SFT Protocol Whitepaper

Summary:

The SFT protocol is a cross-chain communication and modular underlying application public chain based on the Cosmos architecture. It aims to solve the problem of assets that are locked for the medium and long term and cannot be freely circulated, such as FIL, DOT, ETH2.0, etc. It provides a decentralized protocol that enables locked assets to flow freely. By staking the native tokens of the original public chain, SFT tokens are minted to solve liquidity problems. Users can obtain SFT tokens and engage in SFT trading, staking mining/liquidity mining, DeFi lending, DAO governance, NFT minting, public chain node application deployment, hardware infrastructure invocation, and more within the SFT protocol. The SFT protocol supports staking and redemption of native tokens, ultimately achieving on-demand withdrawal. All operations are executed in a decentralized manner by smart contracts and verification nodes.

Under the SFT protocol, a hardware infrastructure that is extended to various blockchain API interfaces is gathered, to build cloud service nodes that are required for the future of Web3 and Metaverse. At the hardware level, it achieves distributed, automatic expansion, and multi-cloud network aggregation, and continuously provides a combination of privacy computing, storage solutions, and high-performance GPU computing, to respond to complex customer demands and provide more secure and efficient infrastructure services, helping enterprises better access the Web3 field. At the same time, the SFT protocol securitizes the underlying hardware assets and maps the income of upper-layer protocols, achieving "cross-chain" of another kind of blockchain and entity economic activity, and providing diversified investment channels for investors.

1. Project Background

With the launch and development of projects such as FIL, Cosmos, and Polkadot, token holders can participate in system consensus by simply staking their tokens. Throughout the process, token holders only need to run a certain standard server or delegate to professional validators to start mining. Early public chains, whether PoW or PoS, integrated incentive measures to encourage more nodes to participate in the operation. Therefore, to strengthen system security by locking up more initially distributed tokens, stakers bear a certain amount of time and opportunity costs. If incentives are low in the early stages, the mainnet will face serious security threats. Public chain token holders can initiate unlocking at any time, but during the unlocking period, tokens cannot be traded, and holders still cannot avoid the risk of token value fluctuations during this stage. This is a contradiction between TokenStake security and token liquidity, causing many people to hesitate to stake their tokens in public chain systems.

Therefore, we decided to create a decentralized protocol to solve the problem of public chain assets being locked up for the medium and long term, allowing locked assets to flow freely. By minting SFT tokens to solve liquidity, while collateralizing the original tokens on the chain, we can simultaneously obtain staking rewards and ensure the security of the public chain system. The SFT protocol will establish a large amount of infrastructure while supporting basic public chains such as FIL, and gather cloud node API interfaces on this basis to provide various cloud services needed to build future Web3 and metaverse, flexibly meeting customers' needs in privacy computing, storage solutions, and high-performance GPU computing.

Since its official launch in 2020, Filecoin has established a large community consensus. However, FIL physical mining involves staking coins, GAS, linear release mechanism, mining efficiency, etc. Miners need to provide a certain amount of staking coins while providing hardware equipment. At the same time, the rewards mined have a linear release mechanism, and the liquidity of FIL is long-term locked. Participants will face weak risk resistance against market fluctuations. Therefore, the SFT protocol proposes a solution. Based on the application instance of the SFT protocol in the Filecoin network, token holders exchange the equivalent SFT tokens for equivalent assets through staking. Users can stake 1 FIL and receive SFT equivalent to the original token (currently 1:1). After the lock-up period ends, users can choose to destroy SFT and recover the staked FIL. Users can stake FIL at any time, trade and redeem flexibly, and exit at any time in the SFT protocol. The goal of the SFT protocol is to build a liquidity mining pool on Filecoin and achieve perpetual computing power revenue. In this way, FIL holders will have stronger ability to resist market fluctuations and more flexible participation methods to achieve maximum investment returns.

2. SFT Protocol Objectives

2.1 On-Chain Contract Protocol:

Solve the problem of public chain assets that are locked by pledging in the medium and long term, provide a decentralized protocol, release liquidity, expand the liquidity ecosystem, integrate with various DeFi ecosystems, and solve the liquidity of public chains and protect user profits by minting SFT tokens.

2.1.1 Releasing Liquidity

The SFT protocol establishes a StakingContract at the upper level, through which holders can initiate staking and receive the SFT token. The holder's stake process and SFT issuance process are automatically executed by contract code, without any third-party endorsement. In addition to no third-party involvement, all SFT issuance rights are returned to the original

chain token holders. The staking of billions of dollars in market value on the POS public chain will increase the quantity of SFT on the market, supporting the SFT derivatives trading market and promoting liquidity in leveraged trading, for example. Holders can continue to earn profits through staking, but the future profit expectations in fiat currency are still volatile, leading to inconsistencies in market expectations for SFT trading. This will encourage a large influx of leveraged trading into the market, bringing more opportunities and possibilities for the creation of decentralized asset trading on SFT.

2.1.2 Expansion of Liquidity Token Protocol

The SFT Protocol based on SC can provide liquidity for locked Staking assets. At the same time, SFTProtocol can create more types of SC for various Staking assets. Developers can use the set of SC development tools provided by SFT to freely build various derivative products on SFT.

2.1.3 Integration with Existing DeFi Ecosystem

The integration of DeFi with existing ecosystems mainly focuses on the asset level. Currently, DeFi projects mainly generate tokens in the form of EVM on public chains. The StakingToken market can obtain more liquidity and asset composition through various DeFi strategies, such as Swap, Liquidity, Fram, Pools, Earn. It can also achieve the pledging of tokens by bridging with existing lending and collateral platforms.

2.2 Cloud Node API Layer:

Collecting blockchain APIs, providing all cloud service nodes necessary to build the future Web3 and Metaverse.

2.2.1 Collect Cloud Node API Interfaces

With the evolution of Web3 and the development of various applications, developers have begun to rapidly develop decentralized applications on various blockchains. Although developing DApps on public chains is feasible, setting up one's own public chain node is still a daunting task that requires a significant amount of time and technical expertise. The SFT protocol solves this problem by providing high-performance public chain node services, collecting APIs from various blockchains, and providing one-click deployment of node services.

2.3 Hardware Infrastructure Level:

Build a globally distributed, automatically scalable, multi-cloud network infrastructure with a flexible combination of privacy computing, storage solutions, and high-performance GPU computing capabilities.

2.3.1 Hardware Infrastructure in SFT Protocol

The SFT protocol matches the enterprise's requirements at the Laas and Naas levels with the hardware architecture service platform under the protocol, providing support for the enterprise's better development in the web3 field. The SFT protocol token is used to pay usage fees to investors willing to invest in the infrastructure field. It also allows new users unfamiliar with cryptocurrency to feel comfortable using SFT protocol tokens and easily start various services. This means that when global enterprises or users use SFT protocol to pay fees for their work, infrastructure node operators receive SFT protocol token rewards based on their workload.

2.4 The SFT Protocol will be implemented in three phases to achieve short-term goals

2.4.1 Phase One:

Initiate the entire protocol ecosystem with Filecoin as the first supported public chain. Users of FIL can flexibly participate, transfer, withdraw or redeem, providing a completely flexible Stake participation method. Integrate existing DeFi functions to provide decentralized trading, borrowing and other services, while expanding the underlying assets to encrypted asset projects that rely on storage and privacy computing, adding more revenue pools.

