Silicoin:
A Domino Effect in Blockchain World

info@silicoin.cc
www.silicoin.cc
October 7th, 2021

1. Introduction

Under the situation of the power consumption of BTC mining is exceeded in Norway, and BTC is being cracked down on by governments worldwide due to environmental issues at the same time. Shouldn't we make changes? FIL, a so-called decentralized storage hard disk, is filled with junk files. Meanwhile, XCH degenerates into a hardware competition with all kinds of PoS projects on the market. Shouldn't we make changes? In terms of PoW, PoS and PoC are driven by capital and desire. Those are gradually moving away from the original intention of decentralization. Shouldn't we make changes?

Digging into the current mainstream encrypted digital currencies, BTC mining is not environmentally friendly. It has been plotted against by many countries, while the mining situation of ETH after being converted to PoS is still unknown. Let alone saying that, FIL mining is unable to temporarily solve the problem of staking cost and storing effective data. What also concerns us is that the threshold of Chia is too low, resulting in an unfair monopoly. As a result, the mining industry is at an impasse, and it seems that there is no successor.

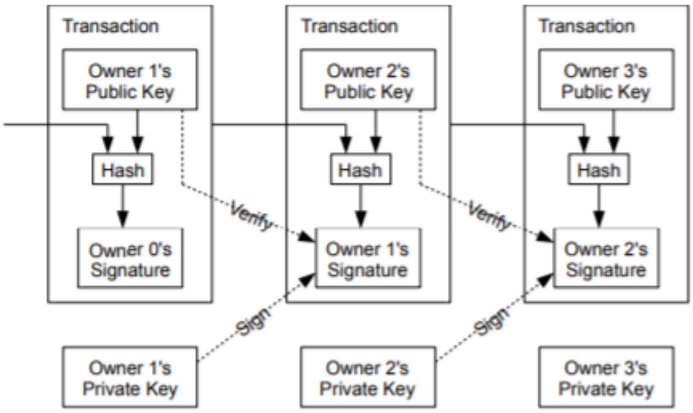
In the current environment of Web3, the blockchain world urgently needs a more environmentally friendly, intelligent, and fair decentralized network ecosystem. Therefore, Silicoin came into being. Silicoin was born to overthrow the traditional mining mechanism. It combines a solution to the flaws of traditional mining mentioned above by forming a new and unique mining logic. It aims to truly balance PoW and PoS and meets the original intention of BTC and Chia: to make mining with ordinary equipment happen and to have the blockchain genuinely decentralized. Perhaps this slight effort can only cause gradual but small changes, but these changes may trigger an earth-shaking evolution.

Silicoin was born in the community in 2021. Studying the Chia code thoroughly, Silicoin's technical team concluded that Chia is highly suitable to transform into PoW+PoS. However, considering the flaws of Chia, no staking, and low threshold, for example, the Silicoin team decided to carry out secondary development based on Chia to achieve the combination of PoW and PoS consensus mechanisms. That's right, this is Silicoin. Under the collision of geek and punk thinking, several unknown programmers and miners came up with an arrogant idea: overthrow and rebuild the whole world of hardware mining. In a brutal system with internal connections like the blockchain, a small initial energy may cause a series of chain reactions just as the domino effect.

2. Technical Overview

2.1. Transactions

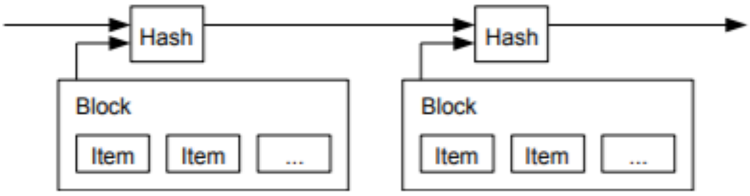
We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



The problem is that the payee cannot verify if one of the owners double-spend the coin or not. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double-spending. After each transaction, the coin must be returned to the mint to issue a new coin, and the only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. We need a way for the payee to know that the previous owners did not sign any earlier transactions. To our concern, the earliest transaction is the one that matters. We do not have to worry about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint-based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions should be publicly announced. Also, we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

2.2. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



2.3. Proof-of-Balance

Bitcoin-like blockchains use a Proof-of-work (PoW) mechanism, where security holds if the majority of the computing power is under the control of honest users. However, this assumption has been seriously challenged recently, and Bitcoin-like systems fail if this assumption is violated. Silicoin proposes a new blockchain structure that combines PoW and Proof-of-Stake (PoS) mechanisms in this proposal. Our analysis shows that the chain is secure as long as the honest users control a majority of the collective resources, consisting of both computing power and stake. In particular, even if the adversary controls more than 50% of the computing power, security still holds if the honest parties hold a sufficiently high stake in the system. As an added value, our chain also remains secure against adaptive adversaries.

