

STARCOIN2.0

Whitepaper

Starcoin: A Reliable, Flexible,
And Progressible Web3 Infrastructure.

66

WE SHOULD FOCUS ON THE NEXT STEP

In the evolution of decentralized technologies, blockchain continues to uphold its role as a potential beacon of innovation, despite experiencing market turbulence and investor caution. The challenges of the market have not hindered the pace at which blockchain technology integrates into our daily lives. With enhanced security and transparency, it is increasingly becoming the cornerstone of the digital economy.

As the market gradually returns to rationality, the core values of blockchain technology — decentralization, immutability, and openness — are being widely understood and recognized. While achieving this goal is a long-term process, blockchain technology has already demonstrated its potential for long-term applications in multiple fields. From simplifying global payments to enhancing traceability in supply chains, and empowering Decentralized Autonomous Organizations (DAOs), blockchain is progressively driving a revolution that does not rely on third-party trust.

The cyclical ups and downs of the industry also bring pivots and opportunities, marking the maturation of blockchain from its nascent stage. We find ourselves at a crossroads shaped by uncertainty and innovation, where establishing trust is more crucial than ever. Only those innovators who can adapt to changes will continue to move forward. While the proliferation of new technologies always encounters obstacles, each challenge also spawns solutions, propelling continual societal progress.

In this era of transformation, the value of blockchain is gradually unfolding and beginning to make its mark in an increasing number of business sectors. Although we cannot predict the ultimate trajectory of blockchain technology, far-sighted investors and developers are using their insights to find their place in the tide of technological innovation. In the future, the only constant will be change itself, carrying endless possibilities and opportunities.

TABLE OF CONTENTS

1 OVERVIEW

2 INTRODUCTION

3 CHALLENGE

4 SOLUTION

4.1 Philosophy

4.2 Technology

4.3 Innovations

5 ECONOMIC MODEL

6 TEAM

7 ROADMAP

1 OVERVIEW

Starcoin: A Reliable, Flexible,
and Progressible Web3 Infrastructure.



Starcoin, launched in 2020 with its mainnet going live in May 2021, is the only project that combines Satoshi Nakamoto's enhanced Proof of Work (PoW) consensus with the next-generation secure programming language, Move, to implement smart contracts. By the end of 2023, it adopted the industry's most advanced parallelization technologies, introducing FlexiDAG and TurboSTM upgrades to its mainnet. This hundredfold speed upgrade significantly enhanced performance, marking the commencement of the Starcoin 2.0 phase, referred to as "Tempus." Derived from Latin, "Tempus" translates to "time." It reflects Starcoin's unwavering commitment to continuous innovation in the blockchain realm, symbolizing our dedication to the rhythm of time, evolution, and ongoing progress. The goal of Starcoin 2.0 is to provide a secure, efficient, and agile decentralized system. Starcoin is not just creating blockchain infrastructure but also contributing to building the Web3 digital life for hundreds of millions in the future.

In its 2.0 phase, Starcoin implemented industry-leading parallelization technology, achieving significant transaction performance improvements. Under the same evaluation conditions, the new parallelization technology, TurboSTM, increased transaction processing capacity by 17 times compared to its 1.0 phase. Based on the new Directed Acyclic Graph consensus algorithm, FlexiDAG, the speed of generating new blocks (BPS) also increased tenfold compared to 1.0. The whitepaper will delve into Starcoin's innovative technologies—TurboSTM and FlexiDAG—and how they collectively enhance the network's scalability and efficiency.

Starcoin envisages creating a decentralized, inclusive digital ecosystem that fundamentally alters how people interact, transact, and participate in the digital economy. We foresee a future where blockchain technology seamlessly integrates into everyday life, enabling individuals to have full control over their digital assets and conduct transactions securely and efficiently with anyone, anywhere. At the forefront of this transformation, Starcoin is committed to fostering innovation, encouraging collaboration, and shaping the future of Web3 infrastructure. Our whitepaper will provide detailed insights into our design philosophy, technological innovations, and explorations that genuinely benefit user experience.

2 INTRODUCTION

Do not step on other tracks,
just go own way.



next-generation secure programming language Move for smart contract implementation. Its mainnet, launched in May 2021, was among the first to practice integrating Move smart contracts with Nakamoto consensus, establishing foundational infrastructure. We have combined the decentralization of PoW consensus with the high security of the Move language, the scalability achieved through FlexiDAG, and the rapid transaction capabilities of TurboSTM. This powerful combination provides us with a secure, efficient, and rapid decentralized system, offering reliable future solutions for the digital life of the Web3 world. Starcoin's mission is to offer a secure, high-performance, and inclusive permissionless blockchain, ensuring the safety of user assets and catering to future large-scale demands. We are dedicated to building a robust blockchain infrastructure, adhering to the principles of security and decentralization, to provide reliable future blockchain solutions and propel the development of the digital economy in the Web3 era.

Our vision with Starcoin is to create a decentralized, inclusive digital ecosystem that revolutionizes how people interact, transact, and participate in the digital economy. We envision a future where blockchain technology seamlessly integrates into daily life, enabling individuals to have complete control over their digital assets and transact securely and efficiently with anyone, anywhere. At the forefront of this transformation, we are committed to fostering innovation, encouraging collaboration, and shaping the future of Web3 infrastructure. We strive to create a world where decentralization, transparency, and trust are the cornerstones of the new digital paradigm, opening unprecedented opportunities for individuals and businesses alike.