2.4.2 Phase Two:

Aggregate various public chain API interfaces and cloud service interfaces, integrate them into the SFT protocol, and provide convenient underlying services for web3 projects and enterprises.

2.4.3 Phase Three:

Build a globally distributed infrastructure node, platforms and tokenize hardware infrastructure, and incorporate it into the entire protocol ecosystem, enabling the long-term expansion and sustainable prosperity of the SFT protocol ecosystem.

3. SFT Protocol Architecture

The SFT protocol architecture includes both software and hardware layers.

Software layer: a decentralized protocol that grants liquidity rights to staked tokens in public chains. It consists of three layers - the bottom layer, contract layer, and application layer -

and provides functions such as staking, redemption, asset custody, DeFi applications, asset trading, cross-chain transactions, and lending through the SFT protocol contract.

Hardware layer: provides a large number of Blockchain Technology API interfaces and hardware infrastructure, executes application deployment, resource scheduling, privacy encryption computation and storage, network services, high-performance computing, etc. It provides decentralized Laas and Naas services in the Web3 field and connects global enterprises with hardware infrastructure node providers who seek to profit from it, flexibly matching the needs of both parties.

3.1 SFT Protocol Underlying

The underlying of the SFT protocol mainly consists of the network module, ledger module, smart contract module, transaction management module, consensus module, and an open-source community.

3.2 SFT Protocol Contract Layer

The SFT Protocol Contract Layer is the core module of the SFT protocol: contract module, transaction module, consensus module.

3.2.1 Contract Module:

The SFT Protocol Contract Module is a customizable blockchain infrastructure composed of micro-kernels and functional modules. By separating events and services, it achieves a highly modular underlying architecture and provides smart contract functionality. Through SFT's modular contract and cooperation with other modules, it provides an on-chain programmable environment, and interacts with smart contracts by sending special transactions to the contract.

3.2.2 Transaction Module:

In the SFT protocol ecosystem, transactions will flow within or between chains, and nodes of each chain need to process more and more transactions, including cross-chain transactions. Therefore, a separate module is needed to handle various transactions. The transaction module is responsible for collecting, verifying, storing, and forwarding transactions.

3.2.3 Consensus Module:

The SFT protocol adopts the POS consensus mechanism. Staking SFT can earn FIL income or SFT protocol tokens. In the distribution of protocol tokens, validators provide validation nodes, and hardware providers provide node services. They need to stake SFT protocol tokens to provide services and earn SFT protocol tokens.

3.3 Application Layer of SFT Protocol

The SFT protocol supports the establishment of decentralized DeFi applications or decentralized financial transactions, cross-chain transactions, computing power transactions, and other financial transactions, such as: computing power token transfer transactions, financial derivatives transactions, lending, futures options, NFT minting and trading, games and social applications.

3.3.1 Decentralized DeFi Applications

Liquidity farming, lending, hedging risks, earning interest, games, social applications, etc.

3.3.2 Decentralized Trading

Deploy existing Swap trading pools, Dex trading, lending markets, options trading, etc.

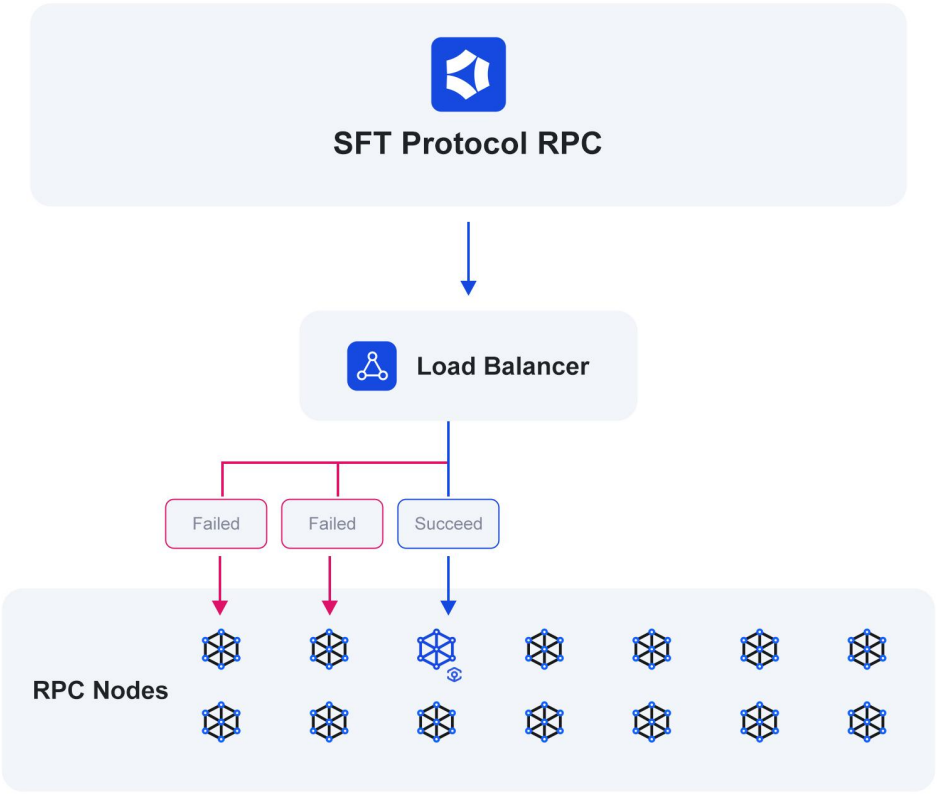
3.3.3 NFT Minting and Trading

Mint non-fungible tokens (NFT) and execute on-chain transactions. Project parties can transfer and trade NFT on the SFT protocol.

3.4 Integration API Protocol

Build a decentralized LAAS and NAAS service platform in the web3 field, providing users' applications and DApps with elastic and dedicated node API services, querying blockchain data and promoting decentralized application operations.

As we all know, building a public chain node requires solving many problems, such as security, network speed, and storage space. As a blockchain development platform, the SFT protocol can solve these problems by directly providing dedicated full nodes.



3.4.1 Dedicated Service Node

Using a dedicated node helps you obtain better blockchain access performance, as it only accepts calls from your dApp.

3.4.2 Multi-region Global Distributed API

The SFT protocol will support multiple different regions, optimizing network call times based on the user's region, thereby improving your dApp's speed and performance.

3.4.3 Multiple Testnet Service Support

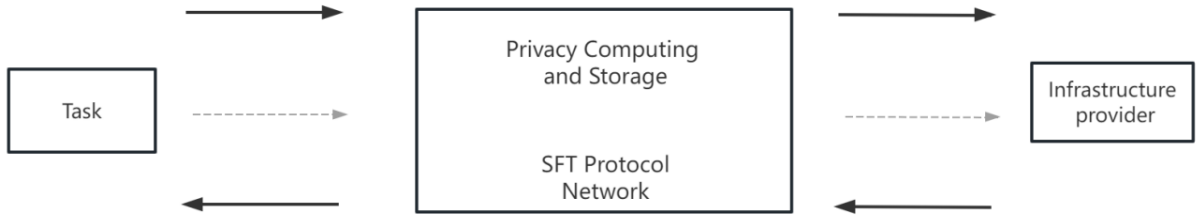
The SFT protocol supports almost all popular testnets, giving developers ample flexibility in their testnet choices, allowing them to test their dApps on the testnet they need.