Thus, the Silicoin network combined the advantages of PoW and PoS, and proposed a new PoB (Proof-of-Balance) consensus mechanism. The Silicoin network operates with its own technology, based on economic models and traditional PoW mechanisms to realize an acceptable coin production method. This method automatically adjusts the difficulty of mining and gradually halves block rewards. Furthermore, it combines the consensus mechanism of PoS to reduce energy consumption requirements, avoiding the paradox of over-centralization of computing power. Taken care of the aforesaid issue, the Silicoin network finally balanced workload and capital, giants and retail investors, interests, and contributions. We call it the PoB consensus mechanism. In this way, the advantages of resource-based and token-based consensus mechanisms are combined to ensure that the attacker would have to be equipped with dual advantages in resources and funds from the security of the consensus. From the fairness of the mechanism, everyone has the opportunity to participate in the Silicoin network.

Mining in the Silicoin network is not mandatory to stake SIT. In order to avoid excessive centralization caused by the monopoly of resources and funds, the mining mechanism of the Silicoin network encourages small and medium miners to contribute to the entire network's computing power. They do not need to stake or excessive stake to achieve mining income. When the computing power of a single miner's account reaches a certain threshold, there will be a staking requirement, and it is the linear weighted staking. That is to say, the more SIT staking under a public key, the higher chance to win the blocks. Under this mechanism, large users need extremely high costs to monopolize computing power, which will damage the interests of small and medium miners and endanger the security of the Silicoin network. They cannot over-occupy network resources based on equipment resources or huge funds. Small and medium miners can join the robust Silicoin network with a low or even zero thresholds, contributing to a more decentralized and fairer blockchain network to gain benefits.

2.4. Mining System

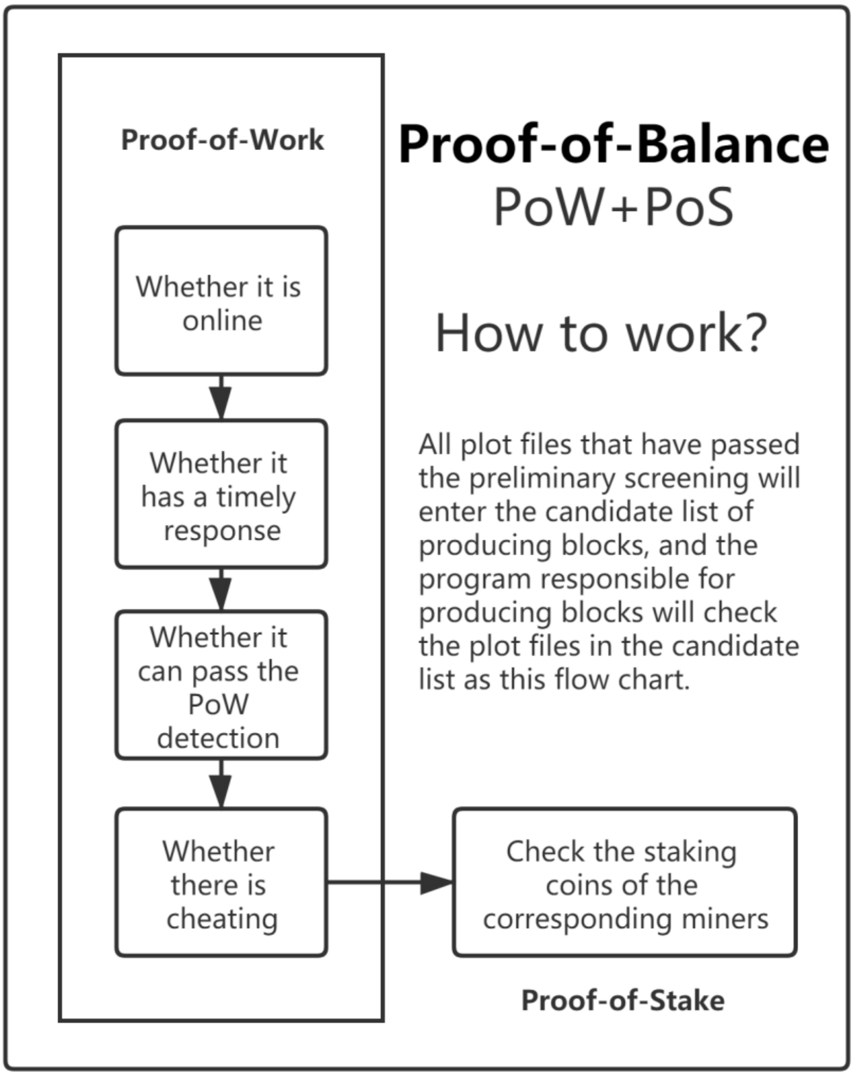
At present, many projects have shortcomings in the block-producing mechanism, which has lots of hidden dangers. Take Chia as an example, it is building a blockchain platform based on Proofs of Space and Time. Nevertheless, what exactly are Proofs of Space and Time? It is a new type of PoW in a way. Then after thoroughly studying the code of Chia, Silicoin's technical team concluded that: Mining system of Chia is very suitable to take it as proof-of-work, and we could add a staking function to finish the proof-of-stake part.

