



Whitepaper SimpleChain 2.0

*The Global RWA Infrastructure Layer
- Powered by Granular Data*

Released in November 2025

SimpleChain Whitepaper v2.1

Abstract

SimpleChain 2.0 is a dedicated blockchain infrastructure focused on Real-World Assets (RWA). It addresses the pain points of traditional public blockchain in RWA scenarios, such as ambiguous asset ownership verification, low data credibility, difficulties in implementing fragmented transactions, and inefficient cross-ecosystem collaboration. Centered on end-to-end trusted data services and digital asset liquidity services, SimpleChain 2.0 establishes a two-way internal-external circulation system. Through a "technology-data-compliance" trinity design, it covers the entire lifecycle of RWA, ultimately achieving seamless integration between physical assets and the digital economy, and providing low-threshold, high-security, and highly compliant RWA transaction services for global institutions and individuals. SimpleChain's mission is:

“To enable every real-world asset to freely, securely, and compliantly
circulate on the blockchain.”

From a global perspective, since 2024, stablecoins and RWA practices have entered a "system-level financial restructuring competition": the U.S. has enacted legislations including the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), the Digital Asset Market Clarity Act (Clarity Act), and the Anti-Central Bank Digital Currency (CBDC) Surveillance State Act; Hong Kong will implement the Stablecoin Regulation in 2025; the EU has incubated RWA projects such as green bonds based on the Markets in Crypto-Assets Regulation (MiCA). At the market level, the on-chain RWA scale reached USD 15.4 billion by the end of 2024 (up 80% year-on-year) and is expected to grow to USD 16 trillion by 2030.

To adapt to market development and application needs and address the bottlenecks of traditional public blockchain, SimpleChain 2.0 takes "granular data" as

its technical foundation and adopts a three-tier support system: the data collection layer connects to the Internet of Things (IoT) and offline compliance systems in real time; the on-chain storage layer balances security and efficiency through "main chain storing core information + sub-chain storing high-frequency data"; the data interaction layer enables cross-ecosystem interoperability via unified protocols. Through the above design, SimpleChain 2.0 reduces RWA investment thresholds, strengthens the "digital-physical" anchoring, improves compliance efficiency, and lowers operating costs.

In terms of technical architecture, SimpleChain 2.0 has built a full-stack system adapted to RWA comprises three layers: technology layer, RWA service layer, and application layer. Technology layer provides a high-performance, low energy consumption, cross-ecosystem compatible blockchain infrastructure. RWA service layer hosts the DataIPO issuance protocol, the CaaS compliance engine, the Oracles data bridge, and the RWA Data Credit system. Application layer builds use cases such as the RWA Launchpad, RWA DEX, and RWA Earn, endowing assets with genuine market liquidity. On this foundation, it will undergo upgrades in three phases: the "Mercury" phase in Q3 2025 will switch from Proof of Work (PoW) to Proof of Stake (PoS), reducing energy consumption by over 99%, the "Copper" phase in Q4 2025 will optimize the economic model; the "Tungsten" phase in 2026 will integrate PoS with HotStuff to form a hierarchical consensus mechanism. Oracles achieve trusted two-way communication between on-chain and off-chain systems through decentralized nodes and multi-data sources, the compliance framework adapts to global multi-regional regulatory requirements through modular execution units, programmable rules, hierarchical supervision nodes (with three-tier permissions: "read-only - early warning - emergency response" for both financial and data compliance), and real-time audit reports.

The economic system of SimpleChain 2.0 is centered on the main chain token SRW (used for paying Gas fees, cross-chain fees, etc.), with its total supply dynamically adjusted as sub-chains are connected. To ensure ecological balance, multiple types of adjustment mechanisms are established, including node lock-up,

node staking rewards, etc. The node lock-up mechanism sets a minimum threshold and builds a co-created lock-up pool of "validator self-lock-up + user delegated staking", while supporting compliant transfer of validators; the node staking reward mechanism is divided into two phases: the "Mercury" phase adopts fixed block rewards, and the "Copper" phase upgrades to a dual-track system of "basic rewards + contribution rewards"; the burning mechanism adjusts circulation volume through "differentiated fee burning by transaction type, regular buybacks, and penalty burning for violations"; the voting mechanism anchors voting rights to lock-up volume, covering three types of proposals (basic parameters, mechanism rules, and emergency adjustments) to ensure scientific decision-making.

Ecological development achieves value growth through "foundation-driven - benefit stacking - excess returns": the foundation layer attracts traditional enterprises and emerging industries relying on RWA while anchoring public blockchain value; the benefit stacking layer amplifies value through scale effects (asset scale → positive liquidity cycle), synergy effects (cross-asset linkage creating additional returns), and leverage effects (structured financial tools amplifying returns); excess returns come from liquidity revaluation (valuation increase of low-liquidity assets after on-chaining), cross-border dividends (globalization reducing transaction costs and converting them into blockchain service fees), and technological iteration (innovative technologies spawning new scenarios).

The SimpleChain Foundation is a non-profit organization composed of the Foundation Council and the Foundation Technical Steering Committee. Adhering to the principle of "value on-chaining and physical asset on-chaining", it nurtures developer communities and empowers the development of emerging economies such as AI and Web3.

Content

1 Overview	1
1.1 Background	1
1.2 Core Positioning	2
1.2.1 Pain Points of Traditional Public Blockchain in Adapting to RWA Scenarios	3
1.2.2 Promotion of Granular data to RWA Ecosystem	4
1.3 Mission	5
1.4 Ecological Development Plan	6
2 Design Principles	8
3 SimpleChain Main-chain Upgrade	9
3.1 Phase 1: Consensus Adjustment	9
3.2 Phase 2: Economic Model Upgrade	9
3.3 Phase 3: HotStuff Mechanism Upgrade	10
4 Overall Architecture Design	11
4.1 Technology Layer	11
4.1.1 Main Chain Consensus Layer	12
4.1.2 Hierarchical Expansion System	18
4.1.2.1 Multi-L2 Sub-chain Support Architecture	18
4.1.2.2 Enterprise-Grade Node Network Architecture	19
4.1.3 Oracle for Ensuring Data Credibility	20
4.1.3.1 Oracle Overview	20
4.1.3.2 Core Functions	20
4.1.3.3 Key Features	21
4.1.4 Cross-Chain and Multi-Scenario Support	22
4.1.4.1 Secure Cross-Chain Mechanism	23
4.2 RWA Service Layer	25
4.2.1 Core Logic	25
4.2.2 Technical Framework	26
4.2.3 System Components and Execution Logic	27

4.2.4 Oracle Components: Modular Data Service Architecture	29
4.2.4.1 Fact Oracle — Business Event Data Oracle	29
4.2.4.2 Price-Oracle — Hybrid Asset Pricing Oracle	29
4.2.4.3 RWA Data Credit System — On-Chain Credit Framework	30
4.2.5 Core Value	32
4.2.6 Application Scenario Examples	32
4.3 Application Layer	32
4.3.1 RWA Launchpad	33
4.3.2 Yield Aggregation Protocol	33
4.3.3 Compliance-Oriented Asset Exchange	34
4.3.4 Structured Credit	34
4.3.5 Liquidity Bridge	35
5 Economic System Design	36
5.1 Main-chain Token SRW	36
5.2 Token Function	37
5.3 Token Supply and Allocation	37
5.4 Revenue and Deflationary Model	38
5.5 Core Mechanisms of Economic Model	38
5.5.1 Node Lock-up Mechanism	38
5.5.2 Node Staking Reward Mechanism	40
5.5.2.1 Fixed Reward System	40
5.5.2.2 Dual-Track Reward System	42
5.5.3 Burning Mechanism	46
5.5.4 Voting Mechanism	47
5.6 Self-driven Positive Feedback Loop Mechanism	49
6 Global Compliance	51
6.1 Compliance Execution Unit	51
6.2 Programmable Rules	52
6.3 Tiered Regulatory Node Permissions	52
6.4 Intelligent On-Chain Activity Audit Report	54

6.5 Specialized Safeguards for Cross-Border Data Security	55
7 Ecological Development	57
7.1 Fundamentals Drive	57
7.2 Benefit Accumulation	59
7.3 Exceeding Expectations in Earnings	62
8 SimpleChain Foundation	64
8.1 Mission and Vision Statement	64
8.2 Standing Bodies of Foundation	64
8.3 Source of Foundation Funds	64
8.4 Team and Technical Council	65
Appendix and Reference Index	65
A. Technical Interface Examples	65
DataIPO Interface Sample	65
CaaS Audit Template Example	66
B. Technical Specifications Summary	66
Conclusion	66

1 Overview

1.1 Background

1. Global Regulatory Restructuring

Since 2024, the Web3.0 technology system, stablecoin mechanisms, and RWA on-chaining practices have been evolving rapidly worldwide. They have shifted from partial experiments at the technical and industrial levels to a "system-level financial restructuring competition" led by various regions. Essentially, this competition is a global game centered on data ownership mechanisms, value anchoring systems, and credit circulation rules in the digital era, which is reshaping the underlying logic of future financial and industrial governance. In this competition, regulatory frameworks and strategic layouts of different countries and regions show significant differences:

- The U.S. has built a regulatory moat through intensive legislation. In July 2025, the House of Representatives successively passed 《Guiding and Establishing National Innovation for U.S. Stablecoins Act》 (the GENIUS Act), 《Digital Asset Market Clarity Act》 (the Clarity Act), and 《Anti-Central Bank Digital Currency Surveillance State Act》 (the Anti-CBDC Surveillance State Act) .
- Hong Kong will implement the 《Stablecoins Ordinance》 in August 2025, establishing the world's strictest stablecoin regulatory framework. It requires 100% reserve support for stablecoins and daily disclosure of asset composition, and allows multi-currency reserves (e.g., Hong Kong Dollar, U.S. Dollar, offshore RMB), forming differentiated competition with the single-currency anchoring of the U.S. GENIUS Act.
- The EU has established a pan-European unified standard based on the MiCA Regulation. The Luxembourg regulatory sandbox has incubated a number of RWA projects covering green bonds, art collections, and other categories. According to World Bank data, the number of investors participating in global asset allocation through RWA in Southeast Asia has increased by 300% in two years, highlighting the key role of regulatory policies in market penetration.

2. In-depth Coupling of Technological Breakthroughs and Market Prospects

RWA is reshaping the global financial landscape and becoming a core link connecting the real economy and the digital economy. This process converts traditional assets (such as bonds, commodities, intellectual property rights, and technology innovation industries) into programmable digital tokens, enabling ownership segmentation, efficient transactions, and transparent management through blockchain technology.

Latest market data shows that the total on-chain RWA scale (excluding stablecoins) reached USD 15.4 billion by the end of 2024, up 80% year-on-year. As of August 23, 2025, the U.S. Treasury RWA market scale was approximately USD 7.4 billion, an increase of 370% compared with 2024. Institutional application scenarios have continued to make breakthroughs: in November 2024, Ripple collaborated with Archax to tokenize abrdn's USD 4.77 billion liquidity fund; Japan's GATES Corporation on-chained USD 75 million of Tokyo real estate through the Oasys platform, enabling minimum transaction shares of USD 100,000, with significantly improved liquidity compared to the traditional market; the Centrifuge protocol focuses on accounts receivable of small and medium-sized enterprises (SMEs), helping enterprises reduce financing costs by 2.3 percentage points. More forward-looking forecasts indicate that the global RWA market scale will reach USD 16 trillion by 2030, accounting for 10% of investable assets. A RedStone report predicts that the asset tokenization ratio will be 10%-30% between 2030 and 2034.

1.2 Core Positioning

SimpleChain 2.0 focuses on end-to-end trusted data services and digital asset liquidity services, establishing a two-way internal-external circulation system. Different from the "pan-scenario design" of general public blockchain, SimpleChain2.0 takes "granular data" as its foundation and builds a technical system adapted to the entire lifecycle of RWA through a "technology-data-compliance" trinity design.

SimpleChain covers diverse RWA categories, aiming to provide "low-threshold, high-security, and highly compliant" RWA digital transaction services for global institutions and individuals, and ultimately achieve "seamless integration between physical assets and the digital economy" to support the large-scale circulation of compliant RWA assets.

1.2.1 Pain Points of Traditional Public Blockchain in Adapting to RWA Scenarios

Current mainstream public blockchain were born in crypto-native scenarios and have not been specially optimized for the "physical attributes, compliance requirements, and dynamic value" of RWA. This leads to three core bottlenecks in implementation, which have become key obstacles restricting the large-scale development of the RWA ecosystem:

1. Insufficient Asset Data Granularity, Making Fragmented Transactions Difficult to Implement

Traditional public blockchain only record the "overall value identifier" of assets and cannot decompose the subdivided attributes of assets or accurately match "shares and subdivided values". This makes it difficult for small investors to participate and limits asset liquidity.

2. Imbalance Between Data Credibility and Real-Time Performance, Leading to Distorted Value Anchoring

The value of RWA assets depends on offline dynamic data (such as operating income, output volume, etc.). However, traditional public blockchain rely on third-party oracles for "batch data synchronization", which has obvious delays and lacks multi-dimensional verification mechanisms. Some projects even have problems such as "false asset on-chaining" or "data disconnection from physical entities", posing risks of triggering trust crises.

3. High Barriers to Cross-Ecosystem Data Collaboration, Resulting in Low Compliance Efficiency

The RWA ecosystem involves multiple roles, including asset owners, compliance parties (regulators, law firms, etc.), and transaction parties (institutional investors). However, traditional public blockchain lack unified data standards and require manual connection to the private systems of asset owners for verification, leading to long review times. At the same time, when cross-regional data is on-chained, it cannot be circulated across chains due to inconsistent data formats, resulting in low collaboration efficiency.