3.4.4 Archive Service Node

The SFT protocol also provides Parity archive service nodes. An archive service node will save a complete copy of the blockchain ledger, while a full node may be pruned due to disk space issues.

3.5 SFT Hardware Protocol and Infrastructure

The SFT hardware protocol network is a peer-to-peer computing network that connects global enterprises with hardware infrastructure nodes and service providers to perform computing and storage tasks. During the execution process, the SFT protocol acts as a connecting bridge, and users use SFT protocol tokens to obtain the right to use the infrastructure, pay a certain amount of DAO, and automatically distribute and process complex business operations through SFT protocol contracts.



4. Specific Implementation of SFT Protocol Software Layer

The implementation of the SFT protocol software layer requires the participation of multiple software modules: pledge contract, multi-signature, asset ownership confirmation, SSV special verification mechanism, and smart contract security, among others working collaboratively.

4.1 Pledge Contract

A contract that interacts with the Stake original chain at the SFT protocol contract level is called the StakingContract (SC). For example, create a FIL-SC to connect FIL and SFT.

4.1.1 Pledge and Create a Multi-Signature Address:

When user A holding FIL initiates a Stake operation on FIL-SC, StakingContract will first create a multi-signature address. It transfers FIL to the address through the FIL original chain. If the transfer is successful, the contract will execute the pledge operation of the multi-signature address. If successful, the tokens will be locked on the original chain.

4.1.2 Proofs:

The SFT protocol will receive a proof of the FIL original chain, and then trigger the contract to generate an equal amount of SFT and send it to the Staker. The update of StakingContract requires the original chain and SFT protocol to work together. Due to the need to monitor the contract status of each chain, the implementation of the Staking contract has many similarities with cross-chain mechanisms.

4.1.3 Casting:

When the holder initiates a Staking request in StakingContract, the generation of the multi-signature account occurs on the SFT protocol. At the same time, the personal assets are transferred to the multi-signature address through the signature of the Stake user. This transfer occurs on the original chain. When the Contract captures the transfer information, it initiates a Stake request from the multi-signature address to the original chain. After completing the Staking on the original chain, SFT will fetch the Stake status of the address on the original chain and verify it. After successful verification, it will immediately cast the corresponding SFT on the SFT protocol.

Throughout the process, the SFT protocol has interacted with the original chain multiple times. Monitoring and capturing the status play an important role in the security of the entire protocol. The SFT protocol captures the original state through time delay and multiple verifications to ensure the final authenticity of the original chain.

4.2 Multi-Signature

In order to ensure the unique correspondence between the ownership of Stake assets and SFT, the SFT protocol designed an intermediate address model.

The ownership of the assets of this address does not belong to anyone, that is, no one can own the private key of this address. SFT ensures the asset neutrality of the intermediate address and ensures that only SFT holders initiate the signature when redeeming through secure multi-party computation technology and threshold multi-signature technology. Secure multi-party computation involves privacy and requires a group of special validators with special functions in SFT to participate. A certain number of validators, nodes called SFTSpecialValidator (SSV), use their private keys to sign and transmit through a secure channel to verify the validity of the signature, and finally realize the recovery of the intermediate address signature. This intermediate address has no private key and is not stored on the SFT protocol. It is only signed by the private certificate of the special certifier

when it needs to be signed. The implementation of threshold multiple signature technology realizes that part, not all, of the generator can generate private key signatures.

4.3 Secure Multiparty Computation

When a holder of SFT initiates redemption of StakeContract, a multi-signature address is required to create private key signatures in the calculation and generation process, with dedicated validators participating. Validators can transmit calculation results through encrypted channels and verify results without revealing their own private keys.

Secure multiparty computation mainly focuses on how to securely calculate predefined functions without the presence of untrusted third parties, addressing the practical problem of results depending on the calculation of data from multiple parties who are unwilling to share their raw data. Through secure multiparty computation, it is possible to verify the final result without revealing the initial input values to third parties, which is a secure way to unlock and redeem StakingContract.

4.4 Ownership Transfer

After the Staking operation is completed, the redemption right of FIL on the multi-signature address is in the hands of the holder of SFT. Only the holder of SFT has the right to redeem and call the FIL-SC contract. If user A trades SFT to user B, user A loses the redemption right to the original chain FIL, and the mapping relationship between the FIL on the multi-signature address in the contract and user A's address is given to user B. User B can initiate redemption according to their own wishes or trade SFT to others. In this process, the multi-signature address completes multiple rounds of ownership confirmation of the original chain FIL through the signature of special validators different from the Polkadot world on SFT, without block consensus.

4.5 SFT Special Verification Person (SSV)

The SFT protocol ensures the security and fairness of verification data through the SSV mechanism.

Unlike the SFTValidator (SV), SSV witnesses asset ownership in the SFTStake contract. When eligible holders initiate redemption from the contract, special verifiers participate in the calculation and complete the transfer of assets from the multi-signature address to the individual address through signature. When no redemption occurs, the special validator stores their private key locally and waits for a call.

A special validator is composed of a randomly selected group of individuals. SFT selects N SSVs from SV through a random algorithm. SFT randomly selects N SSVs for local calculation and transmits the results through a secret channel. After successful verification,

the participating permissions are obtained and saved locally on the server. At the same time, each SSV needs to run a lightweight node of the project supported by the StakeContract to verify the transaction status of the original chain. This program is written into the entire dedicated validator client and performs verification automatically.

4.6 SSV Node Validator Mechanism

In order to ensure the security of redemption data, SFT has dedicated validators who are grouped and executed in a fixed manner. During their respective shifts, a single validator group generates multiple signal addresses and stores keys. After the execution cycle is completed, a new group replaces the previous one, ensuring the participation of the current validator. A validator's term lasts for one epoch (approximately 24 hours). The election for the next group is completed in the previous epoch. SFT selects new SSVs from SV candidates based on block creation rate, staking ratio, and other factors. The new SSV replaces the old SSV's private key with its own, and the system destroys the relationship established with the old SSV private key.

4.7 Validator Incentive and Punishment Mechanism

Due to the importance of special validators, SFT has established incentive and punishment mechanisms to encourage positive behaviors such as calculation and storage, and to punish negative behaviors such as dropping offline or failing to switch in a timely manner. The SFT protocol specifies that participants who generate, calculate, and sign addresses will receive SFT protocol tokens - DAO incentives. On the other hand, SFT's punishment for security issues is severe. SFT will require all validators involved in calculations and storage to maintain a specified online time. If a validator frequently drops offline, they will be penalized. If the offline time exceeds N hours, the validator will be Jailed and will not be able to participate in any calculations or storage of special validators for a certain period of time.