However, Chia got some problems when it detects the plot file, and it causes fake computing power. The Chia network did not carry out a detailed detection of the current status of the plot file. For example, it fails to detect if someone is cheating on the current plot file when producing blocks. Therefore, it is challenging to ensure the efficiency and fairness of the Chia network.

In this regard, Silicoin has designed and optimized the block-producing detection mechanism. In the Silicoin network, all plot files that have passed the preliminary screening will enter the candidate list of producing blocks, and the program responsible for producing blocks will check the plot files in the candidate list in detail in the following order:

-Whether it is online
-Whether it has a timely response
-Whether it can pass the proof-of-work detection
-Whether there is cheating (such as double mining)
-Check the staking coins of the corresponding miners

The block-producing program will automatically eliminate plots that do not meet the requirement of the above checklists. In this case, high-speed operation of the Silicoin network is ensured, and unnecessary hidden dangers would be eliminated.


Proof-of-Work
Proof-of-Balance
PoW+PoS
How to work?
Whether it is online
Whether it has a timely response
Whether it can pass the PoW detection
Whether there is cheating
Check the staking coins of the corresponding miners
Proof-of-Stake

All plot files that have passed the preliminary screening will enter the candidate list of producing blocks, and the program responsible for producing blocks will check the plot files in the candidate list as this flow chart.

2.5. Nodes

A node is a device or data point in a more extensive network. For example, in networking, a node is either a connection point, a redistribution point, or a communication endpoint. A node is an open-source, cross-platform runtime in the blockchain that allows developers to create various services. Nodes of Silicoin network participate in consensus, store copies of data and more services, and provide some specified services in the chain, for which they receive a reward. We named it application node. The tasks of these nodes are different in each phase.

In Silicoin network, the application node is going to be the timelord starting from testnet1. However, as we all know, there is no benefit if the timelord is not on the fastest hardware in both chia network and silicoin. So in order to encourage the application node to be the timelord then help to improve the entire network, there is an airdrop if users deploy their nodes to be the timelords in Chia phase (Tesnet 1). The total bonus is 2 million tSIT tokens for application nodes as an airdrop. 2 million tSIT will be divided according to their conditions. However, these application nodes are prepared for providing more services in the future.

In addition, the application nodes start their new tasks in the Poppy network. All the application nodes carried out the mission that provides token mixing service and gets rewards from transactions.

Moreover, the application nodes have to upgrade in the Rose network. The application nodes should help users create and run the smart contract on the network to benefit from providing service.

Last but not least, the application nodes are going to support more services on the chain after the mainnet launch. One of the most significant advantages is that application nodes can initiate DAO proposals, and the users who hold SIT tokens participate in poll. Another strong point is that the application treasury is managed by a particular group composed of multiple application nodes, and SIT holders select these application nodes.

2.6. Privacy

Privacy has always been regarded as one of the most valuable features in the cryptocurrency community. The Silicoin team was born among the community. It pays great attention to the privacy and security of the community members. On the one hand, anonymity is the predecessor of fungibility, and widely used currency forms will require this feature; on the other hand, most community members do not want assets and transaction records to be fully disclosed, which is also in line with the idea of decentralization. In the field of blockchain, the difficulty of anonymity lies in how to correctly verify the accuracy of user information without disclosing the content of user information and prevent malicious attacks. Among the various encryption schemes currently providing privacy for the blockchain, the zero-knowledge proof algorithm represented by ZK-SNARK (Zero Knowledge-Succinct Non-interactive Argument of Knowledge) and ZK-STARK (Zero Knowledge-Scalable Transparent Argument of Knowledge) is gradually taken seriously by the mass and accepted by many projects and professionals.

