Communications Commission (FCC) and the International Telecommunication Union (ITU), designed to provide reliable and cost-effective broadband communication globally. This advanced technology has a wide range of applications, providing numerous interesting opportunities for various industries and investors.

By delivering reliable global communication, Virtual Geo aligns perfectly with Domi Chain's mission to create a decentralized, secure, and high-performance platform. This collaboration ensures that Domi Chain can reach users and developers worldwide, facilitating its rapid growth.

ArchiveVentures is Domi Chain's key investment institution, establishing, acquiring, and investing in blockchain/cryptocurrency companies globally. With extensive experience in traditional financial fund management, ArchiveVentures has grown into one of the most active VC investment institutions in the crypto space.

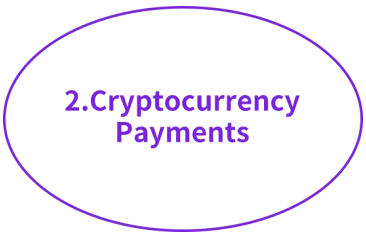
The deep collaboration between the two parties will provide strong support for Domi Chain's steady development in the Web3 infrastructure race, marking an important step in jointly constructing a more open, transparent, and efficient crypto ecosystem.

2.3Ecological Development

The issue of cross-border payments and remittances, with a market size exceeding 680 billion USD, has long been a challenge due to the slow and expensive nature of traditional banking systems. Bitcoin was initially conceived to address this problem. However, due to high mining fees and slow confirmations, using Bitcoin for everyday transactions, especially for smaller amounts, has proven to be difficult. In comparison to other blockchain and cryptocurrency alternatives, Domi Chain network boasts the advantage of low transaction costs and fast settlement speeds. Domi Chain will facilitate instant settlements for cryptocurrencies, including stablecoins such as USDT and USDC.

Domi Chain collaborates with Unbanked (unbanked.com) to provide fiat currency on-ramps for converting fiat currency into stablecoins, enabling immediate transfer and payments.

Domi Chain will offer a non-custodial crypto wallet that includes DOMI, BTC, ETH, USDT, USDC, and other cryptocurrencies. The wallet also serves as a validator node, participating in securing the network and earning rewards in DOMI.



The partnership between Domi Chain and Unbanked (https://unbanked.com) enables users to spend cryptocurrencies using traditional debit cards such as Visa or MasterCard. Users only need to deposit cryptocurrency into their wallets, and the associated debit card

allows them to use their cryptocurrencies at over 50 million merchants on the Visa or MasterCard networks. After users swipe their cards at merchants, Domi Chain, through Unbanked's settlement layer, converts the cryptocurrency into fiat currency.

Unbanked is committed to expanding this service to over 153 countries/regions globally. Once customers without bank accounts can use this service, Domi Chain blockchain users can access similar services.

3.Decentralized Exchange

With lightning-fast transaction speeds, our partners will build a decentralized exchange on the Domi Chain blockchain. Exchange users will experience performance similar to centralized exchanges. Many users recognize the major risk of centralized exchanges: the potential loss of their crypto assets, especially when managed on the exchange's hot wallets. Scalability and availability issues have deterred some users from using decentralized exchanges. Domi Chain addresses both these issues through a blockchain infrastructure that can be massively scaled.

4.NFT Support

Non-fungible tokens (NFTs) are data units stored on decentralized ledgers or blockchains, proving the uniqueness and non-interchangeability of digital assets. NFTs can represent items such as photos, videos, audio, and other types of digital files. NFTs are tracked on the blockchain to provide ownership proof independent of copyright. The NFT market tripled in value in 2020, exceeding $250 million. In the first quarter of 2021, NFT sales surpassed $2 billion.

In the second phase of implementation, the Domino blockchain will add integrated decentralized storage to seamlessly handle large amounts of data stored on the blockchain. This will facilitate NFTs with high-resolution

images or other data types. Most blockchains today lack the capability to handle NFTs with large datasets. Domino blockchain will provide unlimited decentralized storage, low transaction fees, and instant settlements for this growing market.

3.1Design Principles

1) Encryption Security Layer: Domi Chain prioritizes encryption security, implementing robust encryption technologies throughout the entire ecosystem to ensure the security of user data, transactions, and assets. By adopting the latest encryption standards and technologies, Domi Chain provides a highly secure environment for transactions and data transfer, enabling users to trust the platform and safeguard their privacy and assets.

2) High Scalability: Domi Chain's design features outstanding scalability, supporting faster and higher throughput transactions and applications. This scalability applies not only to existing DeFi and Web 3.0 applications but also provides space for future innovations. Domi Chain ensures that its infrastructure can handle the continuously growing demands of users and applications without relying on second-layer solutions or sharding technology.

3) Satellite Synchronized Data: Domi Chain adopts a satellite architecture, offering rapid synchronization of blockchain data, further enhancing the speed of Domi Chain. This architecture efficiently and reliably improves data transmission and synchronization by utilizing satellite technology. This not only enhances network performance but also strengthens decentralization, ensuring data consistency among nodes.

4) Decentralized Storage: Domi Chain introduces decentralized storage as part of the blockchain to offload large or old data. This is particularly useful for storing high-resolution NFT image data. Decentralized storage not only improves system performance but also ensures the persistence and availability of data. This feature makes Domi Chain an ideal choice for the NFT market, supporting high-quality digital asset storage and transactions.