4.8 Pledge Mechanism for Special Validators

Anyone holding SFT tokens can apply to become a special validator for SFT. A special validator needs to pledge DAOToken, which is proportional to the acceptable Stake amount. The more DAO pledged, the greater the value of Stake assets calculated and stored. This effectively increases the cost for special validators to engage in coordinated malicious behavior. The pledged DAO will receive incentives from the system, while also serving as a fund pool for system punishments. Due to the uniqueness of the SFT system, the requirements for special validators are relatively strict, and nodes in the early stages of development will gradually open up to attract validators.

4.9 Staking Contract Security

The asset security of the Staking Contract in the SFT protocol is ensured in multiple ways.

4.9.1 Asset neutrality:

Staking assets are locked on the original chain, and their mapping relationships are recorded in the Staking Contract. A multi-signature address is guaranteed by N SSVs through threshold multi-signal sharing technology. Therefore, the SC is not controlled by any single third party.

4.9.2 Multi-signature address asset usage mechanism:

Special validators are randomly selected by the SFT algorithm. Validators do not know each other, and the possibility of collusion is reduced. Asset protection is dynamically changed within a certain period of time to ensure security.

4.9.3 Punishment mechanism:

Validators need to pledge a certain amount of DAO participation when participating in private key signature calculation and storage. If an attack or illegal behavior occurs, the pledged DAO will be Slashed, and the pledged value can be processed. The value of the asset is proportional. When multiple conditions are combined, the SFT system can effectively punish certain risk factors. Under the assumption that most people are honest, the asset of the Staking Contract can be guaranteed to a certain extent.

4.10 Process

The pledging process is as follows. The user interacts with SC, and SC interacts with the original chain. During this process, in order to make the user's operation simple enough, SC needs to undertake the responsibility of multiple interactions with the original chain. It is important that SC needs to verify whether the pledge is successful before distributing SFT to the user. Users can redeem assets on the original chain at any time by holding SFT. The modification of SC's relationship requires the signature of SSV, because the record relationship of assets is on SC. When the user initiates redemption, SC triggers a signature request. After SSV executes the signature, SC interacts with the original chain and submits an Unbond/Unstake request. Then, SSV verifies the off-chain evidence on the original chain. When the evidence is true, the SFT used to submit the request will be destroyed.

5. Specific Implementation of SFT Protocol Hardware Layer

The SFT protocol hardware layer aims to build a hardware infrastructure for Web3 development. In the SFT ecosystem, users can quickly deploy applications and call nodes

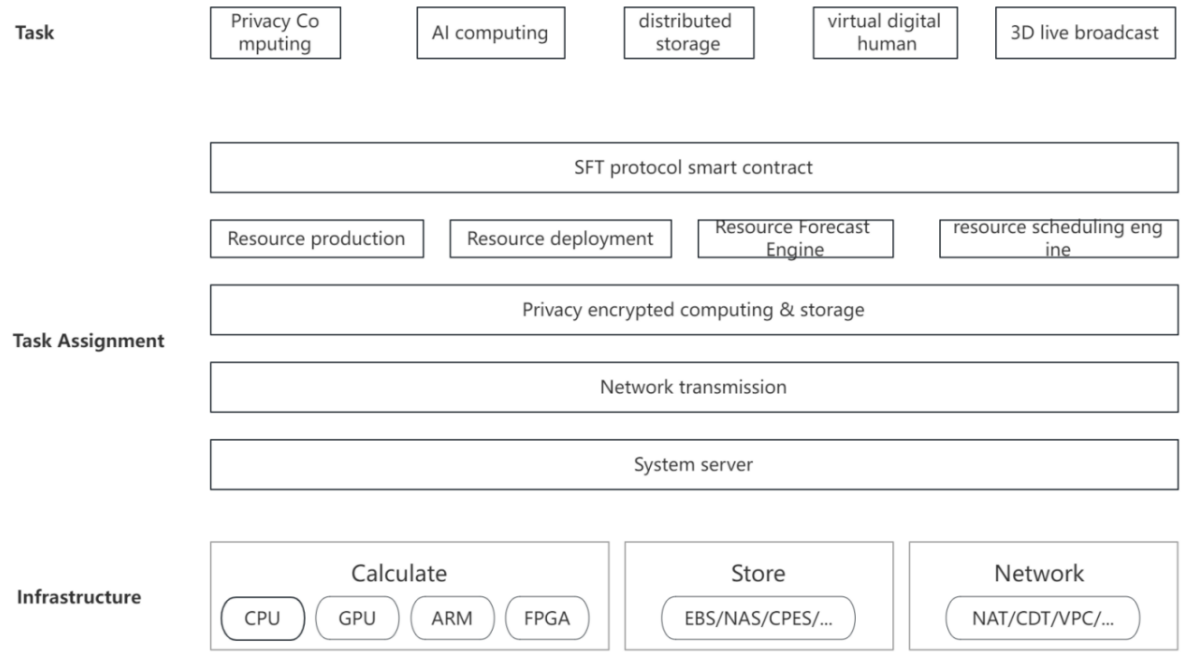
without having to build and configure parameters themselves. Based on the user's network location, it can automatically and quickly match the nearest facility network node service to the user.

5.1 Dynamic Network Services are Required for Building Web3.0 Public Chains

To build a public chain, NaaS dynamic network services are required, with connections that are created temporarily, rather than pre-configured. This is completely different from traditional networks, where administrators install applications in enterprise networks, and the application inherits the network's connectivity and behavior. The application itself specifies the connectivity and performance requirements it needs, and provides them immediately when needed. To respond to such dynamic relationships, a mechanism is needed to create this demand relationship, and the SFT protocol is born to connect dynamic network service providers and users of public chain nodes. When users need public chain node services, they call the SFT protocol, deploy with one click, and the SFT protocol will automatically and quickly match the nearest facility network node based on the user's network location, and provide corresponding services.

