FSC

FON Smart Chain

The world's leading public chain system and blockchain infrastructure

FSC Ecological Development Foundation• 2022

white paper • Global version

Catalog

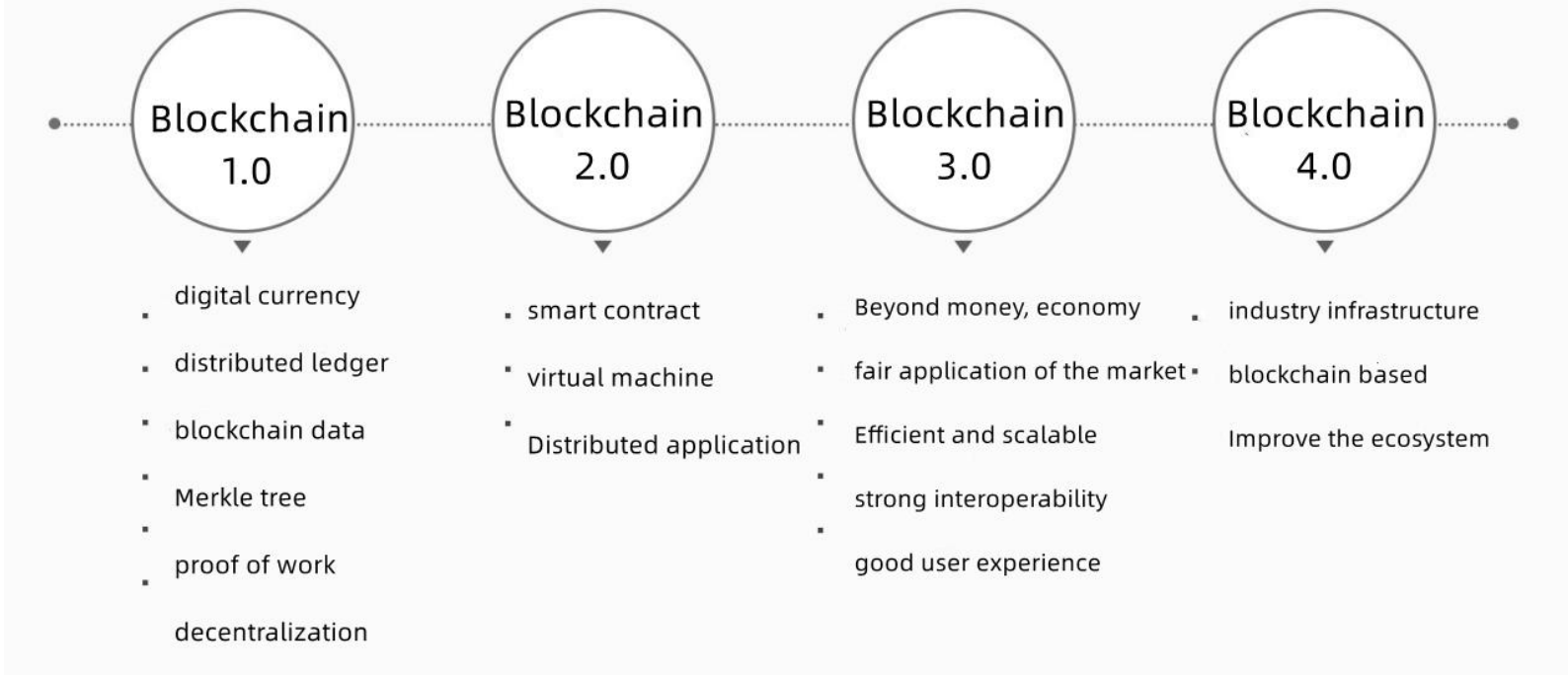
Chapter 1

Overview of the Development of the Blockchain Industry

1.1 Overview of Blockchain Technology

Blockchain technology originated from the groundbreaking paper "Bitcoin: A Peer-to-Peer Electronic Cash System" published in 2008 by a scholar under the pseudonym "Satoshi Nakamoto". In a narrow sense, blockchain is a chained data structure that combines data blocks in sequential order according to time sequence, and is cryptographically guaranteed to be an untamperable and unforgeable distributed ledger. Broadly speaking, blockchain technology is the use of blockchain data structures to verify and store data, the use of distributed node consensus algorithms to generate and update data, the use of cryptography to ensure the security of data transmission and access, and the use of automated scripts. A new distributed infrastructure and computing paradigm for programming and manipulating data using smart contracts composed of code.

At present, blockchain technology is regarded by many large institutions as a major breakthrough technology that completely changes the way businesses and institutions operate. The technical foundation of blockchain is a distributed network architecture. It is precisely because of the maturity of distributed network technology that decentralized, weak centers, sub-centers, and shared, consensus, and shared organizational structures and business structures can be effectively established.



Today's blockchain technology has undergone several iterations:

■ Blockchain 1.0 - Digital Currency In early 2009, the Bitcoin network was officially launched. As a virtual currency system, the total amount of Bitcoin is limited by the network consensus protocol, and no individual or institution can modify the supply and transaction records at will. The underlying technology that supports the operation of Bitcoin-blockchain is actually an extremely ingenious distributed shared ledger and point-to-point value transmission technology, and its potential impact on finance and even all walks of life may be no less than double-entry bookkeeping 's invention.

■ Blockchain 2.0 - Smart Contract Around 2014, the industry began to recognize the important application value of blockchain technology, trying to create a shared technology platform and provide developers with BaaS (Blockchain as a service) services, which greatly improved the It improves the transaction speed, greatly reduces resource consumption, and supports various consensus algorithms such as PoW, PoS and DPoS.

■ Blockchain 3.0 - Blockchain application extension After 2015, with the rise of blockchain 3.0 technologies based on DAG data structures such as Byteball and IOTA, the blockchain system is more efficient, scalable, and interoperable than before. Strong, and has a better user experience, its application has further extended to medical and health, IP copyright, education, Internet of Things, sharing economy, communications, social management, charity, cultural entertainment and other wider applications.

■ Blockchain 4.0 - Perfect Ecosystem The blockchain 4.0 technology based on the HashNet data structure has gradually attracted the attention of the industry. The consensus algorithm based on this data structure can achieve a qualitative leap in transaction throughput and scalability. This will further support the blockchain as the infrastructure of a certain industry, and form a perfect ecosystem based on the blockchain, which will extensively and profoundly change people's way of life.

With the improvement of people's awareness of the scope of application and availability of blockchain technology, people have carried out the research, development and implementation of the underlying core technology of blockchain, on-chain applications and scenarios with great enthusiasm.

The research and exploration of blockchain technology mainly focuses on three levels: First, the underlying technology and infrastructure layer, mainly including basic protocols and blockchain-related hardware content. The second is the general application and technology expansion layer: to provide services and interfaces and related technical services for the vertical application layer of the

industry. The services provided include smart contracts, fast computing, mining services, information security, data services, BaaS, solutions, and anti-counterfeiting traceability. Wait. The third is the vertical industry application layer: implemented in vertical fields such as finance, digital currency, entertainment, supply chain, medical care, law, energy, public welfare, social networking, Internet of Things and agriculture.

At present, people have devoted great enthusiasm to the research and development and application of blockchain technology. Among the teams engaged in blockchain research and development, about 20% are engaged in the research of the underlying technology of blockchain. 80% of the teams are used in various practical application scenarios and vertical industries. Compared with the application layer, the underlying protocol can create token market value, and it also disperses the traditional Internet model of application layer data centering. Under the blockchain system, the application layer project itself has become a complete service provider, and no longer has user traffic and data value. The value of these personal data is distributed to users, and the underlying protocol will be more valuable than the application layer.

1.2 Blockchain key technology

■ The underlying data structure The traditional blockchain was originally a unique way of storing data in cryptocurrencies such as Bitcoin. It is a self-referential data structure used to store a large amount of transaction information. It consists of multiple transaction records. The blocks are linked in an orderly manner from the back to the front, and finally realize the characteristics of being unable to be tampered with and being easy to trace. The block-chain structure of the traditional blockchain is the bottleneck that hinders the blockchain from improving concurrency. Tech geeks are constantly looking for a more efficient form of data block linking, and propose a Directed Acyclic Graph (DAG) and block chain. Chain combined solution, hereinafter referred to as "DAG chain". In DAG, there is no process for the bookkeeper to package blocks, but the bookkeeping process is realized through mutual confirmation of users, which can greatly shorten the time for transaction confirmation.

■ Hash Algorithm Hash operation can realize the mapping of data from one dimension to another dimension. Usually, the hash function is used to realize the information digest. The hash function has a very low probability of collision and can hide the original information. The characteristics of hash functions in blockchain include: function parameters are of type string, fixed-size output, and computationally efficient. Commonly used hash algorithms include MD5 and SHA series algorithms. However, the SHOR algorithm under the quantum computer can reduce the complexity of the attack hash algorithm from o(2n) to o(2n/2), and

the traditional hash algorithm is threatened by quantum attacks.

■ Signature Algorithm The signature algorithm ensures the non-repudiation of the information by encrypting and transforming the information with the private key. The current blockchain mainly uses the ECASDT digital signature algorithm based on elliptic curve. The signature algorithm first needs to generate a personal public and private key pair: (sk, pk) := generateKeys(keysize), the sk private key is reserved by the user, and the pk public key can be Distribute it to others; secondly, you can sign a specific message through sk: sig := sign(sk, message) This will get the specific signature sig; finally, the party who owns the signature public key can verify the signature :isValid := verify(pk, message, sig). However, the SHOR algorithm under the quantum computer can reduce the complexity of attacking the ECASDT signature algorithm from o(2n) to o(n2(logn)(log logn)). The ECASDT signature algorithm cannot resist quantum attacks.

