White Paper 3.0

Next-Generation Blockchain Infrastructure Based on Quantum-Resistant Dual Key Mainnet and SSI

—

Version: 3.0

Publisher: SymVerse Foundation

`

SymVerse 3.0 Executive Summary

SymVerse is a next-generation blockchain platform designed with a high-performance consensus engine and fast finality of approximately 1.5 seconds. This platform aims to implement a digital ecosystem that secures both large-scale usability and interoperability by combining a self-sovereign identity (SSI) system with a security architecture prepared for the quantum computing era.

Five Core Innovations of SymVerse 3.0

1. **Dual Key Based Mainnet:** Builds a future-oriented security system through the first dual-key structure that flexibly accommodates both traditional Elliptic Curve Digital Signature Algorithms (ECDSA) and Post-Quantum Cryptography (PQC).
2. **SSI-centric Account System**: All identities are reconstructed into 10-byte Self-Sovereign Identity (SSI) identifiers. This guarantees user-centric data control by combining the cryptographic key version, network number, and public key hash.
3. **CAD(Consensus Authorization Digest)**: Dramatically compresses authorization data during the consensus process, enhancing verification efficiency and solving the problem of blockchain data bloat.
4. **Enhanced Consensus Algorithm:** Maximizes decentralization, fairness, and unpredictability of node selection by combining improved Proof of Stake (PoS) and Verifiable Random Functions (VRF).
5. **Dual Reward Mechanism:** Implements a rational economic model by separating the contributions of consensus nodes and work nodes. Consensus nodes receive PoS mining rewards, while work nodes receive a distribution of Gas from the transactions they process.

Vision & Scalability

SymVerse 3.0 aims to overcome the limitations of legacy blockchains through long-term security, self-sovereign identification, and a practical reward structure. Furthermore, through a Fractal Network where multiple mainnets sharing the same structure are organically connected, it seeks to complete an infinitely scalable blockchain infrastructure optimized for specific service purposes.

Disclaimer

This document is a draft white paper intended to explain the technical architecture and design direction of SymVerse 3.0. This document is not intended as an investment solicitation and does not guarantee an increase in value or profit for specific assets. Actual network specifications, policies, implementation methods, and schedules are subject to change depending on development progress and governance decisions.

Table of Contents

1. Introduction

Purpose of the White Paper

This white paper is written to explain the architecture of the next-generation blockchain mainnet proposed by SymVerse 3.0 and its technical, economic, and industrial significance. SymVerse has continuously developed fast transaction processing, self-sovereign identification, multi-blockchain structures, and real-use-focused infrastructure to overcome the structural limitations of legacy blockchains, and recently, it publicly presented a direction toward Dual Cryptography and a Quantum-Resistant Mainnet to prepare for the quantum computing era.

Problem Awareness of SymVerse 3.0

Legacy blockchains have exposed various limitations in processing speed, scalability, user experience, regulatory alignment, and reward fairness in the process of securing decentralization and security. Furthermore, the advancement of quantum computing raises new questions about the long-term safety of existing public-key cryptography systems. This trend must be recognized as a survival competition for blockchains and a matter of technological sovereignty, and Web3 infrastructure must break away from its dependence on a single cryptographic system.

Structure of the White Paper

This white paper first outlines the challenges faced by next-generation mainnets, and then explains the core innovations of SymVerse 3.0. Following this, it describes the technical structure focusing on the Dual Key Based Mainnet, SSI, CAD, VRF-based consensus architecture, and the new reward mechanism, and finally summarizes the multi-blockchain, user infrastructure, tokenomics, and roadmap.

Comparison between Legacy Blockchain Structure and SymVerse 3.0 Structure

Comparison Item	Legacy Blockchain	SymVerse 3.0 (Innovation)	Core Value

Security System	Single Crypto	Dual Crypto	Response to quantum threats and multi-standard accommodation
Account Structure	Single Address Structure (Anonymous)	Self-Sovereign Identity (SSI / SymID)	User-centric identity and data sovereignty
Data Processing	Consensus Data Bloat	Consensus Authorization Digest (CAD)	Infinite scalability through data lightweighting
Node Selection	Fixed/Probabilistic Selection (Bias)	Verifiable Random Function (VRF)	Security and fairness of consensus node selection
Reward Model	Single Consensus Reward Mechanism (Concentrated)	Dual Reward Mechanism	Coexistence structure between contributors and providers

2. Challenges of Next-Generation Blockchain Mainnets

Lack of Web2-Level Performance and Practical Usability

Legacy blockchain mainnets often suffer disadvantages compared to Web2 services in terms of responsiveness, throughput, and transaction confirmation times due to the message exchange and verification processes required for consensus. SymVerse has historically presented a blockchain that can be used in everyday life as its design goal, continuously emphasizing 1-second block generation and transaction confirmation, multi-blockchain separation structures, and high-performance processing designs.

Single Cryptography Dependency and Quantum Threats

Currently, the address and signature systems of major blockchains are mostly based on ECDSA-family cryptography. Judging that the advancement of quantum computing could threaten existing public-key cryptography in the long term, SymVerse implemented Dual Cryptography, where multiple cryptographic protocols operate independently at the blockchain core, unlike major legacy mainnets that are discussing gradual or hybrid quantum countermeasures.