1.2.2 Promotion of Granular data to RWA Ecosystem

1. Core Definition and Technical Characteristics of Granular Data

Granular data refers to business events with minimum integrity generated in the digital space, consisting of relevant core business attributes and logical relationships. granular data decomposes the "physical attributes, ownership relationships, dynamic value, and compliance information" of RWA assets into subdivided data fragments that can be independently identified, updated in real time, and verified on-chain. Each piece of granular data has three core characteristics: "unique hash identifier, built-in compliance fields, and dynamic association with entities", and is bound to the corresponding asset token through smart contracts to form a "token-granular data" mapping.

To realize the management of granular data and ensure data accuracy, SimpleChain has built a three-tier (data collection layer, on-chain storage layer, data interaction layer) technical support system.

2. Four Core Promoting Effects of Granular Data on RWA Ecosystem

Granular data solves the implementation pain points of RWA from the perspective of "value circulation logic", and its promoting effects directly cover all roles in the ecosystem:

(1) Reducing RWA Investment Thresholds and Activating Fragmented Transactions

By subdividing asset value, granular data makes small-share transactions technically feasible. With granular data, the investment threshold for RWA assets will

be significantly reduced, and the matching efficiency of fragmented transactions will be greatly improved (as granular data contains subdivided income information, investors can accurately match their risk preferences).

(2) Strengthening "Digital-Physical" Anchoring and Reducing Fraud Risks

The core trust foundation of RWA lies in the "consistency between on-chain tokens and physical assets". granular data achieves this goal through multi-dimensional data cross-verification, and SimpleChain can significantly reduce the fraud risks of RWA assets through the granular data mechanism.

(3) Breaking Cross-Ecosystem Data Barriers and Improving Compliance Efficiency

Multi-role collaboration in the RWA ecosystem relies on "data interoperability". As a universal data language, granular data can be directly connected to the systems of regulators, financial institutions, and asset owners, enabling rapid completion of compliance verification and automatic execution.

(4) Supporting Full-Lifecycle Management and Reducing Operating Costs

The value of RWA assets changes dynamically over time. granular data can capture changes in real time and drive the execution of smart contracts. Through the closed loop of "real-time data - dynamic value - automatic execution", the management costs of RWA assets can be reduced, and the income transparency for investors can be increased to 100%.

1.3 Mission

To provide blockchain infrastructure enabling real-world assets to achieve verifiable ownership, traceability, and compliant circulation.

Through its three-tier architecture, "Technology Layer + Service Layer + Application Layer" SimpleChain achieves the following via a standardized technical framework:

- Standardized Asset Ownership Verification: Unified ownership logic and on-chain registration models;
- Automated Compliance Verification: Embedded compliance rules via CaaS

protocols;

- **Trusted Data Circulation:** Authenticity ensured through granular data mechanisms and decentralized oracles;
- **Integrated Financial Ecosystem:** Enabling asset liquidity and profitability at the Application Layer.

1.4 Ecological Development Plan

To adapt to the implementation of RWA applications and ecological development, the technical infrastructure upgrade of SimpleChain2.0 focuses on two cores: 1. main chain upgrade, including phased consensus iteration and token migration, 2. economic mechanism optimization, building a multi-dimensional guarantee system including node lock-up mechanism, dynamic staking reward mechanism, burning mechanism, and voting mechanism.

In terms of public blockchain ecological construction and functional services, SimpleChain focuses on promoting the following directions:

1. Unified Standards and Mechanisms

Through smart contracts and blockchain, asset ownership verification, value circulation, and rule embedding are realized. Unified ownership verification standards, audit specifications, and judicially enforceable mechanisms are established to ensure the legal validity and credit foundation of on-chain assets, and to ensure the uniqueness of asset identity and compliance of circulation on-chain.

2. End-to-End Compliance Framework

An integrated system covering "on-chain ownership verification + stable payment + automatic contracts + end-to-end auditing" is built. Through modular compliance execution units and programmable rules, a highly trusted RWA circulation environment is formed to promote the automatic generation and efficient circulation of on-chain credit.

3. Digital Financial Infrastructure

A digital financial infrastructure supporting the integrated operation of "on-chain identity - on-chain assets - on-chain value - on-chain contracts" is built to gain

initiative in the global financial restructuring. Through unified standards, interfaces, and regulatory logic, the digital restructuring of a unified large market and the free circulation of financial elements is promoted.

4. Five-in-One Operation and Standardized Services

With unified institutional interfaces and regulatory logic as the core, a "five-in-one" operation mechanism of "identity - assets - payment - contracts - auditing" is built; institutional specifications, pilot layout, risk control boundaries, and standard output are coordinated to support the development of integration experiments in regions, industries, and specific scenarios, and to form replicable and promotable infrastructure and service models.

2 Design Principles

SimpleChain's technical and governance design adheres to the following five core principles:

1. Verifiability

All on-chain assets must establish a verifiable hash mapping relationship with their off-chain counterparts; every piece of data and every contract execution is traceable.

2. Comliability

Through modular CaaS compliance modules, legal templates from different regions (MiCA, HKMA, FINMA, etc.) are parameterized to achieve “Compliance as a Service.”

3. Scalability

Employing PoS + HotStuff layered consensus, heterogeneous Rollup scaling, and cross-chain interoperability mechanisms enables high performance while maintaining security.

4. Practicality

Provides enterprises and financial institutions with plug-and-play SDKs and APIs to automate asset issuance, auditing, and trading workflows.

5. Data-first

Designs core protocols around granular data, empowering it as the driving force for asset ownership verification, valuation, circulation, and governance.

These principles collectively define SimpleChain's design philosophy:

“SimpleChain is building an institutionalized concrete system bridging
the real world to the on-chain economy.”

3 SimpleChain Main-chain Upgrade

According to the upgrade content and schedule, the SimpleChain main-chain upgrade is divided into three phases.

Phase	Name	Upgrade Content
Phase 1 Launch: Q3 2025	SimpleChain2.0 Mercury	Switch from PoW consensus mechanism to PoS consensus mechanism
Phase 2 Launch: Q4 2025	SimpleChain2.0 Copper	Upgrade of the economic model
Phase 3 Launch: 2026	SimpleChain2.0 Tungsten	Upgrade of the HotStuff consensus mechanism

3.1 Phase 1: Consensus Adjustment

In Phase 1 (SimpleChain2.0 Mercury), the consensus mechanism of SimpleChain will be switched from PoW to PoS. This switch will drastically reduce network energy consumption, and the network governance structure will be upgraded from a trusted ledger incentive consensus based on miner mining to an equity consensus among core nodes with the ability to build a new ecosystem. Validators can obtain block rewards (including staking rewards and delegate commission fees) and transaction fees through self-lock-up.

3.2 Phase 2: Economic Model Upgrade

In Phase 2 (SimpleChain2.0 Copper), the economic model will be upgraded with the adoption of a dynamic staking incentive adjustment model. The node staking reward mechanism will be refined into a dual-track system of basic rewards and contribution rewards, and the accuracy of incentives will be achieved through dynamic interest rate adjustment. To consolidate the foundation for ecological development, validators will retain the right to distribute staking rewards, and an equity guarantee mechanism will be established to attract more high-quality nodes to

settle in and jointly promote ecological construction. Validators can share staking rewards (including basic rewards and contribution rewards) with delegators, while transaction fees and delegation commission fees will be owned by validators. A differentiated equity distribution mechanism will be established to build a win-win ecological participation model for validators and delegators.

3.3 Phase 3: HotStuff Mechanism Upgrade

In Phase 3 (SimpleChain2.0 Tungsten), a hierarchical consensus system will be built by combining the PoS consensus mechanism with the HotStuff consensus. The underlying PoS and the second-layer HotStuff will form cross-layer collaboration: the underlying validator set will provide security endorsement for the second layer, and the high-performance execution of the second layer will feed back the ecological value of the underlying layer. At the same time, supporting key technologies will be deployed: HotStuff will compress the message size through BLS aggregate signatures to ensure that communication overhead remains controllable when the committee size increases; the PoS layer will dynamically adjust the validator set; the HotStuff layer will generate proposals based on the latest committee and adjust members based on PoS staking weights to prevent power concentration; in addition, the finality of the second layer will rely on the underlying PoS security model to achieve cross-layer security transmission.

This mechanism not only achieves dual breakthroughs in performance and security but also realizes the coordination between decentralization and efficiency, and optimizes the energy and economic models. Furthermore, in the evolution of hierarchical consensus, plans are made to realize in-depth integration of sharding and hierarchy, enhancement of cross-chain interoperability, and security design for quantum computing.

4 Overall Architecture Design

The SimpleChain2.0 architecture centers on the asset lifecycle as its core logic. It forms a tripartite infrastructure of “technology-service-application” spanning from underlying performance and security capabilities to upper-layer asset circulation and financial products, enabling the trustworthy, compliant, and efficient flow of real-world assets into the Web3 world. The architecture comprises three layers: The Technology Layer manages full-chain performance, security, and cross-chain interoperability. It includes PoS+HotStuff consensus, Rollup scaling solutions, enterprise-grade node systems, and cross-chain protocols, providing high-performance foundational support for large-scale RWA scenarios. The RWA Service Layer serves as the core hub for asset services. Through components like DataIPO (RWA Launchpad), CaaS (Compliance-as-a-Service), Fact & Industry Oracle (Data Bridge System), RWA Data Credit System. The Application Layer focuses on asset liquidity and value growth, enabling secondary market liquidity and capital efficiency for on-chain compliant assets through products like RWA Launchpad, RWA DEX, RWA Earn, and structured credit. Based on this three-tier architecture, SimpleChain2.0 builds the next-generation global RWA infrastructure bridging the real world and Web3, providing a unified operating system for the future Internet of Assets.

4.1 Technology Layer

SimpleChain2.0 features an extreme-performance modular architecture, efficient and convenient on-chain experience, and can securely and seamlessly connect to multi-ecosystem public blockchain.

“The bottom layer of SimpleChain lies the computational power and trust engine for the entire RWA financial ecosystem.”

It endows on-chain networks with foundational capabilities for scalability,

verifiability, and regulatory compliance.

4.1.1 Main Chain Consensus Layer

1. Proof of Stake (PoS) Consensus Mechanism

(1) Core Concepts and Design Principles

Proof of Stake (PoS) is a protocol that achieves distributed consensus through economic incentives. Its core logic is “stake equals power”: validators obtain eligibility to participate in consensus by staking tokens, with the staked amount determining their block production probability and voting weight. SimpleChain 2.0 adopts the PoS mechanism, requiring validators to stake a corresponding amount of SRW to become candidate nodes.

1) Staking and Validator Roles

Staking Threshold: Users must stake a certain amount of SRW to become candidate validators. Higher stakes increase the probability of selection.

Dynamic Validator Set: The network selects block proposers and voting committees from active validators using a random algorithm combined with staking weight.

Multi-Role Collaboration: Validators concurrently fulfill Proposer, Voter, and Syncer responsibilities to ensure chain activity and finality.

2) Consensus Process and Finality

Block Generation: Selected proposers package transactions into candidate blocks and broadcast them to the network. Other validators confirm legitimacy through secondary verification (checking transaction validity and block structure).

Voting Confirmation: Validators conduct two rounds of voting on candidate blocks:

- **Justification Vote:** Requires support from over 2/3 of staked weight to enter “justified” status, significantly increasing rollback costs.
- **Finalization Vote:** Subsequent checkpoint justification votes automatically confirm preceding blocks as “finalized,” eliminating forking possibilities.

3) Economic Incentives and Penalties

Reward Mechanism: Validators receive rewards and transaction fees proportional to their staked weight.

Slashing Mechanism: Validators engaging in double-signing, offline status, or malicious behavior face partial or full confiscation of their staked tokens.

(2) Protocol Structure

POS comprises rules including the Propose Rule, Fork Choice Rule, and Finality Rule.

1) **Propose Rule:** Randomly selects block producers based on staked weight.

2) **Fork Choice Rule:** Selects the authoritative chain when handling forks.

3) **Finality Rule:** Ensures block finality and prevents rollbacks.

(3) Mechanism Characteristics

1) **Low Energy Consumption:** Eliminates high-computational-power competition, reducing energy consumption by over 99% compared to PoW.

2) **Economic Incentives:** Staked token validators are motivated to maintain network security to avoid deposit confiscation for malicious actions.

3) **Progressive Finality:** Blocks require confirmation through multiple rounds of voting.

(4) Key Technologies

1) Random Number Generation and Anti-Manipulation

Random Number Generation: Designs algorithms to generate unpredictable random numbers, ensuring the validator selection process is auditable and tamper-proof.

Prevention of Precomputed Attacks: Validator roles are fixed in advance to prevent attackers from conducting sybil attacks by manipulating random number seeds.

2) Dynamic Validator Management

Dynamic Stake Adjustment: Dynamically adjusts the effective stake of individual validators to optimize network load.

Smooth Rotation Mechanism: Validators gradually release their stakes through

exit queues, preventing network instability caused by mass concentrated exits.

2. HotStuff Consensus Mechanism

(1) Protocol Architecture and Core Process

HotStuff is a deterministic consensus protocol based on Byzantine Fault Tolerance (BFT). Its core design revolves around a three-phase voting chain and linear view switching, achieving an efficient balance between security and liveness.