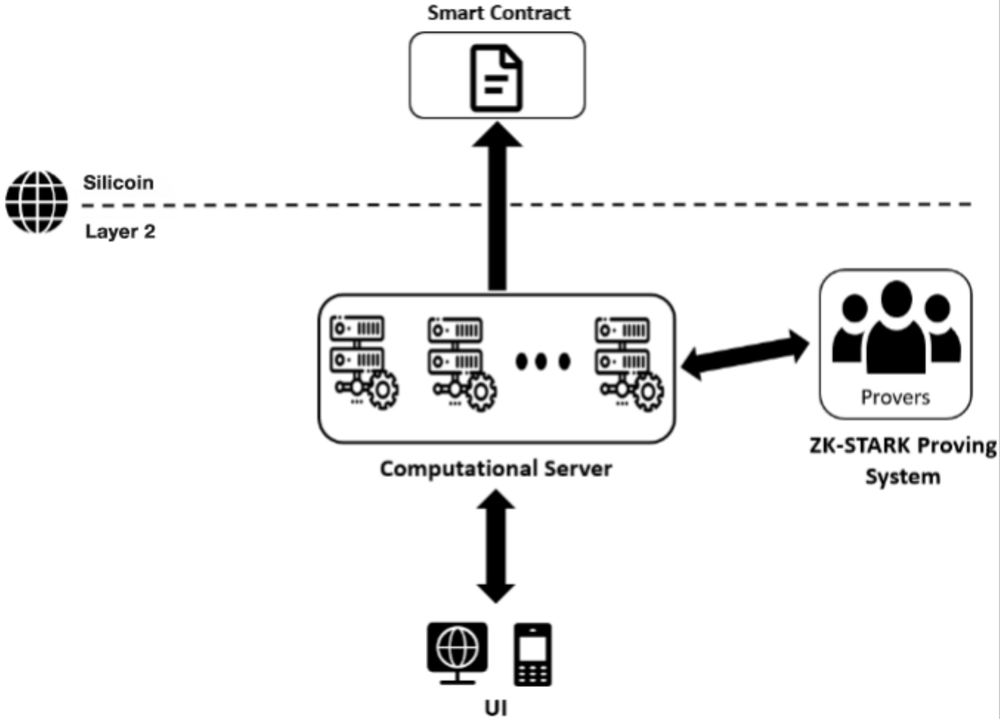
However, considering the time and difficulty of development, Silicoin will adopt a coin mixing system, which is set up off-chain to achieve anonymity in Testnet 3. Then we continue developing ZK-SNARK as the anonymous on-chain feature in later versions once the Silicoin network supports smart contract.

The most significant advantage of the zero-knowledge proof algorithm is that it provides a simplified unforgettable password proof, which allows a user to prove the authenticity of his statement to another user without revealing any information beyond the validity of the statement. The parties involved are usually called provers and verifiers, and the secrets they hold are called proofs. The primary purpose of these functions is to allow as little data exchange as possible between the two parties. This undoubtedly provides a powerful feature set for privacy, and the verification of relatively little evidence can quickly and effectively complete the verification of large-scale calculations. Thus, the zero-knowledge proof algorithm can provide a better decentralization-preserving scale for decentralized exchange protocols while improving transaction processing efficiency and reducing contract gas. After careful consideration and voted by community startup members, Silicoin decided to adopt ZK-STARK with more substantial scalability and security to ensure the anonymity and security of the Silicoin network.

2.7. System Architecture

After the frequency of on-chain transactions has risen to a certain level, a series of problems such as congestion and high gas in the performance of public chains such as Ethereum have been revealed. To this end, the Silicoin system is to adopt a layered design concept to solve the above-mentioned sore points. The hierarchical logic is to complete different operations in different layers. The layers interact through interfaces, and each layer itself is also one or more blockchains. This can significantly improve the overall TPS capability, and by distinguishing the functions of each layer, the computing power and the processing efficiency and capabilities of the program can be expanded, and the corresponding cost (expense) can be reduced. In addition, after the layers are isolated, the security can be further improved. Even if there is a problem in the upper layer, it will not affect the security of the next layer.

The Silicoin system consists of four parts: on-chain interaction layer, computing service layer, zero-knowledge proof, and user UI interface:



- Interaction Layer on the Chain

In the Silicoin system, operations are related to user assets, such as depositing tokens, staking, and mining, and system status recording and verification, such as computing layer status updates and related proof. They are all performed by related smart contracts on the chain. Therefore, the on-chain interaction layer can be seen as a critical hub connecting the on-chain and off-chain.