Absence of Self-Sovereign Identity System

Legacy blockchain addresses are generally strings derived from public keys, which structurally fail to contain version, policy, network affiliation, or identity linkage information. In contrast, SymVerse uses SymID—where the address itself is sovereignty—as an SSI (Self-Sovereign Identity) across the entire blockchain for accounts. This allows individuals to interact with various services while maintaining control over their identity and data. Notably, SymID uses a multi-chain structure to store documents containing information such as public keys, authentication strength, credit, and nationality on the Citizen Chain. These SSI documents maintain the anonymity of the public chain but allow applications to selectively utilize regulatory strength through SSI documents for specific purposes.

Concentrated Reward Systems

In legacy PoS mainnets, there is a strong tendency for rewards to be concentrated based on staking volume or block generation participation. Typically, legacy blockchains like Ethereum adopt a method where nodes participating in the consensus process monopolize and distribute mining rewards and gas fees. Such concentrated reward methods fail to provide motivation for various applications to participate in the network through nodes. To solve this problem, SymVerse 3.0 introduces a reward mechanism that fairly determines compensation by separately evaluating the contributions of consensus nodes and work nodes. Specifically, it applies to mechanism design techniques from economics to determine the distribution ratio fairly.

Necessity and Interoperability of Mainnets with Different Transaction Costs

A blockchain mainnet encompasses diverse transaction parties and various types of transactions. Therefore, if transactions requiring different transaction cost structures are all concentrated within a single mainnet, inefficiencies can occur. Especially as gas costs increase, the demand naturally grows for separate, specialized mainnets capable of

processing transactions requiring low fees, mass-processing transactions, or specialized transactions optimized for specific industry purposes. SymVerse's Fractal Network is designed so that mainnets with different transaction cost structures coexist, while simultaneously interconnecting through SymID to form a single integrated service ecosystem.

Governance and Ecosystem Sustainability Issues

A blockchain ecosystem is not sustained by technology alone. Participants, operators, developers, service providers, and users must all be able to contribute and be rewarded over the long term. Long-term security, self-sovereign identification, fair rewards, and execution-based value distribution are the core challenges that next-generation mainnets must solve.

3. Core Innovations of SymVerse 3.0

1. World's First Dual Key Based Mainnet
2. 10-Byte SymID: A Structure Where the Address Itself is Sovereignty
3. Network Architecture
4. CAD(Consensus Authorization Digest)
5. Improved PoS and VRF-Based Node Selection
6. New Dual Reward Mechanism

3.1 World's First Dual Key Based Mainnet

Quantum Computing Era and Blockchain Security

Quantum computing is a technical variable that fundamentally forces a reassessment of existing public-key cryptography. While Bitcoin and Ethereum are considering gradual or hybrid transitions while maintaining their existing structures, SymVerse is designed to flexibly accommodate various digital signature algorithms, including Post-Quantum

Cryptography (PQC), alongside existing signature methods. This aims for a structure suitable for finance, administration, signatures, and public infrastructure domains that require data integrity and long-term security maintenance even in future quantum computing environments.

Quantum Transition Maintaining Continuity

It is important to accommodate new quantum-resistant accounts without disrupting the account structure of existing users. SymVerse's quantum transition takes the form of a hard fork but is designed so that the network upgrade allows the same chain to continuously operate under expanded rules while fully maintaining existing states, assets, and address systems. Therefore, it operates via an approach that redefines proof-of-authority rules by simultaneously accommodating both the existing cryptographic system and the quantum-resistant cryptographic system.

Independent Operation of Legacy ECDSA and PQC

In SymVerse 3.0, legacy ECDSA keys and PQC keys operate independently without mutual dependence. Users create and sign transactions using the appropriate public key system according to the Key Version indicated by their SSI. The network interprets the Key Version and applies the corresponding verification path. This structure simultaneously provides continuity guarantees for existing user accounts, native accommodation of quantum-resistant new accounts, coexistence of heterogeneous cryptographic systems within the same mainnet, and the possibility of a phased quantum transition.

Differentiation from Existing Hybrid Methods

While a hybrid method is a transitional structure operating ECDSA and PQC address systems in parallel, SymVerse presents a Native Dual Cryptography structure that supports ECDSA and PQC simultaneously at the mainnet level. Transactions include a signature type (SigType), and nodes branch the verification algorithm according to this type. Through this, consensus rules are expanded to accept not only existing ECDSA but also NIST standard post-quantum signatures (e.g., ML-DSA, SLH-DSA, FN-DSA, etc.) as 'formal signatures' of the exact same level. This differentiates it from existing blockchains because it is not a gradual external parallel structure, but a structure where the cryptographic system directly branches internally within the blockchain core execution path.

Balance of Long-term Security and Practical Usability

SymVerse confirms transactions through a process of determining signature type -> checking verification authority by algorithm -> reflecting the state during the transaction approval stage, and limits what the consensus permanently records to a fixed-size summary value of the 'verification passed' result, rather than the original signature. Because blocks bundle these summary values into a single root value and commit them, regardless of which quantum-resistant signature is adopted, it is possible to reduce the trajectory where consensus records continuously inflate in proportion to the signature size.

3.2 10-Byte SymID: A Structure Where the Address Itself is Sovereignty

SymID used in SymVerse advocates "The Address Itself Is Sovereignty". SymID goes beyond a simple wallet address to act as the core structure of Self-Sovereign Identity (SSI) and can be used not only across the SymVerse mainnet but throughout the entire fractal network.

Structure of SymID

SymID consists of a total of 10 bytes. The first 2 bits are the Key Version, the next 14 bits are the Blockchain Network Number, and the remaining 8 bytes are the Public Key Hash-based identification value. SymID is stored on the Citizen Chain alongside a single document (Credential) containing various information.