1) Three-Phase Voting Chain

Each block confirmation requires voting across three phases, coordinated by the Leader to complete with replicas:

- **Prepare Phase:** The Leader generates a proposal (containing the quorum certificate QC for the parent block) and broadcasts it to replicas. After validating the proposal's legitimacy, replicas send signed Prepare votes to the Leader. When the Leader collects $n-f$ signatures (where n is the total number of nodes and f is the maximum number of malicious nodes, $f < n/3$), it generates the prepareQC, marking the proposal as passed in the first phase.

- **Pre-Commit Phase:** The Leader broadcasts the prepareQC encapsulated in a Pre-Commit message. Validators send Pre-Commit votes after verification. Upon collecting $n-f$ signatures, the Leader generates a precommitQC, indicating the proposal enters the final confirmation phase.

- **Commit Phase:** The Leader broadcasts the precommitQC. Validators send Commit votes after verification. Upon collecting $n-f$ signatures, the Leader generates commitQC, formally committing the block. All validators synchronize states and update their local QC chains.

2) Chain Dependency and QC Transmission

Each block contains its parent block's QC, forming a chained evidence chain. For example, block B's prepareQC includes block A's commitQC, ensuring validators only need to verify the current QC's validity without tracing the entire chain. This design reduces traditional BFT's $O(n^3)$ communication complexity to $O(n)$, while compressing message size from $O(n)$ to $O(1)$ through aggregated signature techniques (e.g., BLS signatures), significantly enhancing performance.

3) Linear View Switching

When the Leader fails or times out, the system triggers a view switch via a timeout certificate (TC). The new Leader directly generates proposals based on the previous block's QC without additional coordination.

(2) Key Technologies

1) Decoupling Security and Liveness

HotStuff divides the protocol into a security core layer (ensuring block irreversibility) and a liveness control layer (Pacemaker module). Pacemaker guarantees continuous system operation through timeout mechanisms and view switching, while the security core layer ensures absolute security of committed blocks via three rounds of voting and the QC chain.

2) Progressive Confirmation with Instant Finality

Each block achieves final confirmation during the Commit phase, requiring no subsequent block support.

3) Anti-Sybil Attacks and Dynamic Member Management

HotStuff limits participating node scale via a validator committee mechanism, reducing malicious collusion probability. Committee members are dynamically elected through PoS or similar mechanisms, balancing decentralization and performance.

(3) Security Model and Assumptions

1) Byzantine Fault Tolerance

Assuming no more than one-third of nodes are malicious ($f < n/3$), security is ensured through:

- Quorum voting: Each phase requires $n-f$ signatures, preventing malicious nodes from forging QC.
- Non-forgeable QC chain: QC aggregates signatures from the previous phase, allowing validators to verify QC legitimacy without inspecting individual votes.
- Fork Immunity: Since each block becomes final upon submission, the system eliminates temporary forks, completely preventing “long-range attacks.”

2) Anti-Bribery and Penalty Mechanism

A confiscation mechanism is introduced: If a malicious validator's vote is detected as conflicting (e.g., simultaneously supporting two mutually exclusive proposals), their staked tokens will be partially or fully confiscated. This enhances the protocol's economic security and reduces the incentive for validators to collude with attackers.

3. PoS+HotStuff Consensus Mechanism

(1) Layered Consensus

1) Core Logic of Layered Architecture

Underlying PoS: Elects a validator committee through token staking to ensure decentralization and low energy consumption.

Second-layer HotStuff: Implements high-performance consensus within the committee using a BFT protocol.

Cross-Layer Synergy: The validator set from the underlying PoS layer provides security guarantees for the second-layer HotStuff, while the high-performance execution of the second layer enhances the value of the underlying ecosystem.

2) Key Technologies

Aggregated Signature Communication Compression: HotStuff uses BLS aggregated signatures to compress message size from $O(n)$ to $O(1)$, keeping communication overhead manageable even as the committee size increases.

Dynamic Committee Management: The PoS layer dynamically adjusts the validator set, while the HotStuff layer generates proposals based on the latest committee. It also adjusts committee members based on PoS stake weights to prevent power concentration. Cross-Layer Secure Transmission: The finality of the Layer 2 HotStuff relies on the security model of the underlying PoS.

Cross-Layer Secure Transmission: The finality of the Layer 2 HotStuff relies on the security model of the underlying PoS.

(2) Balancing the “Impossible Trinity”

1) Dual Breakthroughs in Performance and Security

High Performance: HotStuff achieves instant finality (single-block confirmation) and employs a pipelined voting mechanism, enabling throughput of tens of thousands

of TPS—far exceeding PoS systems.

High Security: The deterministic consensus of the BFT protocol mitigates PoS's “long-range attack” vulnerability.

2) Synergy Between Decentralization and Efficiency

Decentralized Election: The PoS layer's token staking mechanism lowers participation barriers, ensuring global distribution of committee members.

Efficient Execution Layer: The HotStuff layer limits node scale through a committee model, enhancing processing speed while maintaining security.

3) Energy and Economic Model Optimization

Low Energy Consumption: The PoS layer consumes only 0.1% of PoW's energy, while the HotStuff layer eliminates computational competition, reducing overall energy consumption by over 99% compared to traditional public blockchain.

Incentive Alignment: The PoS layer incentivizes long-term token holding through staking rewards, while the HotStuff layer motivates committee members via transaction fee distribution.

(3) Evolution of Layered Consensus

1) Deep Integration of Sharding and Layering

Cross-Shard HotStuff: Implements cross-shard consensus using HotStuff variants between shards.

Layered Sharding Architecture: The underlying PoS layer manages global sharding, while the second-layer HotStuff handles intra-shard consensus, forming a “global-local” dual-layer sharding system that further enhances scalability.

2) Enhanced Cross-Chain Interoperability

Multi-Chain HotStuff Committees: Elect cross-chain validator federations via PoS, then employ HotStuff within federations for atomic cross-chain asset swaps.

Cross-Chain Reuse of Security Models: Reuse the underlying PoS validator set to provide security guarantees for the second-layer HotStuff.

3) Quantum Computing and Post-Quantum Cryptography

Post-quantum BFT protocol: Researching post-quantum aggregate signature schemes to ensure HotStuff's security in the quantum computing era.

Post-quantum design for the PoS layer: Employing post-quantum hash functions and VRFs to safeguard the fairness of underlying validator elections.

4.1.2 Hierarchical Expansion System

4.1.2.1 Multi-L2 Sub-chain Support Architecture

(1) Parallel Transaction Sorting Algorithm

An improved Narwhal protocol is adopted to split the transaction dependency graph into non-conflicting batches, and multi-threaded processing is realized through DAG topological sorting.

(2) Heterogeneous Rollup Support

ZK-Rollup: Utilizes the advanced PLONK zero-knowledge proof system to enable efficient off-chain computation through concise proof verification. Key features include:

- 1) Processing thousands of payment transactions per batch;
- 2) Low verification cost per transaction;
- 3) High-speed finality. Particularly suited for high-frequency scenarios such as cross-border micropayments and DEX settlements.

Optimistic Rollup: Utilizes a dynamic fraud proof window mechanism, ensuring security through economic game theory models. Technical features:

- 1) Supports fully EVM-compatible smart contracts;
- 2) Fraud challenge periods automatically adjust based on asset value;
- 3) Gas fees significantly lower than L1. Primarily serves scenarios requiring complex logic, such as GameFi item trading and bulk NFT minting. Both solutions achieve liquidity interoperability through a unified settlement layer, allowing users to freely choose their preferred balance between security and efficiency.

2. Resource Scheduling Optimization

State Sharding Hot Switching: Subchains automatically scale up/down based on load, with cross-shard transactions enabled via atomic hash locks;

Data Availability Layer: Implements efficient solutions to reduce storage costs,

featuring low L2 data anchoring fees.

4.1.2.2 Enterprise-Grade Node Network Architecture

1. Physically Sharding Sequencer Cluster

Provides computational (FPGA-accelerated ZKPs) and storage (IPFS-anchored) physical shards. Containerized resource isolation ensures core process resource utilization remains below 15%.

Sharding Type	Requirements	Scenarios	Description
Computational	FPGA Cards/Nodes	ZK Proof Generation	Utilizes Field-Programmable Gate Array (FPGA) acceleration for zero-knowledge proof computation, enabling parallel processing of complex cryptographic operations to significantly enhance efficiency.
Storage	NVMe Cluster Storage	Blockchain Historical Data Archiving	NVMe protocol-based all-flash storage clusters deliver ultra-low latency and high throughput, supporting rapid writing and compressed storage of full blockchain node historical data.
Compliance	National Cryptographic SM4 Encryption Chip	Financial-Grade Audit Trail	Built-in hardware encryption module certified by the State Cryptography Administration for SM4 algorithm, enabling real-time encryption/decryption of transaction data to meet Level 3 or higher protection requirements under the Financial Data Security Classification Guidelines.

2. Enterprise-Grade Management Features

Resource Isolation: Enforces hard isolation of CPU/memory through Kubernetes namespaces, with critical processes exclusively occupying NUMA nodes.

Regulatory Interface: Provides standardized GRPC protocol access, supporting real-time export of FATF-compliant anti-money laundering reports.

4.1.3 Oracle for Ensuring Data Credibility

Oracles are core middleware connecting blockchain networks to the off-chain real world/external systems. Their core value lies in solving the "data silo" problem of blockchain. Oracles securely and reliably transmit off-chain data to the on-chain system through standardized processes, and can also synchronize instructions from on-chain smart contracts to the off-chain system, supporting the interaction between blockchain and the real world.

4.1.3.1 Oracle Overview

Blockchain's decentralized consensus can only validate the "logical validity" of on-chain transactions, but cannot verify the "authenticity of off-chain data." Oracle technology provides "trusted off-chain data proof" for on-chain smart contracts, enabling them to execute logic based on real-world information. Acting as a "two-way communication bridge between blockchain and external systems," oracles perform "collection, verification, aggregation, and on-chain transmission" of off-chain data, or relay trigger instructions from on-chain smart contracts to off-chain systems.

4.1.3.2 Core Functions

1. Functions

The oracle's functionality revolves around "on-chain and off-chain bidirectional interaction," primarily comprising four major modules.

(1) Off-chain Data Collection: Actively interfaces with off-chain data sources (e.g., API interfaces, databases, sensors, third-party services), supports hardware-based trusted data environment as oracle node access points, and acquires various data required by smart contracts;

(2) Data Validation and Cleansing: Performs authenticity checks and outlier removal on raw data to mitigate bias or falsification from single sources/nodes;

(3) On-Chain Data Writing: Submits validated, standardized data via blockchain

transactions to on-chain “aggregator contracts” for smart contract invocation;

(4) Off-Chain Instruction Execution (Reverse Oracle): Receives instructions from on-chain smart contracts to trigger off-chain operations (e.g., bank transfers, registry system updates).

2. Workflow

The oracle's end-to-end process comprises five steps, forming a closed-loop from data collection to smart contract invocation.

(1) Smart Contract Initiates Data Request

On-chain smart contracts submit data demands through interfaces defined by the oracle.

(2) Oracle Nodes Collect Off-Chain Data

Multiple independent nodes (decentralized node clusters) within the oracle network simultaneously gather target data from predefined multi-sources (e.g., IoT devices, third-party audit agencies), ensuring distributed data origins.

(3) Data Verification and Aggregation

Nodes synchronize data via the “off-chain reporting” protocol, eliminating outliers (e.g., excluding values from nodes deviating beyond thresholds from the majority). Only when data from over the preset proportion of nodes aligns is “aggregated data” generated, ensuring authenticity.

(4) On-Chain Storage of Aggregated Data

Oracle nodes submit the final aggregated data to the on-chain “aggregator contract.” An “agent contract” ensures uninterrupted service during subsequent data updates. The data is now permanently recorded on the blockchain and accessible to all smart contracts.

(5) Smart Contract Data Retrieval and Logic Execution

The requesting smart contract reads data from the aggregator contract via an interface and executes business logic based on this data.

4.1.3.3 Key Features

The core competitiveness of oracles lies in “data trustworthiness,” which ensures

reliability through the following technical characteristics:

1. Decentralization (Resilience to Single Points of Failure)

Node decentralization: Utilizes multiple independent nodes to form the network instead of a single node, preventing data errors caused by node failure or malicious tampering.

Data source decentralization: Integrates with multiple independent data sources to avoid failure or tampering from a single source.

2. Security (Tamper-Resistance and Attack Resistance)

On-chain Verifiability: Once data is recorded on the blockchain, smart contracts can verify timestamps, node signatures, and data source traces to ensure data integrity.

Economic Incentives and Penalties: Nodes must stake assets. Providing false data results in asset confiscation, while nodes providing accurate data receive rewards. This economic mechanism constrains node behavior.

3. Flexibility (Multi-scenario Adaptability)

Multi-data type support: Processes numerical data (prices, interest rates, etc.), non-numerical data (text, image hashes, property registration statuses, etc.), and binary data (raw sensor data, etc.).

4. Timeliness (Meeting Real-Time Demands)

Dynamic Update Mechanism: Controls data refresh frequency via “deviation threshold” and “heartbeat interval.” When off-chain data fluctuations exceed the threshold or the heartbeat interval elapses, it automatically triggers data re-collection and on-chain updating.

4.1.4 Cross-Chain and Multi-Scenario Support

Based on the needs of blockchain ecosystem interoperability and scenario implementation, a full-stack cross-chain and expansion system featuring "security priority, efficient compatibility, and scenario adaptation" is built to realize cross-chain interaction security guarantees, multi-public blockchain ecosystem access, and full-scenario technical support, maximize liquidity and capital efficiency for RWA within the on-chain ecosystem.