3 CHALLENGE

Value exists to Solve Challenges



The blockchain industry is striving to overcome the challenges of decentralization, scalability, and security, commonly referred to as the "trilemma" of blockchain. Among these, transaction speed is a key issue in enhancing scalability, especially considering the anticipated future demand for large-scale transactions. The existing Transactions Per Second (TPS) standard seems insufficient for this need.

TPS measures the number of transactions a blockchain network can process per second, crucial for scalability, rapid transaction processing, enhancing user experience, and gaining a competitive edge. In this age of rapid information and speed supremacy, fast transaction processing is vital for user experience. Users expect to complete transactions swiftly without being hindered by congestion issues.

However, current blockchain technologies often face a design trade-off between decentralization and performance while pursuing high throughput. Some blockchains have achieved higher transaction speeds, but this may involve compromising some aspects of the network's decentralization principles. Meanwhile, to address the issues of mainnet congestion and high transaction fees, many projects in the industry have already or are exploring the adoption of multi-layer architectures, with second-layer (Layer 2) solutions widely regarded as effective in enhancing transaction processing capabilities and reducing costs.

Additionally, innovations in consensus mechanisms are seen as key to enhancing blockchain performance and scalability. Nonetheless, the introduction of these new consensus mechanisms must also balance their potential impact on the network's decentralization. Newer schemes like Proof of Stake (PoS) are being adopted for efficiency, but their long-term effects remain to be observed and assessed.

In this rapidly evolving industry, Starcoin is committed to finding a balance that offers both efficiency and scalability while maintaining a firm stance on decentralization to ensure the security of the network and the equality of all participants. Starcoin must continue to address the challenges of speed and efficiency to meet user demands and drive broader adoption.

4 SOLUTION

Starcoin offers a reliable and future-proof blockchain solution that addresses the evolving needs of the digital economy.



4.1 PHILOSOPHY

Decentralization: Upholding The Fundamental Principle Of Blockchain

Starcoin steadfastly adheres to the principle of decentralization, which is not only the cornerstone of our technology but also the very foundation of our existence. We believe that decentralization is the true source of blockchain's power, ensuring the network's autonomy and fairness. To this end, we have adopted an enhanced version of the Proof of Work (PoW) consensus mechanism, a market and time-tested mechanism that strengthens the network's decentralized characteristics and ensures that all participants can contribute and benefit in a fair environment.

Security: Paramount For Digital Assets

Security is a core tenet at Starcoin. Our goal is to establish an environment of utmost trust for our users, where security is the primary consideration, whether it involves the execution of smart contracts or the storage of assets. By adopting the resource-oriented programming language Move, we have enhanced the security of our smart contracts. We continually strengthen and iterate these security measures to maximally safeguard against any potential threats.

Scalability: Paving The Way For Future Large-Scale Applications

Starcoin is acutely aware that a successful blockchain platform must be secure, decentralized, and capable of adapting to the ever-growing demands of future applications. Therefore, we continually enhance the network's scalability through innovations like FlexiDAG and TurboSTM. This ensures that while maintaining high performance, the network can support the large-scale application demands of the future. Our goal is to provide a platform that not only meets current market demands but is also equipped to adapt to future growth.

The philosophy of Starcoin is built on three years of deep technological cultivation, constantly pursuing technological innovation and optimization. We believe that through continuous technological innovation, we can enhance the network's performance and scalability without sacrificing decentralization and security. This relentless pursuit fuels our commitment to create a blockchain ecosystem that is both trustworthy for users and developers and holds potential for the future. The Starcoin 2.0 phase is a testament to this commitment and a significant step towards the future.

4.2 TECHNOLOGY

4.2.1 Decentralization — Enhanced PoW Consensus

The "Enhanced PoW Consensus" in Starcoin's whitepaper represents a significant innovation, combining the inherent advantages of the traditional Proof of Work (PoW) with advanced technological improvements. This section outlines how Starcoin's consensus mechanism innovates on top of Nakamoto consensus and highlights its adaptability, efficiency, and resistance to censorship.

Adaptive And Efficient Network Operation

Starcoin's consensus mechanism innovates upon the traditional Nakamoto consensus by introducing an adaptive approach to accelerate block production and reduce transaction confirmation times. This is achieved by incorporating real-time data like uncle block rates into network operations. These data points are used to dynamically and intelligently adjust key network parameters such as block production times, difficulty, block rewards, and block sizes. This adaptability improves network utilization, ensuring the system can handle varying levels of demand without compromising efficiency, significantly reducing user wait times.

Scalability

A core aspect of Starcoin's Enhanced PoW Consensus is its focus on scalable security. The network manages key consensus parameters, thresholds, and other data in a unified manner through on-chain configuration. This approach not only maintains the decentralized nature of the blockchain but also ensures the secure scalability of the network. The integration with on-chain governance mechanisms makes the consensus model more responsive and adaptable, capable of evolving with changing network demands and external conditions.

Security

The decentralized nature of PoW, where any user can contribute to network security, is preserved in Starcoin's model. This inclusiveness ensures the network remains beyond the control of any single entity or group, maintaining the fundamental blockchain principle of decentralization. It further protects users' data ownership, ensuring the network is an open and fair platform for all participants.

In conclusion, Starcoin's Enhanced PoW Consensus represents a forward-looking adjustment to the traditional PoW model. It maintains PoW's inherent decentralization and resistance to censorship, while significantly improving scalability, network efficiency, and adaptability. This innovative approach positions Starcoin as a cutting-edge blockchain platform, ready to meet the challenges of the modern digital economy and the evolving needs of blockchain users.