■ Anonymous transaction protection In the public blockchain, every participant can obtain a complete data backup, and all transaction data are open and transparent, but for many blockchain applications, this is fatal. Not only does the user want his account privacy and transaction information to be protected, but for commercial organizations, account and transaction information containing important assets and business secrets should be protected. The idea of Bitcoin's privacy protection is to achieve anonymity by isolating the relationship between the transaction address and the real identity of the address holder. However, such protection is very weak. By observing and tracking the information of the blockchain, the relationship between accounts and transactions can still be

traced through address ID, IP information, etc. In order to solve the privacy protection problem of blockchain, there are several methods such as one-time key, ring signature, homomorphic encryption, and zero-knowledge proof.

■ P2P communication at the network layer P2P network technology is a networking technology for the blockchain system to connect peer nodes, which is translated as a peer-to-peer network by academia, and is called "peer-to-peer" or "end-to-end" in most media A network is an overlay network built on the transport layer. Different from the centralized network mode, the computer status of each node in the P2P network is equal, each node has the same network power, and there is no centralized server. But the information of nodes is easily leaked.

■ Consensus layer consensus mechanism At present, there are mainly several types of consensus mechanisms: PoW, PoS, DPoS, PBFT. PoW Proof of Work is the familiar Bitcoin mining. By calculating a random number that satisfies the rules, the bookkeeping right is obtained, and the data that needs to be recorded in this round is issued, and other nodes in the whole network are verified and stored together. It can achieve complete decentralization, and nodes can enter and exit freely, but mining causes a lot of waste of resources, and the cycle for reaching consensus is long, which is not suitable for commercial applications. PoS Proof of Equity, an upgraded consensus mechanism of PoW, reduces the mining difficulty proportionally according to the number and time of tokens occupied by each node, thereby accelerating the speed of finding random numbers. PoS still requires mining, which essentially does not solve the pain points of commercial applications. The DPoS share authorization proof mechanism is similar to board

voting. Token holders vote a certain number of nodes to represent them for verification and accounting. The entire consensus mechanism still relies on tokens, and many commercial applications do not require tokens. PBFT: Practical Byzantine Fault Tolerance, a practical Byzantine Fault Tolerance algorithm, is a state machine copy replication algorithm, that is, a service is modeled as a state machine, and the state machine is replicated in different nodes of the distributed system, and each state machine copy is The state of the service is saved, and the operation of the service is also implemented. Although there can be more than 3f+1 replicas, the extra replicas do not improve reliability other than reduce performance.

■ Incentive layer incentive mechanism In order to ensure the normal operation of the blockchain distributed system, a large number of honest nodes are required to remain online, and the incentive mechanism is used to reward these users who have contributed to the system. From the perspective of game theory, incentives The mechanism should make the benefits of users' honest behavior far outweigh malicious behavior.

■ Smart Contracts Blockchain-based smart contracts include transaction processing and preservation mechanisms, as well as a complete state machine for accepting and processing various smart contracts. Bitcoin only supports a simple scripting language, and Ethereum has a Turing-complete smart contract language, but the formulation and deployment of smart contracts are very cumbersome and vulnerable to attack. Byteball's smart contract is simple and easy to deploy, but it is not Turing-complete, which is not conducive to the expansion of contract

applications.

1.3 Problems existing in the current industry

At this stage, various underlying protocol projects such as EOS, NEO, ArcBlock and other projects are emerging one after another, but most of the underlying protocol projects are iterated on the basis of Ethereum, which has a certain gap with the standard of blockchain 3.0, let alone Blockchain 4.0. Most of the teams that carry out blockchain landing business are limited by the performance, scope and stability of the underlying protocol, and are currently in the early stage of exploration. Although a large number of industry applications can be seen in the future, the underlying protocol continues to At the same time of the change, more than 98% of the projects will be eliminated by the times. To sum up, the current blockchain technology mainly has the following problems.

■ Low performance: Low performance is one of the main challenges facing the current blockchain technology. The blockchain used by Bitcoin can theoretically only process up to seven transactions per second. Ethereum is slightly improved, but it is still far from meeting the needs of applications. For example, a simple DApp application, CryptoKitties, can slow down Ethereum transaction throughput and dramatically increase transaction fees. Today's consumer applications must be able to handle tens of millions of daily active users. In addition, some applications only make sense if they meet a certain transaction throughput, so the platform itself must be able to handle a large number of concurrent users. Long transaction delays can hinder user adoption, making blockchain-based applications

significantly less competitive with existing non-blockchain alternatives.

■ High barriers to use: Today's blockchain applications are built only for the few technologists who know how to use the blockchain, not mainstream consumers. Almost all blockchain applications require users to run blockchain full nodes or light nodes. The high cost of learning has seriously hindered the progress of blockchain to the masses. For example, the Ethereum-based game CryptoKitties may be the easiest DApp ever to use, but it still requires users to install the Metamask light wallet browser extension, and users also need to know how to buy Ethers securely and use it with Metamask, This greatly affects the user experience. To attract widespread use by the general public, blockchain applications should be as simple as today's internet and mobile applications.

■ High cost of use: The high cost of use of blockchain technology is another major obstacle preventing it from becoming mainstream, and it also limits developers who need the flexibility to build free services. In contrast to the Internet, blockchain technology should be able to support free applications. Making the blockchain free to use is the key to its widespread adoption. A free platform will also enable developers and businesses to create valuable new services.

■ Platform lock-in: As in the early days of any computer technology, blockchain has a serious "platform lock-in" problem. Developers must first decide which blockchain to adopt and then write code for that specific platform, making it very difficult to switch applications to other blockchains. Developers do not want to be locked into one blockchain technology, but need these applications to run on

multiple platforms to improve the efficiency of development reuse.

■ Narrow scope of application: At present, people have high expectations for the blockchain, especially with the rising price of encrypted digital currency, major news media have drawn a very good blueprint for the blockchain. But in fact, blockchain technology is still in its infancy, and most blockchain services lack rich functions and have a narrow range of applications. There is also a lack of corresponding incentive mechanisms in the blockchain development community.

Therefore, there is an urgent need to carry out research on the underlying protocol of blockchain, overcome the underlying core technology of blockchain, redesign or improve various dimensions of blockchain technology, and solve and meet transaction congestion, high transaction fees, and long transaction confirmation times. , Weak anti-quantum attack ability, low node communication anonymity, lack of transaction anonymity protection function, weak cross-chain communication and multi-chain integration capabilities, large storage space, etc., optimize and improve the protocols of blockchain technology at all levels and mechanism to realize the support protocols at all levels of the truly practical value transmission network, provide infrastructure for various value transmission applications, provide the underlying development platform for the development of various DApps, and provide a realistic and feasible technical approach for building a global value Internet.

1.4 The Birth of FON Smart Chain

The rapid development of decentralized finance "DeFi" in 2020 will allow the rapid integration of blockchain technology into the financial system, enabling the technology to be implemented and the ecology to flourish. People found that in the blockchain world: financial gameplay is more diverse, the combination is more flexible, the data is more real, and the access is unlimited. What I have experienced is to break the various constraints of traditional finance and realize financial services: "trusted operation", "millisecond-level access", "unlimited application", "world-class integration", and finally realize the integration of global financial assets change.

The development of DeFi started on the Ethereum network and led to a big bull market in the crypto market in 2020. Hundred times coins and thousand times coins were born in the DeFi network. People marveled at and chased this new way of finance, triggering waves of wealth booms. However, as the price of Ethereum increases and the number of participants increases, the Ethereum network becomes slower and slower, and the gas cost is getting higher and higher, and ordinary users can no longer afford it. By 2021, the development of the Ethereum ecosystem has stagnated, and ordinary users can no longer afford the Ethereum network. As a result, a blockchain infrastructure competition with the public chain as the main track has been launched.

Based on the above background, FSC Ecological Development Fund has built the FON smart chain. Based on the "consensus trust" mechanism and encryption

algorithm of the blockchain, every transaction in the user scenario is recorded on the blockchain without relying on third-party intermediaries. The organization is completely open, transparent and traceable, establishes an ecosystem system trusted by the whole people, and realizes efficient consensus, multiple application scenarios, scalability, high performance, high security, high-speed access, and efficient operation.

FON Smart Chain is a decentralized, high-efficiency and energy-saving ecological public chain: programmable smart contracts are seamlessly compatible with the Ethereum network, reducing development and migration costs. In addition, decentralized DApps created on the FON smart chain can include privacy expansion, liquidity mining, DeFi wealth management, privacy swap, lending, cross-chain transactions, NFT, social networking, payment, entertainment, e-commerce and other application directions . FON Smart Chain will establish point-to-point direct and reliable trust, remove the interference of intermediaries in business scenarios, form a new digital currency system, payment method, and credit mechanism, and create a high-efficiency, low-cost, and safer value ecosystem chain.

Chapter II

Overview of FON Smart Chain

2.1 Introduction to FON Smart Chain

FON Smart Chain, FON Smart Chain referred to as FSC, is committed to becoming the world's leading public chain system and blockchain infrastructure.

FSC is compatible with EVM at the base layer, has the ability to create and deploy smart contracts, and is compatible with the Ethereum Virtual Machine (EVM). The leading cryptocurrency exchange seems to be starting to fully dive into the cryptocurrency world and expand from a mere trading exchange to the entire ecosystem with FON Smart Chain.

Basically, the new mechanism operates as an independent blockchain without relying on any chain to proceed. EVM compatibility enables Ethereum tools and dApps to work well with FSC with zero or minimal changes. It is worth noting that users need to modify some settings to set up dApps like MetaMask to work on FSC.

The operation of the FON Smart Chain is as follows:

Consensus: While the proof-of-work (PoW) mechanism is valuable, it negatively impacts the ecosystem and also requires more than half of the network to maintain security. FON Smart Chain uses a consensus mechanism. Authority-Proof-of-Stake-(APoS) to keep the ecosystem in sync. APoS is a mechanism for validators to stake FON and prove the validity of transactions. Compared to other variants, this model is more efficient and less expensive from an energy point of view. Governance related to the APoS consensus algorithm of

21 transaction validators will provide decentralization and enable massive participation in market transactions.