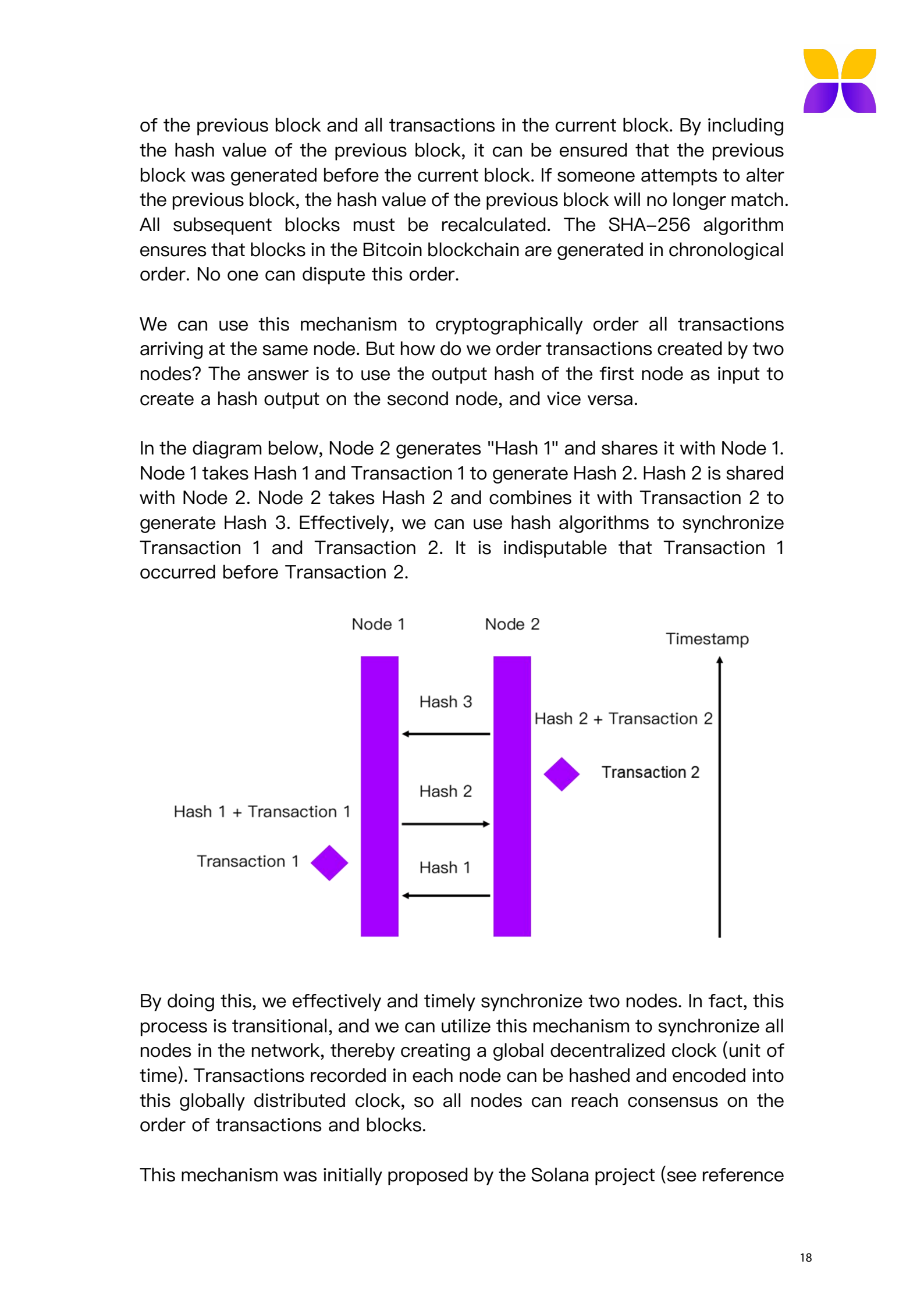
These design principles collectively form the core architecture and value proposition of Domi Chain, providing a robust infrastructure for the DeFi and Web 3.0 ecosystems while meeting high user demands for security, scalability, and data storage.

3.2Blockchain Architecture

1) Proof Of Time And Cryptographic Global Clock

Due to the decentralized nature of blockchain systems, achieving consensus among nodes on the order of transactions comes at a high cost. This is because each node's clock is slightly different, causing transactions to arrive at each node in a different order. Not to mention that some nodes may behave maliciously and intentionally conduct transactions in a way that benefits their financial advantage. To address this issue, Bitcoin introduced a block time of approximately 10 minutes to impose a sufficiently long delay, allowing all nodes to reach consensus on the order of transactions. Ethereum managed to shorten the block time to 15 seconds. This may be the minimum achievable with a Proof of Work (PoW) system. For Proof of Stake (PoS) systems, block times are shorter. Tendermint has a timeout window of 3 seconds, Libra around 10 seconds, and Aglorand about 5 seconds. However, for financial systems handling a large number of transactions, this delay is still a considerable amount of time. What if there was a way to order transactions without relying on PoW or PoS consensus mechanisms? This should significantly reduce block time and increase blockchain throughput.

Indeed, there is a method to address this issue using cryptography, specifically the SHA–256 hash. SHA–256 is a one–way hash algorithm that can reduce any amount of data to a constant number of bytes (a 256–bit hash). It is also deterministic—if you apply the algorithm to the same data again, you will get the same hash value each time. Calculating the hash is also very fast. If you take the same data and change one bit, the hash value will be vastly different. It is impossible to guess the input data from the resulting hash value. In fact, the Bitcoin blockchain is created using a double hash with SHA–256, linking blocks into a sequentially ordered chain over time. Each block contains a hash value calculated from the hash value



of the previous block and all transactions in the current block. By including the hash value of the previous block, it can be ensured that the previous block was generated before the current block. If someone attempts to alter the previous block, the hash value of the previous block will no longer match. All subsequent blocks must be recalculated. The SHA–256 algorithm ensures that blocks in the Bitcoin blockchain are generated in chronological order. No one can dispute this order.