4.2.2 Security —— Move Smart Contract

Unparalleled Security Standard

In the realm of blockchain and smart contracts, security is paramount. Starcoin, adhering to this principle, has chosen Move, one of the most secure smart contract languages available, as the foundation for smart contract development. The fundamental reason for choosing Move is its resource-oriented programming paradigm, which fundamentally redefines how data operations are handled between users, the chain, and contracts. This approach grants users greater control over their data ownership, fully aligning with the vision of Web3, where users realize and utilize the value of their digital assets.

Smart Contract Security Revolution

Move represents a revolution in smart contract security. Learning from vulnerabilities observed in the real world, Move is inherently designed with numerous security features. These include inherently safe resource types, stable static calls, and a comprehensive testing system. Most importantly, Move employs systematic formal verification tools, significantly lowering the barrier for developers to create secure code, thereby enhancing the overall security of user data on the blockchain. This systematic approach to security makes Move an ideal choice for Starcoin, as it aims to provide users with a secure and robust environment.

Key Features Of The Move Language

Resource-Oriented Programming: This unique aspect of Move allows developers to easily create digital assets that are inherently safe, non-duplicable, and non-disposable. This mechanism ensures the integrity and security of digital assets, which is crucial in the context of blockchain.

General-Purpose Programming Support: Move's support for general-purpose programming enables assets to be freely combined, protocols to be easily extended, and applications to be more open. This flexibility is key in establishing a dynamic, adaptable ecosystem on Starcoin.

Static Typing and Calls: The use of static typing and calls in Move eliminates uncertainties in programs, reducing the security risks associated with dynamic calls. This feature enhances the stability and reliability of the code, ensuring that smart contracts execute as expected and do not exhibit unforeseen behaviors.

In summary, Starcoin's strategic decision to adopt Move for smart contracts is aimed at providing the highest level of security in the blockchain domain. Move's resource-oriented approach, coupled with its systematic security features, positions Starcoin at the forefront of secure, decentralized blockchain platforms. By leveraging the inherent advantages of Move, Starcoin is well-equipped to offer a secure, efficient, and scalable platform, ideally suited for the evolving needs of Web3 applications and the digital economy.

4.2.3 High-Performance Parallelization

In its 2.0 phase, Starcoin has adopted industry-leading parallelization technology, achieving a significant boost in transaction performance. Using the new parallelization technology, TurboSTM, the transaction processing capacity has increased by 17 times compared to the 1.0 phase. Additionally, based on the new Directed Acyclic Graph consensus algorithm, FlexiDAG, the speed of generating new blocks (BPS) has also increased by 10 times compared to 1.0. This section delves into the innovative technologies adopted by Starcoin — TurboSTM and FlexiDAG — and explores how they collectively enhance the network's scalability and efficiency.

FlexiDAG: Balancing Parallel Processing And Security

Starcoin 2.0's consensus is an enhanced version of the Bitcoin Nakamoto consensus, representing the latest attempt to improve the performance and security of Nakamoto consensus. By incorporating a Directed Acyclic Graph (DAG) structure and building upon the PoW research from Starcoin 1.0, we have effectively enhanced Starcoin's performance, increasing the system's efficiency and usability. To speed up block generation and reduce transaction confirmation times, we introduced a DAG structure and real-time network efficiency data analysis. This allows for dynamic adjustments to block generation time, difficulty, and rewards, optimizing network usage and minimizing user wait times. Moreover, we've enabled dynamic adjustments to the blockchain, with key parameters modifiable through on-chain governance mechanisms.

Nakamoto consensus, first adopted by Bitcoin, has been a widely used consensus method in the early stages of blockchain. It remains the most fault-tolerant public chain consensus mechanism to date, known for its simple design, low communication overhead, and decades of validation. However, it has limitations, including low throughput and extended block generation times, leading to poor user experience. Therefore, we chose to enhance Nakamoto consensus, endowing Starcoin with the following features:

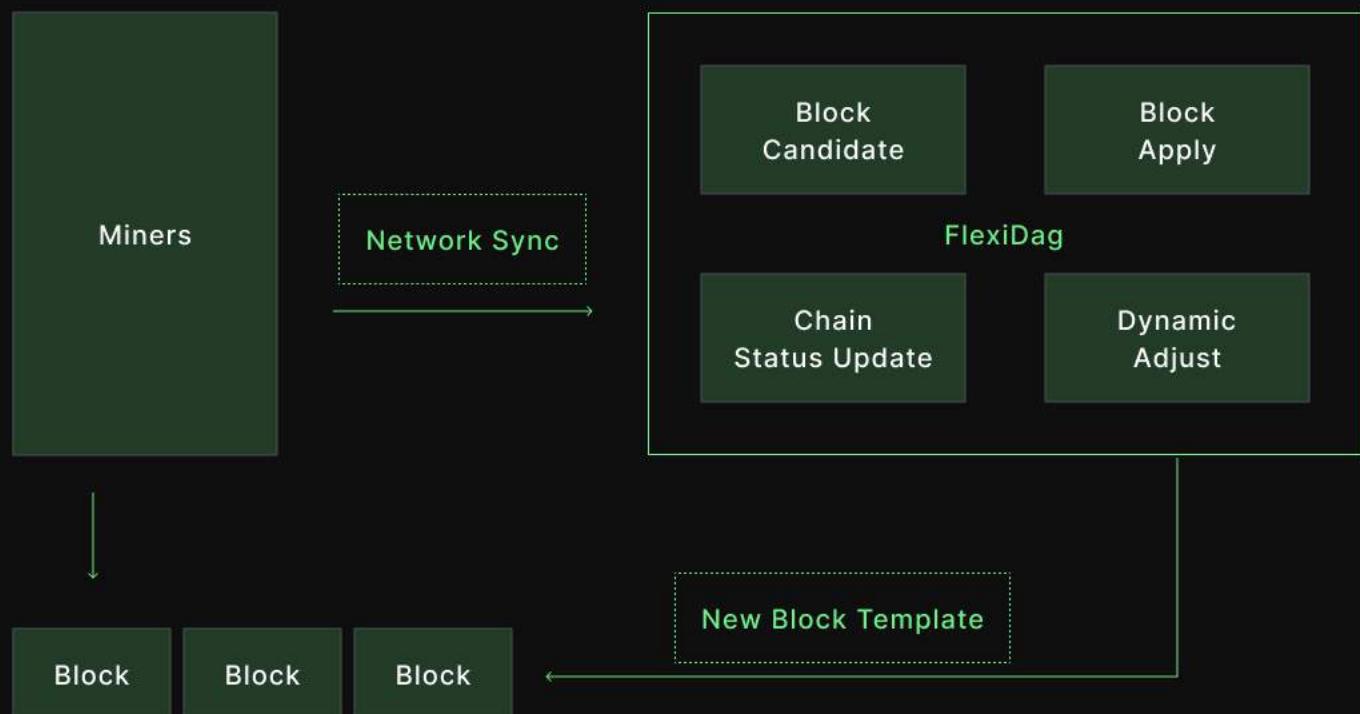
1. The ability to generate blocks in parallel, where multiple miners in the network can simultaneously produce blocks that are acknowledged by the main network, rather than being discarded as uncle or orphan blocks.
2. Dynamic adjustment of block generation speed and size, seeking a balance between security, network throughput, and user experience.
3. Consensus-related parameters can be modified through community governance and contract upgrades.