■ Cross-chain compatibility: The need for blockchain interoperability is becoming more and more important. Cross-chain compatibility enables interoperability between two or more blockchains. This function can easily exchange assets from BSC as well as TRON protocol to FON Smart Chain. Even when the two blockchains work independently, they can still communicate with each other. Users can use the solution to convert three of FON's most popular FEP standards: FEP2, FEP8 and FEP20 tokens.

Ethereum Compatibility: In addition to native cross-chain communication, the FON Smart Chain is compatible with the Ethereum mainnet to support all existing Ethereum tools or coins with lower transaction fees and faster processing times compared to the normal base .

In addition, FON Smart Chain will support existing token assets on BSC and TRON protocols, with EVM-compatible programming capabilities and native support for cross-chain communication, developers will enhance functionality.

As a practical value interconnection blockchain infrastructure, FSC provides a series of technical and functional characteristics to support the value mapping between the real world and the virtual world, and will surely provide a feasible realization path for exploration and early realization of value mapping . Therefore, our goal is to build a general-purpose, well-supported, high-performance, easy-to-use, user-friendly, and scalable blockchain 4.0 infrastructure based on

enhanced directed acyclic graphs, and to build a blockchain that supports various on-chain applications. Blockchain 4.0 Ecosystem. Therefore, FSC focuses on the core technology of blockchain infrastructure and platform layer, and builds a completely distributed anonymous P2P network communication protocol, a new anti-quantum attack cryptographic hash algorithm and signature algorithm, an original two-layer consensus and mining mechanism, and supports transactions. Anonymity protection, Turing complete smart contracts and other features, adopt a fair distribution mechanism, support third-party asset issuance, cross-chain communication, multi-chain integration and other functions, and can be implemented in practical application scenarios in the form of public chains, alliance chains, and private chains.

In the future, FSC will realize various key technologies of value transmission network, build a global value Internet, and provide basic network and complete ecosystem support for various value transmission applications.

2.2 Design principles

Standalone Blockchain: Technically, FSC is a standalone blockchain, not a layer 2 solution. Most of the FSC underlying technology and business functions should be self-contained so that it can function properly even if other packages are temporarily stopped.

Ethereum Compatibility: The first practical and widely used smart contract platform was Ethereum. In order to take advantage of relatively mature applications and communities, FSC chose to be compatible with the existing Ethereum mainnet. This means that most dApps, ecosystem components and tools will work with FSC and require zero or minimal changes; FSC nodes will require similar (or higher) hardware specifications and skills to run and operate. The implementation should leave room for FSC to catch up with further upgrades to Ethereum.

Staking participation in consensus and governance: Staking-based consensus is more environmentally friendly, leaving more flexible options for community governance. It is expected that this consensus should enable better network performance on the [proof-of-work] blockchain system, i.e. faster block times and higher transaction capacity.

Native cross-chain communication: All FSCs will natively support cross-chain communication between two blockchains. Communication protocols should be bidirectional, decentralized and trustless. It will focus on moving digital assets

between FSC and other chains, namely [FEP2] tokens, and eventually, other FEP tokens will be introduced later. The protocol should care about the minimum of other items stored in the blockchain state, with a few exceptions.

Based on the above design principles, the consensus protocol of FSC should achieve the following goals:

■ The blocking time should be shorter than the Ethereum network, eg 5 seconds or less.

■ Confirming the finality of the transaction takes a limited time, such as around 1 minute or less.

■ The native token has no inflation: FSC, block rewards are collected from transaction fees and paid in FSC.

■ Compatible with the Ethereum system as much as possible.

■ It allows for modern [proof-of-stake] blockchain network governance.

2.3 Application goals

The core value of the blockchain is to build a trustworthy decentralized system, and upgrade the decentralized and independent individual centers to a unified multi-center with multi-party participation, thereby improving the efficiency of trust transfer and reducing transaction costs.

The goal of FSC is to use self-developed public chain technology and combine the technical characteristics of blockchain to build a fair and open comprehensive application system. Solve the trust and fairness issues currently faced by the industry, and make the entire competitive environment more fair, open and efficient. FSC's mission is to build a complete value ecosystem for global businesses and users in the blockchain era, and hope that this ecosystem can provide protection for users' free will and personal value, especially the value of time.

Major platforms are creating barriers in the business world, splitting the entire crypto world, becoming isolated islands one after another, and the bridges between various economies have long been ruthlessly demolished. 's fence. FSC hopes to provide global users with a more ideal ecological environment in the era of blockchain and realize the interconnection between independent ecosystems. FSC will build bridges between each continent, allowing everyone to understand this blockchain from a new dimension. A new world of encryption built.

The original intention of FSC's design is to build a multi-dimensional public chain system. Through cross-chain technology, a complete set of cross-chain solutions is built on the FSC public chain, and the unified digital currency produced by blockchain technology is used for rewards:

- Token Economic Solutions

- Multi-application interoperability (digital currency trading, DeFi, NFT) solutions

- Digital asset issuance and circulation ecosystem

- Payment Ecosystem Interoperability Solution

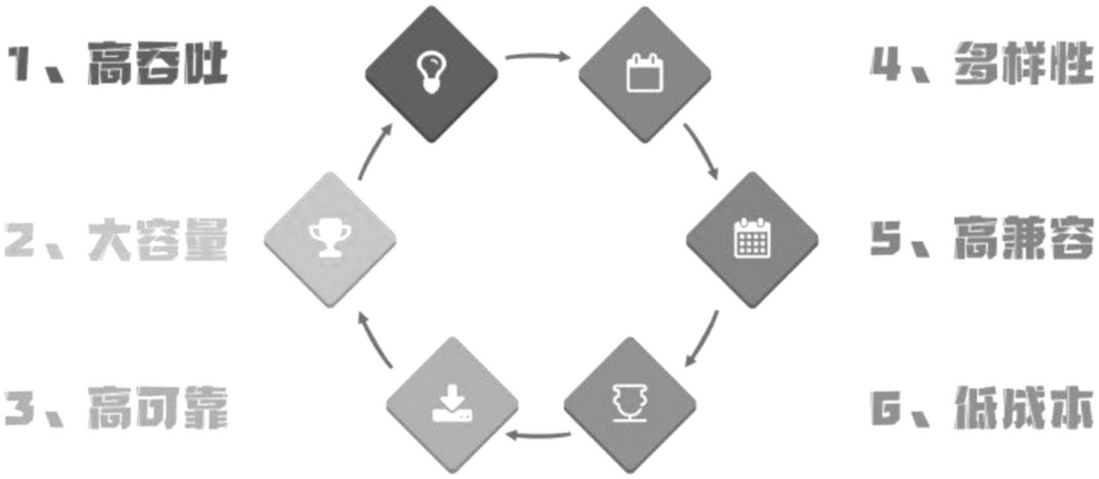
When FSC participants make contributions to FSC, according to the calculation of the contribution mechanism, we provide them with corresponding reasonable returns. As a commercial application-level blockchain solution, the ecological construction and transformation and upgrading of third-party commercial organizations can also be solved through the application of FSC.

FSC fully absorbs the advantages of existing blockchain 1.0, blockchain 2.0 and blockchain 3.0 projects, solves their outstanding problems and technical defects, and builds a more prosperous application ecology. FSC innovatively designed the on-chain and off-chain data mapping mechanism, a new enhanced data structure based on Directed Acyclic Graph (DAG) and HashNet, a two-layer consensus mechanism based on HashNet consensus and BA-VRF consensus, and the introduction of external triggers Conditional advanced Turing-complete smart contracts, Keccak512 hash algorithm and NTRUSign signature algorithm based on anti-quantum attack, transaction anonymity protection mechanism based on ring signature and zero-knowledge proof, with fast transaction confirmation, anti-quantum attack, node anonymous communication, transaction anonymity Protection, advanced smart contracts, data on-chain and other functional features of blockchain 4.0, and by adopting a fair distribution mechanism, it supports third-party asset issuance, cross-chain communication, multi-chain integration and other functions.

FSC will provide a basic blockchain network for various value transmission applications, and support various practical applications in the form of public chains, alliance chains, and private chains. In specific applications, FSC performs Hash operations on the data of specific application scenarios, and the Hash values are stored on the FSC public chain. The application scenarios are not limited to the digital currency applications represented by Bitcoin in the context of blockchain 1.0, and are not limited to regional The financial field that combines digital currency and smart contracts under the background of blockchain 2.0, as well as the application attempts of blockchain 3.0 in the fields of government, health, culture and art; the blockchain 4.0 public chain based on FSC will become a multi-functional The infrastructure of each industry and the formation of a perfect industry ecosystem based on blockchain will extensively and profoundly change people's way of life.

FSC will completely reshape the operating model of the existing Internet, turning the economic incentive system itself into a system that can circulate within the system, creating a completely decentralized Internet value transmission ecosystem, and also a completely open community ecosystem, beyond borders, so that every participant can obtain the corresponding value.

2.4 FSC technical advantages



1) high throughput

The higher TPS of FSC is improved through the second-layer network, and the theory is that it can reach the level of tens of millions per second.

2) Large capacity

Through encryption and deduplication technology, the underlying network file system of FSC is improved, and the larger storage space of FSC is increased to more than a thousand times.

3) High reliability

By expanding the blockchain network structure of FSC, combined with the dual layered consensus of super nodes and edge nodes, a reliable and feasible value system is built to ensure the stable operation of the entire network.

4) Diversity

By expanding FSC's smart contract implementation mechanism and task scheduling model, combined with edge computing grids, more smart contract adaptation scenarios can be constructed.

5) High compatibility

By expanding the FSC smart contract writing specification, it is compatible with mainstream public chains in the market, combined with the multi-contract virtual machine mechanism, making smart contracts compatible across chains and lowering the entry threshold for developers.

6) Low cost

By expanding the FSC economic model, combined with multiple tokens and multiple incentive mechanisms, a virtuous cycle of consumption and production systems can be realized, providing operating costs unmatched by other centralized designs and competing products.