We can use this mechanism to cryptographically order all transactions arriving at the same node. But how do we order transactions created by two nodes? The answer is to use the output hash of the first node as input to create a hash output on the second node, and vice versa.

In the diagram below, Node 2 generates "Hash 1" and shares it with Node 1. Node 1 takes Hash 1 and Transaction 1 to generate Hash 2. Hash 2 is shared with Node 2. Node 2 takes Hash 2 and combines it with Transaction 2 to generate Hash 3. Effectively, we can use hash algorithms to synchronize Transaction 1 and Transaction 2. It is indisputable that Transaction 1 occurred before Transaction 2.

By doing this, we effectively and timely synchronize two nodes. In fact, this process is transitional, and we can utilize this mechanism to synchronize all nodes in the network, thereby creating a global decentralized clock (unit of time). Transactions recorded in each node can be hashed and encoded into this globally distributed clock, so all nodes can reach consensus on the order of transactions and blocks.

This mechanism was initially proposed by the Solana project (see reference

1). Solana is capable of using this mechanism to create a blockchain network with a block time of 400 milliseconds and maintaining 50,000 transactions per second on a test network with 200 high-performance nodes. The reason for such significant improvements over other blockchains is that the encrypted sorting of transactions eliminates the delays associated with achieving transaction order through consensus mechanisms.

The Solana network restricts nodes to high-bandwidth servers, sacrificing some decentralization to improve scalability. Domi Chain leverages the concept of Proof of History but differs in architecture and implementation. Additionally, Domi Chain introduces innovative methods to achieve unlimited decentralization and enhanced security without sacrificing scalability. Details of these methods are described in the following sections.

2) Fast Byzantine Agreement and Leader Selection

In the implementation of Proof of History (PoH) in Solana (see reference 1), due to the rotation of block proposers, the blockchain still has many opportunities to fork into multiple paths. Consensus needs to be reached to determine which fork will be used as the final direction for chain growth. We introduce a deterministic algorithm to select the next block producer that can be easily verified, ensuring that only one path can effectively grow the chain. This further reduces network traffic and latency, enabling higher throughput.

We divide time into epochs, each lasting 1 second (referenced as epochs). Each epoch is further divided into 5 slots, with each slot lasting 200 milliseconds. In the first step, a block is produced for each slot. The second step involves selecting the block proposer for this epoch through a very short message vote. The third step involves proving the block through a random committee to verify no double-spending, overspending, and block validity. We use a Verifiable Random Function (VRF) to execute all three

steps, ensuring randomness and minimizing security risks.

VRF consists of three algorithms: Keygen, Evaluate, and Verify.

Keygen(r) → (VK, SK): The key generation algorithm randomly generates a verification key (VK) and a secret key (SK) pair.

Evaluate(SK, X) → (Y, ρ): The evaluation algorithm takes the key SK and a random seed X as input, producing a pseudo-random output string Y and a proof ρ.

Verify(VK, X, Y, ρ) → 0/1: The verification algorithm takes the verification key (VK), seed (X), output (Y), and proof (ρ) as input. It outputs 1 only if it verifies that Y is the output generated by the evaluation algorithm for the input (SK, X).

For a given input pair (SK, X), the output (Y) is unique, meaning it is impossible to find another output (along with a valid proof) for a given key pair (VK, SK) and seed X.

Each account in the network holds a secret participation key (SK), while the verification key (VK) is publicly known.

In the block proposal phase, selected accounts propose new blocks to the network. This stage begins with each node in the network iterating through each account it manages. For each online and participating account, it runs VRF to determine if that account should propose a block.

Y/ ((2^hashlen)–1) <= P (known selection probability)

The output Y of VRF is pseudo-random and uniformly distributed from 0 to (2^hashlen)–1 (hashlen is the length of the hash). The staked token DOMI is used to compute weighted priorities, ensuring that the selection probability is proportional to the amount of DOMI tokens to prevent Sybil attacks (see reference 2).

Once an account is selected, each node propagates the proposed block along with the VRF output, proving the account is a valid proposer. Each node in the network receives block proposals from other nodes. Subsequently, each node runs VRF for each participating account it manages to check if they are selected to join the validation committee. If an account is chosen, it votes weighted by its DOMI amount. Each selected account contributes to filtering the proposals down to one through voting. These votes are used to calculate the minimum VRF block proposal

determined at the timeout, and are sent along with the VRF proof to other nodes. Each node verifies the VRF proof of committee members before adding to the vote count. Once a leader's selection reaches a 2/3 majority, a new committee is chosen to verify if the selected block proposals in the selection phase have any issues such as overspending or double-spending. If valid, the committee votes again to prove the block. This process is completed in a manner similar to the selection vote, with each node iterating through its managed accounts to choose a committee and send votes. These votes are collected and verified by each node until a 2/3 majority is reached, triggering the round's end and prompting nodes to create a certificate for the block and write it to the ledger. A new round begins at this point.