To implement the parallelization of Nakamoto consensus in Starcoin 2.0, all uncle blocks that comply with block creation rules are simultaneously added to the blockchain. This means that uncle blocks are effectively acknowledged as valid blocks, eliminating the need to rejoin the transaction pool.

If multiple valid blocks can be created simultaneously at a certain point in time, each new block can be seen as a child block of several recently created blocks, pointing to them. Based on this, the blockchain's topology transitions from a chain to a DAG.

Challenges addressed in implementing this method include distinguishing malicious or illegal blocks, resisting 51% attacks, and confirming the order of blocks within the DAG.

Therefore, in the traditional Nakamoto consensus, the collection of blocks constructed based on cumulative computational work determines the chain for building subsequent blocks, known as the longest chain. In contrast, the core of FlexiDAG consensus is to identify a well-connected subgraph, where subsequent blocks can be built based on cumulative computational work. This subgraph should exhibit strong connectivity, minimal isolated blocks, and tight node interconnections, forming the confirmed block set to be added to the blockchain, becoming the "longest chain."



The FlexiDAG Consensus Process

- 1. Constructing New Blocks:** A new block is created, pointing to eligible leaf nodes in the DAG, which are nodes that have not yet been referenced by other blocks.
- 2. Selection of Optimal Parent Node:** A new block is created, pointing to eligible leaf nodes in the DAG, which are nodes that have not yet been referenced by other blocks.
- 3. Consensus Election:** The counter-cone nodes of the optimal parent node (those nodes that are reachable but not directly connected to the optimal parent node) are examined. Nodes meeting specific criteria are selected from these, ensuring their inclusion does not disrupt the overall connectivity of the DAG. These nodes are then added to the set of blocks awaiting confirmation, expanding the scope of the candidate blocks.
- 4. Node Sorting and Application:** The selected set of nodes is sorted based on their workload and applied serially (added) following the optimal parent node, determining the final sequence of blocks.
- 5. Finalizing the State Update of the Chain:** From the forked chains, the sequence with the longest chain is selected to determine the latest block header, maintaining the integrity of the blockchain.
- 6. Ensuring Compliance with Restrictions:** As blocks, elected successfully, are added, it is ensured that the intersection number between the counter-cone set of the confirmed block collection and the confirmed block collection does not exceed a given limit size. This ensures the effectiveness of the solution and adherence to consensus rules.

This process reflects the innovation of FlexiDag in blockchain consensus mechanisms, enhancing system security and scalability by combining the DAG structure with Proof of Work.

FlexiDag Security Analysis

1. Double Spending Attack: Attack Description: Double spending refers to a malicious user attempting to use the same funds for two or more transactions on the blockchain.

In FlexiDag, blocks and transactions are ordered to confirm the entire DAG's execution state. Once transactions are included in a sufficient number of confirmed blocks, they are considered final, reducing the possibility of double spending.

2. Selfish Mining or Long-Range Attacks: Attack Description: Selfish mining involves miners deliberately not broadcasting newly discovered blocks to gain a competitive advantage.

In FlexiDag, since blocks are formed based on the DAG structure, each block references all its legitimate parent nodes. If a miner tries to hide a block, other miners will continue mining on the known latest block. Also, as block consensus accumulates based on their position in the DAG, rewriting history over time would require immense computational power, making the attack increasingly costly.

3. Sybil Attack: Attack Description: In a Sybil attack, the attacker creates numerous false identities to gain disproportionate influence within the network.

Since FlexiDag is based on Proof of Work, an attacker would need to control a significant amount of computational resources to execute a Sybil attack effectively. The cost and complexity of such an attack make it an impractical option.

4. Denial of Service (DoS) Attack: Attack Description: A DoS attack involves flooding the network with a large number of invalid transactions or requests, rendering it unable to process legitimate transactions.