5.2 Infrastructure Architecture

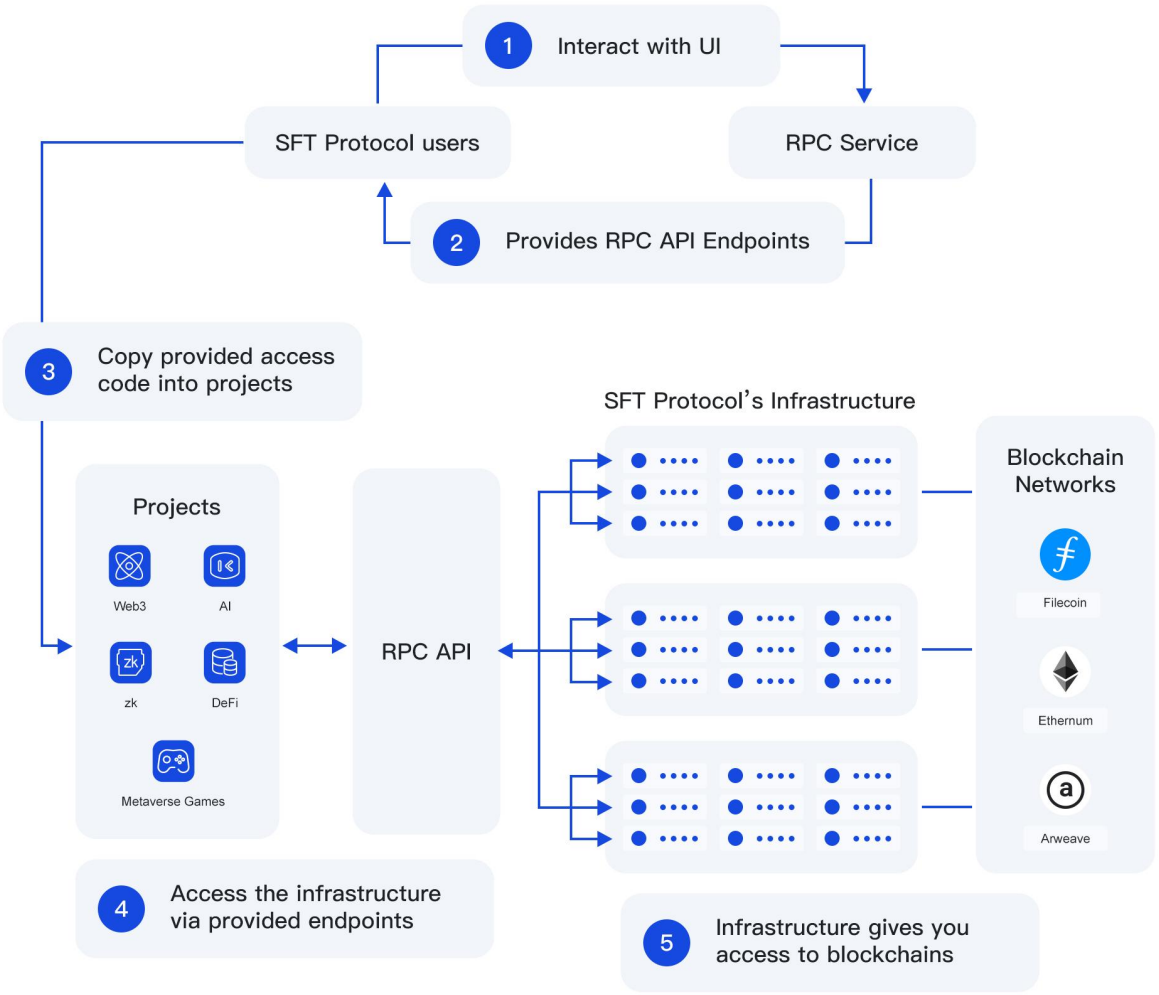
The infrastructure architecture of the SFT protocol includes the business application layer, protocol scheduling, and infrastructure. Users pay infrastructure service provider node fees using SFT tokens based on their workload. The SFT protocol will automatically allocate the currently idle hardware devices offline according to the user's business needs and provide corresponding business services.



6.Integration of SFT Protocol with Filecoin Software and Hardware Technology

Currently, Filecoin is the first public chain network supported by the SFT protocol. The SFT protocol will gradually expand its development in liquidity support, DeFi applications, asset trading, and node services, starting from Filecoin.

The SFT protocol focuses on the integration of underlying technological innovation and basic hardware infrastructure construction, especially the development of Filecoin public chain and the construction of large-scale hardware infrastructure. This will promote the construction, security, and ecological development of Filecoin public chain nodes. The SFT protocol will also expand to the physical field, providing users with secure and trustworthy blockchain infrastructure services such as Filecoin, deeply integrating the digital economy with the real economy, empowering the overall upgrade of the real economy, and enabling various industries to find new development space.



6.1 Compatibility between SFT Protocol and Mining Pool Hardware Providers

The compatibility between SFT Protocol and hardware mining providers promotes the infrastructure construction and development of the Filecoin public chain. As we all know, FIL mining requires a long-term pledge period of 540 days. Although the FIL community is committed to making the network and its economy open to all participants, the minimum hardware requirements and the learning cost for setting up nodes still discourage many potential storage providers, hindering many users from using hardware mining devices.

In the initial stage of SFT Protocol, the focus is on the integration and development with the Filecoin public chain, solving the liquidity of FIL token pledge, constructing decentralized node mining, and forging asset tokens SFT. Applications such as liquidity mining pool, perpetual trading of computing power, etc. can be formed based on SFT protocol by pledging FIL token and forging SFT, achieving liquidity mining, farming, asset trading, asset lending, etc. functionalities.

6.2 SFT Protocol Fully Participates in the FVM Ecosystem.

The Filecoin network is a robust platform that stores NFTs, public datasets, Web3, and metaverse resources in a verifiable manner, and provides access services. Smart contracts (FVM) can create intelligent and dynamic storage solutions that were difficult to achieve in the Web2 era. The SFT protocol will work with FVM to build decentralized applications, distributed node services, fully contract-based protocol management, approval, and more. For example:

6.2.1 Distributed computing based on data stored on Filecoin

Perform calculations on the data where it is stored, without moving it first.

6.2.2 Crowdfunding data preservation plan

Anyone can fund the storage of important data for society, such as crime or climate-related data.

6.2.3 Intelligent storage market

Dynamic adjustment of storage fees based on different times of the day, replication levels, and accessibility within a certain area.

6.2.4 Multi-generational storage and perpetual custody

Store data so that it can be used by future generations.

6.2.5 Data DAO or tokenized dataset

Model the value of data as tokens and form DAOs to coordinate and trade computations carried out on them.

6.2.6 Locally stored NFTs

Collaboratively locate NFT content with registration records that track NFTs.