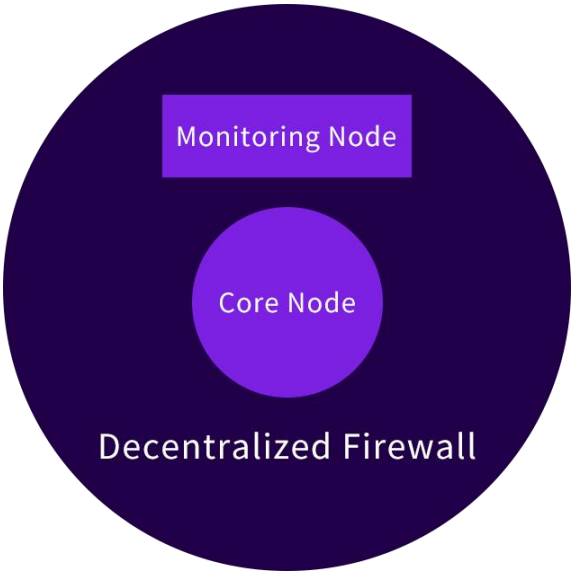
We are implementing the Fast Byzantine Agreement (FBA) protocol (see reference 2). This protocol does not execute among all users in the network. Instead, it is limited to small user committees randomly selected each round. FBA can scale to millions of core nodes because the protocol is executed by a small committee. The increase in the user group does not slow down the protocol; instead, it enhances its robustness and security. Due to our unique implementation of the protocol, different committees will be responsible for authenticating different blocks, contributing to increased throughput. Further explanation will be provided in the following sections. An epoch leader will sequentially produce 5 blocks, each authenticated by a separately selected random committee to ensure security.

The uniqueness and pseudo-random properties of VRF ensure that no user can brute-force multiple outputs Y until finding one within the desired range. The uniqueness of VRF mitigates such attacks since, once the seed X is fixed, VRF can only be used to generate a single output. Additionally, the verification key VK must be input into the system before the current epoch, at which point the seed X is essentially unpredictable.

The aforementioned computations are very inexpensive. Each user needs to execute the Evaluate function once to determine if they are selected as committee members.

A new independent committee is selected for each FBA round. This is possible due to the unique property called player replaceability. In essence, different users can participate in different rounds of FBA without needing to pass any state between them. This allows us to achieve a high level of security, permitting users to dynamically corrupt after any message they send as part of the protocol.

In the leader selection phase, the proposed value is the hash value of the block, and it is propagated in parallel with the actual block. The protocol allows users to choose the epoch leader from the block hash in step 2 without needing to see the complete block. Since hashes and selection votes are short messages and propagate much faster than the full block, when most honest nodes receive the actual block, they should already have received the 2/3 selection vote for that block if the leader is honest. Therefore, most honest nodes can authenticate it at the moment of receiving the block and generate a certificate in just one voting step after block propagation. Since each leader will consecutively produce 5 blocks, we only need to choose a new leader every 5 blocks. However, each block will be authenticated by a separately selected random committee to ensure security.



3.3 Separating Block Production from Block Validation

In a typical PoS network, a selected block producer verifies transactions and chooses which transactions to include in a new block, effectively performing both block production and validation within a single node. While this approach is easier to implement and reduces network traffic, it opens the door for attackers to manipulate blocks by exploiting invalid transactions.

In our FBA implementation, the protocol consists of three steps: block proposal, leader selection, and block certification. Each step is executed by independently chosen random nodes acting as a committee. This significantly reduces the likelihood of block manipulation to a very small and negligible probability when Byzantine nodes are less than 1/3 of the total stake (see reference 2).

3) Monitoring Nodes And Decentralized Firewall

In the Domi Chain network, there are two types of nodes: core nodes and monitoring nodes. Core nodes propose blocks, select block leaders, validate blocks, and replicate validated blocks to all nodes. Monitoring nodes are responsible for network monitoring and transaction endorsement. In a sense, monitoring nodes act as a decentralized firewall, ensuring the health of the network and all nodes, acting honestly. If there are adversary nodes, they are quickly detected, exposed, and eliminated to limit damage to the network.

In the previous section, we described block proposal, leader selection, and block certification. In this section, we will describe transaction endorsement and monitoring of the network.

After a transaction is submitted, it is immediately forwarded to several monitoring nodes for endorsement before being broadcasted to the network. These nodes are selected based on the network topology to improve efficiency and incentivize social participation. This process is very fast (less than 3 seconds), and users should not notice any significant delay. Social relationships are recorded when monitoring nodes join the network, and endorsement monitoring nodes are selected based on these social

relationships. Nodes with higher stakes are also more likely to be selected. The selected monitoring nodes endorse the transaction by checking signature validity, account balance, and pending transactions to ensure its validity, preventing double-spending or overspending. If everything is in order, each monitoring node endorses the transaction through a digital signature and returns it to the submitting node. The submitting node collects all signed endorsements, packages them into a transaction, and submits it to the network through a core node close to the submitter. If the submitting node has no social connections to monitoring nodes, the system randomly selects several monitoring nodes to endorse the transaction. Endorsing nodes are compensated with a portion of the transaction fee for each endorsement. Typically, each user (monitoring node) is part of a social tree structure, and the selection process goes from leaves to the root. We encourage users to stake a significant amount of DOMI, especially when they have a large network in their social tree.

The endorsement selection algorithm can be changed by the majority of 2/3 core nodes and monitoring nodes.

In practice, producer/validator nodes and monitoring nodes perform different types of work and have different hardware requirements. Producers typically need high bandwidth and multi-core CPUs or GPUs. Depending on the type of validation to be performed, some validation tasks can be executed by lower-spec computers or even mobile devices. We use the SHA256 hashing algorithm in our design. Calculating the SHA256 hash by providing input data is very fast and can be achieved using a single-core CPU or GPU. After calculating the hash value, it is compared with the hash value previously calculated by the block producer and attached to the block header. Block producers/validators require high-performance and high-bandwidth servers, while monitoring nodes can be any type of computer, laptop, or even a mobile device.