FlexiDag's DAG structure allows for parallel processing and faster block confirmation, thus improving the overall network throughput and resilience against attacks.

FlexiDag Block Synchronization Process

After upgrading to FlexiDag, the block synchronization strategy has been modified. In FlexiDag, synchronization relies on the properties of an accumulator, which is essentially an implementation of a Merkle tree in the blockchain. In the FlexiDag accumulator, each leaf node represents a collection of blocks generated within a specific block production period. Generally, the block collection of the previous leaf node serves as the parent node of the next block collection.

The benefit of using an accumulator is that FlexiDag blocks can leverage the properties of the Merkle tree. This allows for a quick comparison of two different FlexiDags, rapidly pinpointing a specific Merkle tree node where the data before it is consistent, and the data after it differs. This avoids the need to synchronize from the initial node, thus enhancing efficiency.

Synchronization Step 1 Generating The FlexiDag Accumulator

In a specific time window, concurrently generated blocks are placed in the rightmost leaf node of the accumulator. Each leaf node is a hash value serving as a key, whose corresponding value is a structure detailing block information produced within that time window and the accumulator information for that period. Each block in the next leaf node has parent nodes originating from blocks within the previous leaf node.

Synchronization Step 2 Synchronizing The Accumulator

With the accumulator, nodes only need to compare their respective root values of the accumulator to determine if they are the same. The leaf node number of the accumulator is used for synchronization progress control. Specific sync details include:

- The leaf nodes of the accumulator.
- The block information corresponding to the key of the accumulator leaf nodes, i.e., block information produced in the time window and the snapshot information of the accumulator during that period.

For example: If Node A has 10 leaf nodes in its accumulator and Node B has 15, and it is found that the root value of the third leaf node is the same for both A and B, then synchronization will start from the fourth node. Node A will pull data from Node B, and vice versa, ultimately resulting in both nodes having the same accumulator and thus indicating the same DAG object. Finally, the accumulator data of Nodes A and B will merge, resulting in the same accumulator.

Synchronization Step 3 Synchronizing Blocks

After synchronizing the accumulator, the block information corresponding to its leaf nodes can be synchronized. Similar to the mining process, once the block information is retrieved, it is executed by the virtual machine and incorporated into the DAG object.

TurboSTM: Reshaping The Execution Of Smart Contracts

As smart contracts evolve, blockchain systems are encountering new challenges. Traditional execution of smart contracts is carried out using a single-threaded approach, meaning that only one transaction is processed at a time. This becomes a significant bottleneck, especially when multiple transactions are bundled into a block, particularly when there are thousands of transactions in a block. Starcoin 2.0 innovatively introduces TurboSTM, a groundbreaking, high-performance, multi-threaded in-memory computing engine that fundamentally transforms the way smart contracts are executed.

TurboSTM utilizes Multi-Version Concurrency Control (MVCC) and optimistic concurrency control(OCC) to achieve synchronous data reading and timely updates. This approach significantly reduces bottlenecks related to the execution of smart contracts, thereby enhancing transaction throughput.

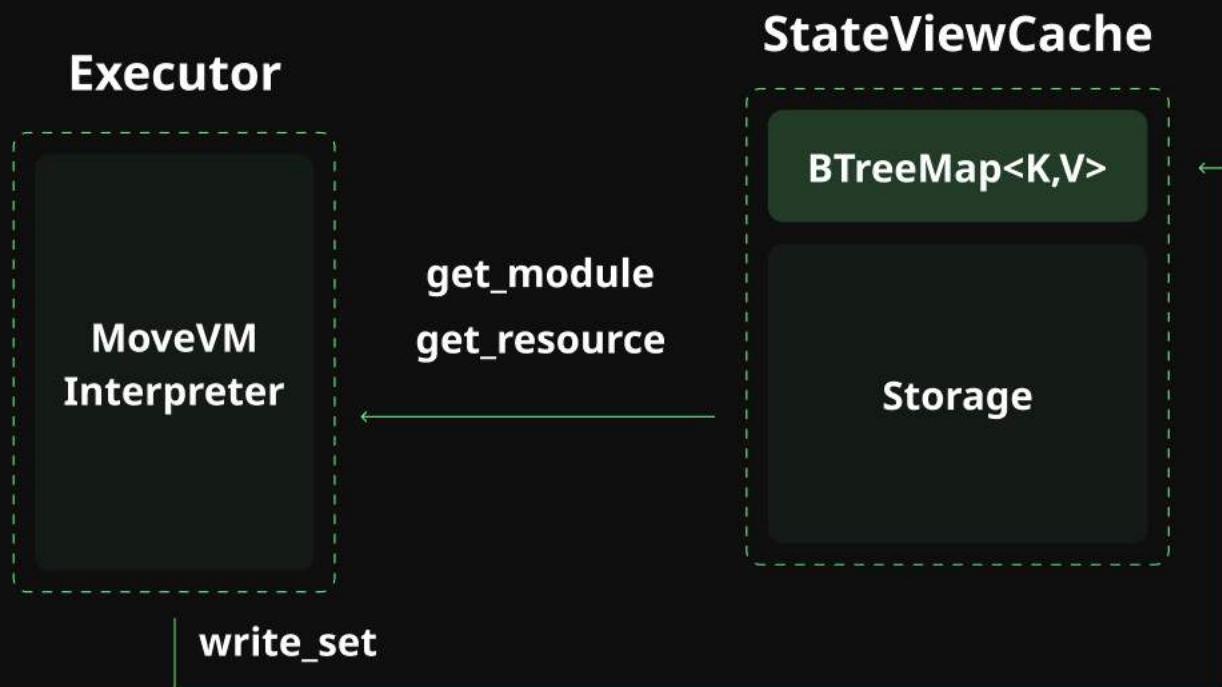
It Is Important To Outline The Process Of Sequential Transaction Execution, As Follows:

- Executor Module: This module is responsible for executing transactions. During a transaction, it handles various transactional information, such as the transaction payload, typically provided by front-end wallet plugins or DApps.
- Storage Module: This module stores transaction information and the results of their execution.
- MoveVM Module: The Move virtual machine executor is used for executing Move code. It takes Move code as input, computes the execution results, and identifies the resources modifications involved.