2.5 Landing advantages

Benefiting from the advantages of continuous development and innovation of blockchain technology, extensive commercial applications, and refined governance, FSC is competitive in the following aspects:

1) Technology

FSC has very mature and strong technical support. It has accumulated rich industry and technical experience in various fields such as blockchain bottom layer, encrypted communication, mathematics, Web3, and information technology. It has achieved industry-leading results in the development and application of blockchain technology Leading Breakthrough.

2) Industry resources

The FSC team brings together senior people from multiple industries, many years of practical operation experience, and deep insights into industry development. In addition, the FSC team will sign a strategic cooperation agreement with the top leading companies in the target industry, which will provide strong support for FSC to enter the application, so as to truly promote FSC to access more projects and developers.

3) Business Governance

Different from general public chains, FSC has a clear and definite strategic plan for the target industry. More focused and professional, with the help of the distributed decentralization, immutability, encryption security and point-to-point transmission of value of blockchain technology, we can penetrate into the target industry and quickly gain market share.

4) Fund management

FSC's fund management will strictly abide by the principles of fairness, impartiality and openness, and take the development of the FSC platform as the primary

purpose. The FSC team specially keeps and ensures the safety and sustainability of funds. The use of all funds of the FSC public chain and the FSC Ecological Development Foundation will be regularly disclosed to all investors to ensure the openness of the use of funds.

5) Development space

FSC's target industries are all trillion-level blockchain infrastructure and encryption markets. The development team effectively manages general affairs, code management, financial management, compensation management, and privileged operating scope by formulating a sound governance structure to ensure sustainable development.

FSC perfectly inherits the characteristics and advantages of the traditional blockchain ecosystem technology, and solves the technical bottleneck of the current blockchain, truly combining the blockchain with commercial applications. In addition, FSC vigorously and continuously invests in the research and development and innovation of commercial technology represented by blockchain technology, and applies it to enhance the value of traditional industries and promote the vigorous development of blockchain technology in various industries. A clear and clear strategic development direction to create a mutually beneficial and win-win blockchain public chain ecosystem in the future.

Chapter III

FSC Technical System

3.1 Proof of Stake

Although Proof of Work (PoW) has been recognized as a practical mechanism for enabling decentralized networks, it is not environmentally friendly and also requires a large number of participants to maintain security.

Ethereum and some other blockchain networks such as MATIC Bor, TOMOChain, [GoChain, xDAI, be sure to use [Proof-of-Authority(APoS)] or its variants for different scenarios, including testnet and mainnet. APoS provides some defense against 51% attacks, improving efficiency and tolerance for certain levels of Byzantine players (malicious or hacked). It can be used as an easy choice as a base.

At the same time, the APoS protocol is most criticized for not being as decentralized as PoW, since validators (i.e. nodes who take turns producing blocks) have all authority and are vulnerable to corruption and security attacks. Other blockchains such as EOS and Lisk have introduced different types of [Delegated Proof of Stake (DPoS)] to allow token holders to vote and elect validator sets. It increases decentralization and benefits community governance.

FSC proposes APoS consensus here, as follows:

- Blocks are produced by a limited set of validators
- Validators take turns producing blocks in an APoS fashion, similar to [Ethereum's Clique] consensus design
- Validator sets are elected and exited according to stake-based governance

1) Quorum of validators

During the genesis phase, some trusted nodes will operate as the initial set of validators. After the block starts, anyone can compete as a candidate to join the election as a validator. The stake state determines the top 21 most staked nodes to become the next validator set, and such an election will be repeated every 24 hours.

2) FSC is the token used to pledge FSC.

In order to maintain the same compatibility as Ethereum and upgrade to future consensus protocols to be developed, FSC chooses to rely on an innovative model for staking management. There is a dedicated FSC staking module. It will accept FSC stakes from FON token holders and calculate the highest staked node set. At every midnight UTC, FSC will issue a verifiable `ValidatorSetUpdate` cross-chain message, informing FSC to update its validator set.

Existing FSC validators periodically check for a "ValidatorSetUpdate" message relayed to the FSC as more blocks are generated. If there are, they will update the validator set after an epoch period (i.e. a predefined blocking time). For example, if FSC produces a block every 5 seconds, and the epoch period is 240 blocks, the current validator set will check and update the validator set for the next epoch in 1200 seconds (20 minutes).

3) Security and certainty

Given that there are more than ½ * N+1 validators that are honest, APoS-based networks can generally function securely and correctly. However, there are still situations where a certain number of Byzantine validators can still manage to attack the network, for example through a "[clone attack]". To be safe, we

encourage FSC users to wait until they receive more than ⅔ * N+1 blocks sealed by different validators. In this way, the FSC can be trusted at a security level and can tolerate less than ⅓ * N Byzantine validators.

For 21 validators, if the block time is 5 seconds, it takes (⅔ * 21+1) * 5 = 75 seconds for ⅔ * N+1 different validator seals. Any critical application of FSC may have to wait ⅔ * N+1 for relatively safe finality. However, in addition to such an arrangement, FSC does introduce Slashing logic to penalize Byzantine validators for double-signature or inavailability, which will be covered later in the "Staking and Governance" section. This slashing logic will expose malicious validators for a short period of time and make "clone attacks" very difficult or extremely unhelpful to perform. With this enhancement, ½ *N+1 or even fewer blocks are sufficient as confirmations for most transactions.

4) Rewards

All FSC validators in the current validator set will be rewarded with fees in transaction FSC. Since FSC is not an inflation coin, it does not generate mining rewards like Bitcoin and Ethereum networks, and gas fees are the main reward for validators. Since FSC is also a utility token with other use cases, delegators and validators will still enjoy the other benefits of holding FON tokens.

Validator rewards are fees collected from transactions in each block. Validators can decide how much to give back to delegators who stake FSC to them to attract more staking. Each validator will take turns producing blocks with the same probability (if they stick to 100% activity), so all stable validators may receive a similarly sized reward in the long run. At the same time, each validator may have different stakes, so this creates a counterintuitive situation where the more users

trust and delegate to a validator, the less rewarded they may be. Therefore, as long as the validator remains trustworthy, rational delegators will tend to delegate to those with less stake (insecure validators may present reducible risks). In the end, the stake changes for all validators will be smaller. Part of the gas fee will also be rewarded to relayers for cross-chain communication.

3.2 Smart Contract

Blockchain technology provides a secure and credible execution environment for smart contracts, which facilitates the realization of the concept of smart contracts. Smart contracts are event-driven, stateful programs that run on a replicable, shareable ledger and hold assets on the ledger. The purpose is to enable a complex set of digital commitments with trigger conditions to be The will of the participants, executed correctly. Smart contracts can not only receive and store value, but also send information and value to the outside world. The entire process can be automated and intelligently executed without a center or trust.

Smart contracts are designed to strike a balance between security and functionality. Existing blockchain projects mainly focus on the design of a single type of smart contract, seeking a balance between security and functionality under the conditions limited by the type of smart contract, often failing to meet the user experience of diverse user groups and diversified user transactions desired effect. The transaction script of the Bitcoin blockchain is the prototype of a smart contract, which is a non-Turing-complete smart contract, with the advantages of low complexity and light weight, and there has been no security in the Bitcoin blockchain network for nearly ten years. problem, but the Bitcoin

transaction verification script supports very limited functionality and is only used for payment verification. The Ethereum blockchain supports Turing-complete smart contracts written in the Solidity high-level language, which greatly enriches the functions of smart contracts and expands the application field of blockchain technology. However, writing Ethereum smart contracts is prone to security vulnerabilities. The DAO The incident was precisely because of a security breach in the Ethereum smart contract written, which caused the Ethereum community to split.

FSC adopts a layered idea similar to the computer storage architecture in the realization of smart contract functions. The Moses Virtual Machine (MVM) supports declarative non-Turing complete smart contracts and advanced Turing complete smart contracts. Users choose to use these two types of contracts according to their user experience and transaction needs, balancing computing security and computing functions as well as computing costs and computing complexity to meet transaction diversification needs. Declarative smart contracts are easy to deploy, have high security, and are closer to legal contract languages; advanced Turing-complete smart contracts are relatively difficult to deploy, and are mainly used to develop DApps with more complex program logic. The fee mechanism for the deployment of the two types of smart contracts is different. The fee for a declarative smart contract is calculated based on the bytes occupied by the contract, while the fee for an advanced Turing-complete smart contract is the FSC Token consumed by the program running.

3.3 Cross-chain mechanism

FSC uses a proof-of-stake consensus protocol that has the opportunity to fork and require more blocks to be confirmed. A block has only one validator's signature, so it is difficult to rely on a block to verify data from FSC.

To take full advantage of the validator quorum of other chains, an idea similar to that of many [Bridge] or Oracle blockchains is adopted:

Cross-chain communication requests from FSC will be submitted as transactions and executed on FSC. The execution of transactions emits `Events` which can be observed and packaged in some "Oracle*" to other chains. This type of "Oracle" package does not have Block Headers, Hash and Merkle Proofs, but directly contains cross-chain information for actions such as sender, receiver and transfer amount.

To ensure the security of the oracle machine, the validators of other chains will form another quorum "Oracle Relayers". Each validator of other chains should run a dedicated process as Oracle Relayer. These Oracle Relayers will use the same validator key to submit cross-chain communication packages (like oracles) to other chains and vote. Any packet signed by more than ⅔ * N+1 Oracle Relayers voting power is as secure as any block signed by ⅔ * N+1 validator voting rights of the same quorum.

By using the same quorum of validators, it saves light client code on other chains and keeps continuous block updates on other chains. Such Oracles also have Oracle IDs and Types to ensure ordering and proper error handling.

1) Timeout and error handling

There are scenarios where cross-chain communication fails. For example, relay packets cannot be executed on FSC due to some coding errors in the contract. Timeout and error handling logic** are used in such scenarios. For identifiable user and system errors or any expected anomalies, both networks should repair themselves. For example, when the transfer from other chains to FSC fails, FSC will issue a failure event, and Oracle Relayers will execute the refund of other chains; when the transfer from FSC to other chains fails, other chains will send refund packets to Relayer for relaying to unlock funds. However, unexpected errors or exceptions can still occur during any step of cross-chain communication. In this case, Relayers and Oracle Relayers will find the corresponding cross-chain channel stuck in a specific sequence. After the timeout period, repeaters and Oracle repeaters can request a "SkipSequence" transaction, and the stuck sequence will be marked as "unexecutable". Corresponding alerts will be raised and the community must discuss how to handle this situation, such as paying back through validator sponsors, or clearing funds during the next network upgrade.