- Computing Service Layer

The computing service layer can be considered the Layer 2 protocol in the Silicoin network, a program module that processes all transactions running under the chain. The computing server interacts with users through the WebSocket interface and monitors transactions in the interaction layer on the chain. All legitimate transaction requests are placed in the Silicoin memory pool, then finally handled by the Silicoin Engine. The Block Proposer rolls up the transaction to generate a new block while the State Keeper updates the status of all tokens in Layer 2. Next, the State Keeper sends the state to the Commuter, who is responsible for communicating with the Prove server and obtaining the corresponding transaction proof. The last phase would send the state and the corresponding STARK proof to the XXSwap smart contract on the chain through the sender.

- Zero-knowledge Proof System

Silicoin's zero-knowledge proof system adopts a distributed architecture and employs the most secure zero-knowledge proof algorithm STARK to generate proofs. Prove server supports multiple Prover. It actively inquires the proof task in the Prove server, and then it generates the proof and sends it back to the Prove server. STARK does not rely on mathematical problem assumptions and does not require trust initialization. It is believed to be quantum-resistant. At the same time, thanks to the extremely high verification efficiency, STARK has more substantial scalability. It is worth mentioning that Silicoin will take coin mixing system instead of ZK-SNARK in Testnet 3. ZK-SNARK proof system will be conducted when the mainnet launch.

- Front-end User Interface

The convenient and easy-to-operate visual front-end user interface can facilitate users to perform a series of functions such as exchange, sending, access, and staking.

2.8. NFT module

NFT is the abbreviation of Non-Fungible Token. The term homogenization was originally a technical term used to describe the characteristics of commodities in economics, meaning broad similarities. Contrary to the meaning of homogenization, uniqueness and scarcity are important attributes of NFT assets.

NFT and blockchain technology is consistent in many aspects. Blockchain can ensure the rarity of NFT and maximize its value. NFT and DeFi are not only a combination of great creativity and development potential but also an important direction for Silicoin's function expansion. The core value of the combination of NFT and DeFi lies in the expansion of asset territory and the enhancement of liquidity. In theory, NFT can achieve the intention of mapping various scarce assets in the real world on the blockchain, which can help DeFi further extend the asset method to the real world, such as artworks, land, and real estate. These are all assets that can be used as mortgages, loans, pawns, etc. At the same time, a reasonably designed DeFi system is capable of relatively enhancing the liquidity of these rare assets. The assets mapped on the chain allows not only avoiding the authenticity of the assets but also balancing the time cost and value loss caused by the centralized transaction intermediary structure.

In terms of NFT, Silicoin creatively proposed the concept of NFT development module, which aims to lower the threshold for users to generate and use NFT. The NFT development module program can use smart contracts to parameterize any NFT, which means that even if you are completely unfamiliar with the computer programming code and the NFT production process, it is still possible for you to design and fill in the NFT parameters in the template according to your own preferences and needs. Then, to generate NFT with one click is all you need to do.

3. Testnet & Mainnet

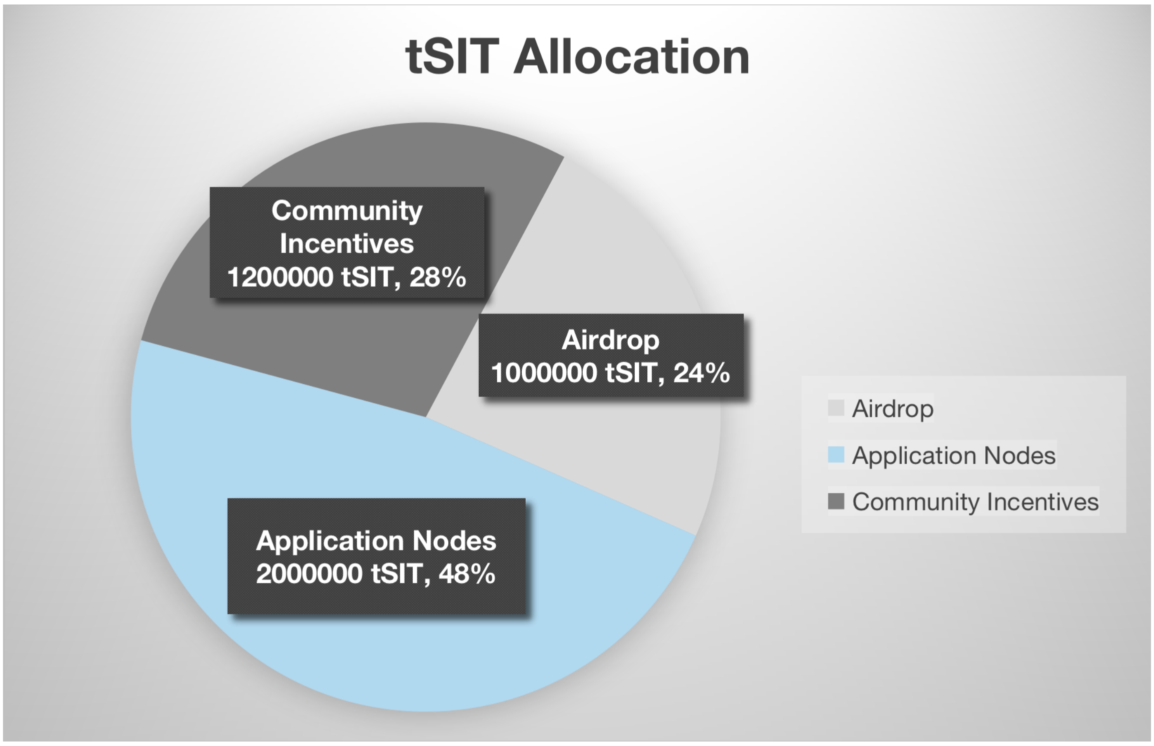
Mainnets and testnets are common technical terms used in the cryptocurrency world to denote blockchain networks that possess vital functions. A testnet is often used as a testing site for the development and continual enhancement of the mainnet, while the mainnet itself is the actual, functioning protocol that powers the blockchain network.