6.2.7 Time-locked data retrieval

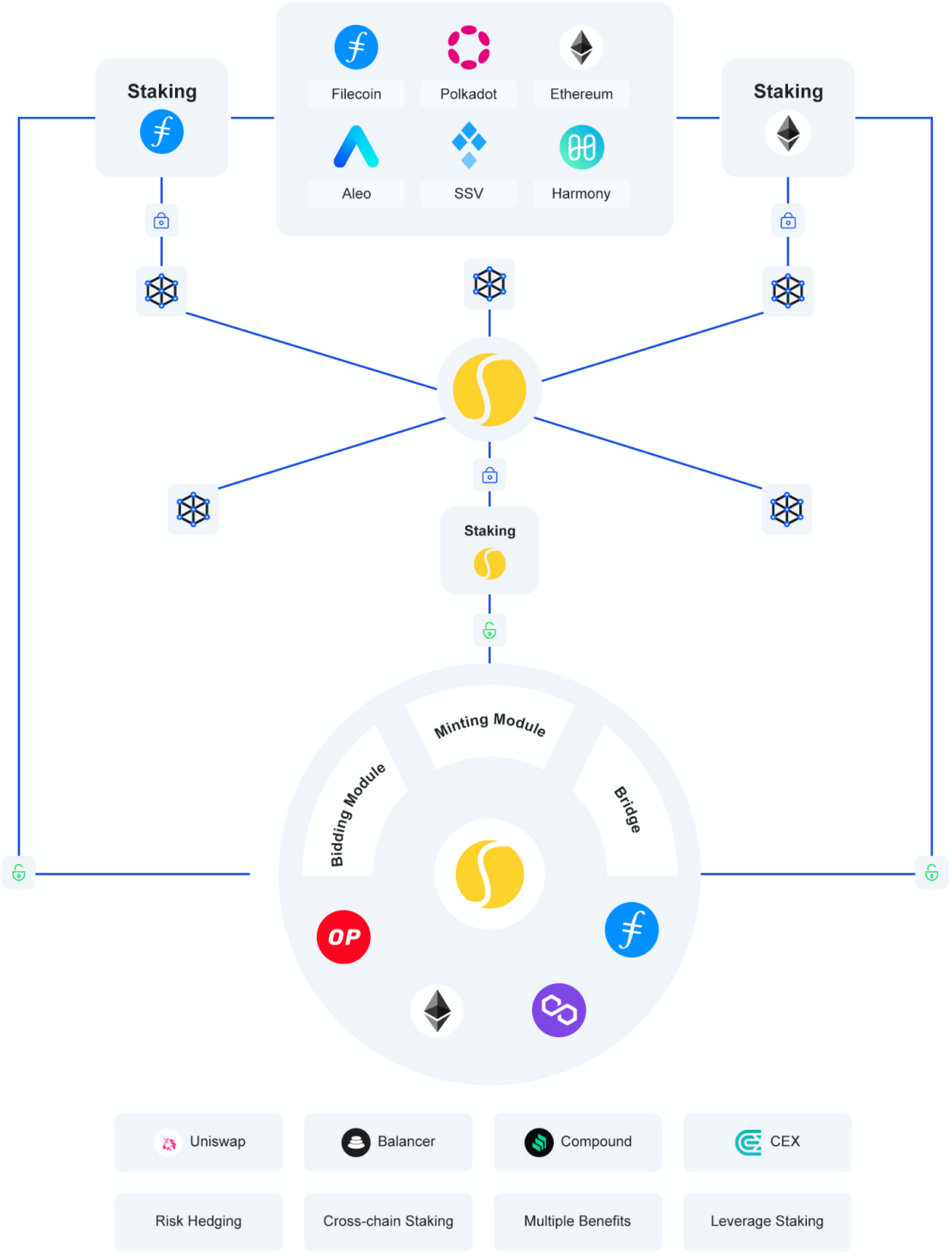
Unlock relevant datasets only after company records are made public.

6.3 Various Financial Derivative Schemes of SFT Protocol in Filecoin

The SFT protocol will further establish financial derivative schemes in the Filecoin ecosystem, such as computing power lending, liquidity mining, options trading, pledging, lending, Swap trading, cross-chain transactions, etc.

The highly scalable, open, and financial nature of the SFT protocol will support the development of the FIL ecosystem, fully utilize the FVM, and support hardware service providers' network and mining pool protocols. The SFT protocol promotes various participation models for hardware service providers, such as encapsulation, revenue distribution, unlock management, and validation nodes, to verify and monitor contract data.

As a way to share liquidity, applications based on FVM can be deployed to other chains (such as Ethereum, BSC, Solana, etc.).



6.4 Vision: SFT Protocol Participates in Building Web3.0 and Metaverse

As more and more NFT digital assets in the Metaverse, IPFS & InterPlanetary File System can be used for underlying data storage. In recent years, IPFS network has already stored billions of files, and against the background of major cloud storage giants experiencing downtime events, the advantages of IPFS, which are more secure, faster, and more efficient, are more prominent. Whether it is Web3.0, NFT, or the currently popular Metaverse, they cannot do without Filecoin distributed storage as the underlying infrastructure.

SFT Protocol layout for the future development of Web3.0 and Metaverse. The edge computing, distributed storage, edge CDN services built in the SFT Protocol help Filecoin public chain in the use and development of the Metaverse, and the storage calls will consume the equipment resources of the data center. SFT Protocol will open multiple interfaces for third parties, and the overall cost model will be priced in DAO. The system will calculate the computing resources and storage resources paid by nodes when calling.

6.5 Hardware Infrastructure Under Construction

SFT protocol collaborates with physical hardware service providers to jointly promote the construction of hardware infrastructure. Currently, data centers and basic hardware facilities have been established in the United States, Singapore, Vietnam, Hong Kong, Malaysia, and other places. New infrastructure construction will gradually be carried out in Europe, North America, Canada, Japan, and other places.

Unlike ordinary cooperative models, the basic infrastructure construction under SFT protocol is fully managed under the protocol and is subject to audit by trusted third parties.

7. Token Economics

The SFT protocol creates value by providing liquidity for staking assets. Stakers can earn rewards while circulating SFT, and the protocol captures the value of the liquidity and feeds it back into the protocol. DAO is the local digital encrypted security utility token of the SFT protocol, providing economic incentives. The DAO manages the SFT protocol and plays an important role in the functionality of the SFT ecosystem.

Each block's generation requires validators to contribute their computing, bandwidth, and storage resources, so the DAO generated by the same block is used to compensate validators for their efforts. Additionally, due to the special design of the SC, the protocol also requires upper-level validators to provide security services such as multisignature services, light node services, and oracle services. The corresponding services will also be incentivized through the distribution of DAO tokens. DAO is an essential part of the SFT protocol because without DAO, users have no incentive to consume resources to participate in activities or provide services to benefit the entire ecosystem on the SFT protocol.

7.1 Token Model

There are two types of tokens in the SFT protocol: Alternative tokens (currently SFT) and Native tokens (DAO). The roles of the two tokens in the protocol are different. SFT mainly

serves as a medium of liquidity and has functions of ownership attribution and rights inheritance from StakingToken. DAO, as the native token of the SFT protocol, mainly serves as a system transaction medium, responsible for value capture, consensus incentives, prevention of system abuse, and system voting governance.

7.2 Validator Staking and Incentives

An open PoS network requires incentives for validators. At the same time, to prevent cheating, validators must first stake DAO as collateral before participating in validation. After completing the calculation and storage, they are entitled to receive DAO rewards allocated by the system. The staked DAO will be locked, and if the validator engages in misbehavior, the locked DAO will be slashed. SSVs are selected from SVs. Candidates will be evaluated based on several criteria, such as online time, ratio of free tokens to equity tokens, etc. Generally, to ensure the security of contract assets, the system stipulates that the number of Staking DAOs is proportional to the amount of Stake assets that can be processed. In other words, the more DAOs staked, the more Stake contract assets that can be processed, and the more DAO rewards that can be obtained. If the system detects dishonest behavior from SSVs, it will also slash their Staking DAOs, and the slashing ratio depends on the severity of the misconduct.

7.3 Transaction Fees

The StakeContract created on SFT obtains SFT circulating on the SFT protocol through staking on the original chain. To obtain computing power on the SFT protocol, SFT circulating on the SFT protocol needs to pay DAO fees. Validators package transactions and upload them to the latest block data. Once the latest block height is updated, the SFT transaction is completed. The amount of DAO fees depends on the size of the transaction data to be processed. Finally, the fee is priced by the DAO. If the paid DAO is higher than the resources required for system operation, the system will return the remaining DAO to the contract account after the transaction is completed. Otherwise, the system will stop running when there is no DAO payment for resources.

7.4 CallStaking Contract Business Call - DAO Valuation Method

The SFT protocol will open multiple interfaces for third parties. Contract calls consume system data center computing resources. In order to limit malicious low-cost attacks and meet certain commercial calls, when the contract call frequency reaches a certain level, the caller needs to pay a certain amount of computing resources. Of course, the business caller can customize the payer, which can be a platform user or the platform itself. The overall cost model is based on DAO valuation. The system will calculate the computing and storage resources paid by the node when the call is made, and compare it with the DAO paid by the caller to determine the final model. All transaction fees obtained from the protocol will be allocated to SV and the protocol treasury in a certain proportion.