The Execution Process Is As Follows:

- The Executor locates the contract execution code (via the get_module interface) and the necessary resources (through the get_resource interface) based on the payload in the incoming transaction.
- The MoveVM's Interpreter is then called upon to compute the results. The resulting modifications are output to a write_set collection, which is subsequently stored in the Storage module

Below Is A Flowchart Of The Sequential Execution Process.



Considering the parallel execution process, some approaches employ a pre-declaration method, which is not developer-friendly as it requires adding lists of reads and modifications made during contract execution into the transaction. TurboSTM, however, employs a user-transparent approach.

TurboSTM Has Several Core Elements:

1. Version = (TxnIndex, ExeCnt): Here, 'TxnIndex' represents the transaction's position within the block, and 'ExeCnt' indicates the count of transaction executions.
2. MvCCMap: A thread-safe multi-version data structure used to store multiple versions of transaction results. Each entry in MvCCMap consists of 'ExeCnt' and a value ('value'). The code definition is as follows:

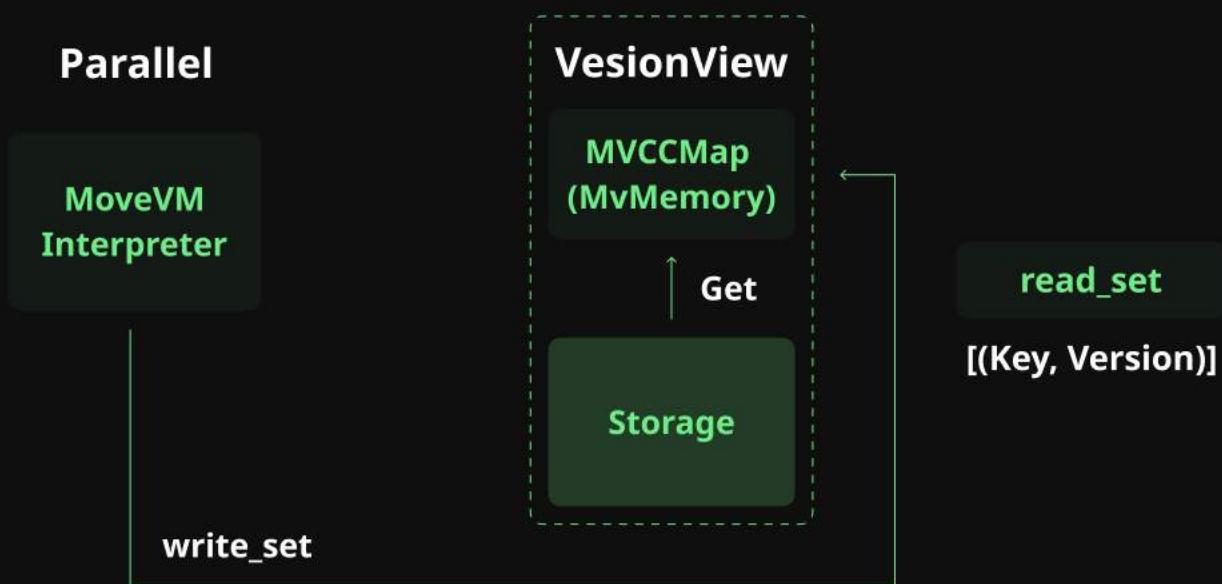
```
class Entry {  
    int ExeCnt;  
    string value;  
};  
  
MVCCMap = Map<Location, Map<TxnIndex, Entry>>  
TxInputList = List<List<Location, Entry>>
```

3. Task Types: There are two different types of tasks defined: ExecutionTask, ValidationTask, NoTask (empty task), and Done (completion task). To implement parallel execution, we divide transactions into two queues: the Execution Task Queue

The Implementation Works As Follows:

- When executing transactions within a block, we retrieve transactions from the queue and generate execution tasks to add to the Execution Task Queue. Each time a transaction is executed, we write the transaction-generated 'Location' into the multi-version data structure and record the data (read_set) of the 'Location' read by the transaction into the TxInputList.
- During the Validation Task for transactions, we compare whether the version number (ExeCnt) of the 'Location' read by the transaction taken from TxInputList and the version number obtained from the multi-version data structure match for validation. This process is akin to the version number in a lock-free queue's ABA problem.

Here Is The Execution Flow:



TurboSTM, as mentioned above, introduces a merge operation to optimize conflicts in parallel write operations to a specific location. Each transaction generates an incremental execution result. When all transactions in a block are completed, these increments are merged to produce the final result, thereby achieving the goal of parallel execution.

TurboSTM, in combination with Starcoin's Easy Gas mechanism (which aims to make transaction costs both affordable and scalable), lays the foundation for Web3 to become synonymous with fast, economical, and secure transactions. This parallelization approach ensures that users enjoy a seamless experience even during periods of high demand. The integration of FlexiDAG and TurboSTM in Starcoin 2.0 represents a significant advancement in blockchain technology, setting new standards for scalability's feasibility. By addressing the limitations of traditional blockchain architecture and leveraging the advantages of DAG and STM technologies, Starcoin uniquely positions itself to support the growing diverse demands of the Web3 world. These technological advancements make Starcoin not just a scalable platform, but also a secure and efficient one, capable of meeting the needs of the rapidly evolving digital ecosystem.