4) Domino Consensus Algorithm

In addition to endorsement, monitoring nodes continuously observe the network by ensuring the following:

- Transactions are correctly signed.
- No double spending or overspending occurs.
- The block structure is correct, with headers and valid payloads.
- The next block producer is selected according to the correct algorithm (which is deterministic).

- There are no malicious producers or validators.
- No parallel chains exist.

Whenever an error or adversary is detected, a broadcast is sent to 10 randomly selected monitoring nodes in the network to alert all nodes about the error. Each monitoring node verifies the error or violation. Upon confirmation, the monitoring node randomly selects 10 nodes and notifies them of the error. This process confirms the error. Once confirmed, the erroneous node is removed from the network for a configurable period, and the stake is reduced. We refer to this as "Domino Consensus" because it resembles a domino effect in the error detection process.

The design inspiration for Domino Consensus comes from Avalanche Consensus (see reference 3). In Avalanche Consensus, each node samples a set of randomly chosen nodes. If a majority chooses a color, the node will adopt that color. This process repeats several times until the network reaches a quasi-stable state, achieving consensus. Avalanche Consensus is a novel consensus algorithm different from classical consensus and Nakamoto consensus, allowing faster consensus among a large number of distributed nodes.

Domino Consensus is a variant of Avalanche Consensus. The difference lies in that when nodes randomly sample, they do not need to choose one color over another. Instead, they collect all potential errors from the selected nodes. The node does not blindly inform other nodes of errors. Instead, it verifies each error and alerts only 10 additional random validators about the confirmed error. This eliminates the risk of malicious nodes intentionally spreading false error signals to disrupt the network. This consensus mechanism enables monitoring nodes to quickly discover and confirm errors in the network, allowing immediate action to address errors and protect the network.

In most cases, errors can be detected even before they are submitted to the blockchain because many nodes actively monitor the network continuously. When block validators verify a block, they check for errors and ensure the absence of any in the block.

Monitoring nodes will continue to observe producers/validators to ensure correct block generation and that the right leader is producing blocks. Any misconduct is flagged and propagated throughout the entire network. Producers identified as engaging in misconduct will be removed from the producer list, and the staked tokens will be reduced.

Monitoring nodes will continually check for the following errors:

- Double spending
- Overspending
- Dust attacks
- Long-range attacks
- Signature forgery
- Misbehaving producers and validators
- Parallel chains

Monitoring rewards are calculated based on errors discovered by monitoring nodes. The first to discover and subsequently verify an error will receive the highest reward. The second node to verify the error will receive half the reward. The third node to verify the error will receive half of the second reward, and so on. The reward amount for each error is fixed. This incentivizes monitoring nodes to discover new errors in the network and verify them early, exposing network errors as soon as possible.

3.4 Domi Chain Virtual Machine And Smart Contracts

The Ethereum Virtual Machine (EVM) serves as the first-generation decentralized application platform and runtime environment for smart contracts. However, the EVM faces performance and efficiency issues and lacks scalability.

WebAssembly (WASM) is a web browser standard developed by the W3C working group, including entities like Google and Mozilla. It supports various languages compiled into WASM. WASM is high-performance as it is designed to closely resemble native machine code while being platform-independent. Its small binary code can be transmitted over the internet to low-bandwidth devices. WASM extends support to languages such as Rust, C/C++, C#, Typescript, Haxe, and Kotlin. It has been continually developed by standard committees and major companies like Google, Apple, Microsoft, Mozilla, and Facebook.

The Domi Chain Virtual Machine (DVM) is being constructed to be compatible with WASM and removes floating-point operations from the consensus algorithm. Additionally, DVM will support Solidity, enabling seamless migration of any existing Ethereum smart contract code to Domi. Similarly, the next-generation blockchain interoperability protocol, Polkadot, is building WASM support from the ground up. The Ethereum Foundation is also committed to implementing WASM support in geth and researching the use of WASM in sharding.

In the future, we plan to design a visual programming tool that can create smart contracts with drag-and-drop UI support, eliminating the need for programming skills. This will significantly enhance adoption as most individuals lack programming experience.

5) Domi Chain Decentralized Storage

As the scale of blockchain grows, there is a need for a storage solution to offload blockchain data. Domi Chain plans to build a decentralized and censorship-resistant integrated storage mechanism on monitoring nodes, following the Swarm protocol. One of the primary reasons for choosing Swarm over IPFS is that Swarm's core storage component functions as immutable content-addressed block storage rather than a general-purpose distributed hash table. This makes unloading blockchain data to Swarm more straightforward.

4. Domi Token Introduction

4.1Token Allocation

Domi

Total Supply: 1 billion tokens

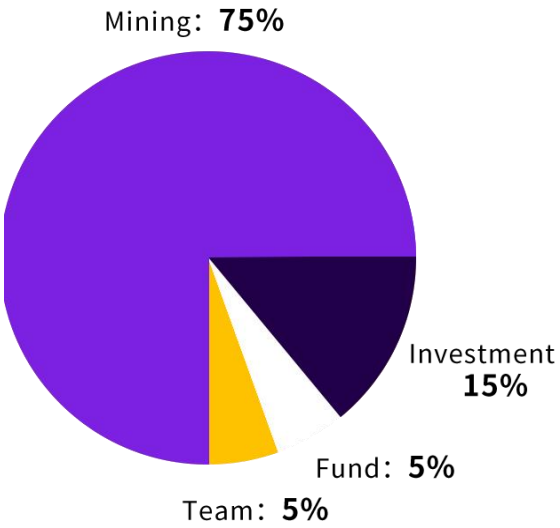
Allocation is as follows:

Investment: 15%

Mining: 75%

Fund: 5%

Team: 5%



The initial circulation of DOMI (Domi Coin) is only 250 million coins, with 100 million of them being locked up for one to three years. Therefore, the initial circulating supply is only 150 million coins. Similar to the Bitcoin mining halving mechanism, through a mathematical formula, the total supply of Domi is permanently capped at 1 billion coins. Out of this, 750 million coins are slowly released to core nodes and validation nodes over 100 years.