2) Cross-chain user experience

Ideally, users want to use two parachains as if they were using one chain. It would require adding more aggregated transaction types to cross-chain communication to achieve this, which would add enormous complexity, tight coupling, and maintenance burden. Other chains and FSCs here only implement the basic operations to enable value flow at initial startup, leaving most of the user experience work to the client UI, such as wallets. For example, a great wallet might allow users to sell tokens directly from FSC onto other chains' DEX order books in

a secure manner.

3) Cross-chain contract events

Cross-chain contract events (CCCE) are designed to allow smart contracts to trigger cross-chain transactions directly through contract code. This is possible based on:

■ Provide standard system contracts to serve operations that can be called by general smart contracts;

■ Standard events can be issued by standard contracts;

■ Oracle Relayers can capture standard events and trigger corresponding cross-chain operations;

■ Dedicated, code-managed addresses (accounts) can be created on other chains and accessed by contracts on FSC, here named "Contract Addresses on Other Chains" (CAoB).

Several standard operations are implemented:

■ FSC to other chain transfers: This is implemented in the same way as normal FSC to other chain transfers, only triggered by standard contracts. Funds can be transferred to any address on other chains, including the corresponding CAoB of the transfer originating contract.

■ Transfer on other chains: This is a special kind of cross-chain transfer, and the real transfer is from CAoB to any other address (even another CAoB).

■ Transfer from other chains to FSC: This is achieved through two cross-chain

communications. The first time it is triggered by the FSC contract and propagated to other chains, then on the second pass, the other chains will start the normal other chain to FSC cross-chain transfer, from CAoB to the contract address on FSC. It is important to note that the FSC contract only increases the balance on any transfer in the second pass, and the error handling in the second pass is the same as for normal other chain to FSC transfers.

■ IOC (Immediate-Or-Cancel) Trade Out: The main goal of transferring assets to other chains is to conduct transactions. This event will instruct to trade a certain amount of an asset in the CAoB into another asset as much as possible, and transfer all the results of the trade, i.e. the source remaining and the target token of the trade, back to the FSC. Other chains will handle such relay events by sending an "immediate or cancel" (i.e. IOC order) to the trading pair, and once the next match is done, the result will be relayed back to the FSC, which can be one or two assets.

■ Auction Trade Out: This event will instruct other chains to send an auction order to trade as much as possible a certain amount of assets in CAoB for another asset, and transfer all results back to the FSC auction at the end. FSC will launch an auction function.

Trade Out has some details:

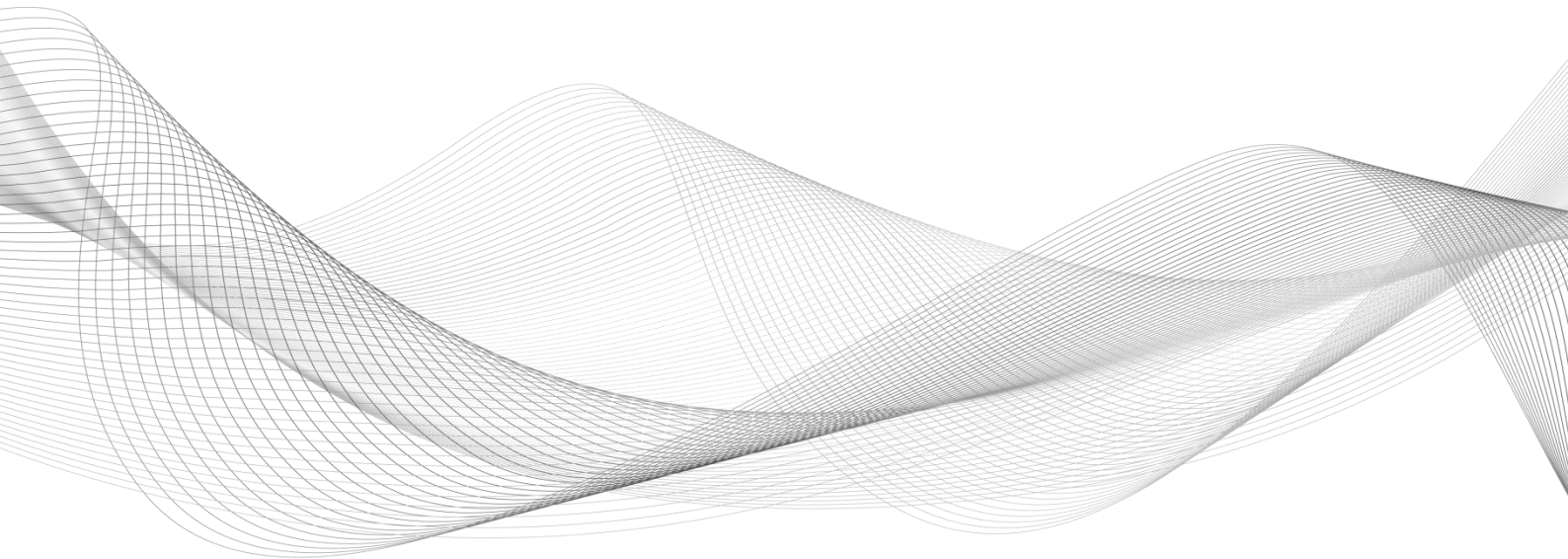
■ Both can have limit prices (absolute or relative) to trade;

■ The final result will be written as a cross-chain packet and sent back to FSC;

■ Assets transferred back to FSC may be charged cross-chain communication fees;

■ The FSC contract maintains a mirror of balances and outstanding orders on the CAoB. Whatever errors occur during Trade Out, the final state propagates back to the original contract and clears its internal state.

With the above features, it simply adds cross-chain transfer and exchange functions with high liquidity to all smart contracts on FSC. It will greatly increase the application scenarios on smart contracts and dApps, and realize 1 chain + 1 chain > 2 chains.



3.4 Repeater

1) Relayer

The relayer is responsible for submitting cross-chain communication packets between the two blockchains. Due to the heterogeneous parallel chain structure, two different types of Relayers are created.

FSC repeaters Repeaters used for other chain to FSC communications are called "FSC repeaters", or simply "repeaters". Relayer is an independent process that can be run by anyone anywhere, except Relayer must be registered with FSC and deposit a certain amount of refundable tokens. FSC only accepts relay requests from registered relays.

The packages they relay will be verified by on-chain light clients on FSC. A successful relay needs to pass sufficient verification and needs to pay gas fees on FSC, so there should be incentive rewards to encourage the community to run Relayer.

2) Oracle Repeater

Relays that communicate from FSC to other chains use the "Oracle" model, so-called "Oracle Relayers*". Every validator must (and only validators in the validator set) run an Oracle relay. Each Oracle Relayer observes changes in the state of the blockchain. Once it captures the cross-chain communication packet, it submits the request for voting. The cross-chain action will be performed after the

Oracle Relayer in 2/3 of the voting power of other chain validators votes for the change.

Oracle Replayers should wait for enough blocks to confirm finality on FSC before committing and voting on cross-chain communication packets to other chains.

Cross-chain fees will be distributed to other chain validators along with normal other chain block rewards.

This oracle type relay relies on all validators to be supported. Since all votes for cross-chain communication packets are recorded on the blockchain, it is not difficult to have a metric system to evaluate the performance of Oracle Relayers. The worst performers may get their rewards back through another slashing logic introduced in the future.

3.5 Hard Forks, Norms and Dispute Resolution

Different distributed ledger systems often differ in underlying political philosophies and technical choices. The original promise of the Ethereum project was to achieve "unstoppable applications" where "code is law". After an important smart contract was hacked, due to the lack of a non-code description of what the program was intended to do, a debate arose over whether what happened could at all be described as a hack. The disagreement eventually led to divisions within the community.

Because FSC contracts are simple zip files, it can easily contain documents in PDF or other formats that describe the actual intent of the contract. There is no requirement that this mechanism be used, nor that these documents have legal force. Nonetheless, in the case of financial use cases, if disagreements arise, it is more important that they contain contracts in the legal sense than the software implementations they contain.

It is technically possible to write a non-upgradable contract. If such a contract governs an asset that exists only on a ledger, such as a cryptocurrency, then this could provide an approximation of "code as law". We leave the discussion of the wisdom contained in this idea to political scientists and reddit. Platform logs do not have a mechanism in FSC that is directly equivalent to a "hard fork" of the blockchain, so give up on problematic transaction chains or fraudulent transaction chains. The only way is to agree out-of-band to discard a full transaction subgraph. Since there is no global visibility, this consensus need not include all participants

on the network: only those who may have received and processed the relevant transactions. Another consequence of the lack of global visibility is that there is no single point where exactly who has seen which transaction. Determining the set of entities that must agree on discarding a subgraph implies the need to associate the node's activity log.

FSC nodes log sufficient information to ensure that such a correlation can be achieved. The platform defines a stream available to anyone to assist in this process. A tool is also provided that can generate "survey requests" and send them to a seed node. The flow informs the node administrator that a decision is required, and sufficient information is passed to the node to attempt to persuade the administrator to participate (such as a signed court order). If the administrator accepts this request through the node browser, subsequent jumps in the transaction chain are returned. The tool semi-automatically crawls the network in such a way that it finds all participants who would be affected by the proposed rollback. The platform does not participate in determining what type of transaction rollback is justified, and provides only minimal support for implementing rollback operations in addition to locating the parties that must agree.

There are at least two strategies for modifying the ledger once the participants involved are identified. One is to extend the transaction chain with transactions that simply modify the database to match the expected reality. For this approach to be possible, smart contracts must be written that can be arbitrarily modified outside of normal business logic when submitted signatures reach a sufficient

threshold. This strategy is simple and makes the most sense when the state contains a small number of parties and none of them have an incentive to leave harmful information on the ledger.