7.5 Token Initial Allocation

A large portion of the initial allocation of DAO is allocated for community rewards. Users can participate in Staking through StakingContracts to receive community rewards. The amount received is proportional to the total value of the work performed through StakingToken. This process is called StakingDrop. StakingDrop is an initial incentive mechanism designed by SFT to stimulate early adoption of SFT. New incentive measures can increase the collection of circulation fees.

8. Summary

It is expected that the market value of Staking assets will reach the level of hundreds of billions in the next 2-3 years. Many assets will be locked due to security issues, and the liquidity value will also decrease. SFT protocol, based on Staking assets, aims to create a decentralized asset protocol. In the early stage, it will focus on providing Staking assets without the need for third-party trust endorsement, to solve the contradiction between Staking asset liquidity and security. Whether it is FIL, ATOM, or DOT, they will issue SFT as a token liquidity on the SFT protocol.

In the cloud service node API interface: it will gather various blockchain APIs and provide all cloud service nodes needed to build the future Web3 and Metaverse. In terms of hardware infrastructure: it will build a globally distributed, automatically scalable, multi-cloud network infrastructure, continuously providing different privacy computing and storage solution combinations, simplifying customers' complex needs, providing customers with more secure and efficient infrastructure, and helping global enterprises enjoy new generation blockchain infrastructure through secure and proprietary connections, achieving digital transformation.

The provided node NAAS service and hardware infrastructure service will benefit the SFT protocol ecosystem and SFT DAO token, develop financial derivatives based on SFT as a benchmark, and establish a prosperous ecosystem in a DAO way, while avoiding damage to the security of the original chain. Therefore, the SFT protocol will become an indispensable infrastructure for DeFi applications, realizing the full integration of Web3.0 and Metaverse, the entity economy and digital economy, which is also a goal for our future development.

9. Future Work and Challenges

SFT has been widely circulated and the development of derivative assets based on SFT is thriving, but there are still many challenges ahead. The security of Staking assets managed by the SFT protocol is a prerequisite. Otherwise, there will be fewer Stakers willing to use SFT for Staking. If we have a secure protocol, SFT can survive network security attacks and black swan events, even if it manages countless Staking assets. With security in place, developers may be willing to develop more applications based on SFT and derive more assets. Therefore, there is still much work to be done for SFT.

- **On-chain Governance**

SFT is a decentralized protocol, and its upgrade direction is closely related to governance. For many PoS consensus projects, one of the most important practices is to set TokenStaking as a voting method. Different projects adopt different Staking methods, and the specific implementation may vary, such as incentivizing participation in voting, providing reference through prediction markets, or even using delegation to avoid convergence of voting results. However, participation and voting results have been widely criticized. Providing more references and incentives can effectively solve the voting problem. However, there is currently no perfect solution to the voting mechanism. Most solutions are indirect and combined with blockchain optimization. Therefore, voting is always a tricky problem. Although the combination with blockchain improves efficiency, it does not solve some fundamental issues. SFT will initially implement basic voting logic and then upgrade to on-chain governance logic, putting the solution to the voting problem in a long-term optimization plan.

● Private Key Maintenance Method

Currently, the private key signatures of multi-signature addresses are carried out by a threshold multi-signature algorithm that involves multiple special validators. The private keys of validators are stored on their local servers (encrypted), but asset custody and the existence of validators are not permanent, so the two parties may not always reach a consensus in reality, which endangers the storage security of assets. Currently, SFT ensures the randomness and timeliness of private key storage through regular rotation, but frequent replacement of validators is a waste of computing resources, so the frequency needs to be maintained at a reasonable level. Currently, the optimal frequency has not been determined, and future work will focus on balancing frequency and security.

Similarly, threshold multi-signature technology still needs to trust random validators. SFT is studying new algorithms that can be used to reduce the level of trust and promote protocol security upgrades. Currently, the research direction of privacy computing such as MPC and TEE has potential cooperation opportunities with the security model required by SFT. Privacy computing technology is also rapidly developing, and engineering application projects are emerging like bamboo shoots after a spring rain. Therefore, we will continue to explore this in the future contract layer work.

● Distributed Smart Contracts

When holders initiate Staking through the Staking contract, their tokens will be locked on the original chain. The security mechanism of the original chain ensures the security of the pledged tokens. However, due to the existence of cross-chain bound asset SFT, the mapping relationship of the asset multi-signature account will be saved in the Staking contract. The more tokens on the original chain, the easier the contract is to be attacked. Although the mapping relationship is not the decisive factor for redeeming the original chain assets, attacks will harm the system. SFT attempts to create an allocation system that generates Staking contracts based on the value of Staking assets. Each Staking contract will set a threshold. When the threshold is exceeded, Staking of the contract will stop, and a new contract will be created instead. Dynamic setting solves the problem of asset centralization and reduces the risk of large assets being attacked. There are complex settings in the industry that can ensure that the Staking contract does not fully own the locked Staking

assets. Instead, when the Staking contract is called, an independent contract with only the holder's rights will be created. This contract has a strong correlation with a single Staker. In addition, this contract will be audited by a third-party auditing agency before it is released.

● Original Chain Asset Security

The issuance of SFT depends on the proof of the original chain. When Staking on the original chain, SFT will be minted and sent to the corresponding user. The SFT protocol ensures the unique correspondence between SFT and the original chain assets, ensuring redemption. However, if there is a problem with the Staking module on the original chain, the value of SFT will be correspondingly devalued. This mechanism is still being polished and improved, and it is also one of the future work priorities of SFT.

● Allocation of Alternative Tokens

The DAO issued through SFT represents various rights of the original StakingToken (such as redemption rights, income rights, voting rights, or other ecosystem rights). StakingContracts currently implements basic redemption and income rights. And it is developing and researching corresponding SFT rights on the original chain, and even providing more rights on other chains.

At the same time, the fairness of rights allocation needs to be further polished. Due to the inconsistent allocation mechanism of different PoS public chains, the access to SC still needs time to be improved. A perfect product can be exactly the same as the original chain, or even better. Establishing a universal permission allocation mechanism is very important, which can not only reduce development difficulty but also improve user satisfaction. Currently, SFT uses a simple and easy-to-understand equity allocation method, adhering to the principle of sharing/assuming risk and equity openly, and allocating equity to Stakers. However, due to the inconsistency with the original chain mechanism, there may be some questions. We still face many challenges.

● Issuing More Alternative Tokens Besides Staked Assets

The essence of SFT is to issue alternative tokens based on Staking assets. Conversely, the underlying assets for issuing alternative tokens are Staking assets. What if the underlying assets can be extended to more forms of encrypted assets, or even derived from non-encrypted assets? The prospects will be enormous if this can be achieved. This is a medium- to long-term direction worth exploring.