4.1.4.1 Secure Cross-Chain Mechanism

Centering on data circulation and security as core objectives, this mechanism establishes a trustworthy and efficient cross-chain interaction system through standardized cross-chain protocols and multi-layered security verification mechanisms. It enables asset and data interoperability across different public blockchain ecosystems, ensuring transactions are tamper-proof, irreversible, and low-risk.

1. Multi-Series Public Blockchain Adaptation

Deeply adapts to the underlying architectures of mainstream public blockchain, covering high-performance, ecosystem-oriented, and specialized chains such as Solana, EVM-based, and MOVE-based chains to meet cross-chain demands across diverse scenarios.

2. Comprehensive Cross-Chain Core Capabilities

Enables end-to-end support across the entire cross-chain process, from asset transfers to application interactions:

- **Cross-Chain Atomic Transactions:** Utilizes Hash Time-Locked Contracts (HTLC) or multi-signature verification to ensure transaction execution and prevent asset loss from unilateral transactions.
- **Cross-chain asset transfers:** Supports various asset types including fungible tokens (FT) and non-fungible tokens (NFT), providing real-time asset mapping, cross-chain settlement, and reconciliation functions while strictly controlling asset arrival latency.
- **Cross-chain DApp interactions:** Enables cross-chain contract invocations and data interoperability, breaking application barriers within single-chain ecosystems.

3. Multi-Layered Security Mechanisms

Builds cross-chain security architecture from the technical foundation to defend against common cross-chain risks:

- **Cryptographic Verification:** Employs zero-knowledge proofs (ZKP) and multi-signature (Multi-Sig) technologies to encrypt and authenticate the entire

cross-chain transaction process—initiation, verification, and execution—ensuring transaction data cannot be forged.

- **Real-Time Risk Monitoring:** Deploys cross-chain node monitoring systems to detect public blockchain node statuses, network congestion, and abnormal transaction behaviors in real time. Immediately triggers transaction suspension or rollback mechanisms upon detecting risks (e.g., node outages, transaction anomalies).

- **Smart Contract Auditing:** Conducts security audits on core cross-chain protocol contracts to fix potential vulnerabilities. Supports seamless contract upgrades to prevent cross-chain interruptions caused by updates.

4.1.4.2 Multi-Scenario Expansion

Deploying dedicated Rollup coprocessors (Layer 2 scaling solutions) provides customized scaling capabilities tailored to the performance and functional requirements of diverse blockchain applications (DeFi, GameFi, etc.). This approach ensures security while circumventing the limitations imposed by underlying public blockchain.

1. Core Value of Dedicated Rollup Coprocessors

As “middleware” bridging underlying public blockchain and upper-layer applications, coprocessors deliver:

- **Performance Boost:** Offloading bulk transactions and computations to Rollup processing while submitting only final results to the underlying chain. This achieves 10-100x throughput gains over native chains and significantly reduces gas fees.

- **Scenario Adaptation:** Optimizes computational logic and data storage methods for diverse use cases, preventing efficiency losses from one-size-fits-all scaling solutions.

- **Security Inheritance:** Leveraging the underlying chain's security, the Rollup coprocessor handles transaction execution only, with final state validation and storage performed by the chain—ensuring security integrity remains intact during scaling.

2. Comprehensive Scenario Adaptation and Empowerment

Provides customized scaling support for core blockchain applications including

DeFi (Decentralized Finance), GameFi (Gaming Finance), PayFi (Decentralized Payments), and DAO (Decentralized Autonomous Organizations), achieving precise alignment between scenario requirements and technical capabilities.

4.2 RWA Service Layer

The RWA Service Layer serves as the “institutional engine” and “value hub” of the SimpleChain technology ecosystem.

Driven by AI + DePIN technology, it employs a dual-layer TDS + SLC framework to fully automate and trace the rights confirmation, verification, compliance, issuance, and credit assessment of real-world assets. This establishes a compliant, secure, trustworthy, and liquid global asset issuance foundation.

“The middle layer of SimpleChain serves as the gateway for the real world
to enter the Web3 financial order.”

It transforms real-world assets into verifiable, issuable, and traceable
on-chain value units.

4.2.1 Core Logic

The RWA service layer serves as SimpleChain's core narrative layer and operational hub, handling all critical actions for on-chain real-world assets: rights confirmation, verification, compliance, issuance, and listing.

SimpleChain leverages AI + DePIN (exclusive IoT device collection) technology to build an underlying system comprising TDS (Trusted Data Space) and SLC (Smart Legal Contract Network). This infrastructure provides automated compliance verification and data trust assurance for the digital mapping of real-world assets.

Core Process:

Physical Asset Registration → CaaS Compliance Verification → DataIPO
Issuance Mapping → Oracle Verification & Rights Confirmation → Data Credit

Generation

The system automates the entire process from real-world data collection to on-chain asset rights confirmation, forming SimpleChain's three-dimensional support framework in the RWA domain:

CaaS = Compliance Pre-filtering Layer

DataIPO = Asset Issuance Execution Layer

Oracles + Data Credit = Data Trustworthiness Support Layer

4.2.2 Technical Framework

(1) TDS — Trusted Data Space

TDS serves as SimpleChain's foundational data infrastructure, enabling trusted collection, on-chain recording, and traceability of real-world data within the DePIN ecosystem.

Its design philosophy evolves from the “Granular Data” concept in the previous whitepaper, advancing into verifiable Data Domains.

TDS Architectural Layers:

- **Data Collection Layer:** Real-time acquisition of physical asset and business data via the DePIN node network (IoT, mobile terminals, enterprise APIs);
- **Verification and Signing Layer:** Validates data sources using Zero-Knowledge Proofs (ZKP) and BLS multi-signature mechanisms;
- **Data Hashing & On-Chain Layer:** Generates GranularHash, which is embedded into the state tree after on-chain recording;
- **Data Access Layer:** Authorized compliant parties (CaaS, Oracle, regulatory nodes) read and invoke data.

Each granular data record contains: AssetID | EventType | Timestamp | Value | ValidatorSig | AuditHash, and is signed and notarized by multiple validator nodes.

TDS serves as the trusted gateway for all real-world data entering the chain. It transforms data collected by DePIN devices into legally binding digital evidence.

(2) SLC — Smart Legal Contract Network

SLC is SimpleChain's “Smart Legal Engine” extended from the CaaS protocol. It

automatically parses regulatory rules, audit logic, and legal texts via AI to generate compliant smart contract templates (Policy-as-Code).

Core SLC functionalities include:

- Smart Contract Template Generation: AI automatically extracts constraints from local legal texts to form contract rule templates;
- Multi-Jurisdictional Compatibility: Supports parameterized loading of regulatory standards like MiCA, HKMA, FinCEN, and MAS;
- Real-time Risk Control & Anomaly Detection: AI models monitor transaction behaviors and generate compliance risk scores;
- Cross-border data transmission auditing: Executes privacy reviews and cryptographic verification via CaaS nodes.

The integration of SLC and TDS positions CaaS as the execution layer for “Regulations-as-a-Service,” achieving seamless fusion and automated enforcement of real-world regulations, data collection, and on-chain behavior.

4.2.3 System Components and Execution Logic

① DataIPO Protocol (Asset Issuance Protocol)

The DataIPO Protocol is SimpleChain's core issuance protocol, mapping real-world assets into tradable on-chain tokens. It integrates five stages—title verification, valuation, fractionalization, issuance, and listing—to form a “one-click asset-on-chain process.”

Process Structure:

- Asset Title Verification: Generates a unique AssetHash identifier through TDS granular data and Oracle validation.
- Valuation and Fractionalization: Industry Oracle retrieves market data to execute valuation and share allocation.
- Compliance Verification: CaaS module loads SLC rule templates for review execution.
- Issuance Mapping: DataIPO contract generates a dual-layer mapping structure (local compliant token + global circulating token).

- Listing & Trading: Automatically synchronized to the RWA Launchpad.

Dual-Layer Token Mapping Architecture:

- Inner-Layer Token (Reg-Token): Corresponds to asset registration in the compliance zone, adhering to local regulations.
- Outer-Layer Token (Global-Token): Consortium blockchain token mapped to SimpleChain for global circulation, representing income rights or derivative rights.

This “dual-layer mapping + compliance isolation” design enables a global asset issuance model characterized by “internal compliance and external liquidity.”

② CaaS Protocol (Compliance-as-a-Service)

CaaS is SimpleChain's modular compliance service system. Its technology is based on the AI + DePIN TDS + SLC architecture, providing integrated services from regulatory rules to cross-border auditing.

Key Functions:

- KYC/KYB Verification: Supports individual and institutional identity validation;
- AML Anti-Money Laundering Detection: Identifies anomalous fund flows via AI models;
- Cross-border Secure Data Transmission: Utilizes multi-signature + national cryptographic algorithms (SM2/SM4) encryption;
- Automated Audit Report Generation: Records compliance events in real-time, outputs PDF/JSON audit reports, and stores them on-chain as evidence.

Execution Logic:

- DataIPO initiates asset issuance request;
- CaaS reads asset information and loads corresponding jurisdictional templates;
- Generates ComplianceHash upon successful verification;
- Audit nodes synchronize records with regulatory nodes (RegNode).

CaaS Design Philosophy:

“Before initiating a DataIPO action, CaaS must first undergo verification.”

This ensures that on-chain issuance and trading remain lawful, traceable, and subject to regulation at all times.

4.2.4 Oracle Components: Modular Data Service Architecture

Within the RWA service layer, SimpleChain modularizes its oracle system into three foundational components, each delivering trustworthy data services across distinct dimensions. This framework draws inspiration from leading oracle networks (such as Chainlink and Pyth Network) while integrating SimpleChain's unique advantage of granular data coupled with composable modules.

4.2.4.1 Fact Oracle — Business Event Data Oracle

Definition: For entity operational data (e.g., cash flow, equipment monitoring, operational metrics), Fact Oracle provides off-chain business event collection, verification, and on-chain writing capabilities.

Implementation:

- Combines DePIN/IoT node networks to collect device data;
- Multi-source data aggregation + anomaly filtering + zero-knowledge proof (ZKP) verification;
- Generates granular data structures written to TDS, ultimately submitted on-chain.

Distinctive Comparison: While mainstream oracles focus on price/quotation data, Fact Oracle deeply supports “asset lifecycle event” data.

4.2.4.2 Price-Oracle — Hybrid Asset Pricing Oracle

Definition: Price-Oracle provides on-chain pricing capabilities covering both Web3 native assets and RWA hybrid assets. It inputs data from Fact Oracle + Industry Oracle to output unified “Pricing Facts.”

Implementation:

- Receives multi-source inputs D_i , calculates the pricing value using weights w_i and credit adjustment factor $\phi \times C_{credit}$;
- Binds pricing results to granular data structures and writes them to the state tree.

Formula Example:

$$P_{asset} = \sum_{i=1}^n w_i \times D_i + \phi \times C_{credit}$$

- w_i : Weight of the i -th data source;
- D_i : Price or valuation data provided by the i -th data source;
- ϕ : Credit adjustment factor;
- C_{credit} : On-chain credit rating (from the RWA Data Credit system).

Feature Comparison: While mainstream oracles like Pyth focus on high-frequency price data, Price-Oracle in SimpleChain extends capabilities to include “asset lifecycle data + compliance modules + credit modeling,” forming a pricing foundation with stronger RWA characteristics.

4.2.4.3 RWA Data Credit System — On-Chain Credit Framework

The RWA Data Credit System is an on-chain credit rating framework being developed by SimpleChain. It aims to establish a traceable, verifiable, and dynamically updated credit evaluation standard for RWA assets and their participants.

Currently in its initial architecture phase (v1 Prototype), this system will serve as a critical module within SimpleChain's financial infrastructure layer, providing quantifiable credit foundations for RWA asset issuance, trading, staking, and governance.

(1) System Logic and Data Sources

The credit system is built upon CePass compliance audits and the Oracle data network, generating On-Chain Credit Profiles through multidimensional data

aggregation.

The foundational model relies on four core data dimensions:

1. Compliance Records (L): Audit logs and regulatory verification status from CePass/CaaS modules;
2. Historical Transaction & Yield Records (T): Operational event and yield distribution data provided by Fact Oracle;
3. Market Valuation Volatility (P): Industry valuation and price stability data provided by Industry Oracle;
4. Behavioral Activity & Risk Exposure (B): Asset operation frequency and risk distribution information from DataIPO and Launchpad modules.

(2) Credit Scoring Model (Initial Version)

The initial mathematical model for RWA credit scoring is defined as:

$$C = \alpha L + \beta T + \gamma P + \delta B$$

Where:

- L: Compliance coefficient (based on CePass audit results);
- T: Transaction and income activity level;
- P: Price and valuation stability;
- B: Behavioral credibility and risk preference indicators.

Parameters α , β , γ , δ will undergo dynamic calibration with real-world data during Mainnet Phase II. Subsequent versions will integrate AI adaptive weighting and zero-knowledge privacy computation to achieve interpretable and privacy-secure credit scoring.

(3) Application Scenarios for Credit Outcomes (Planned)

Future credit outcomes will serve as the ecosystem-wide “Base Credit Factor,” influencing and driving the following core business logic:

- Launchpad asset listing priority and margin requirements;
- Liquidity allocation weights and matching priority in RWA DEX;
- Risk coefficients and interest rate curve adjustments in staking and lending protocols;
- Voting weights and proposal eligibility criteria in governance systems.