In the case of an asset state resulting from theft or fraud, the involved participants will resist all attempts to patch it in the above way, since they can benefit from the real world between the time difference between when the ledger goes wrong and before it is restored to the actual state. For this case, a more sophisticated approach is required, where all but the non-cooperating participants agree to mark the relevant state as no longer consumed or spent. This is essentially a restricted form of database rollback.

3.6 Diversified technical support

FSC will provide the underlying API of the blockchain for third-party projects, realize the connection of application scenarios, and realize the superposition of digital assets, so as to solve the relevant practical problems in the industry. In order to realize this vision, FSC has made corresponding layouts in the bottom-level design and top-level applications.

1) Second-level fast transaction verification

Through the optimization of key links such as signature algorithm, ledger structure, data operation, serialization, consensus mechanism, and message diffusion, FSC will achieve fast transaction verification in seconds. Satisfy the user experience of financial scenarios under most blockchain applications.

2) Storage of massive financial data

The double-entry bookkeeping mode of the blockchain has accumulated a large amount of data in the continuous application of the system, resulting in a decrease in the running speed. FSC will realize the mechanism of separate storage and sub-table storage to realize the mass storage of data.

3) Improvement of transaction throughput

The essence of blockchain is a distributed shared accounting technology, and its distributed characteristics are mainly reflected in distributed consistency rather than distributed concurrent processing. In order to ensure data consistency and prevent Byzantine generals problem, some specific links can only be executed

serially, but not in parallel. Through long-term testing and optimization practices, the processing performance of FSC will further greatly improve transaction throughput.

4) Fast synchronization of node data

FSC will develop a mirroring mechanism, which can regularly mirror the local ledger to implement a convenient rollback mechanism. Under a unified consensus, mirror labels can be specified for rollback. At the same time, the cycle for newly added nodes to join the operation is shortened, and it only needs to synchronize the latest image and a small number of recent transaction sets to integrate into the network and participate in consensus verification.

5) Data access control strategy

FSC provides two types of permission control policies for data information writing and reading. Data information write permission, set up multiple users under the same account, and set corresponding permissions for different operations to meet the usage scenarios of multi-party signature control. The data information read permission, the user can grant and revoke the data operation permission for a single user or user group, and the user group can be flexibly configured by the user. The data includes user account information, transaction information, etc. The granularity can be refined to various attribute fields of transactions or accounts.

6) Diversified expansion development

The blockchain structure of FSC can meet the needs of different business fields and improve the scalability and maintenance efficiency of the system. It can be

used to mark assets and asset transfers, provide multi-dimensional event records that cannot be tampered with, and can also be used for traceability to track the flow of financial assets.

7) Multiple privacy protection

In order to facilitate users to use FSC products and services, in addition to the traditional client generation and storage mechanism, FSC also provides two solutions: network hosting access and private key hardware access (U-key). Network hosting access, that is, the user name and password are mapped into a private key through a specific algorithm and stored on the server. The private keys stored on the server side are all encrypted data, and the private keys can only be decrypted on the client side; the hardware private keys are used to meet the needs of the financial industry.

At the same time, it provides multiple privacy protection functions. First of all, the bottom layer of FSC provides homomorphic encryption. All user data is encrypted and stored, and only the user can see it. Secondly, provide encryption middleware services, users can choose according to business needs. Finally, the upper-layer application can encrypt the data during input, and the FSC is responsible for writing and reading the encrypted data generated by the user.

8) Visual operation and maintenance support

FSC will provide the visualization tools required for operation and maintenance management. System monitoring services deployed on FSC nodes: support business (blocks, transactions, contracts, consensus, etc.), network (networking,

delay, throughput, etc.), data information monitoring at the system level (CPU, memory, disk, etc.) . At the same time, it provides a complete log, alarm and notification mechanism to facilitate the maintenance of financial commercial systems.

Chapter IV

Token Economy

4.1Economic model

FON Smart Chain will issue FON tokens. FON token is a token issued to encourage users and third-party collaborators to participate in ecological construction and other behaviors, and has the internal value resources and rights and interests of the FON smart chain that can be exchanged. At the same time, as an underlying infrastructure that integrates multi-form digital assets, FON smart chain can derive more other smart assets through financial smart contracts. In the future, the FSC public chain will drive the value growth of FON tokens through more innovative models.

Fonvity (FON) Smart Chain Explorer

A total of 26 million native FON tokens

The top 21 nodes will receive the node block reward

FON Smart Chain is used for effective governance proposals to enrich the healthy development of the ecosystem

Creating a node requires a creator to pledge 9999 FON to create a node

The maximum number of alliance nodes is 99, after which it cannot be created

The top 21 nodes are core nodes and can directly initiate core proposals for governance

The creator of the node can withdraw from the alliance node at any time, and the 9999 FON will also be returned.

Node election method, voting on nodes through FON pledge

Nodes refresh their rankings every three hours

Overall, the FON token has a profound logical relationship with the value, incentives, governance and security of the bottom layer of the FON smart chain, reflecting the value characteristics of the FON token.

■ From the perspective of value, FON token condenses the carrier of "trust value" and "consensus value";

■ In terms of incentives, FON tokens are economic rewards that motivate the participation of "bookkeepers" in the network;

■ From a governance point of view, FON token is a certificate of rights and interests to participate in the FON smart chain network;

■ From a security point of view, the existence of value incentives improves the network security of the FON smart chain.

The FON token will run on the FON Smart Chain just like ETH runs on Ethereum, so it is the "native token" of the FON Smart Chain. This means that in addition to the FON token being used to pay most of the fees on the FON Smart Chain, B will be used to:

■ Pay "fees" to deploy smart contracts on the FON smart chain

■ Pledge selected FON smart chain validators to get corresponding rewards

■ Carry out cross-chain operations, such as transferring token assets across other chains and FON smart chains

4.2 Seed Funds and Other Tokens

1) Seed Funding

A certain amount of FON tokens will be burned and minted on the FON Smart Chain during its genesis phase. This funding, known as the "seed fund," circulates after the first block and will be distributed among the initial relayers and the initial set of validators introduced at genesis. These FON tokens are used to pay transaction fees upfront to transfer more FON tokens from the FON Smart Chain to other chains through a cross-chain mechanism.

The cross-chain transfer of FON tokens will be discussed later, but for transfers, generally, the FON tokens on FON are locked from the source address of the transfer to the address controlled by the system, and the corresponding amount is unlocked from the special contract to the FON smart chain The destination address of the transfer, or conversely, when transferring from the FON smart chain to other chains, is to lock the FON token from the source address on the FON smart chain into a special contract, and change the locked amount on the other chain from The system address is released to the target address. The logic is

related to native code on other chains and a series of smart contracts on the FON smart chain.

2) Other tokens

FEP Standard: FEP2, FEP8, and FEP20 tokens, which are native assets that can be transferred and traded (if listed) with fast transactions and sub-second determinism. At the same time, since the FON smart chain is compatible with Ethereum, it naturally supports ERC20 tokens on the FON smart chain, which is called "FEP2E*" (the real name will be introduced by the future FEP, and may also cover FEP8). FEP2E can be "enhanced" by adding more methods to expose more information, such as token denominations, decimal precision definitions, and owner addresses that can determine cross-chain token bindings. FON Smart Chain to ensure that a token can be circulated in two formats with confirmed total supply and used for different use cases.

3) Cross-chain transfer

Cross-chain transfers are a critical communication between two blockchains. The essential logic is:

■ A "transfer out" blockchain locks the amount of the source owner address into a system-controlled address/contract;

■ A "transfer-in" blockchain will unlock the amount from a system-controlled address/contract and send it to the destination address.

Transmitting packet messages across chains should allow relayers and oracles to verify:

■ A sufficient amount of token assets are removed from the source address and locked in the system control address/contract on the source blockchain. This can be confirmed on the target blockchain.

■ An appropriate amount of token assets are released from system-controlled addresses/contracts and distributed to target addresses on the target blockchain. In the event of a failure, confirmation can be made on the source blockchain to release the locked tokens back (fees may be deducted).

■ After the transfer is completed, the sum of the total circulation of the token assets of the two blockchains will not change regardless of whether the transfer is successful or not.

4.3 Staking and Governance

Proof of stake brings decentralization and community participation. Its core logic can be summarized as follows. You may see similar ideas from other networks, especially Cosmos and EOS.

■ Token holders, including validators, can “bond” their tokens into staking. Token holders can delegate their tokens to any validator or validator candidate in the expectation that it can become a real validator, then they can choose a different validator or candidate to re-delegate their tokens ¹.

■ All candidate validators will be ranked according to the number of tokens bound on them, and the top ranked will become the real validators.

■ Validators can share (part of) their blocking rewards with their delegators.

■ Validators may suffer "slashing", which is a penalty for their bad behavior, such as double-signing and/or instability.

■ Validators and delegators have an "unbinding period" for the system to ensure that tokens remain bound if bad behavior is detected, during which time the principal will be slashed.

1) Rewards

Both validator updates and reward distributions happen daily around 00:00 UTC. This is to save the cost of frequent staking updates and block reward distribution. This cost can be high because blocking rewards are collected on the FON Smart Chain and distributed to FON token validators and delegators. A deliberate delay is introduced here to ensure fair distribution:

■ Blocking rewards are not sent to validators immediately, but are distributed and accumulated in the contract;

■ After FSC receives the validator set update, it will trigger several cross-chain transfers to transfer the rewards to the corresponding validator's escrow address. The escrow address is owned by the system, so the rewards cannot be used until the commitment is allocated to the delegators.

■ To make synchronization easier and to allocate time for slashing, the N-day reward will only be distributed on N+2 days. After the delegator gets the reward, the rest will be transferred to the validator's own reward address.