The steps to develop the Silicoin network are as follows:

- **Step 1**

Chia Network - Testnet 1 & Testnet1.5
The Chia net is the first phase of testing, which is based on a fork of the Chia project. During the Tulip test, 4.2 million SIT test tokens (tSIT) will be airdropped as mining startup capital. Airdrop, application nodes, and community incentives take the proportion by 1 million, 2 million, and 1.2 million accordingly.

Besides, one block of this phase will be generated every ten minutes, and each block generates 64 tSIT as a reward. Apart from being the application nodes, users can plot the file to mine the tokens without staking as well. All the test tokens for the first phase, we named tSIT, can be exchanged for the test tokens for the next phase later.



- **Step 2**

Tulip Network - Mainnet

After all the test function is stable, the project enters the Tulip stage, and the Silicoin mainnet will be officially launched. In this phase, all test tokens in the testnet are mapped to the mainnet.

The total amount of initial SIT test tokens in this phase is 1,000,000 tokens, of which 50% are development fund and application treasury quotas, and the rest 50% can be exchanged for test coins produced during the Tulip Network stage mining.

Development fund and application treasury will be released in installments and is for the contributors who participated in chain maintaining and applications development on the chain. Development fund gets 200,000 SIT for whoever contributes the codes for improving Silicoin network and it stays frozen for 4 years. On the other hand, 300,000 SIT is the bonus to help developers start their program on Silicoin network and this token is frozen as well.

Regarding tSIT exchange to SIT, Silicoin will take a snapshot at a block height. Total tSIT at the block height divided by 500,000 will be the confirmed exchange rate.

At this stage, the staking and mining functions are available at the same time to further test the Silicoin consensus mechanism (Proof-of-Balance) and mining system. Users can plot the file to mine the tokens with staking tSIT.

Silicoin's mining system in this phase will linearly weigh both the user's computing power and the number of staking. The higher the staking amount, the higher chance to win the blocks, which is aiming to achieve a balance between retail and large investors and take into account the interests of all members of the community.

- **Step 3**

Poppy Network

The application nodes start their task in this phase. All the application nodes carried out the mission that provides SIT mixing service and get rewards.

- **Step 4**

Rose Network

The mining system is not going to make any adjustment during this test phase but the application nodes would have to be upgraded then it can support the smart contract running on the rose network.

Smart contract is the most important function at this stage. The mission of rose network is testing whether smart contract works well on the chain.