Key Version

The Key Version indicates which cryptographic key system the account uses, expressed in hexadecimal. For example, if the SymID is '0x0...', it is a legacy ECDSA account, and if it is '0x4...', it can be clearly identified as a PQC account, serving as the core foundation of the Dual Key Mainnet.

Blockchain Network Number

The network number serves to distinguish which network a particular SymID belongs to within a multi-mainnet structure where fractal networks (physically independent blockchains), virtual mainnets (mainnets using different network numbers within the same blockchain), etc., are interconnected.

Public Key Hash

The remaining 8 bytes are derived from the public key hash and link the integrity between the account identifier and the actual public key. This structure signifies that the address is not a simple string, but a self-sovereign identifier created directly by the SymID owner based on their public key.

Field	Length	Meaning	Purpose
Key Version	2bit	Identifies encryption key system version	Distinguishes ECDSA and PQC accounts
Blockchain Network Number	14bit	Identifies network or virtual mainnet	Distinguishes fractal networks and multi-mainnets
Public Key Hash	8 byte	Identifier value linked to public key	Guarantees account integrity and self-sovereign identification

SymID Functions and Service Scalability

SymID enables KYC/AML, SSO, service permission management, account status, credit, authentication strength, nationality, etc., to be stored as documents on the Citizen Chain for future use. Utilizing this, application providers can offer diverse forms of services such as Fintech, IoT account management, or service integration.

Name Service Matching SymID

The Name Service allows users to set a name corresponding to a SymID for use on the SymVerse network, providing the following key functions.

- **Domain name registration and management:** Users can register their desired name on the Citizen Chain and manage it. The registered name is connected to the SSI, enabling users to operate more intuitively on the blockchain.
- **Transaction and service integration:** Registered names can be used to replace SymID in various services within the blockchain. This improves the user experience and enhances the accessibility of blockchain services.
- **Security and privacy protection:** The Name Service provides high-level security and data privacy by leveraging the characteristics of blockchain technology. All

name registrations and transactions are transparently recorded, while the user's personal information is protected.

3.3 Network Architecture

Characteristics of the Consensus Algorithm

SymVerse's consensus algorithm is the world's fastest Byzantine Fault Tolerance (BFT) algorithm, guaranteeing block confirmation times within 1.5 seconds, and is a consensus method that introduces a voting system including a veto right. This is the consensus method used by consensus nodes participating in block generation, where newly generated coins are allocated according to the staking balance of each participating node and candidate node, based on the roles and contributions of each node. The design of the consensus algorithm applied the Gibbard-Satterthwaite theorem of Social Choice Theory to architect the consensus mechanism.

The consensus algorithm consists of 25 consensus nodes, divided into two groups.

- **Group A:** Consists of 9 nodes selected by the foundation. Group A nodes hold a certain amount of deposit and can only exercise voting rights. They can collectively exercise a veto to prevent collusion among consensus nodes.
- **Group B:** Consists of 16 consensus nodes selected from candidate nodes holding deposits, and each node performs a specific role in the consensus process. A Primary node is selected via VRF among the 16 consensus nodes for every block generation.

Block sizes may vary depending on the block type. The Primary node verifies transaction records and requests the consensus nodes to verify them. If two-thirds or more of the consensus nodes approve the block, the Primary node records the signatures of the nodes that participated in the verification, and the generated block achieves finality. The Primary node propagates the generated block to all nodes. Simultaneously, consensus participation details are recorded in the Warrant Block, and the coins generated per block are distributed to consensus nodes every 2,400 blocks.

Prevention of Manipulation by Malicious Nodes

The consensus algorithm fundamentally prevents the possibility of block manipulation by malicious nodes for the following reasons.

There is Group A holding collective veto power, making it impossible for the elected consensus nodes in Group B to collude for profit. Also, because all transactions sent from wallets must pay a network fee, any Sybil Attack from a malicious wallet would incur massive Gas fee costs, allowing work nodes to fundamentally block them. In the case of malicious wallets, work nodes conduct primary verification, and if a work node is malicious or behaves improperly, it cannot become a consensus node candidate.

Prevention of MEV (Maximal Extractable Value)

If block generation times are long, such as in Ethereum or Solana, the Primary node can manipulate the transaction order within a block using Gas fees. Among the approximately 1.5 seconds required for SymVerse's consensus, the block generation time averages 0.3 seconds, making it difficult to implement MEV through external programs. Because the Gas fee for all transactions is the same, and the Primary node records transactions in the exact order received from the work node, manipulating transaction order is impossible.

Overall Network Architecture

SymVerse 3.0 utilizes the existing structure of SymVerse 2.0 but takes a design approach that separates consensus, execution, identification, and service functions by role unit by strengthening the functions and roles of consensus nodes, work nodes, and wallet nodes on the network. This simultaneously secures security and processing efficiency.

A wallet with an account always processes transactions through a work node connected to the blockchain. The work node list is frequently updated, and all communication from the wallet node is processed by connecting to 3 work nodes. If connection to a specific work node fails, another work node is selected. Work nodes process transactions received from wallets and deliver them to consensus nodes. After transaction details are shared with consensus nodes, a new block generated through the consensus process is propagated to the blockchain.

Consensus Node

Consensus nodes are the core nodes participating in block proposals, verification, and final consensus, consisting of Group A with 9 nodes and Group B with 16 nodes. Under the

improved PoS structure, a new node is randomly set as a consensus node from the pool of candidate nodes participating in Group B, and the oldest consensus node reverts to a candidate node. 30% of the Gas generated in every block is distributed to consensus nodes every 2,400 blocks.