2) Beheading

Slashing is part of on-chain governance to ensure that malicious or negative behavior is punished. Anyone can submit an FSC slash. Transaction submissions require slash proofs and cost fees, but also bring greater rewards when successful. So far, there are two curable cases.

3) Double standard

When a validator signs multiple blocks with the same height and parent block, this is a very serious mistake, and most likely a deliberate offense. The reference protocol implementation should already have logic to prevent this from happening, so only malicious code can trigger this. When double signing occurs, the validator should be removed from the Validator Set immediately. Anyone can slash requests with FSC signature evidence, which should contain 2 block headers and parent blocks with the same height, sealed by the offending validator. After receiving the proof, if verifying it is valid:

■ Instance FSC validator set update cross-chain update, remove the validator from the validator set;

■ A predefined amount of FSC will be deducted from the validator's self-delegated FSC; neither the validator nor its delegators will receive staking

rewards.

A portion of the slashed FSC is allocated to the submitter's address, which is a reward greater than the cost of submitting a slash request transaction

The slashed FSC will be distributed to the escrow addresses of other validators and distributed to all delegators in the same way as blocking rewards.

4) Not available

The liveness of FSC relies on everyone in the proof-of-stake validator set being able to produce blocks in time when it is their turn. Validators may miss their turn for any reason, especially issues in their hardware, software, configuration, or network. This operational instability can hurt performance and introduce more uncertainty into the system.

There could be an internal smart contract responsible for recording the blocking metrics missed by each validator. Once the metric is above a predefined threshold, the validator's blocking reward will not be forwarded for distribution, but shared with other better validators. In this way, underperforming validators should gradually be voted out of the validator set as their delegators will receive less or no rewards. If the metric remains above another higher level threshold, the validator will be withdrawn from the rotation, which will be propagated back to the FSC, which will then slash a predefined number of FSC validators from the self-delegated FSC. Neither validators nor delegators receive their staking rewards.

5) Governance parameters

There are many system parameters that control the behavior of FSC, such as slash amount, cross-chain transfer fees. All these parameters will be jointly determined by the FSC Validator Set based on their stake through a proposal voting process.

4.4 Examples of future FSC circulation

In the future, the circulation value of FSC will be reflected in the following aspects:

1) Ecological circulation

On the basis of the FON smart chain, many applications will be derived, such as mining wallets, DEX exchanges, blockchain payments, etc., while FON tokens can be exchanged with all digital currencies to support circulation and payment in all aspects of the ecosystem , such as receipt and payment, transfer, legal currency transaction, deposit, withdrawal, listing voting, STO gateway, currency allocation, lending, public welfare, games, shopping malls, etc. All circulation transactions are served by FON tokens. And settlement with fiat currencies around the world.

In addition to the circulation in the FON smart chain ecosystem, it will also be circulated in third-party applications developed based on public chain technology, and it will exist as the only value token. This will accelerate the circulation of FON tokens, add more circulation value attributes to the scarce FON tokens, and increase the overall value and price.

2) Generality

FON Smart Chain can adapt to diverse business needs and meet data sharing across business chains, which means that FON Smart Chain has enough general and standard data recording methods to represent various structured and unstructured information. , and can meet the cross-chain requirements required as the business scope expands. And this provides the value basis for the versatility of FON tokens. Let FON tokens circulate more calmly in various industries and scenarios around the world.

Chapter V

Global Team

5.1 Core team

Algernon - Formerly a famous blockchain software development engineer, responsible for the cross-platform porting of mining algorithms for virtual currencies such as Bitcoin and ETH, and the development and management of mining machine software. Algernon has accumulated rich industrial experience in the technical architecture of virtual digital currency wallets and virtual digital exchanges.

Bradley - Bradley's research focuses on big data parallel computing and distributed algorithm optimization, and has extensive research experience in blockchain, cryptography, and data mining. Bradley will provide in-depth algorithm support for the project at the core mathematical model of blockchain, core algorithm of artificial intelligence, and parallel computing of big data.

Chapman - MS and PhD in Electrical Engineering and Computer Science from Columbia University. His research involves data mining, business travel data and algorithm optimization. Chapman is responsible for the construction and optimization of the project's artificial intelligence algorithm.

Wesley — — Proficient in the principles and implementation of mainstream blockchain technologies such as Bitcoin, Ethereum, HyperLedger, etc., and has a deep understanding and rich practice of blockchain consensus mechanism, smart contracts, cross-chain technology, side chain technology, privacy protection, etc. The blockchain network it has built has been operating stably for many years,

currently carrying hundreds of thousands of transactions every day, and the monthly transaction amount exceeds one billion.

Samuel - both a world-class mathematician and a great hedge fund manager. Samuel set up Datong Fund for quantitative trading in 1998. Datong Fund finds out the mathematical relationship between changes in financial product prices, macroeconomics, market indicators, technical indicators and other indicators through statistics on historical data, and finds that the market currently exists. Opportunities to profit and make quick and massive trades with leverage.

Daniel - Proficient in several languages, has lived in the US, UK, Italy, Germany, United Arab Emirates. He is a researcher of the World Blockchain Foundation, a senior collaborator and professional consultant of the open source website building system. Since 2003, he has participated in the collaboration of international open source software, and is well versed in the operation mechanism of open source projects and decentralized autonomous organizations. Currently in-depth application of blockchain.

5.2 Advisory Team

Brian —— Bright is a former Airbnb engineer and holds a Ph.D. in computer engineering from Yale University. During his tenure at Airbnb, he participated in a number of core technology development and platform architecture involving IoT and supply chain projects, with professional technical standards and rich operational experience . During his Ph.D. study at Yale University, he began to

work on the project. The platform he built was recognized by Google and was wholly acquired.

Richard Dobrow, an American blockchain technology expert, graduated from Virginia Tech in 2002 with a doctorate in computer science. Worked at IBM Computer Research Center. Through the paper "New Directions of Cryptography", he was exposed to digital cryptography, and verified the feasibility of distributed ledger through asymmetric encryption, elliptic curve algorithm and other means. At present, he has participated in the design of more than 10 digital currencies and found several security vulnerabilities. He is a trusted and well-known member of the digital currency community.

Karina Dalmas - Large scale software and supply chain systems development in Singapore. Entered the world of Ethereum 2 years ago, and currently leads the team to use Solidity, Python, C/C++ and C# languages to program and write the project blockchain source code.

Justin Drake - Advising crypto companies, crypto startups, venture capital funds and international decision makers on blockchain solutions. Director of the Private Investment Funds Institute (PIFI). Previously, he worked with Cravath, Swain & Moore LLP (New York) and Goldman Sachs (London). Currently working as a financial operation consultant, 30 years of experience in the financial industry can help FSC understand the actual needs of customers.

Chapter VI

FSC Ecological Development Foundation

6.1 Foundation overview

In order to achieve the rapid development of the FSC project, the FSC Ecological Development Foundation, as the advocacy entity of the FSC project, will be committed to the development and construction of the project, advocacy and promotion of governance transparency, and promote the safe and harmonious development of the open source ecological community.

The FSC team entrusts a credible third-party organization to assist the team in setting up an operation center entity, and maintain the daily operation and reporting of the entity structure. Through the foundation, select appropriate community participation members, join the foundation functional committee, and jointly participate in the actual management and decision-making.

6.2 Foundation Organizational Structure

The establishment of the foundation refers to the operation of traditional entities, and various functional committees will be established, including a strategic decision-making committee, a technical review committee, a compensation and nomination committee, and a public relations committee.

The Strategic Decision Committee is the highest decision-making body of the Foundation. The main goal of its establishment is to negotiate and resolve important decision-making issues faced in the process of community development, including but not limited to:

- Modify the foundation governance structure;

■ The formation and rotation of the decision-making committee;

■ The appointment and rotation resolution of the secretary general of the foundation;

■ Appointment and dismissal of executive officers and heads of functional committees

■ Deliberation and revision of the foundation's charter;

■ FSC's development strategy decision;

■ Change and upgrade of FSC core technology;

■ Emergency decision-making and crisis management agenda, etc.

The term of the members of the Strategic Decision Committee and the chairman of the foundation is two years, and the chairman of the foundation cannot serve for more than two consecutive terms. After the term of the decision-making committee expires, the community will vote to elect community representatives according to the consensus mechanism of the next generation of FON tokens, and then elect the core members of the decision-making committee. The selected core personnel will make important and urgent decisions on behalf of FSC, and It is necessary to accept a credit investigation during the term of office, and to disclose the salary information. The above important matters need to be voted by the decision-making committee by registered ballot. Each decision-making committee member has one vote, and the chairman of the foundation has two votes. Decisions made by the decision-making committee must be approved by

more than half of all incumbent committee members. In addition, when one of the following situations occurs, the executive director shall convene the decision-making committee to hold an extraordinary meeting within 5 working days:

■ When the Secretary-General of the Foundation deems necessary;

■ When more than one-third of the members of the decision-making committee jointly propose;

The meeting of the decision-making committee shall be attended by the members of the committee in person. If you are unable to attend for any reason, you may entrust other members of the committee in writing to attend. Those who do not appoint a representative shall be deemed to have waived their right to vote at the meeting.

Secretary-General: Elected by the strategic decision-making committee, responsible for the permanent operation and management of the foundation, the coordination of the work of various subordinate committees, and presiding over the meeting of the decision-making committee. The Secretary-General is the top person in charge of FSC administrative affairs, who provides unified guidance and coordination for the foundation's daily operation, technology development, community maintenance, public relations, etc., and connects each business unit with the functional committees at the governance structure level. The Secretary-General reports to the decision-making committee on a regular basis.

Technical Review Committee: composed of core developers in the FSC development team, responsible for making decisions on the direction of

blockchain technology research and development, underlying technology development, open port development and review, technology patent development and review, etc. In addition, members of the technical review committee regularly learn about the dynamics and hotspots of the community and the industry, communicate with participants in the community, and hold technical exchange meetings from time to time. Examples include corporate customers, suppliers, regulators, and third-party service providers.