4.3 Innovations

4.3.1 Clear Ownership Of State Storage

State storage mechanisms in blockchain systems are one of the key aspects of their design, significantly impacting the performance and security of the chain. Starcoin's state storage, adopting a model similar to Ethereum's account model, comprises a state tree mapped through addresses. Beginning from the genesis state, the state advances to a new state with each transaction as input, generating a new state tree.

Ethereum distinguishes between contract accounts and user accounts. Contract accounts are used for deploying contract codes and storing contract states, and the states of users in a contract are saved under that contract account, with read-write permissions controlled by the contract itself. While this design offers high flexibility, it leads to unclear ownership of the contract state, posing security risks and difficulties in addressing the "state explosion" problem.

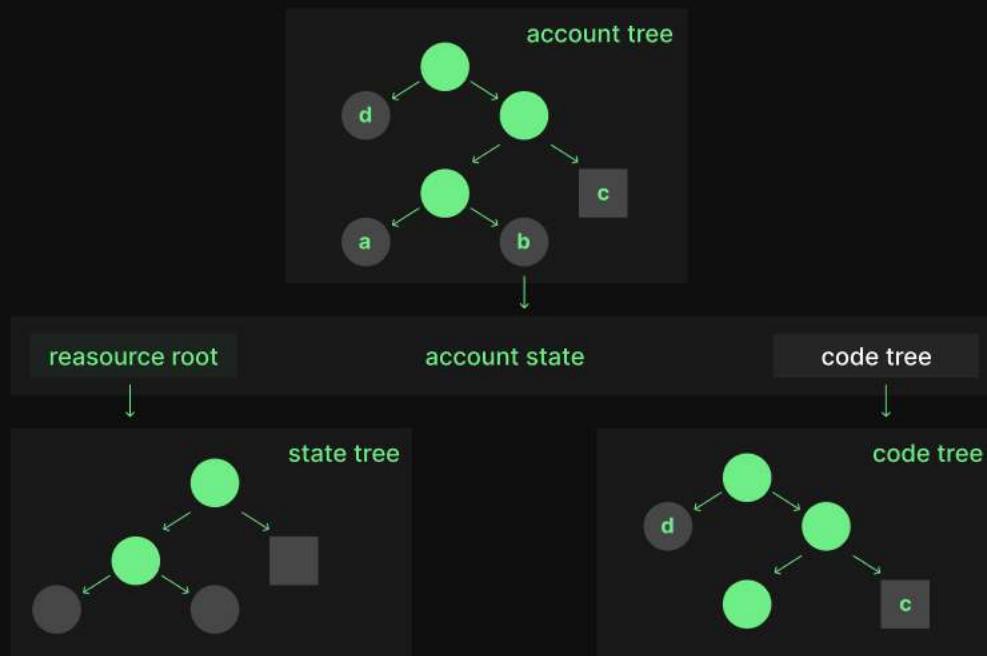
Starcoin has made the following improvements on the Ethereum account model:

- Elimination of contract accounts; any account can deploy smart contracts, with the deployed contracts residing under the current account.
- By changing the state storage mechanism in the contract programming language, it becomes easier for smart contract developers to distribute the contract's state across the user addresses to which the state belongs, thus clarifying the ownership of the state.

These modifications enhance the chain's ability to protect user states' security and pave the way for state-based billing.

Two-Level State Model

Building on Diem's Jellyfish-Merkle tree, we added forkable functionality as a foundational component for state storage, encapsulating it into a two-tier state tree structure. The Jellyfish-Merkle tree is a prefix query tree structure. The entire chain's state forms a global tree, where the leaf nodes represent each user's state (AccountState), and the query path is the account address. The AccountState contains the root hash values of the user's Resources and Code in a secondary Merkle tree, as illustrated below:



The leaf nodes of the Code tree are the code for each contract Module, with the query path being the Module name. In the Resource tree, the leaf nodes are the states within the contract, and the query path is the state type, StructTag. Thus, within the contract, the `borrow_global<T>(address)` method can be used to read the state, or the `move_to(address, resource)` method to write the state.

By employing a two-level state model, Starcoin can conveniently provide proof of state existence and ownership.

Billing Strategy

As the state of the blockchain network increases with the addition of accounts, and since the read/write operations on the state are charged through a one-time Gas calculation during transactions, users do not bear additional costs for occupying chain state over a long period. Consequently, there is no incentive to delete or clean up obsolete states. Therefore, the blockchain technology community has been exploring an appropriate state billing mechanism. Proposals like state rent on Ethereum have been suggested, but due to the previously mentioned issue of unclear state ownership in Ethereum contracts, implementing state billing is quite challenging. Starcoin, with its clear state ownership mechanism, makes state billing feasible.

Starcoin's state billing strategy adopts a post-collateralization method, where the storage space available to users (STCBytes) is dynamically calculated based on the amount of STC they hold. Before executing a transaction, the user's STCBytes balance is checked (using the formula below), and the transaction is denied if the balance falls below a threshold.

Balance Calculation Method:

$\text{STCBytes} = \text{STC} * \text{Exchange Rate} - \text{Size of STCBytes already used by the user}$

The STCBytes balance is calculated before each transaction, reflecting the user's storage state up to the end of their last transaction. This allows for one-time over-usage by the user, meaning the current transaction doesn't need to be considered when calculating STCBytes. This approach encourages users to proactively release unused resources, reducing their STCBytes usage and thereby facilitating the healthy development of the system.