Work Node

Work nodes collect user transactions, verify validity, relay them to the network, and support the DApp execution layer. In SymVerse, work nodes are considered value producers for actual service processing, and 70% of the total Gas aggregated every 2,400 blocks is distributed according to the weight of each work node's credits.

CA Node

The CA (Citizens Alliance) node is a core node for SymID issuance and related document management, operating as a passive network component through its own SymID. Every mainnet is issued a CA node account through an issuance server holding the SymVerse Foundation's Master CA account, and all mainnet components, such as wallets or nodes, are issued SymIDs via the CA nodes.

SymScan

SymScan functions as the infrastructure for querying transactions, accounts, consensus, and reward statuses on the SymVerse blockchain network. (https://scan.symverse.org)

Sallt

Sallt is a self-sovereign wallet hub where owners directly manage all assets without a central administrator, acting as a connection point linking communication between fractal networks and external mainnets based on the SSI, SymID. (https://sallt.io/)

SymPose Integrated Development Environment (IDE)

SymPose is an execution environment for deploying smart contracts and services, and its features can be utilized by integrating with the Sallt wallet.

3.4 CAD(Consensus Authorization Digest)

Concept and Role of Consensus Data and CAD

SymVerse applied CAD (Consensus Authorization Digest) technology to its architecture to solve the problem of structural blockchain bloat that occurs when adopting PQC. CAD technology separates heavy signature data during the consensus process while applying PQC signatures, and records only a lightweight, fixed-size (32-byte) CAD, maintaining proof size and maximizing overall efficiency.

Consensus Data Condensation Method

CAD organizes the core data required to maintain consensus node approval status, quorum fulfillment, and verifiability into simple verification units, allowing the legitimacy of blocks to be confirmed efficiently. Compared to existing ECDSA-based consensus data, it stores consensus data at 50% of the size in the blockchain's CADRoot.

Contributions of CAD

CAD aims for consensus data size reducstion, propagation cost savings, verification efficiency improvement, storage burden reduction, and scalability improvement when node counts increase. This is a structure that reduces consensus data while maintaining consistency and verifiability, which aligns with SymVerse's emphasized direction of balancing security and practical performance.

Comparison of Consensus Data Processing Characteristics Before and After CAD Adoption

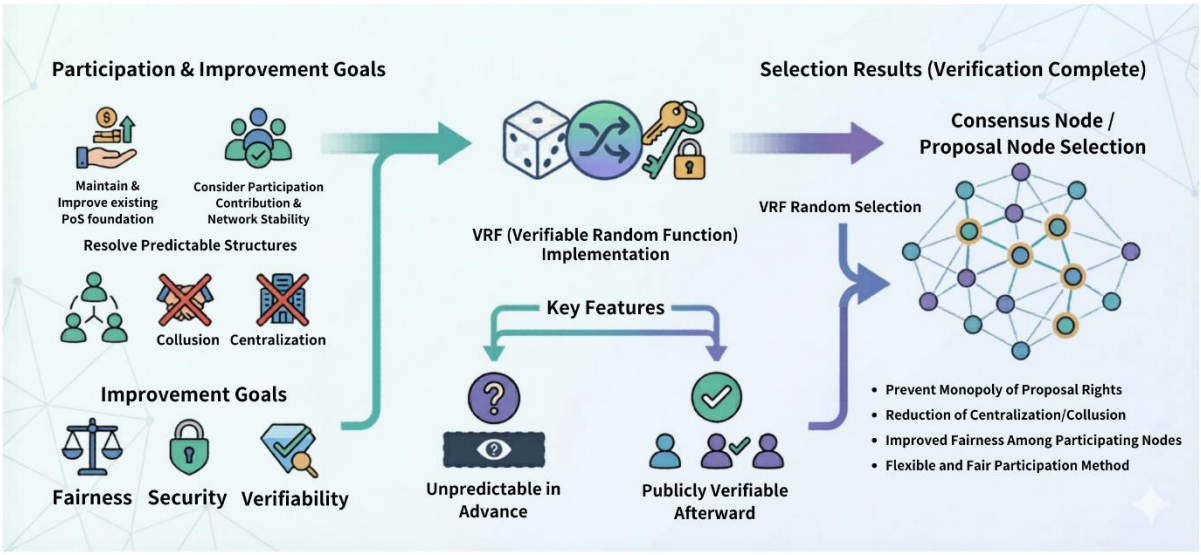
Item	Legacy Structure	CAD Applied Structure
Consensus Data Size	Increases as approval info and metadata accumulate	Records only summarized core approval results (32 bytes)
Verification Complexity	May require reinterpreting entire consensus history	Fast verification possible based on summary structure
Propagation Efficiency	Increases message and data volume	Reduces propagation burden with condensed data
Storage Efficiency	Expands node storage burden	Improves storage efficiency through lightweight consensus results

3.5 Improved PoS and VRF-Based Node Selection

SymVerse 3.0 maintains the legacy PoS structure but designs the participation and addition methods of consensus nodes to be more flexible and fair. The selection of consensus nodes and proposing nodes is improved in a direction that simultaneously considers participation contribution, network stability, fairness, security, and verifiability.