4.2.5 Core Value

1. Integrated Service System for RWA Issuance

- Compliance-First (CaaS) + Automated Issuance (DataIPO) + Real-Time Verification (Oracle + Data Credit)
- Full-chain closed-loop from registration to listing; developers can complete issuance with one click via API.

2. Data-Asset Convergence (Data-Fi)

- Treats data itself as a tradable asset, endowing AI, IoT, energy, carbon emissions, and other data types with financial attributes.
- TDS transforms raw data into auditable asset units, laying the foundation for the future AI Data Economy.

3. Regulator-Compliant, Verifiable Financial Infrastructure Layer

- Each asset possesses “dual trust attributes”: data trustworthiness + compliance verifiability.
- CaaS + TDS + SLC collectively form an “institutional-grade trusted computing environment,” supporting upper-layer scenarios like DeFi, RWA DEX, and structured credit.

4.2.6 Application Scenario Examples

Real Estate Asset Tokenization: CaaS Audit → DataIPO Issuance → Industry Oracle Verification → Token Listing on RWA Launchpad;

Green Energy/Carbon Asset Trading: IoT Data Integration → Fact Oracle Verification → CaaS Compliance Confirmation → DataIPO Fractional Issuance;

AI Model Rights Confirmation & Data Authorization: DataIPO Registration of AI Model Hash + Metadata → CaaS Privacy Audit → RWA Data Credit Generates Credit History.

4.3 Application Layer

The Application Layer is the most market-facing layer within the SimpleChain

ecosystem. It provides liquidity for RWA assets that have been verified, compliant, and validated, enabling these assets to enter DeFi markets, financial institutions, and individual users' investment portfolios.

“The upper layer of SimpleChain is the marketplace where on-chain assets achieve liquidity, pricing, and value growth.”

It enables assets to be tradable, composable, and financializable, forming a true global capital network.

4.3.1 RWA Launchpad

The RWA Launchpad (DataIPO) serves as SimpleChain's asset issuance and listing platform. It provides issuers (institutions or enterprises) with standardized processes to rapidly convert traditional assets into tradable RWA Tokens. Simultaneously, DataIPO offers pre- and post-investment management services to capital providers, fulfilling the needs of multiple stakeholders including asset issuers, investment institutions, and individual investors.

Core Functions:

- Asset Listing: Issuers submit materials via DataIPO; CaaS automatically performs compliance reviews.
- Investor Onboarding: Tiered participation based on investor risk profiles and KYC/KYB outcomes.
- Allocation & Settlement: Supports Public Offerings and Private Placements.
- Secondary Market Bridge: Listed assets automatically connect to RWA DEX for instant trading and liquidity.

RWA Launchpad functions as an “on-chain IPO platform,” enabling RWA project teams to enter capital markets with minimal technical barriers and maximum transparency.

4.3.2 Yield Aggregation Protocol

RWA Earn is an aggregation protocol delivering stable returns to token holders and institutions. It supports staking RWA Tokens into yield pools, where the protocol automatically allocates funds to optimal asset portfolios for income generation.

Revenue sources include:

- Base staking rewards (derived from SRW token inflation)
- Liquidity staking and transaction fee rebates
- Asset income dividends (e.g., bond interest, rental yields)
- Incentive programs (funded by the ecosystem fund)

RWA Earn supports auto-compounding and employs its CaaS module for periodic audits of revenue distribution compliance.

4.3.3 Compliance-Oriented Asset Exchange

SimpleChain integrates an RWA DEX (Decentralized Exchange), redesigning matching and settlement logic for compliant asset trading scenarios.

Features:

- Credit-tiered matching: Prioritizes liquidity for high-credit assets based on RWA Data Credit scores;
- Dual-layer settlement mechanism: On-chain matching with off-chain settlement results verified via on-chain reconciliation;
- Stable Yield Pools: Supports asset collateralization and reinvestment of market-making returns.

The RWA DEX integrates traditional exchanges with DeFi protocols, enabling institutional assets to flow within a fully transparent and compliant environment.

4.3.4 Structured Credit

SimpleChain provides institutions with structured credit products and lending markets.

By tranching RWA Tokens, investment products with varying risk levels can be generated.

Example Rating Criteria:

Tier	Risk Level	Yield	Investor Type
A Tier (Senior)	Low	2-5%	Banks/Insurance Funds
B Tier (Mezzanine)	Medium	6-10%	Professional Investment Institutions
C Tier (Junior)	High	15%+	DeFi Users/High-Risk Funds

This mechanism attracts institutional liquidity while enhancing overall capital utilization.

4.3.5 Liquidity Bridge

The Liquidity Bridge serves as the connector between SimpleChain and external DeFi protocols. It enables users to map RWA Tokens from SimpleChain to other public blockchain ecosystems (e.g., Ethereum, Solana) to participate in their DEX or lending markets.

Through cross-chain locking and token mirroring mechanisms, RWA liquidity can be shared across multiple chains, achieving an “asset-agnostic multi-chain” interoperability framework.

5 Economic System Design

To ensure the sustainable development and ecosystem construction of the public blockchain, and to build a decentralized, secure, stable, and reasonably incentivized blockchain ecosystem, SimpleChain2.0 continues to adopt a hybrid governance approach of on-chain and off-chain. It achieves healthy network development and value stability through five core mechanisms: node lock-up mechanism, node staking rewards mechanism, token burning mechanism, voting mechanism, and self-sustaining positive feedback loop mechanism. This approach balances node incentives with community interests, guaranteeing ecosystem sustainability.

Type	Function	Economic Mechanism
Main-chain Token (SRW)	Payment of gas fee/commission fee, cross-chain transaction fee, DApp consumption, voting, etc.	Node lock-up mechanism, staking rewards mechanism, burning mechanism, etc.

5.1 Main-chain Token SRW

The main chain token SRW is a utility token supporting SimpleChain on-chain operations, such as paying gas fee, cross-chain transaction fee, and DApp consumption.

The initial total supply of SRW is determined based on the active accounts on the SimpleChain validation chain and the RWA market conditions. Subsequently, the circulating supply of SRW is influenced by the staking volume at each phase and incorporates a burning mechanism. Multiple parameters and algorithms are combined to adjust the circulating supply of SRW, thereby meeting the needs of the chain ecosystem development and RWA market promotion.

The supply of SRW will increase when new sub-chain join the SimpleChain network. It is adjusted according to some features of the sub-chain, such as type, tokens supply and price of sub-chains. Type of the sub-chain considers the existence of tokens in sub-chain. In some cases, consortium or private blockchain do not have tokens. Tokens supply is the sum of total tokens in the sub-chain. The value of the

sub-chain refers to the price of token at the time when it join the SimpleChain network.

Assume that n sub-chain join the SimpleChain and ξ indicates whether one sub-chain has tokens or not ($\xi=0$ means sub-chain has no tokens, $\xi=1$ means just the reverse). The total volume of token on the sub-chain i is c_i , while the token price is u_i and SRW price is U_i at the beginning. So the increment of SRW with n sub-chains calculated as:

$$C_{add} = \sum_{i=1}^n \left((1 - \xi_i) \cdot c_i \cdot \alpha + \xi_i \cdot c_i \cdot \left(\beta + \frac{u_i}{U_i} \cdot \gamma \right) \right)$$

Where α represents the impact factor of the sub-chain on main-chain when the sub-chain does not have tokens, β represents the impact factor of the total volume of token on the sub-chain when the sub-chain has tokens, γ represents the impact factor of the sub-chain value on main-chain when the sub-chain has tokens.

5.2 Token Function

SRW is the native utility token of the SimpleChain network, serving the following purposes:

- Gas payments: Transaction and smart contract execution fees;
- Staking and governance: Node elections and voting rights allocation;
- Incentives and rewards: Validator and ecosystem contributor incentives;
- Compliance settlement: Settlement unit for CaaS service fees and audit reports.

5.3 Token Supply and Allocation

Initial Supply: 5,000,000,000 (with slight inflation as the ecosystem grows)

Initial Supply Allocation:

Allocation Party	Percentage	Release Cycle
Early Investors/ Validator Nodes	30%	Node staking, non-unlockable
Operating Team	15%	Node staking, non-unlockable
Ecosystem Fund	20%	Delegated Staking
Financing	15%	Quarterly release starting 12 months later, fully released over three years

Community/Airdrop	15%	Partial circulation post-TGE, remainder released quarterly over one year (details TBD)
Strategic Advisors/ Ecosystem Partners	5%	Quarterly release starting 12 months later, fully released over three years

5.4 Revenue and Deflationary Model

SRW's economic cycle comprises three components:

- Inflation Sources: Newly issued block rewards;
- Burn Mechanism: Partial destruction of transaction fees and compliance service fees;
- Buyback and Redistribution: Foundation periodically repurchases SRW to reward long-term nodes.

The objective is to maintain a long-term Inflation-Neutral Model, ensuring stable token value and sustained network incentives.

5.5 Core Mechanisms of Economic Model

5.5.1 Node Lock-up Mechanism

Nodes must adhere to the ecosystem's lock-up mechanism, complete token staking operations in a system lock up, and meet minimum server resource threshold to qualify for the validator candidate list. The top 13 nodes in the lock-up amount ranking become validators. The node lock-up mechanism introduces new ecosystem collaboration rules, primarily including validator lock-up threshold, co-creation lock-up pool, and validator transfer mechanism, as detailed below:

1. Validator Node Lock-Up Threshold

Validator nodes (there are m validators in total, $m=13$) have an ecosystem minimum lock-up threshold P_{hold} (this threshold parameter can be adjusted via ecosystem development voting). Validator nodes must maintain a self-locked amount S_i consistently greater than or equal to P_{hold} . If a validator node wishes to exit, it must defer to on-chain transfer rule based on the validator node transfer mechanism in SimplChain2.0.

2. Co-creation Lock-up Pool

Ordinary users can choose a validator node for delegated staking. The total locked amounts from validators and ordinary users of delegated stake form the co-creation lock-up pool. Assuming the i -th validator node has k delegators, and the delegated stake amount of ordinary users is S_{ij} ($i=1,\dots,m, j=1,\dots,k$). Then, the main chain token quantity in the i -th lock-up pool is P_i :

$$P_i = S_i + \sum_{j=1}^k S_{ij}$$

Where S_i represents the self-locked amount of the i -th validator node, and S_{ij} represents the delegated stake amount of the j -th delegator under the i -th validator node. P_i and S_{ij} , as the key indicators of the node ecosystem contribution rewards, it corresponds to the distribution ratio of staking reward.

3. Validator Node Transfer Mechanism

If a validator node wishes to exit, it must defer to on-chain transfer rule based on the validator node transfer mechanism in SimplChain2.0. First, the validator node must be active and have fulfilled the minimum lock-up requirement ($\geq P_{hold}$). Second, the validator node must ensure that there are no pending penalty records (e.g., double-signing, offline violations) exist prior to transfer; otherwise, the transfer operation will be restricted.

The transfer process synchronously transfers the validator node's identity and rights. Transferring the node identity means transferring operational control (including node configuration information) to the new validator node. All processes must be completed via on-chain transactions, with identity changes recorded on SimpleChain 2.0 to ensure network-wide node consensus. The total locked pool of the validator node (including self-locked shares and delegator-locked shares) is not directly "transferred". However, the new validator inherits management rights of the node's locked pool, synchronously transferring associated entitlements. This means the original delegators' locked shares remain within the node's locked pool, and the new validator must continue fulfilling responsibilities such as block production and reward distribution.

To guarantee network consistency, the entire transfer process requires on-chain confirmation and implements a transition period mechanism. The original validator node initiates the transfer by signing a transaction specifying the new validator node's address and submitting it on-chain. Concurrently, the transfer transaction must be confirmed by other validator nodes and written into a block to take effect, ensuring network-wide consensus on the identity change. Based on the network's transition period settings (e.g., 1-2 epochs), the original validator node remains responsible for node duties during this phase while the new validator node gradually assumes control, preventing network disruption.

Delegators retain control over their assets. Upon completion of the validator node transfer, corresponding delegators may choose to continue delegating to the new validator node or "undelegate" to transfer staked tokens to other validator nodes. During the entire transfer process, the rights and interests of delegators remain unaffected, preserving their entitlement to reward distribution and staking redemption.

5.5.2 Node Staking Reward Mechanism

The node staking reward mechanism adapts to iterative upgrades of the economic model, primarily implemented across two phases: SimpleChain2.0 Mercury and SimpleChain2.0 Copper. During the Mercury phase, staking rewards are distributed via fixed block rewards method; while the Copper phase employs a dynamic staking incentive adjustment model for reward distribution.

5.5.2.1 Fixed Reward System

During the Mercury phase, validator nodes earn block rewards (including staking rewards and delegator commissions) and transaction fees through self-locking. Delegators can also share block rewards and transaction fees through delegated staking. Staking rewards and delegator commissions enter the lock-up pool as fixed block rewards upon block generation. Delegator commissions can be set by validators and are included in their shares. Transaction fees are determined by the actual transaction volume packaged in the block and are injected into the lock-up pool

synchronously with block generation.