Seventy-five percent (750 million) of the total supply is allocated to miners and validators. Within this 750 million, core nodes receive 70%, and monitoring nodes receive 30%. Mining and validation rewards for DOMI are highest in the early stages of operation, decreasing by 50% every four years. After 100 years, the distribution of the 750 million mining tokens will

be completed. With the development of the network and the increase in the price of DOMI, the rewards for miners and validators should increase over time in terms of equivalent USD value.

Transaction fees are approximately 0.001 DOMI per transaction.

Fifteen percent (150 million) of the total DOMI supply is allocated to investors through private or public sales of DOMI tokens.

Five percent (50 million) of the total supply is allocated to the DomiChain team for blockchain development and maintenance, with these coins being locked up for three years.

Finally, the remaining 5% of the supply (50 million) is allocated to the Domi Foundation for marketing, community development, and encouraging application development on Domi Chain, with these coins being locked up for one year.

4.2Token Value

1) Transaction Fees: Holders use the token to pay for transaction fees incurred when executing smart contracts, transactions, or other operations on the Domi Chain network.

2) Governance Rights: Holders can use the token to participate in governance decisions on the network, including proposing and voting on changes.

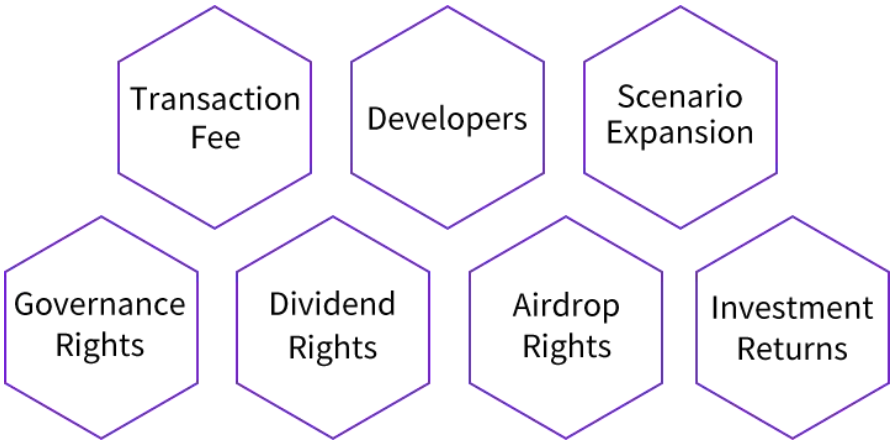
3) Ecosystem Expansion: Partners can integrate Domi tokens into products, services, or platforms, enhancing the practical value of the token.

4) Staking for Mining: Holders can stake their tokens to support network security and performance, earning token rewards in return.

5) Dividend Rights: Holders can stake their tokens to support network security and performance, earning token rewards as dividends.

6) Investment Value: Holders can benefit from investment returns. The token's scarcity, demand, and market conditions contribute to its value.

7) Developers: Tokens can be used to pay for the deployment and execution costs of smart contracts. High performance and low costs make it the preferred choice for developers building decentralized applications.



5. Decentralized Autonomous

5.1 Overview Of DAO

DAO (Decentralized Autonomous Organizations), also known as decentralized autonomous entities, is an organizational form based on blockchain technology. It operates and is managed by the community through a transparent decision-making process. The rules for the organization's management and operation are encoded on the blockchain in the form of smart contracts. Through intelligent management and distributed economic incentives, DAO achieves self-operation, self-governance, self-evolution, and, consequently, the optimal efficiency and value circulation of the organization. With the growing popularity of the decentralized spirit in the crypto industry, organizations based on the DAO model are experiencing widespread expansion. DAO enables communities to become creators and sharers of value.

DAO introduces a new way of governing communities and sharing value, utilizing rapidly evolving governance and incentive systems to allocate decision-making authority and rewards. As human activities and values shift towards the digital domain, collaboration between distributed communities and stakeholders becomes increasingly important. As a novel economic organizational form native to the internet, DAO breaks away from traditional organizational models, providing a way of thinking that transcends traditional boundaries. DAO requires the organization to have a common visionary goal, driven by a group of individuals who share consensus on this vision, leading to spontaneous collaborative behaviors of co-creation, co-building, co-governance, and sharing. This effectively stimulates organizational efficiency and facilitates value circulation.

Domi Chain will leverage the immutability and public transparency advantages of blockchain technology to reshape the credit system and enhance the efficiency of digital economic activities.

5.2 DAO Advantages

1) High Transparency

Data in DAOs is stored on the blockchain, allowing every activity, transaction, and financial flow within the organization to be visible on the chain. This transparency significantly reduces the risks of corruption, abuse of power, and other internal malpractices.

2) Global Accessibility

Anyone can join a DAO organization, and it permits individuals to work under the same conditions by adhering to a set of standardized rules applicable to all parties. DAOs are often more easily able to achieve global reach since they are not constrained by geographical locations.

3) Full Organizational Participation In Voting

DAOs enable members within the organization to decide or alter a decision through voting. This ensures that DAOs do not overlook or exclude members' opinions, and it guarantees that all votes are calculated and displayed with a certain level of transparency.