Because a predictable selection structure can induce collusion or centralization, VRF (Verifiable Random Function) is introduced to impart verifiable randomness to the selection process of consensus nodes and proposing nodes. VRF provides a random selection structure whose results are difficult to predict in advance but can be verified by anyone afterward. This makes it difficult for specific nodes to continuously monopolize proposal rights or be selected as consensus nodes. The VRF-based structure features unpredictability in node selection, improved fairness among participating nodes, reduced likelihood of centralization or collusion, and the assurance of post-verification capability.

VRF-based Consensus Node / Candidate Node Selection Structure



3.6 New Dual Reward Mechanism

PoS Reward Mechanism

All nodes in the SymVerse network can participate in the consensus process by depositing

a certain amount of SYMM into their accounts as a deposit. Consensus nodes participating in the consensus process receive distributions of generated SYMM every 2,400 blocks.

SymVerse considers the total amount of SYMM deposited by nodes as a deposit to be equal to the total amount of mining power (NodePower: SNP). Therefore, each node participating in PoS is made to hold an equal amount of NodePower. Furthermore, each consensus node distributes the mined SYMM to NodePower holders according to their respective ratios.

NodePower is generated at a 1:1 ratio on the SymVerse mainnet and can be held and circulated by consensus nodes. One NodePower can mine SYMM proportionate to the ratio of (1 / total NodePower quantity).

Conditions for PoS Participation

- **Consensus Nodes:** Group A consensus nodes must hold a minimum SYMM deposit, and Group B must hold a minimum amount of NodePower.
- **Work Nodes:** All work nodes must hold the same amount of NodePower as Group B to mine.

Category	Group A Consensus Node	Group B Consensus Node	Consensus Node Candidate Group
SYMM Deposit	6,000,000	X	X
Minimum NodePower	X	6,000,000	6,000,000

Properties of NodePower

- **Perpetuity:** The amount of NodePower proves a permanent ability to mine SYMM. Every time SYMM is generated in a block, it is distributed to registered mining accounts.
- **Upper Bound:** The supply quantity of NodePower is limited and can only be issued within the amount of SYMM held by the foundation.

Improvement of Legacy PoS Reward Mechanism

Legacy PoS rewards tend to be concentrated on block generation and staking weight. SymVerse 3.0 separates network security contributions and service execution contributions, and designs corresponding separated rewards. Consensus nodes receive PoS mining rewards, and work nodes receive a distribution of Gas from the transactions they processed. This aims to evolve the blockchain from a simple staking economy into a reward distribution structure based on actual usage.

In SymVerse 3.0, Gas functions beyond a simple fee, acting as financial resources for distributing execution layer contributions. This structure forms a new paradigm called Gas Mining. The new reward mechanism leads to separated rewards for consensus contribution and execution contribution, a structure where increased practical use translates directly to increased rewards, expanded service node participation, and a transition from capital-centric rewards to contribution-centric rewards.

When work nodes receive rewards according to their transaction execution contributions, DApp and service operators acquire a direct economic incentive for network activation. This expands the usability and diversity of the ecosystem. This distribution system determines the distribution ratio of the total Gas amount based on papers grounded in mechanism design theory from economics. These distribution ratios can be adjusted long-term depending on the size of mining rewards and Gas rewards.

SymVerse 3.0 Dual Reward Mechanism

This figure illustrates the SymVerse 3.0 dual reward mechanism. It demonstrates the structure in which Consensus Nodes receive PoS Mining Rewards while Work Nodes receive Gas Distributions and outlines the flow of how User and DApp activities drive this reward system.

4. Multi-Blockchain Data Structure

Multi-Blockchain Design Principles

SymVerse utilizes a multi-blockchain structure that separates transaction, identification, consensus, and policy data into functional chains. This serves as the foundation for the fractal network SymVerse envisions, enabling an expandable mainnet structure where mainnets with the same structure are distinguished by network numbers yet can directly

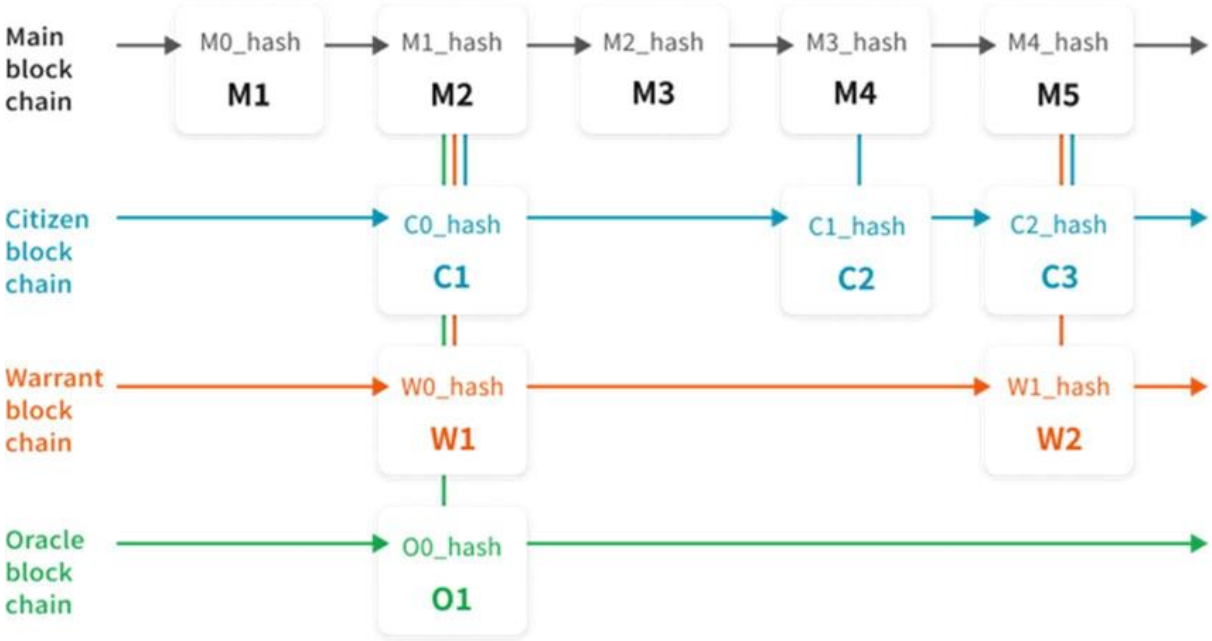
interoperate. The functions and primary roles of each blockchain are as follows:

- **Main Chain:** Records transactions, rewards, gas distribution, and execution results. It guarantees Block Finality upon block generation, with an average block generation time of under 1.5 seconds.
- **Citizen Chain:** Records SymID, account status, credential documents, and identification-related data.
- **Warrant Chain:** Records consensus participation information, CAD, verification status, and node activity history.
- **Oracle Chain:** Records policy parameter changes, cross-chain linkage information, external data, governance results, etc.

Inter-Chain Data Linkage Structure

By separating data functionally, the entire system is not bound by the bottleneck of a single chain even if transaction volume increases. Additionally, this structure provides applications with quick access to utilize the functions of each chain, and major chain data is processed in real-time in the MemPool, offering fast data processing speeds.

Multi-blockchain Structure



Interconnectivity Between Blockchain Mainnets

Blockchain mainnets encompass diverse transaction parties and diverse transaction types.

Therefore, if transactions requiring different gas structures are mixed within a single mainnet or if overall gas costs rise, demand naturally increases for professional separate mainnets capable of handling transactions requiring low fees, or specialized transactions optimized for specific purposes. Reflecting this reality, SymVerse's fractal network is designed so that mainnets sharing the same structure but possessing different network numbers can be directly interconnected.

Blockchain integration can be achieved by registering with each other's oracle chains. Fractal chains registered on the oracle chain allow a SymID from one blockchain to operate on another blockchain through connections between CA nodes. Through this, specific networks can be optimized for low-cost, high-volume transactions, while other networks are optimized for high-value-added or professional service processing, and while each mainnet operates independently, applications can interconnect multiple mainnets as needed to form a single integrated service ecosystem. Consequently, the fractal network is a core concept that expands the SymVerse ecosystem by simultaneously accommodating transaction cost diversity, service specialization, and network scalability.

5. Sallt and User-Centric Sovereign Infrastructure

Sallt is a self-sovereign wallet that allows users to directly manage their assets, accounts, and access permissions. Sallt is an independent application that acts as the hub of the fractal network connecting all SymVerse-based mainnets.

The main features of Sallt are as follows.

- **Dual Account:** Functions as a user hub that manages both ECDSA-based accounts and PQC-based accounts.
- **SymID Integration Feature:** Based on SSI, it becomes a user interface supporting linkages with account versions, network affiliations, and credential documents.
- **Web3 Service Hub:** Operates as a network hub connecting various mainnets within the fractal network, and functions as a core platform connecting Web3 service access, DApp authentication, and various services beyond a digital asset storage medium.

- **Mainnet Universality:** Different networks such as Bitcoin, Ethereum, Polygon, Tron, Binance Smart Chain, etc., can be registered and operated.
- **OS Universality:** Provides applications with identical functionalities across Android, iOS, Mac OS, Windows, etc. Through this, users can conveniently use the same wallet across multiple devices.
- **Enhanced User Connectivity:** Supports social features allowing users to add friends through a Name Service that uses intuitive names instead of complex addresses, and to simultaneously perform real-time chats and transfers within the wallet.

6. Tokenomics and Ecosystem Value Circulation

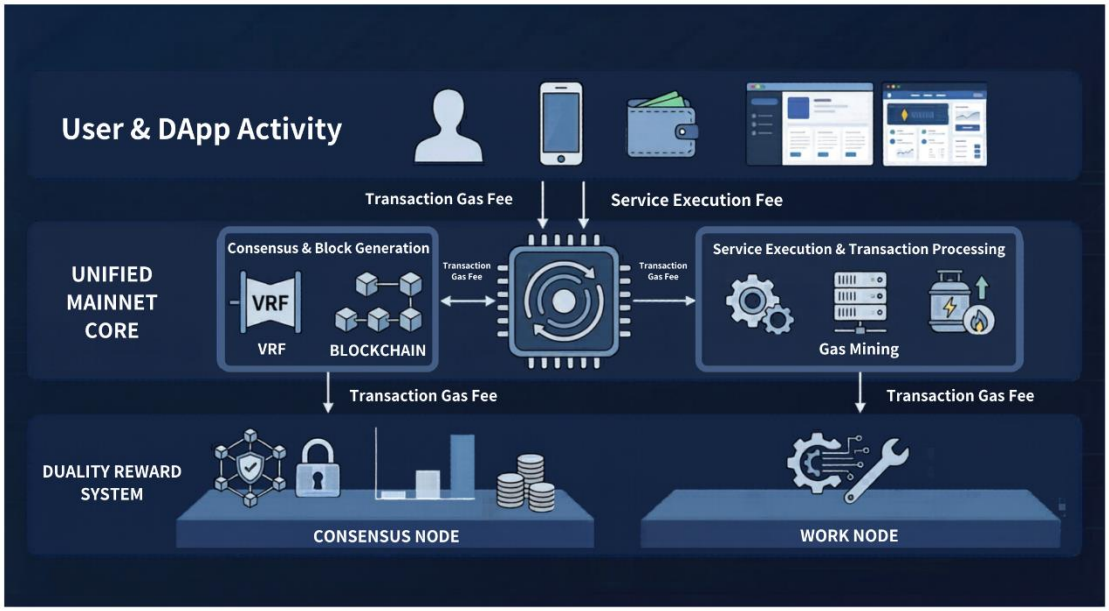
Role of Tokens and Value Circulation

In the SymVerse ecosystem, tokens are not simple investment assets, but value mediums connecting security, execution, service, and governance.