When validators and delegators participate in SRW staking, their staked shares directly determine their proportion in reward distribution. Assuming the i -th validator node has k delegators, and the delegated shares is W_{ij} ($i=1, \dots, m, j=1, \dots, k$). Then, the main chain token shares (i.e., shares value) in the i -th ($i=1, \dots, m$) lock-up pool is D_i :

$$D_i = W_i + \sum_{j=1}^k W_{ij}$$

Where W_i represents the shares of the i -th validator, and W_{ij} represents the delegated stake shares of the j -th delegator under the i -th validator node. As staking volume increases, the shares of validators and delegators increase accordingly, and the corresponding increase shares are ΔW_i and ΔW_{ij} , and vice versa. Concurrently, as block rewards and transaction fees are injected, commission fees are earned by validators, and their increased shares is $\Delta W_i'$, while the delegators' shares remain unchanged.

Validators and delegators share block rewards and transaction fee rewards, with their respective shares determining withdrawable amounts. To ensure the long-term stable operation of SimpleChain2.0 ecosystem and drive technological iteration and ecosystem expansion, Foundation Council will collect the "ecosystem contribution fee" at a fixed rate from on-chain transaction fees and staking rewards. To accelerate transactions reaching finality, the ecosystem has designed the "fast finality confirmation reward mechanism" to incentivize validators to actively participate. A fixed proportion of block rewards is allocated to validators conducting rapid finality voting, thereby expediting transaction finality. Assuming the block reward is T , the fixed rate is κ , and the fast finality confirmation reward ratio is τ , the Foundation's ecosystem contribution fee would be κT , while validator nodes' fast finality confirmation reward would be τT . Then, the remaining block reward is T' :

$$T' = T - \kappa T - \tau T$$

The remaining block reward T' will be fully allocated to the lock-up pool. Validators may set delegate commission rate based on their own ecosystem

development needs. To incentivize delegators to participate in staking, they may set the commission value to 0, and the maximum delegate commission rate threshold is $\rho_{commission}$, with all remaining rewards will be feedback to delegators. Assuming the delegate commission rate of the i -th validator is ρ_i ($0 \leq \rho_i \leq \rho_{commission}$), the corresponding additional delegate commission shares for this validator is $\Delta W_i'$:

$$\Delta W_i' = \frac{\rho_i \times T' \times D_i}{P_i + T' \times (1 - \rho_i)}$$

Staking rewards are distributed based on the shares of validators and delegators. Assuming the validator's increased delegate commission shares is $\Delta W_i'$, while the delegators' shares remains unchanged, the total staking yield for the i -th validator is R_i :

$$R_i = \frac{(W_i + \Delta W_i') \times (P_i + T')}{D_i + \Delta W_i'} - S_i$$

Then, the total staking yield for the j -th delegator under the i -th validator node is R_{ij} :

$$R_{ij} = \frac{W_{ij} \times (P_i + T')}{D_i + \Delta W_i'} - S_{ij}$$

Where S_i represents the self-locked amount of the i -th validator node, S_{ij} represents the staked amount of the j -th delegator under the i -th validator node, P_i represents the main chain token quantity in the i -th lock-up pool, and T' represents the remaining block reward; W_i represents the shares of the i -th validator node, W_{ij} represents the shares of the j -th delegator under the i -th validator node, $\Delta W_i'$ represents the increased delegate commission shares of the i -th validator node, and D_i represents the main chain token shares in the i -th lock-up pool.

5.5.2.2 Dual-Track Reward System

In Copper phase, the economic model will be upgraded by adopting a dynamic staking incentive adjustment mechanism. The node staking reward system is refined

into a dual-track framework comprising basic rewards and contribution rewards, achieving precision in incentives through dynamic rate adjustments. To solidify the foundation for ecosystem development, validator nodes retain distribution rights over staking rewards. This equity protection mechanism attracts more high-quality nodes to join, collectively advancing ecosystem construction. Validators can share staking rewards (including basic and contribution rewards) with delegators, while transaction fees and delegate commissions belong solely to validators. This differentiated rights distribution mechanism establishes a mutually beneficial ecosystem participation model for validators and delegators.

1. Basic Reward

Basic rewards R_b are determined by the nominal interest rate r_b , which is set at a fixed rate to ensure stable returns for validators and delegators. To adapt to ecosystem development needs, this rate can be adjusted through an ecosystem voting mechanism, balancing return certainty with mechanism flexibility. Assuming the self-staked amount of the i -th validator node is S_i , the delegated staked amount of the j -th delegator under the i -th validator node is S_{ij} ($i=1, \dots, m, j=1, \dots, k$), the annual block count of the blockchain is d_{year} , and the number of blocks within the consensus cycle is d_{epoch} , then the basic reward for the i -th lock-up pool is $R_{b,i}$:

$$R_{b,i} = (S_i + \sum_{j=1}^k S_{ij}) \times \left\{ \left(1 + \frac{r_b}{d_{year}} \right)^{d_{epoch}} - 1 \right\}$$

2. Contribution Reward

Contribution rewards adopt a dynamic interest rate adjustment model. The contribution reward rate r_c is linked to multi-dimensional ecological indicators such as inflation rate, validator uptime rate, delegate commission rate, network-wide staking rate, contribution staking rate. This creates an ecosystem self-balancing mechanism of "dynamic metric feedback and intelligent rate adjustment", ensuring reward distribution aligns with validator and delegator contributions while incentivizing nodes to enhance uptime stability and optimize commission strategies. This achieves a win-win for incentive fairness and ecosystem stability.

The inflation rate uses the initial total issuance of the main chain token as a fixed benchmark. Additional tokens are issued based on the release of staking rewards, forming an inflation logic where "rewards drive issuance while the benchmark remains fixed and transparent". This approach safeguards the staking income sources for validators and delegators while allowing ecosystem participants to clearly perceive the dilution of initial equity caused by inflation through the fixed benchmark. Assuming the initial token issuance amount of main-chain is Q_{init} , the additional token issuance amount in the $(t-1)$ -th year is $Q_{issued,t-1}$, the annual issuance amount of basic reward in the $(t-1)$ -th year is $\Delta Q_{b,t-1}$, and the annual issuance amount of contribution reward in the $(t-1)$ -th year is $\Delta Q_{c,t-1}$, then the inflation rate in the t -th year is $r_{inflation,t}$:

$$r_{inflation,t} = \frac{\Delta Q_{b,t-1} + \Delta Q_{c,t-1}}{Q_{init} + \sum_{i=1}^{t-1} Q_{issued,i}}$$

The network-wide staking ratio serves as a crucial metric for evaluating participants' engagement in staking, as well as the network's security and stability. It represents the proportion of the total staked amount of main-chain token SRW relative to the circulating supply amount. The circulating supply denotes the current number of tokens issued and freely tradable on the market, excluding any tokens that have been burned. Assuming the current total issued supply is Q_{total} , the current total burned supply is Q_{burned} , and the main-chain token quantity in the i -th lock-up pool is P_i , then the total network-wide staking ratio is $r_{staking}$:

$$r_{staking} = \frac{\sum_{i=1}^m P_i}{Q_{total} - Q_{burned}}$$

The contribution staking ratio quantifies a validator node's core contribution to the ecosystem. Delegators prioritize validator node with high credibility and stable service, while validators attract delegators to stake in order to increase their contribution staking reward rates. The total staked amount by delegators within a lock-up pool directly reflects a validator node's "trustworthiness and ecosystem influence". Higher delegated staking volumes indicate stronger ecosystem recognition

for the validator node. Assuming the staking amount of the j -th delegator under the i -th validator node is S_{ij} , and the main chain token quantity in the i -th lock-up pool is P_i , then the contribution staking ratio of the i -th validator node is:

$$\varphi_i = \frac{\sum_{j=1}^k S_{ij}}{P_i}$$

The uptime rate of validator nodes is a core metric for measuring the stability and reliability of validator nodes within a blockchain network. It indicates the participation level of validator nodes in consensus block generation, enabling determination of whether they remain continuously online and fulfill their validation responsibilities. In the consensus mechanism, validator nodes are required to collect, verify, and package the transaction data generated in the network within a certain period of time to form new blocks, and broadcast them throughout the network. Therefore, the total number of blocks that each validator node should produce under the condition of "remaining online throughout the process and performing duties normally" is jointly determined by the consensus mechanism, the validator's qualifications, and the duration of the consensus cycle. During the consensus cycle, assuming the total number of blocks produced that the i -th validator node should participate in according to consensus rules is $V_{epoch,i}$. If the missed number of blocks produced it failed to generate blocks within the specified time due to "offline status, network failure, node crash" is $V_{missed,i}$, then the validator node uptime rate is θ_i :

$$\theta_i = \frac{V_{epoch,i} - V_{missed,i}}{V_{epoch,i}}$$

Assuming the inflation rate in the t -th year is $r_{inflation,t}$, the network-wide staking rate is $r_{staking}$, the uptime rate of the i -th validator node is θ_i , the delegate commission rate of the i -th validator node is ρ_i , and the contribution staking rate of the i -th validator node is φ_i , then the contribution reward rate of the i -th validator node is $r_{c,i}$:

$$r_{c,i} = r_{inflation,t} \times \theta_i \times (1 - \rho_i) \times \frac{1}{r_{staking}} \times \sqrt{\varphi_i}$$

The calculation of contribution rewards is primarily based on the contribution reward rate, so the level of this rate directly impacts the contribution reward income of validator nodes. Assuming the self-staked amount of the i -th validator node is S_i , the delegated staked amount of the j -th delegator under the i -th validator node is S_{ij} ($i=1,\dots,m, j=1,\dots,k$), the annual block count of the blockchain is d_{year} , and the number of blocks within the consensus cycle is d_{epoch} , then the contribution reward for the i -th lock-up pool is $R_{c,i}$:

$$R_{c,i} = (S_i + \sum_{j=1}^k S_{ij}) \times \left\{ \left(1 + \frac{r_{c,i}}{d_{year}} \right)^{d_{epoch}} - 1 \right\}$$

5.5.3 Burning Mechanism

The burning mechanism is designed through three dimensions "transaction consumption + market regulation + slashing for violations" to achieve dynamic balance in token circulation and value anchoring.

1. Transaction Fee Burning

Differentiated burning ratios are set for various transaction types (determined by time-based voting) to precisely match network resource consumption:

- Regular Transfer Transactions: Assuming the burning ratio of regular transfer transaction is p_1 , then the transaction burned amount D_{p1} = regular transfer transaction fees $\times p_1$.
- Smart Contract Deployment/Invocation: Assuming the burning ratio of smart contract deployment is p_2 , then the smart contract deployment burned amount D_{p2} = smart contract deployment fees $\times p_2$. Assuming the smart contract invocation burned ratio is p_3 , the smart contract invocation burned amount D_{p3} = smart contract invocation fee $\times p_3$. Complex contracts (e.g., code length > 1000 lines) incur the additional burning ratio;
- Cross-chain transactions: Assuming the burning ratio of cross-chain transaction is p_4 , then the cross-chain transaction burned amount

D_{p4} = cross-chain transaction fee $\times p_4$. Cross-chain transactions require multi-node verification, resulting in higher resource consumption

All burned token is recorded to the burning address (black hole address) in real-time. The total burning amount is periodically updated and publicly disclosed.

2. Buyback and Burning

Periodically repurchase tokens from the market and destroy them to smooth price fluctuations and strengthen token value support.

3. Slashing Burning

Implement staked token burning method for node violations to strengthen compliance constraints:

- Minor Violations (e.g., uptime below threshold p_r , data synchronization delays): No staked token burned, only partial monthly rewards are deducted.
- Moderate Violations (e.g., validation error rate exceeding specified threshold, refusal to provide basic services): Assuming the moderate violation ratio is p_c , then the burning amount of moderate violations D_{pc} = staked amount of validator $\times p_c$.
- Severe violations (e.g., malicious forking, data tampering, unauthorized signing): All staked tokens of the validator are burned. If the validator has delegators, a proportional reward burning applies to associated delegators (without burning token staking).

5.5.4 Voting Mechanism

The voting mechanism centres on "anchoring voting rights to locked quantities to determine core parameters", employing dynamic weighting design to ensure scientific decision-making. Specific rules are as follows:

1. Voting Rights: Locked and Calculation

Voting rights are obtained by locking main-chain tokens, with locking actions directly linked to voting weight. A user's voting weight is calculated as:

$$V = S \times t_k \times l_k \times n_k$$

Where each parameter is defined as follows:

- S represents the amount of tokens voluntarily locked by the user (excluding basic lock-up, requiring additional locking)
- t_k represents the lock-up time coefficient (unlocking is prohibited during the lock-up period; voting rights expire upon unlocking)
- l_k represents the user tier coefficient (verification nodes, ordinary users, etc., possess distinct coefficients)
- n_k represents the historical participation coefficient (determined by the number of voting cast).

Total voting count $V_A = \sum V$, with each node's voting weight is V/V_A , determining its influence on proposals.

2. Voting Parameters and Proposal Categories

The voting mechanism focuses on adjusting core economic parameters, categorising proposals into three types:

- Core Parameter Proposals: Adjust nominal interest rate, inflation rate, minimum staking thresholds for validator nodes, etc.
- Mechanism Parameter Proposals: Adjust burning ratios of fees, repurchase pool allocation percentages, etc.;
- Emergency Parameter Proposals: Under extreme market conditions, temporarily modify reward rate decay rates, emergency repurchase trigger thresholds.

3. Voting Incentives and Constraints

- Participation Rewards: Nodes participating in valid votes (non-blank ballots) receive token allocations from the reward pool;
- Invalid Vote Constraints: Nodes casting blank ballots three consecutive times or failing to vote five cumulative times will have their voting weight coefficient reduced to the standard user level or corresponding tier's minimum value in the following quarter;
- Parameter Execution Oversight: Following parameter adjustments, smart contracts automatically log execution outcomes. Blockchain explorer display

real-time comparisons of economic metrics (e.g., inflation rate, nominal interest rate).