10. Risks and Disclaimers

Nature of the Whitepaper:

The Whitepaper and the website are for general reference only and do not constitute a prospectus, an offer document, a securities offering, an investment solicitation or any offer to sell any product, project or asset (whether in digital form or otherwise). The information herein may not be comprehensive and does not imply any elements of a contractual relationship. No statement, warranty or undertaking is given or made as to the accuracy or

completeness of such information. The Foundation, the distributor, their respective affiliates and/or teams have not independently verified the accuracy or completeness of such information from third party sources. Furthermore, you acknowledge that circumstances may change and that the Whitepaper and the website may become outdated; the Foundation and Distributor are under no obligation to update or correct this document in connection therewith.

Token Documentation:

The contents of the Whitepaper or the website are not intended to be a sale of any token (as defined herein) and shall not be relied upon in any way in connection with the sale of any tokens, including any part thereof or any statement or fact relating to the same, nor does it form the basis of, or be relied upon in connection with, any contract or investment decision whatsoever. The contents of the Whitepaper or the website may not and shall not be considered as a prospectus or offering document, and are not intended to solicit the purchase of securities or financial instruments in any jurisdiction. Any agreement regarding the sale, purchase or transfer of tokens is to be governed solely by the terms of a separate agreement and/or token purchase agreement (as the case may be) and the terms and conditions of such agreement shall be provided to you and/or made available on the website. The terms and conditions document shall be read in conjunction with the Whitepaper.

Deemed Representations and Warranties:

By accessing the Whitepaper or the website (or any part thereof), you shall be deemed to have represented and warranted to the Foundation, the distributor, their respective affiliates and teams as follows:

(a) you shall not rely on any statements set forth in the Whitepaper or the website in making any decision to purchase any tokens;

(b) you shall be responsible for ensuring that you comply with all applicable laws, regulations requirements and restrictions (as the case may be) in relation to your purchase of any tokens;

(c) you acknowledge, understand and agree that the tokens may have no value, may not represent any right to any tangible or intangible property and are not intended to be a security or any other kind of investment product, including any speculative investment;

(d) the Foundation, the distributor, their respective affiliates and/or team members shall not be responsible or liable for the value of the tokens, their transferability and/or liquidity and/or the availability of any market through third parties or otherwise;

(e) you acknowledge, understand and agree that you are not eligible to purchase any tokens if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country where the sale of tokens may be interpreted as securities (howsoever named), financial services or investment products and/or where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including but not limited to the United States of America, Canada, New Zealand, the People's Republic of China (excluding Hong Kong, Macau and Taiwan), Thailand, and

Vietnam of the People's Republic of China); for this purpose, you agree to provide the Foundation, Distributor and their respective affiliates and teams with any know-your-customer and/or anti-money laundering documentation as may be required by them from time to time;

The Foundation, the distributor and the teams shall not be liable to you or any third party for any indirect, special, incidental, consequential or other damages of any kind in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or the website or any part thereof, including but not limited to any errors or omissions contained therein or any other material published or made available by the Foundation or the Distributor. Potential token purchasers should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the token sale, the Foundation, the distributor and the teams.

Token Characteristics: Emphasis

(a) There is no tangible or physical manifestation, and there is no inherent value (nor has anyone made any statement or commitment regarding its value);

(b) Non-refundable and non-exchangeable for cash (or any other virtual currency's equivalent value) or any payment obligation of the Foundation, distributors, or any of their affiliates;

(c) Does not represent or grant token holders any form of rights related to the Foundation, distributors (or any of their subsidiaries) or their income or assets, including but not limited to any rights to collect future dividends, income, shares, ownership or equity, securities, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licensing), receipt of accounts, financial statements or other financial data, the right to request or participate in shareholder meetings, nominate directors, or any other financial or legal rights or equivalent rights, intellectual property, or any other form of participation or association with the Protocol, Foundation, distributors and/or their service providers;

(d) Does not intend to represent any rights under contracts such as CFDs or any other contracts intended or disguised for the purpose of ensuring profits or avoiding losses;

(e) Does not intend to represent any kind of financial instrument or investment, including but not limited to currencies (including electronic currencies), securities, commodities, bonds, debt instruments, units in collective investment schemes, or any other types of financial instruments or investments;

(f) Is not a loan to the Foundation, distributors or any of their affiliates, nor does it represent any debt owed by the Foundation, distributors or any of their affiliates, and no profits are expected; and

(g) Does not provide token holders with any ownership or other interests in the Foundation, distributors or any of their subsidiaries.

The contributions in the token sale will be held by distributors (or their respective subsidiaries) after the token sale, and contributors will have no economic or legal rights or beneficial interests in these contributions or the entities.

If a secondary market or exchange for tokens does develop, it will be completely independent of the Foundation, distributors, token sale, and Protocol to operate and operate. The Foundation and distributors will not create such a secondary market and will not act as a token exchange.

For Reference Only:

The information listed here is only conceptual and describes the future development goals of the Protocol. In particular, the project roadmap shared in the white paper is for an overview of the team's plans and is for reference only and does not constitute any binding commitment. Please do not rely on this information to make a purchase decision because ultimately, the development, release, and timing of any product, feature, or functionality are determined by the Foundation, distributors, or their respective subsidiaries, and may change. In addition, the white paper or website may be modified or replaced from time to time. There is no obligation to update the white paper or website.

Regulatory Approval:

No regulatory agency has formally or informally reviewed or approved any information listed in the white paper or website. No such action or guarantee has been taken or made under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution, or dissemination of the white paper or website does not imply compliance with applicable laws, regulations, requirements, or rules.

Notice Regarding Forward-Looking Statements:

All statements contained herein, any statements made in press releases or in any public accessible place and any oral statements made by the Foundation, distributors, and/or the team that may constitute forward-looking statements (including statements about intentions, beliefs, or current expectations regarding market conditions, business strategies and plans, financial condition, specific provisions and risk management practices) should be noted. Please note that excessive reliance on these forward-looking statements should not be placed because such statements involve known and unknown risks, uncertainties, and other factors that may cause actual future results to be significantly different from those described in such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions.

References to Companies and Platforms:

The use of any company and/or platform name or trademark herein (except those related to the Foundation, distributors, or their respective affiliates) does not imply any affiliation with any third party or endorsement by any third party. References to specific companies and platforms in the white paper or website are for illustrative purposes only.

English:

The white paper and website may be translated into languages other than English for reference only. In the event of any conflict or ambiguity between the English version and any translated version of the white paper or website, the English version shall prevail. You acknowledge that you have read and understood the English version of the white paper and website.

Distribution Prohibited:

No part of the white paper or website may be copied, reproduced, distributed or disseminated in any manner without the prior written consent of the Foundation or distributor. By participating in any demonstration of this white paper or accepting any hard copy or soft copy of the white paper, you agree to be bound by the foregoing restrictions.

Contract Risk:

Contract risk is the highest priority when deploying the SFT protocol. Users should investigate its risks before using the SFT protocol.

DAO Key Management Risk:

All SFT multi-signature contracts and DAO contracts are managed using threshold signature schemes. Although threshold signatures are currently the safest way, there is still a non-zero probability of failure. If at least (n-m+1) signers lose their key shares, are hacked, or defect, funds may be locked. If m or more key shares are leaked, funds may be stolen (after the transfer is unlocked).