Token staking is the foundation of consensus participation and security maintenance, and consensus nodes receive PoS mining rewards in exchange for this. Additionally, transaction execution is performed through the contributions of work nodes, and the Gas generated in this process becomes the reward resource for execution contributions. As DApp and service usage increases, transaction execution grows, leading to an increase in work node rewards. Simultaneously, as the demand for network security also increases, it connects to the consensus node reward structure.

Ultimately, SymVerse aims for a value circulation ecosystem where staking, consensus, execution, service usage, and reward distribution are interconnected so various applications operate.

Value Circulation Ecosystem Structure of SymVerse 3.0



Issuance and Circulation of SYMM and SYM (ERC-20)

In SymVerse 1.0, 900 million SYMM were initially issued after the mainnet was completed. Out of the 1 billion SYM (ERC-20) mentioned in White Paper V1.0, the circulating volume is scheduled to be fully exchanged into SYMM according to the exchange schedule provided by the foundation. Once the exchange of circulating SYM (ERC-20) from the initially issued 1 billion SYM (ERC-20) is completed, SYM (ERC-20) will not be circulated and will be permanently retired.

In SymVerse 2.0, 6 million SYMM is staked in each of the 25 mainnet nodes. Excluding the total 150 million SYMM staked out of the initial 900 million SYMM, 750 million SYMM are retired through burning, etc. Therefore, on the SymVerse mainnet, only SYMM staked in PoS and mined SYMM are circulated.

All general management associated with SYMM circulation, such as market supply, burning, recovery, and coin conversion, is executed by the foundation.

Exchange of SYMM and SYM (ERC-20)

Starting in 2025, SYM (ERC-20) is exchanged for SYMM mined by the foundation. In SymVerse 2.0, mining is based on the initial 150 million SYMM. 1 billion SYM (ERC-20) were issued, but excluding the 100 million mining allocation, the total volume is 900 million. Therefore, theoretically, the initial baseline 150 million SYMM must be exchanged with 900

million SYM (ERC-20), making the exchange ratio between SYMM and SYM (ERC-20) 1:6.

Because the SYMM volume for SYM (ERC-20) exchange is secured through SNP held by the foundation, it is exchanged through mining over a certain period. The exchange is conducted every 2 months for a total of 18 months, distributing SYMM equivalent to 1.18 times the total exchange volume across 9 installments.

The exchange method involves first exchanging SYM (ERC-20) for a new exchange proof token (SCT21), after which it is finally paid as SYMM during the corresponding period, and the fee (Gas) required to transfer SYM (ERC-20) to the foundation is borne by the SYM (ERC-20) holder. Once exchanged for SYMM, it cannot be exchanged back for SYM (ERC-20).

Details regarding the exchange will be announced at https://swap.symverse.org.

SYMM Supply Function Upon Block Generation

The SYMM supply function takes the form of a step function where the coin mining amount halves every 47,000,000 blocks.

Based on the minimum block generation time of 1.5 seconds, the maximum number of blocks generated annually is under 22,687,770. The maximum size of SYMM mined over 20 years is 367,920,000 SYMM.

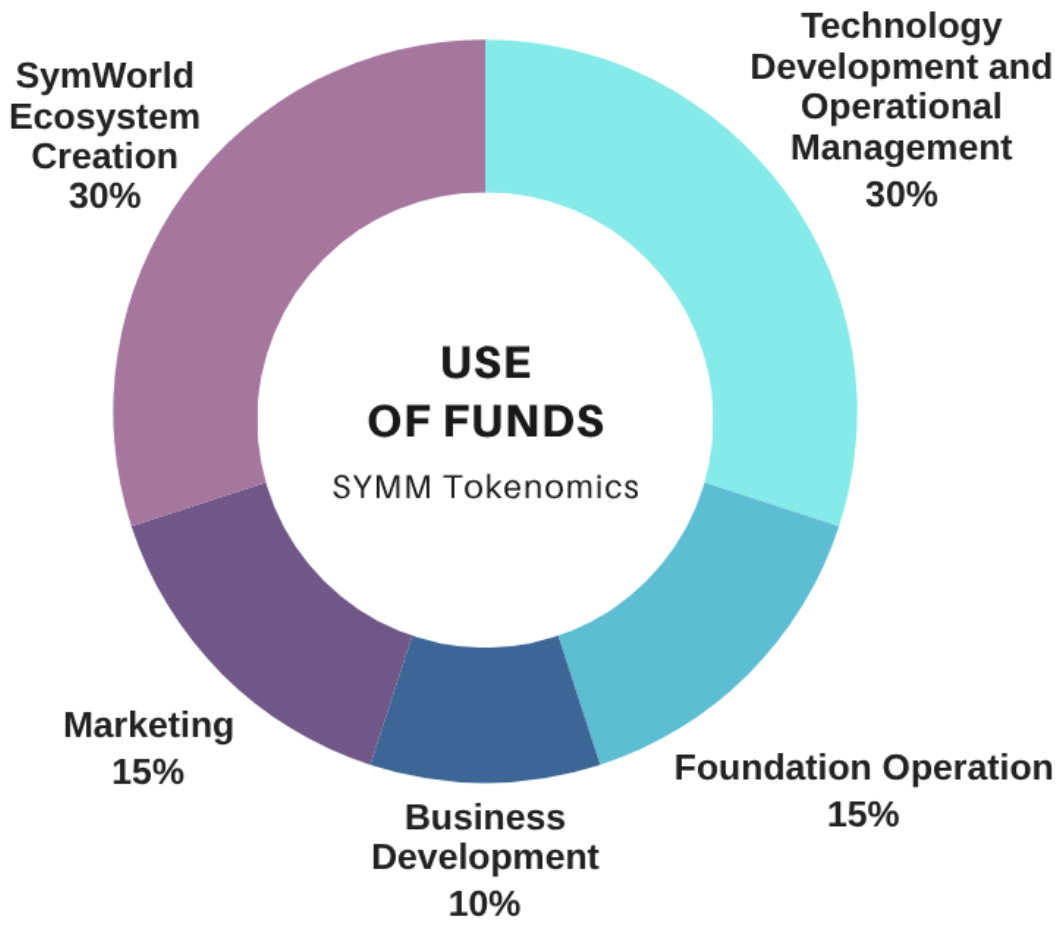
The following table indicates the expected annual SYMM mining volume.