5.6 Self-driven Positive Feedback Loop Mechanism

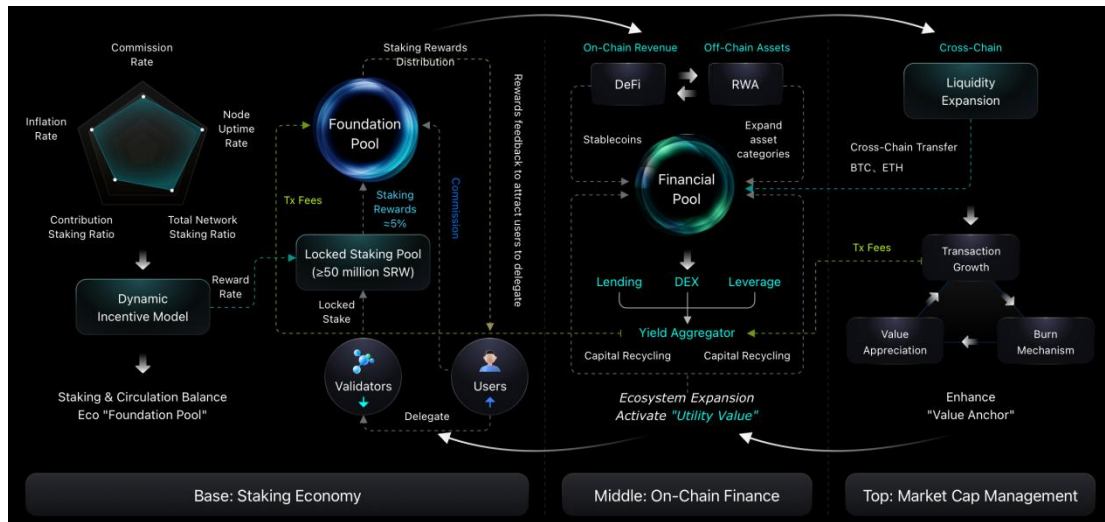


Figure Positive Feedback Loop

Building upon the economic model upgrades in the Copper phase, SimpleChain2.0 ecosystem embeds a closed-loop feedback logic of "incentive regulation–financial activity– market capitalisation transmission", further establishing a self-driven positive feedback loop mechanism. Leveraging dynamically optimised economic parameters (such as the dynamic contribution staking ratio and delegated commission rates) from the incentive adjustment model, this mechanism initiates capital pool ecosystems to stimulate on-chain financial activities (e.g., lending, DEX, leverage), the mechanism activates capital utilisation value through scaled expansion of both RWA and DeFi ecosystems. Cross-chain interactions and token burning mechanisms then drive market capitalisation growth, which in turn reinforces incentive efficacy. This ultimately forms a self-sustaining virtuous cycle: "incentive adjustment → financial activity → market cap growth → incentive optimisation".

The bottom layer of ecosystem is its staking economy layer. Ordinary users may participate in staking via the low-barrier method of "delegating to validator nodes" to earn rewards from the basic liquidity pool. Concurrently, the dynamic staking incentive adjustment model continuously optimises incentive rules in real-time,

dynamically regulating user staking willingness and token circulation scale. This ultimately establishes an ecological equilibrium between "staked lock-up volume" and "market circulation demand". The middle layer of ecosystem is the on-chain finance layer, integrating three asset dimensions—staking reward, stablecoins, and RWA assets—to form a financial capital pool. Cross-chain interactions introduce cross-chain assets, continuously enriching the pool's asset categories and scale. Yield aggregation mechanisms then generate targeted capital reflux, activating the financial value cycle: "asset pooling → yield generation → capital reflux → asset expansion". The upper layer of ecosystem is the market capitalisation management layer. On the one hand, it reduces transaction friction and enhances trading activity through liquidity expansion. On the other hand, it employs the burning mechanism to decrease circulating supply, thereby strengthening token scarcity and elevating value anchors. Furthermore, elevated market capitalisation translates into ecosystem appeal, attracting new users to participate in on-chain staking and financial activities while amplifying enthusiasm for asset tokenisation. Then, the incentive framework towards greater efficiency and precision through dynamic data feedback mechanism, ultimately creating a mutually reinforcing relationship between token incentives and market capitalisation.

6 Global Compliance

Establish a protocol system compliant with global multi-regional regulatory requirements. Embed financial cross-border security and data cross-border security rules into business processes through technical components, while providing regulators with secure, efficient collaboration tools to achieve synergistic advancement of “blockchain innovation” and “regulatory compliance.”

6.1 Compliance Execution Unit

Translate financial compliance and data compliance requirements into automatically executable technical logic, ensuring all on-chain financial activities and data flows operate within the compliance framework.

1. Modular Architecture Design

The Compliance Execution Unit (CEU) adopts a “core engine + plug-in modules” structure: the core engine handles rule parsing, execution scheduling, and result verification; plug-in modules support on-demand integration for specific compliance scenarios (e.g., Know Your Customer (KYC), transaction limit controls), enabling rapid adaptation to regional regulatory details.

2. Real-Time Compliance Monitoring and Interception

Continuously scans on-chain transactions, asset transfers, and user interactions against embedded compliance rules. Upon detecting compliance risks, the CEU automatically executes interventions—such as transaction suspension, risk alert notifications, or triggering manual review workflows—to intercept non-compliant activities.

3. Cross-Border Data Compliance Coordination Module

CEU's built-in data classification engine automatically identifies cross-border data types circulating on the chain and matches them to corresponding cross-border rules based on sensitivity levels. It interfaces with major global cross-border data compliance systems, synchronizing regulatory updates in real time. When cross-border data flows change, it automatically switches compliance validation logic.

If non-compliant cross-border data activities are detected, it immediately blocks data transmission while generating a Cross-Border Data Risk Report, which is pushed to the protocol compliance department and relevant regional regulators.

6.2 Programmable Rules

Breaking free from traditional “fixed rule” limitations, it enables customization of Anti-Money Laundering (AML) rules and cross-border data-related programmable rules based on business type and regional requirements, achieving collaborative configuration of “finance + data” compliance rules.

1. Combination of Rule Templates and Customization

Built-in standardized rule templates: Includes standardized AML rule templates and cross-border data compliance templates, such as “Large Transaction Reporting,” “Suspicious Transaction Identification,” “Security Assessment Trigger for Cross-Border Personal Data,” and “Data Outbound Whitelist Control.”

Support for Custom Rule Syntax: Configure bespoke rules via a visual interface or API. Rule updates automatically synchronize to the CEU module without interrupting on-chain operations.

2. Traceability of Rule Execution

All rule creation, update, and execution records are chain-based and notarized, including details such as “Rule Creator,” “effective date,” “execution cases,” and “modification logs,” ensuring auditable and traceable rule execution while mitigating compliance risks.

6.3 Tiered Regulatory Node Permissions

Provides regulators with a tiered, controllable node permission system, enabling precise intervention at specific stages. This approach safeguards regulatory requirements while preventing excessive interference with normal on-chain operations.

1. Permission Levels and Functions

Attribute	Permission Level	Core Function	Applicable Scenarios
Financial Compliance	Read-Only Audit	View on-chain transaction records, user identity mapping relationships (after data masking), compliance rule execution logs, etc.	Routine regulatory audits, data statistical analysis.
	Risk Alert	On top of read-only access, receive compliance risk alerts pushed by CEU and initiate manual review requests.	Risk event tracking, compliance spot checks.
	Emergency Intervention	Temporarily freeze high-risk account assets and suspend non-compliant transactions on top of alert permissions; intervention records are immediately recorded on-chain.	Handling major non-compliance incidents, emergency AML responses.
Data Compliance	Read-Only Audit	View cross-border data flow records, data anonymization logs, overseas recipient registration information, etc.	Daily cross-border data compliance audits, cross-border data flow statistics.
	Risk Alert Authority	Receive cross-border data risk alerts pushed by CEU and initiate data compliance review requests.	Track cross-border data risk incidents and conduct spot checks on sensitive data outbound transfers.
	Emergency Intervention Authority	Building upon alert authority, temporarily block high-risk cross-border data transfers and require parties to submit supplementary materials for data outbound transfers. Intervention records are recorded on the blockchain in real time.	Emergency handling of non-compliant cross-border data and prevention of core data leakage risks.

2. Permission Control and Safeguards

Regulatory nodes employ a “multi-signature authorization + identity binding” mechanism: Regulatory permissions require multi-signature confirmation to activate, and node identities are bound to official regulatory agency credentials to prevent unauthorized access. All permission operations are fully audited: Every action by

regulatory nodes generates tamper-proof operation logs detailing the operator, time, content, and outcome, enabling traceability and auditability by higher-level regulatory authorities.

6.4 Intelligent On-Chain Activity Audit Report

Focusing on “full-scenario coverage of on-chain activities, real-time report generation, and flexible export adaptability,” we establish an end-to-end real-time workflow from on-chain data collection to report delivery. This enables audit reports to be generated and exported as soon as on-chain activities occur.

1. Real-Time Collection and Integration of On-Chain Activity Data

Establishes the data foundation for real-time report generation by building an efficient on-chain data synchronization mechanism covering all dimensions of on-chain activities.

- Comprehensive Data Collection Scope: Real-time synchronization of all on-chain activity data, including financial, data, user, and system categories;
- Millisecond-Level Synchronization Support: Utilizes a “direct on-chain node connection + stream processing engine” architecture to capture data within a defined timeframe after on-chain events occur. Data undergoes real-time cleansing, classification, and synchronization to the report generation database, ensuring zero delay and no omissions;
- Data authenticity verification: Collected data is bound to on-chain block hashes. Each activity record includes triple verification information—block height, timestamp, and transaction hash—ensuring report data is traceable, tamper-proof, and resistant to forgery.

2. Real-Time Generation Mechanism for On-Chain Activity Audit Reports

Breaking away from post-event aggregation, this achieves full-process automation and real-time execution: “Activity Occurs → Data Synchronization → Report Fragment Generation → Complete Report Assembly.”

- Real-time Multi-dimensional Template Matching: An integrated library of standardized real-time report templates covers high-frequency regulatory scenarios.

When on-chain activity triggers a specific scenario, the system automatically matches the corresponding template.

- **Dynamic Report Generation Logic:** Employing a “fragmented generation + real-time assembly” approach, each synchronized on-chain activity immediately generates a corresponding report fragment. Upon user instruction to generate a report, the system assembles these fragments into a complete audit report.

- **Real-time updates and version management:** If subsequent status changes occur in on-chain activities, the system automatically updates corresponding report fragments and generates new report versions. These versions are annotated with “update time, update content, and update reason,” while historical versions are retained for traceability.

3. Flexible real-time export functionality for on-chain audit reports

Designed around “multi-role, multi-scenario, multi-format” requirements, a highly adaptable real-time export mechanism ensures reports can be delivered quickly and used directly:

- **Multi-trigger adaptability:** Supports both “manual one-click export” and “automatic scheduled export” modes to accommodate diverse use cases;

- **Full format compatibility:** Export formats cover regulatory and operational requirements, including compliance archiving (PDF), secondary data analysis (CSV/Excel), and system integration (JSON/XML);

- **Export Permissions & Security Controls:** Export permissions are configured based on the “least privilege” principle, allowing each role to export only reports within their authorized scope. All export operations generate logs, which are instantly recorded on the blockchain for evidence storage, preventing unauthorized exports or loss of export records.

6.5 Specialized Safeguards for Cross-Border Data Security

1. Pre-Cross-Border Data Transfer: Compliance Access Controls

Pre-Assessment Mechanism: Automatically initiates compliance assessments for proposed cross-border data to determine if it qualifies as “core data” or “important data.” If so, triggers regulatory approval processes; data failing approval is prohibited from leaving the country. **Recipient Verification Mechanism:** Overseas recipients must submit regulatory filing certificates, compliance pledges, and data security assurance plans. Only after dual verification by the CEU and regulatory nodes can they be added to the cross-border data whitelist.

2. During Cross-Border Data Transfer: Transmission Security Protection

Encrypted Transmission Channels: Establish dedicated cross-border data transmission channels to prevent data theft or tampering during transit. **Real-time Monitoring & Alerts:** Continuously monitor cross-border data traffic volume, speed, and frequency. Immediately suspend transmission and trigger alerts upon detecting anomalies.

3. Post-Cross-Border Data: Traceability & Control

End-to-End Evidence Storage: Transmission records, compliance verification results, and recipient processing logs are all stored on-chain as evidence, with retention periods compliant with regional regulations.

The Audit Module of CaaS periodically generates audit reports:

- Report formats comply with ISO/IEC 27001 and FATF requirements;
- Report summaries are recorded on the blockchain, with full texts stored encrypted;
- Authorized parties may export reports via access interfaces.

Cross-border data transmission employs encrypted tunnels and multi-region node relays to ensure compliance with local data protection laws across different jurisdictions.

7 Ecological Development

Breaking the "crypto-native loop" through the on-chain of real assets, deeply coupling real-world cash flows and credit systems with SimpleChain's programmability, activates the ecological vitality of the public blockchain, and achieves the economic development of the network ecosystem through the "benefit overlay model", generating economic value beyond expectations.