- **Step 5**

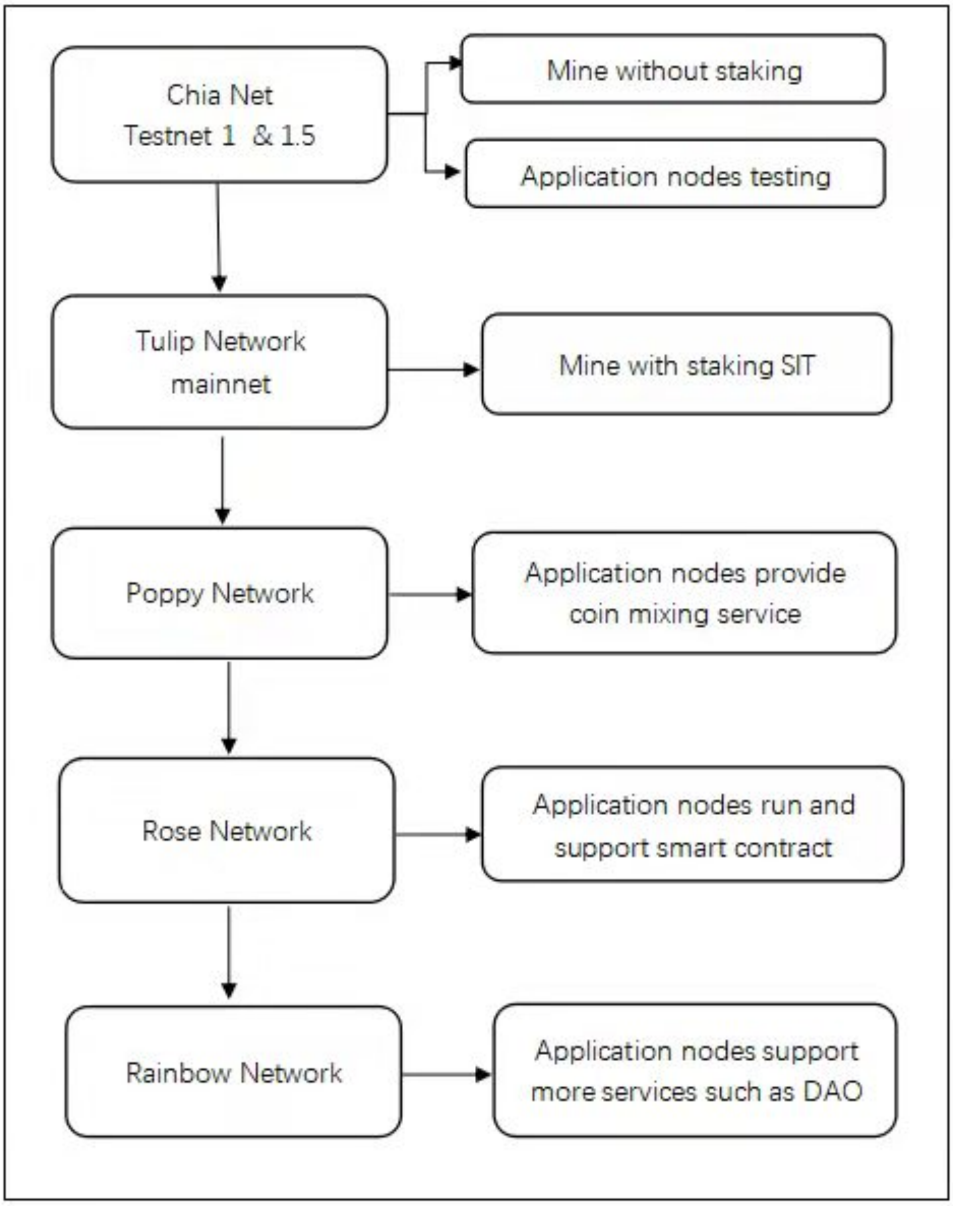
Rainbow Network - Mainnet 2.0

At that time, Silicoin starts creation mining, and gradually launches a series of DeFi expansion functions such as SIT financial payment, NFT casting, SilicoinSwap, etc., to create a complete

Silicoin financial win-win ecosystem and token economy.

4.1 Token Distribution

SIT is Silicoin's protocol token. In terms of Silicoin's decentralization and community, most of the total amount of SIT is to be generated by continuous mining activities and distributed to community participants who maintain the operation of the system. The output and distribution rules of SIT are as follows:



- **Output**

There is no upper limit on the total amount of SIT. The output rules of the test phase are mentioned in detail in the project planning of the previous chapter. Starting from the Rose Network stage, the Silicoin network generates blocks every 10 minutes. The initial single block production produces 32 SIT, which means the initial annual output is 1,681,920. After that, SIT production is estimated to be halved every 3 years.

- **Private Placement**

There is no private sale of SIT in any phase.

- **Development Fund**

The development fund is expected to compensate the contributors who participated in maintaining the core codes of Silicoin. Development fund got 200,000 SIT in Poppy network for who contribute the codes and help to improve Silicoin network. These tokens are to stay frozen for four years before releasing in installments. The members of the management team should be experts from various fields, especially blockchain technology and finance.