Estimated Year	Total Mining Amount per Block	Annual Mining Amount	Daily Mining Amount	Daily Mining Amount per SNP	SYM Mining Amount per SNP
2024	4.00	84,096,000	230,400	0.001536	0.56
2025	4.00	84,096,000	230,400	0.001536	0.56
2026	2.00	42,048,000	115,200	0.000768	0.28
2027	2.00	42,048,000	115,200	0.000768	0.28
2028	1.00	15,768,000	43,200	0.000288	0.11
2029	1.00	15,768,000	43,200	0.000288	0.11
2030	0.75	10,512,000	28,800	0.000192	0.07
2031	0.75	10,512,000	28,800	0.000192	0.07
2032	0.50	8,409,600	23,040	0.000154	0.06
2033	0.50	8,409,600	17,280	0.000154	0.06
2034	0.40	6,307,200	17,280	0.000115	0.04
2035	0.40	6,307,200	11,520	0.000115	0.04
2036	0.30	4,204,800	11,520	0.000077	0.03
2037	0.30	4,204,800	11,520	0.000077	0.03
2038	0.20	4,204,800	11,520	0.000077	0.03
2039	0.20	4,204,800	11,520	0.000077	0.03
2040	0.20	4,204,800	11,520	0.000077	0.03
2041	0.20	4,204,800	11,520	0.000077	0.03
2042	0.20	4,204,800	11,520	0.000077	0.03
2043	0.20	4,204,800	11,520	0.000077	0.03
Total	-	367,920,000	-	-	2.48

Use of Funds

The SYMM held by the foundation is allocated as follows to provide balanced support for the growth, sustainability, and ecosystem expansion of SymVerse.

- **Technology Development and Operational Management:** 30%
- **Foundation Operation:** 15%
- **Business Development:** 10%
- **Marketing:** 15%
- **SymWorld Ecosystem Creation:** 30%



7. Roadmap

History

2018

- SymVerse Corporation Founded

2019

- SymVerse Dubai Corporation established
- Decentralized wallet SymWallet launched
- Acquired world's first patent for multiple blockchains
- Acquired patent for node proof method consensus process and blockchain generation method
- Listed on global exchange DigiFinex
- Mainnet V1.0 released

2020

- Passed TTA (Telecommunications Technology Association) certification test by Ministry of Science and ICT
- Acquired GS Certification Class 1 for the first time in the blockchain wallet sector
- Blockchain-based voting protocol developed
- Acquired patent for digital identification system (DID) using distributed ledgers

2021

- BBP (Blockchain Broker Platform) developed
- SymScan site opened
- SymVerse mainnet integrated into 2 domestic exchanges
- CAII (DID Authentication Server) standard announced
- Decentralized blockchain wallet Sallt launched

2022

- SVM (SymVerse Virtual Machine) developed
- Smart contract development environment SymPose launched
- Blockchain integration module developed
- Fractal/Virtual Mainnet Solution launched

2023

- Content community platform Communy launched
- Sallt, SymPose versions updated

2024

- Core network TPS (transactions per second) performance improved
- PoS mechanism upgrade
- Mass transfer system launch
- Wallet Provider upgrade
- SymVerse 2.0 (Proof of Stake and Soft Mining) launch

2025

- SymID Name Service (SCT31) and related DApp service launches
- Scan 2.0 portalization including SymID login feature
- Retirement of 750 million SYMM via burning, etc.
- Blockchain internal parameter adjustment function using Oracle Chain
- Consensus node replacement and addition functions via Oracle Chain

RoadMap

2026~

- Sallt V2 launch integrated with various DApp functionalities
- SymVerse 3.0 (Quantum-resistant Mainnet and SSI-based infrastructure) launch

- CAD (Consensus Authorization Digest) application
- Reward mechanism upgrade
- VRF (Verifiable Random Function) applied to consensus algorithm
- BaaS portalization for various token and NFT providers
- SYM (ERC-20) retirement