The total economic benefits of the ecosystem R_{total} follow the three stages of RWA ecosystem value growth (base layer, amplification layer, incremental layer) :

$$R_{total}=R_0\times(1+e_s+e_c+e_l)+\Delta R$$

Variable definition:

- R_{total} : The total economic benefit SimpleChain gains from the RWA ecosystem (including fees, staking income, ecosystem share, etc.);
- R_0 : Basic benefits (linear returns on a single asset/scenario, such as initial transaction fees, simple staking interest, etc.);
- e_s : Scale effect coefficient (reflecting the amplification effect of asset size growth on returns);
- e_c : Synergy coefficient (reflecting the additional benefits brought by cross-asset/scenario linkages);
- e_l : Leverage coefficient (reflecting the amplification effect of financial instrument leverage on returns);
- ΔR : Unexpected returns (liquidity revaluation, cross-border dividends, technology iteration, and other non-linear increments).

7.1 Fundamentals Drive

The fundamental drive R_0 of the RWA ecosystem to SimpleChain, from "traffic injection" to "ecosystem closed loop", that is, the anchoring role of the foundation layer in the three stages, represents the "linear returns" (such as initial transaction fees, simple staking interest) in a single asset/scenario, and is the value anchor point of the entire ecosystem. The core feature of RWA is that it must rely on the cash flow or

value base of real assets rather than pure crypto-native bubbles, such as the entire industrial chain assets of drones, computing power and Internet of Things devices, to ensure that the public blockchain returns are supported by physical value.

1. Cross-circle penetration of users and funds

RWA brings traditional financial institutions (banks, asset management companies), physical enterprises (high-tech enterprises, manufacturers), and a vast number of long-tail investors into the public blockchain ecosystem. For instance, the fragmentation of emerging industries attracts ordinary investors, and the tokenization of government bonds attracts institutional funds seeking low-risk returns. These participants are neither native crypto users nor bring in incremental funds. According to Chainalysis data, 63% of the funds flowing into the RWA track in 2024 came from traditional financial channels, directly driving a 210% increase in daily active users of public blockchain and a \$34 billion increase in total value locked (TVL).

2. An exponential expansion of application scenarios

Derivative scenarios based on RWA extend from basic "asset trading" to "staking lending", "insurance hedging", and "supply chain finance". Companies can use accounts receivable tokens for staking financing on public blockchain to reduce financing costs; Investors can hedge risks by combining Treasury tokens with emerging industry tokens. These scenarios drive the expansion of the public blockchain developer ecosystem, with the number of teams focused on RWA tool development growing rapidly in 2024, forming a full-chain service system from asset on-chain, compliance audits to transaction clearing

3. Anchoring of network value

Cash flows from traditional assets (such as bond interest, operating income) are continuously injected into the public blockchain through orchards, transforming the public blockchain token from a "purely speculative target" into a "value carrier backed by real returns". By anchoring fiat currency or government bonds, high interest income is generated annually and distributed to token holders according to rules, directly enhancing the intrinsic value of the token and reducing price volatility.

7.2 Benefit Accumulation

The benefit superposition model creates multi-dimensional value resonance to generate multiplier effects. The economic benefits of the RWA ecosystem are not the linear accumulation of a single link, but rather through the superposition of "scale effect $\times$ synergy effect $\times$ leverage effect" to produce multiple amplification effects, that is, the multiplier effect of the amplification layer $(1+e_s+e_c+e_l)$. The superposition of the three major effects of scale (e_s), synergy (e_c), and leverage (e_l) is essentially the nonlinear amplification of the underlying value by the network effect.

The value growth of the RWA ecosystem is not a linear accumulation but a mutual energize among assets, scenarios, and tools: the expansion of asset scale enhances liquidity (e_s), the improvement of liquidity promotes cross-scenario linkage (e_c), and when linkage matures, it gives rise to financial instrument innovation (e_l), and the three form a "positive feedback loop".

1. Scale effect: The positive cycle of asset size and network effect

As more assets go on-chain, the liquidity pool depth of the public blockchain increases and the transaction slippage (bid-ask spread) decreases, further attracting new assets to enter and forming a positive cycle of "asset size $\rightarrow$ liquidity $\rightarrow$ new assets", which will cause the transaction fee income of the public blockchain to show an "exponential growth". Therefore, the scale effect coefficient:

$$e_s = k_s \times (\ln A - \ln A_0)$$

Where A is the current total size of RWA assets; A_0 is the initial asset size, k_s is the scale sensitivity coefficient, a core parameter for measuring the intensity of the interaction between asset size and economic benefits. The higher the asset liquidity, the greater the scale sensitivity coefficient (for highly liquid assets, the impact of scale on benefits is more significant due to active trading and obvious cost dilution).

In the early stage of asset size growth, liquidity increases significantly and earnings grow rapidly; But when the scale exceeds the critical point, marginal improvement in liquidity weakens and earnings growth slows. Therefore, the scale effect shows the characteristics of being "fast in the early stage and stable in the later

stage." The relationship between the value of the public blockchain and the size of its assets conforms to Metcalfe's law (the value of the network is proportional to the square of the number of nodes), but RWA, constrained by the supply of physical assets, cannot expand infinitely. The logarithmic function is modified to "moderate amplification", reflecting the network effect while avoiding excessive optimism.

As the asset size grows, the value of the public blockchain (which can be measured by metrics such as market capitalization, transaction fees, user activity, and the number of ecosystem applications) shows the characteristic of "growing with the square of the number of interconnections of assets". Value grows slowly when the asset size is small in the early stage, and then explosively when the asset size exceeds the critical point in the growth stage. When the asset size approaches saturation in the mature stage, value growth slows (constrained by the "effective connection cap").

2. Synergies: Doubling of returns through cross-scenario linkages

Different assets and scenarios within the RWA ecosystem can empower each other to generate additional revenue. For example, drone token holders can stake their assets to lending protocols to obtain stablecoin loans, which can then be reinvested in high-yield private credit tokens to create a secondary appreciation of "staking interest + investment income"; In supply chain finance scenarios, the accounts payable tokens of the core enterprise can be split and circulated by small and medium-sized enterprises upstream and downstream, reducing overall supply chain costs while generating more transfer fees for the public blockchain and enhancing the liquidity premium of the core enterprise token. Synergy will make the overall revenue of the public blockchain (fees + staking income + ecosystem share) much higher than the expected revenue in the single-asset scenario.

Synergies come from cross-asset/scenario linkages, positively correlated with asset diversity and interaction frequency, with the core being the additional value created by asset diversity and interaction frequency:

$$e_c = k_c \times \sum_{i=1}^n \sum_{j=i+1}^n (a_i \times a_j \times f_{ij})$$

Where n is the number of RWA asset types; a_i is the proportion of the scale of

assets of class i , $\sum a_i = 1$. f_{ij} is the interaction frequency between assets of class i and assets of class j , the higher the frequency, the greater the synergy value; k_c is the synergy coefficient. When the complexity does not exceed the carrying capacity of the synergy mechanism, the more complex the scenario is, the greater the value of the synergy coefficient will be.

Value comes from connection rather than isolation. The returns of a single asset are limited, but when linked with multiple assets, new value is generated. When the types of assets increase, the number of cross-items grows geometrically, showing the rule that "the higher the diversity of assets, the greater the potential for synergy," which is consistent with the phenomenon of accelerated revenue growth in the RWA ecosystem as it expands from a single asset to a full category in reality.

3. Leverage effect: The amplification of returns by financial instruments

The programmability of public blockchain enables the development of structured financial products (such as options and futures) based on RWA, and amplifies returns through leverage. Such tools, though accompanied by risks, objectively increase the trading activity of public blockchain.

The leverage effect is positively correlated with the average leverage multiple of financial instruments. Financial instruments can controllably amplify returns, but not unboundedly magnify risks.:

$$e_l = k_l \times (L - 1) \times r$$

Where L represents the average leverage multiple of RWA derivatives; r is the proportion of leveraged transactions in total transactions. The more leveraged transactions there are, the greater the impact on total returns. $(L - 1)$ represents the "excess amplification multiple", and the product of r and it directly reflects the degree to which leverage amplifies returns.

k_l is the leverage risk coefficient, a "risk constraint parameter" set based on the risk characteristics of assets (such as volatility, liquidity, credit risk, etc.), with a value range typically between 0 and 1. The higher the leverage stability, the greater the value of the risk coefficient. The introduction of the leverage risk coefficient k_l is

due to the fact that while leverage amplifies returns, it also magnifies risks, and a coefficient is needed to balance this. For instance, assets with high volatility have a lower value to prevent the risk of liquidation caused by excessive leverage. Compared to native crypto assets, the application of leverage in RWA places more emphasis on risk control, and thus incorporating risk constraints aligns with the "compliance first" nature of the RWA ecosystem.

7.3 Exceeding Expectations in Earnings

The source of the unexpected returns is non-linear variables and "unexpected dividends". The unexpected returns of the RWA ecosystem often come from non-linear variables that break through the initial design, which are unique advantages of the public blockchain that are difficult to replicate in the traditional financial system.

$$\Delta R = \Delta R_1 + \Delta R_2 + \Delta R_3$$

The variables are defined as:

ΔR_1 : Liquidity revaluation gains, $\Delta R_1 = \text{Public blockchain share ratio of asset} \times \text{appreciation after tokenization}$;

ΔR_2 : Cross-border dividend, $\Delta R_2 = \text{traditional cross-border cost savings} \times \text{public blockchain service fee ratio}$;

ΔR_3 : Technology and service iteration revenue, $\Delta R_3 = \text{Incremental revenue from new scenarios}$.

1. The revaluation dividend of liquidity release

In traditional markets, a large number of assets are severely undervalued due to poor liquidity or difficulty in liquidity (such as drone ownership or operational income rights, etc.). After going on-chain, enhanced liquidity leads to a revaluation of value, and valuations will rise significantly. The increase in asset value feeds back to the public blockchain through transaction fees, staking interest, etc., generating better-than-expected returns.

2. Frictional cost dividends in cross-border circulation

The global nature of public blockchain enables RWA to break through

geographical limitations and significantly reduce the time and capital costs of cross-border transactions. Some of the cost savings are used as chain service fees to generate incremental revenue, and this cross-border advantage has enabled chain revenue growth in emerging markets to far exceed expectations.

3. Unexpected scenario dividends from technological and service iterations

Iterations of public blockchain technologies (such as zero-knowledge proofs, cross-chain protocols) and related services introduced into the ecosystem (compliance, auditing, etc.) often give rise to unforeseen RWA scenarios. The continuous improvement of the ecosystem will attract different types of assets and bring unexpected staking and trading returns.

8 SimpleChain Foundation

8.1 Mission and Vision Statement

The SimpleChain Foundation focuses on operating the open-source community. Guided by the development philosophy of "blockchain services for simple, efficient and high-performance" and adhering to the principle of "value on-chaining and physical asset on-chaining", it cultivates developer communities and empowers emerging economies such as AI and Web3.

8.2 Standing Bodies of Foundation

The standing bodies of this foundation are Council, who is responsible for a comprehensive community governing as a whole for healthy development, and Technical Steering Committee, who is focusing on the technological development of the SimpleChain and technical community. Two standing bodies make decision by members voting for their own responsibilities respectively. The operational funds comes from donation of the SimpleChain community.

- Registered Location: Singapore
- Nature: Non-profit organization responsible for ecosystem governance and fund allocation
- Primary Responsibilities:
 - a. Maintain mainnet operations and open-source code governance;
 - b. Fund ecosystem projects and community developers;
 - c. Manage SRW reserves and ecosystem funds.

8.3 Source of Fundation Funds

The operational funds of SRW comes from the SimpleChain's community members' donation and the foundation serves as a non-profit organization for SimpleChain. SimpleChain foundation will have designated digital asset wallet address and smart contract account to receive either direct-digital asset or computing power donation. For the pre-determined rules of consensus mechanism of SimpleChain2.0, 5% of the total staking rewards and transaction fees will automatically transfer to the smart contract account of SimpleChain foundation.

8.4 Team and Technical Council

Core Team: Responsible for system architecture design and technical iteration;

Tech Council: Composed of core developers and node representatives;

Compliance Board: Composed of legal counsel, regulatory advisors, and third-party auditors;

Advisors: Industry experts and institutional consultants.

Appendix and Reference Index

A. Technical Interface Examples

DataIPO Interface Sample

Plain Text

```
POST /api/dataipo/register
```

```
{  
  
  "asset_id": "RWA-2025-0001",  
  
  "issuer": "Company A",  
  
  "valuation": 1000000,  
  
  "segments": 1000,  
  
  "oracle_source": "IndustryOracle",  
  
  "compliance_check": "CaaS"  
}
```

CaaS Audit Template Example

Plain Text

```
{  
  
  "jurisdiction": "HK",  
  
  "modules": ["KYC", "AML", "DataCrossBorder"],  
  
  "report_type": "audit",  
  
  "output": "encrypted_pdf"  
  
}
```

B. Technical Specifications Summary

Project	Parameters
Consensus Mechanism	PoS
Average Block Time	0.75 seconds
Transaction Confirmation Time	<2 seconds
TPS	4,000+
Node Requirements	16GB RAM/1TB SSD/100Mbps network
Security Audit Frequency	Quarterly

Conclusion

SimpleChain is not merely a public blockchain project, but a systematic solution for tokenizing real-world assets. Centered on the core principles of technological trustworthiness, data integrity, and regulatory compliance, it establishes a complete ecosystem for Real-World Assets (RWA), spanning from ownership verification to seamless circulation. Against the backdrop of the rapidly expanding global RWA market, SimpleChain is committed to serving as a bridge connecting the real economy with Web3 finance, driving the digitization, compliance, and globalization of traditional assets.