- **Application Treasury**

Application treasury allocates 300,000 SIT during Poppy network, and all of them are to remain frozen until the mainnet launch. As soon as Silicoin complete the smart contract and launch the Rainbow network, these tokens shall be released in installments. It is the bonus of the contributors to help developers start their program on Silicoin network. The application treasury is managed by a special group, which is composed of multiple application nodes that SIT holders vote for.

- **Staking**

Silicoin combines the features and strengths of both Proof of Space & Time (PoST) and Proof of Staking (PoS). In the process of producing blocks, Proof of Space is still the foremost consideration; the more plots miners have, the greater the probability that they will be selected to produce blocks. And as more miners join, space on the network will increase, and so the difficulty of the "hashing calculation" will need to be adjusted accordingly.

In Chia's consensus mechanism, the difficulty coefficient is the same for all miners. In the consensus mechanism of Silicoin, the system will first provide a base difficulty that is consistent across the entire network, and then the nodes will adjust corresponding individual difficulty according to the number of coins staked by each miner. The lower the difficulty coefficient, the greater the probability of being selected to produce the block.

D is Difficulty of the Entire Network； D' is Individual Difficulty; SF is Staking Factor; S is the Amount of Staking; N is Miner's space Size(TiB), $N > 0$, $N = 1$ TiB, which 1TiB equal to 1. Then the staking formula is as follows:

When $S \geq N$, $SF = 0.5+1/ (S/N + 1)$
When $S < N$, $SF = 0.05+1/ (S/N + 0.05)$

The Individual Difficulty of every miner is equal to the Difficulty of the entire network multiplied by a Staking Factor. That is to say,

Individual Difficulty(D') = Difficulty(D) * Staking Factor(SF).

When $S \geq N$, $SF = 0.5+1/(S/N + 1)$. That is, The individual Difficulty is equal to the Difficulty of the entire network if the miner stake the amount of SIT same with his plots size(TiB) and the miner can significantly increase the probability to win the block if he stake the amount of SIT more than his plots size(TiB). But when $S < N$,$SF = 0.05+1/(S/N + 0.05)$. So your individual difficulty will increase from 1 to near 20, according to the formula.

4.2 Use cases

The SIT token serves three distinct purposes: to govern over the network, to stake and DeFi applications, to power the Silicoin network.

- **DAO**

Silicoin is a decentralized public chain led by the community. Since SIT is the only token on the platform, it should become a credential for community participation in governance.

Application nodes that hold a certain amount of SIT can initiate upgrade proposals, such as staking weighting coefficients, development plan adjustments, etc. All SIT token holders can vote on the proposal. Whichever gets the majority of the votes shall be passed. Implementation is soon to be followed up by the development team.

- **Staking**

Staking encourages token holders to participate in fairways. In order to avoid centralization caused by massive tokens, a staking requirement is to be conducted when the size of plots is over the threshold. This approach ensures the network stays secure.

The staking function stimulates the demand for SIT tokens because the difficulty of mining will significantly affect the revenue in the future. If the miners want to obtain higher returns, they need to buy or keep more SIT for staking, so that their mining income will be higher.

What is more, the more plots miners have, the greater the probability that they will be selected to produce blocks in the past. But everything has changed in Silicoin. If a big miner mine Silicoin without staking SIT, his chance to win blocks may lower than the smaller miners who stake SIT more than its plots size.

In this economic logic, Silicoin not only avoids the monopoly of giants, but also helps small miners increase their profits.

- **DeFi application expansion**

DeFi is the track that the Silicoin team attaches great importance to. With the mainnet 2.0 officially launched, the design and development of the SilicoinSwap exchange protocol shall be put on the agenda. In this case, Silicoin will officially enter the DeFi track. At that time, the application scenarios of SIT will be greatly expanded. Users who hold SIT in possession can achieve currency listing through voting or staking, and they can also use SIT for convenient cross-chain exchange. The Silicoin team will contact offline partners to promote the value of SIT as well, for expanding SIT’s offline financial payment capabilities.

- **NFT section**

A non-fungible token (NFT) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable. NFTs can be used to represent items such as photos, videos, audio, and other types of digital files.

In terms of NFT, Silicoin creatively proposed the concept of NFT development module, which aims to lower the threshold for users to generate and use NFT. The NFT development module program can use smart contracts to parameterize any NFT, which means that even if you are completely unfamiliar with the computer programming code and the NFT production process, it is still possible for you to design and fill in the NFT parameters in the template according to your own preferences and needs. Then, to generate NFT with one click is all you need to do.