Remuneration and Nomination Committee: Responsible for deciding the selection and appointment of key management personnel of the Foundation. The committee sets procedures, assesses the competence of managers, and authorizes appointments. At the same time, the committee sets a compensation system to motivate those who have made important contributions to the foundation. The Remuneration and Nomination Committee regularly evaluates the performance of all members of the Foundation. Propose the adjustment of human resources structure, propose different incentive measures, attract and retain talented experts.

Public Relations Committee: The goal is to serve the community, responsible for the promotion of FSC technology, the establishment and maintenance of FSC and business alliances, the collaboration and resource exchange of FSC's participation in various alliances, the business promotion and publicity of FSC, and community crisis public relations and social responsibility, etc. . The committee is responsible for regular press conferences, announcements and inquiries on important matters to the outside world. In the event of an incident affecting the Foundation's reputation, the Public Relations Committee will serve as a unified communication channel to issue an authorized response.

Supervision and Management Committee: As a highly independent and autonomous form, it is set up within the foundation as an independent supervision and risk control management for the overall operation of the foundation. The Supervisory Management Committee provides daily guidance to the Foundation's legal and compliance departments. At the same time, the foundation has established a transparent and open reporting mechanism, and the supervision and management committee will directly accept internal and external reporting matters, and take corresponding investigations and improvements to ensure that the operation of the entire foundation is in perfect compliance and legality. progress within the risk level. The Supervisory Management Committee reports directly to the Strategic Decision Committee and does not conflict or overlap with other functions of the Foundation.

Other functional departments: The foundation refers to the company's institutional structure to set up daily operation departments, such as human resources, administration, finance, marketing, research and development (or laboratory) units, etc. The establishment of functional departments is to maintain the normal operation of FSC and directly respond to relevant parties in the business society.

6.3 Governance Principles of the Foundation

The design goals of the foundation's governance structure mainly consider the sustainability of project development, the effectiveness of strategy formulation, management effectiveness, risk control and efficient project operation. The Foundation proposes the following principles in terms of governance structure:

1) Integration of centralized governance and distributed architecture

Although there have always been arguments that blockchain is an autonomous community system centered on "decentralization" or "distribution", we believe that complete decentralization may bring absolute "fairness" or more "Inefficient". Therefore, the foundation will still absorb certain core ideas of centralized governance in the management structure, including the highest decision-making authority of the strategic decision-making committee and the centralized deliberation power of major matters, so as to improve the efficiency of the entire community operation.

2) Coexistence of functional committees and functional units

Under the daily affairs of the foundation, resident functional units will be set up, such as the research and development department, the market development department, the operation department, the finance and human resources department, etc., to deal with the current affairs. At the same time, a professional functional committee is set up to make decisions on important functional matters of the foundation. Unlike functional units, functional committees exist in a virtual structure, and committee members can come from around the world without

having to work full-time. However, it must meet the requirements of the committee's expert qualifications and be able to promise to attend and express opinions when the committee needs to conduct discussions. The functional committee will also set up a regular meeting system to ensure the effective advancement of major decision-making matters.

3) Risk-Oriented Governance Principles

In the process of research to determine the strategic development and decision-making of the foundation and the project, risk management will be set as the first important element. As a computer technology with significant transformative significance, the development of blockchain is still in its infancy, so it is particularly important to grasp its development direction. The principle of risk management is to ensure that when the foundation makes important decisions, it fully considers risk factors, risk events, and the possibility and impact of their occurrence, and formulates corresponding response strategies through decision-making. This ensures that the development and iteration of the FSC project is on a correct path.

4) Technology and business coexist

Adhering to the purpose of promoting the development of blockchain technology and the transformation and upgrading of the underlying infrastructure, the establishment of the foundation also follows this purpose. Even if the foundation exists in the form of a non-profit organization, the foundation hopes to gain the recognition of the business world as much as possible, win the benefits of commercial applications, and feed back to the foundation and the community to

further promote the development of the foundation and the FSC project with the upgrade.

5) Transparency and Oversight

Referring to the governance experience of the traditional business world, the foundation also plans to set up a special monitoring and reporting channel. With the designated personnel in the strategic decision-making committee as the window, community participants are welcome to participate in the management, participate in the supervision of operations, and be able to quickly and confidentially report "found matters". These matters include, but are not limited to: new breakthroughs or proposals that have a significant impact on the foundation or blockchain technology, community-operated issues, crisis information, reporting fraud or fraud, etc.

6.4 Risk assessment and decision-making

As an innovative technology, blockchain is not only a subversive breakthrough in computer core technology, but also an innovation in various industries. Therefore, the importance of risk management system is self-evident. The foundation upholds the establishment of a risk-oriented and sustainable blockchain community. The Foundation will conduct continuous risk management for the operation of the Foundation. Including a series of activities such as risk system establishment, risk assessment, and risk response. For major risks, the Foundation's strategic decision-making committee needs to discuss and make decisions.

The foundation will classify events according to the characteristics of events, such as the degree of event impact, the scope of impact, the amount of tokens affected, and the probability of occurrence, and make decisions based on priorities. For high-priority events, organize relevant committees of the foundation to make decisions as soon as possible.

Chapter VII

Disclaimer

Nothing in this white paper constitutes legal, financial, business or tax advice and you should consult your own legal, financial, commercial or other professional advisors before engaging in any activity related to this. Community staff, project R&D team members, third-party R&D organizations and service providers are not responsible for any direct or indirect damages and losses that may be caused by the use of this white paper. This white paper is for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation of investment or any offer to sell any product, item or asset, whether digital or otherwise. The following information may not be exhaustive and does not imply any element of contractual relevance.

The White Paper cannot guarantee the accuracy or completeness of the information, nor does it guarantee nor promise to provide a statement of the accuracy and completeness of the information. Where this white paper contains information obtained from third parties, the community and team have not independently verified the accuracy and completeness of such information. In addition, you need to understand that the surrounding environment and situation may change at any time, so this white paper may be out of date, and the community has no obligation to update or correct the content and documents related to this.

No part of this white paper constitutes and will not constitute any offer by the community, distributors, and any sales team (as defined in this agreement), nor may any statement of the white paper be relied upon as any contractual and investment decision The basics. Nothing contained in this white paper can be

taken as a representation, promise or guarantee of future performance. BY ACCESSING AND USING THIS WHITE PAPER, OR ANY OF THE CONTENT, YOU ARE PROVIDING THE COMMUNITY, ITS AFFILIATES AND YOUR TEAM THE FOLLOWING WARRANTIES:

In any decision to purchase Token, you have not relied on any statement in this white paper;

You will voluntarily assume the costs and ensure compliance with all legal, regulatory requirements and restrictions applicable to you (as the case may be);

■ You acknowledge, understand and agree that Token may have no value, neither guarantee nor represent any value and circulation properties, and cannot be used for speculation-related investments;

■ The community and its affiliates and team members are not responsible or liable for the value, transferability, liquidity of Tokens and any market that provides FSC through third parties or other means;

■ You acknowledge, understand and agree that if you are a citizen, national, resident (tax or otherwise relevant), residence or country green card holder of a geographic region or country that Token qualifications:

i. The sale of Tokens may be defined or construed as the sale of securities (however named) or investment products;

ii. The law prohibits access to and participation in the sale of Tokens or countries

and regions where Tokens are prohibited by laws, policies, regulations, treaties or administrative regulations.

The community and team do not and do not intend to make any representations, warranties and commitments to any entity or individual, and hereby disclaims any responsibility (including but not limited to the content of this white paper and the accuracy of the content of any other material published by the community, completeness, timeliness and reliability). To the maximum extent permitted by law, the community, related entities and service providers are not responsible for any use of the white paper content, related materials published by the community and related content presented in other forms (including but not limited to any errors or omissions) Liability for indirect, special, incidental, indirect or other damages arising out of tort, contract disputes or otherwise (including but not limited to any liability for breach of contract or negligence arising therefrom, any revenue and loss of profit and loss of use and data). Potential buyers should carefully consider and evaluate all risks and uncertainties (including financial, legal and uncertain risks) associated with sales, communities, distributors and teams.

The information provided in this white paper is for community discussion only and is not legally binding. No one is obliged to enter into any contracts and binding legal commitments for the acquisition of FSC, and other than that, this white paper will not accept any virtual currency or other forms of payment. The sale and purchase agreement for Tokens and the long-term continued holding of Tokens are subject to a set of separate terms or a purchase agreement (as the case may be) containing relevant terms and conditions, which are provided to you separately or

available on the website. In the event of any inconsistency between these Terms and Conditions and this Whitepaper, these Terms and Conditions shall prevail.

Regulators have not reviewed or approved any of the information set out in this white paper, and there is nothing in the laws, regulatory requirements and rules of any jurisdiction that states that it is or will be required to do so. The publication, distribution or dissemination of this white paper does not imply that the requirements or rules of applicable laws, regulations or rules have been fulfilled and complied with. This is just a conceptual white paper to describe the long-term development goals of the FSC to be developed. This white paper may be revised or replaced from time to time. There is no obligation to update the white paper and provide the audience with other information beyond the scope of this white paper.

All statements, press releases and publicly accessible statements contained in this white paper, as well as oral statements that may be made by the community and the FSC team, may constitute forward-looking statements (including related statements of intent and statements regarding current market conditions, business strategies and plans, financial position, specific regulations and confidence and expectations for risk management decisions). You are cautioned not to place undue reliance on these forward-looking statements, as these statements involve known and unknown risks, risks of uncertainty and other factors that could cause actual future results to differ materially from those described in these forward-looking statements , at the same time, it should be noted that no independent third party has reviewed and judged the

reasonableness of these statements and assumptions. These forward-looking statements speak only as of the date indicated in this white paper, and the community and the FSC team expressly disclaim any responsibility (whether express or implied) for the consequences or events arising out of and arising from revisions to these forward-looking statements after that date.).

The use of any company or platform name or trademark herein (other than content related to the community or its affiliates) does not imply any affiliation with or endorsement by these third-party platforms and companies. The specific companies and platforms mentioned in this white paper are for informational and illustrative purposes only.