4) Immutability Of Rules

The rules and decisions of DAOs are executed through smart contracts on the blockchain. The formulation of new decisions or changes to old rules requires consensus within the organization before they can be enforced. The established rules within a DAO organization are immutable, ensuring the fairness of governance and the efficiency and transparency of the DAO organization.

5.3 Governance Rules

DAO is fundamentally designed to facilitate the governance process within the protocol. Through this process, votes are recorded on the blockchain, and results are determined after the voting period. As the platform evolves, more activities will be handled through on-chain governance, which will follow the sequence of proposal introduction, advisory opinions submitted by advisors, council member voting, and various subsequent procedures depending on the voting results.

Individuals with the authority to propose can ensure a vote on each proposal by presenting an introduction. Once a proposal is made, the overseer must conduct an expert analysis of the proposal, submit an opinion statement, and declare the results. Members of the DAO governance committee have the right to vote on introduced proposals and will consider the overseer's opinion statement when voting on what the platform deems as the best option. If the vote count exceeds the threshold, the proposal will be accepted; otherwise, it will be rejected. The subsequent actions of approved proposals will be overseen by the chairperson, who is responsible for implementing all proposals that the council has passed throughout its history. The specific proposal voting and subsequent actions follow the outlined procedure:

1) Core Content

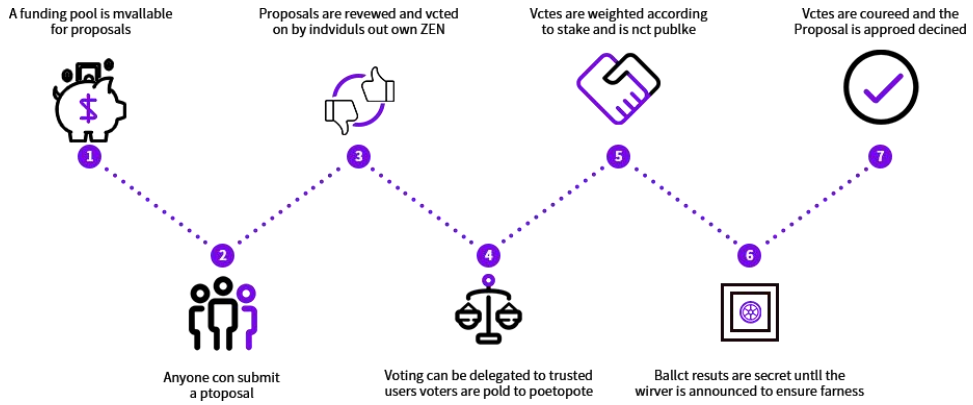
These proposed updates to the codebase are voted on online, but even if the code updates are approved, software updates must occur on a set date to implement the code. Therefore, software updates will also be proposed, and if approved, core updates will follow the established software update schedule.

2) Quantity Changes

Proposers can initiate a vote, which will occur on-chain during the designated voting period. Each voter's choice will be stored in the block header, and once the voting period ends, the vote will automatically close. Once the vote is closed, after the same length of time as the voting cycle, the decision will be automatically executed on the platform.

3) Standard Proposals

Proposals involving the requirement for approval of new standards undergo online voting, and approved proposals will only see official announcements of formally approved standard changes. To provide flexibility and configurability to support the process, Domi Chain will endorse on-chain governance based on the platform's weighted voting rights.



6. Application Scenarios

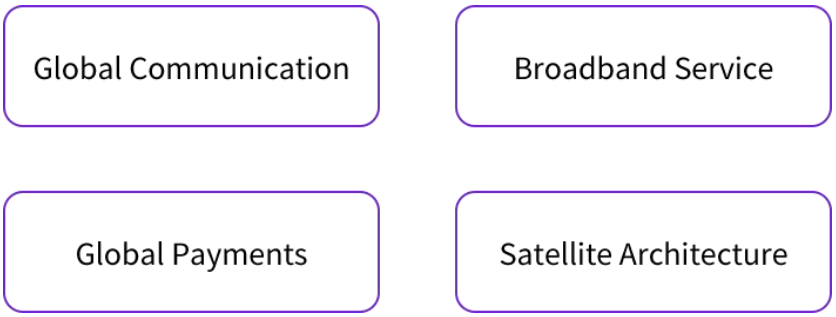
1) Global Communication: Domi Chain offers end-to-end encrypted global telephone and SMS services, ensuring user communication privacy. This technology can be applied in various fields such as government agencies, corporate communication, and the encrypted communication needs between individual users. Additionally, Domi Chain's positioning navigation system can be used for highly secure location services, suitable for industries requiring precise location, such as logistics and emergency response.

2) Bandwidth Services: Similar to SpaceX's Starlink project, Domi Chain's bandwidth services enable people anywhere to access high-speed broadband internet connections. This is significant for remote areas, internet accessibility in developing countries, remote work for institutions and businesses, and meeting the global demand for digitization.

3) Global Payments: Domi Chain drives a global payment revolution, making instant cross-border transfers a reality. This can be applied not only in the financial services sector but also plays a crucial role in supply chain management, accelerating logistics and fund flow. Additionally, Domi Chain provides instant payments for the NFT market, facilitating the trading and circulation of digital assets.

4) Satellite Architecture: Domi Chain's satellite architecture provides a highly secure blockchain network. In addition to ensuring security for global communication and location navigation systems, it also ensures the decentralization of the system. This architecture can be used in strengthening areas such as defense and military communication, as well as various applications requiring high security and decentralization, including smart contracts and digital identity verification.

Domi Chain is not just a blockchain; it is a multifunctional ecosystem that meets global communication, internet access, payment, and security needs. While connecting the world, it ensures the security of data and funds, providing innovative application scenarios to support various fields in the digital age. This highly integrated system will accelerate the adoption of technology, bringing tremendous potential for the development of global society and economy.



7. Team Introduction

Domi Chain's team is composed of a group of passionate and experienced professionals with a profound background and years of practical experience in blockchain technology, satellite technology, traditional finance, and entrepreneurship. The core members of this team include:

Jack Ding

Dr. Ding is Founder and CEO of Domi Chain. Previously he served as Chief Blockchain Officer for BlockJunction and CEO/CTO for Tiptop Wireless Technology. He has 25 years of experience designing and implementing high performance distributed software solutions for Nasdaq, the World Bank, Freddie Mac and Fannie Mae. He has a Ph.D. degree from Dartmouth College, a M.S. degree from Johns Hopkins University, and a B.S. degree from Tsinghua University, Beijing, China.

David Castiel

Dr. Castiel is Chief Satellite Officer for Domi Chain. Previously he served as President and CEO for Virtual Geosatellite and Ellipso. Ellipso was one of only a handful of licensed satellite telephony companies at the inception of the industry, and through its Virtual Geosatellite LLC affiliate pioneered a revolutionary space concept with applications to broadband communications in the commercial and military fields. As founder of these companies, Dr Castiel developed the concepts and patents and directed the domestic and international licensing efforts, the funding and early implementation of the Ellipso system with Boeing as system integrator. In that process Dr. Castiel was instrumental in forging strategic partnerships with the largest aerospace and high technology companies in the world, including Boeing, Westinghouse, Harris, IAI, Lockheed–Martin, and L3–Com.

Ellipso and its affiliates were able to obtain over $100 million in actual investments and further commitments reaching $750 million when it began construction of the Ellipso system. Ellipso and its affiliates established marketing and distribution alliances worldwide with several small and large telecom operators. Dr. Castiel also attracted high–ranking Department of Defense and State Department members to the Board of Ellipso, including the Chairman of the leading launch system company in Europe.

David Castiel received his BS in Physics from the University of Montreal and attended McGill University for the MS program in Solid State Physics. He received his doctorate in Theoretical Solid State Physics, with high distinction, from the University of Paris (Orsay), France, and is a graduate of the Institut Politiques of Paris (Sciences–Po) where he concentrated in Economics and Finance. He was a post–doctoral research fellow at the University of California at Irvine, where he conducted research in Surface Solid State Physics. He has published numerous scientific, technical and business papers, and has been a regular speaker at several industry events. Dr. Castiel holds numerous patents for his inventions and was named among the Satellite 100 in recent years.

Matthew Czarnek

Matthew Czarnek is the Chief Architect of Domichain. He has 8 years of experience in the cryptocurrency field many of which involve working on a startup designed to create a completely decentralized blockchain that gave everyone equal mining rights using social network analysis to verify individuals as unique. This blockchain was also designed for high performance and to dampen unstable price swings.

Mr. Czarnek has 12 years of experience programming for high security projects, 10 of which included working on programs that required high performance. He managed to optimize a video streaming server to accomplish 20x lower CPU usage and to use 20x less memory. This allowed the same servers to handle 20x more streams. He also optimized a crime investigation tool used by the Atlanta Police force to achieve 10x faster performance while using 3x less memory.

Mr. Czarnek has also designed and is currently building a compiler for his own programming language, Flogram. This is the first programming language that is extremely high performance, high security, yet simple and easy to use. Early benchmarks are showing this programming language will be significantly faster than even C++, use 4x less memory than garbage collected languages while also significantly shortening development time.

The Domi Chain team collaborates with top industry consultants and partners, providing strategic guidance and support to the public chain. These professionals and organizations contribute to the strategic direction of the public chain, empowering the platform to achieve greater breakthroughs and accomplishments in Web3.

All team members are dedicated to establishing DomiChain as a globally leading high-performance blockchain platform. Through technological innovation and community collaboration, they aim to assist billions of people in creating assets and accessing networks in a fair, decentralized, and permissionless manner.

8.Roadmap

2018 Q3–2023 Q2

· Product Framework
· Solution
· Market Research
· Blockchain Browser

2023 Q3–2024 Q1

· Product Testing
· Capital Cooperation
· Community Development
· WASM Virtual Machine

2024 Q2–2025 Q2

· Mainnet Launched
· Node Mining
· Token Listing
· Decentralized Storage

2025 Q3–2026 Q2

· More Scenarios
· Multi-Chain Support
· Global Roadshows
· Developer Tools

9.Partners


{redsteep}


Archive
Ventures


logicworks


金色财经


aws


RELIABLE GLOBAL CONNECTIVITY
FOR ANYONE ANYWHERE

10. References

1. Anatoly Yakovenko, Solana Whitepaper, https://solana.com/solana-whitepaper.pdf

2. Jing Chen, Sergey Gorbunov, Silvio Micali, Georgios Vlachos, Algorand Protocol, A Fast and Partition-Resilient Byzantine Agreement Algorithm, https://eprint.iacr.org/2018/377.pdf

3. Team Rocket, Maofan Yin, Kevin Sekniqi, Robbert van Renesse, Emin Gün Sirer, Cornell University, Achieving Scalable and Probabilistic Leaderless BFT Consensus via Subleadership, https://assets.website-files.com/5d80307810123f5ffbb34d6e/60xD3a6445C8Bf5F1A20210910B3390148E2937e4EADnPeUv000000000000