4.3.2 Easy Gas

As the first PoW public chain in the Move ecosystem to support "Easy Gas," Starcoin aims to significantly improve the user-friendliness of transactions on the blockchain. This innovation fundamentally changes the handling of gas fees, making it more convenient for both users and developers to manage gas expenses and reducing restrictions related to gas fees.

Challenges Of Traditional Gas Payment Methods

Traditionally, transactions require payment of gas fees in the network's native token to compensate miners for their computational efforts. This system often creates barriers to entry, especially for new users unfamiliar with the complexities of blockchain. The need for specific native tokens for gas payments not only complicates transactions but also adds to the burden of developers in educating users about acquiring and using these tokens.

Starcoin's 'Easy Gas' Solution

Starcoin's "Easy Gas" allows users to pay gas fees using any token supported by its platform, without needing to hold the native STC token, thereby directly addressing these challenges. This approach simplifies transactions, making them more convenient and user-friendly, especially for newcomers to blockchain technology. By integrating this feature with Starcoin's DAO governance, the platform ensures flexible and democratic decision-making regarding eligible gas payment tokens.

Technical Innovations Of Easy Gas

- **Seamless Integration:** Easy Gas is natively supported on-chain by Starcoin, allowing the direct specification of gas payment tokens in transactions. This integration requires no intermediary nodes and no complex code modifications, unlike Ethereum's Gas Station Network (GSN) system.
- **Simplified Process:** The process of paying gas fees with Starcoin is straightforward. After submitting a transaction, the "Prologue" step calculates the required gas fee and checks if the user has sufficient funds. Post-transaction, in the "Eprologue" phase, the designated gas fee token is converted into STC and queued for payment to miners. This process is supported by PriceOracle and Dao&& GasOracleProposalPlugin, where the former provides accurate token pricing and the latter manages gas token eligibility and pricing updates.

Revolutionizing Experience

Starcoin's Easy Gas demonstrates the platform's commitment to user-centric innovation. By simplifying gas payments and eliminating barriers to initiating transactions, Easy Gas paves the way for wider adoption and participation in decentralized applications (DApps). This advancement not only enhances the user experience but also places Starcoin at the forefront of blockchain innovation, setting new standards for transaction accessibility and usability in the Web3 domain.

4.3.3 On-Chain Governance: DAO

Promoting Decentralized Governance Through On-Chain Mechanisms.

Starcoin's DAO (Decentralized Autonomous Organization) represents a significant advancement in on-chain governance. By integrating DAO functionalities directly into the blockchain, Starcoin has established a more inclusive, transparent, and efficient governance process, enabling community members to actively participate in the network's development.

Innovative Approach To DAO Functionalities

- **Proposal Process:** The governance process of Starcoin DAO is streamlined and user-friendly. It begins with an initiator proposing a change or new policy. Subsequently, users of the Starcoin network participate in voting, expressing their preferences for each proposal with their tokens.
- **Unique Implementation Method:** Unlike other DAO models, Starcoin employs a distinctive approach, where different types of proposals are controlled by different contract modules. This modular system is a result of Move's static function call distribution, requiring all code calls to be predetermined at compile time.

Enhancing User Participation And Proposal Flexibility

- **Decentralized Voting:** Starcoin's DAO uses a token-based voting system, where the number of votes is proportional to the number of tokens held. This method ensures fair distribution of decision-making power among stakeholders, reflecting their vested interests in the network.
- **Proposal Lifecycle:** Proposals go through a comprehensive lifecycle, including stages like pending, activation, failure, agreement, queuing, executable, and executed. This structured process ensures each proposal undergoes thorough community evaluation and deliberation before implementation.

Advantages Of Starcoin DAO Governance

- Transparency and Security: The on-chain nature of Starcoin DAO governance ensures transparency and security, with clear, tamper-proof records of all decisions and transactions.
- Efficiency: The direct governance model simplifies the decision-making process, eliminates intermediaries, and reduces bureaucratic delays.
- Community Empowerment: By allowing every token holder to vote, Starcoin's DAO model enhances the community's capability, enabling each member to contribute to the network's future development direction.

Starcoin's on-chain DAO governance model reflects the platform's commitment to creating a genuinely decentralized and democratic blockchain ecosystem. By leveraging the capabilities of the Move language and adopting a unique governance structure, Starcoin ensures the adaptability, security, and alignment with diverse community interests of its network. This approach not only strengthens the governance process but also sets new standards for community participation and decentralized decision-making in the blockchain space.

4.3.4 Formal Verification

Ensuring Maximum Security With Formal Verification In Starcoin

In the blockchain technology field, where digital asset security is crucial, Starcoin has taken an important step by integrating formal verification technology into its platform. This approach highlights Starcoin's commitment to protecting user assets and providing a robust security environment.

Formal Verification: A Secure Mathematical Method

- Cutting-Edge Security Technology: Formal verification represents the forefront of programming security technology. It uses mathematical methods to scientifically prove the security of programs. This process is critical in the blockchain environment, where risks are high and the cost of vulnerabilities can be significant.
- Move Language and Formal Verification Tools: Starcoin utilizes the Move programming language, which supports a set of sophisticated formal verification tools. These tools enable developers to write specifications (SPEC), rigorously test, and prove the security of their programs. By leveraging these tools, developers can significantly reduce security risks and ensure the robustness of smart contracts.

Reducing Risks And Enhancing Stability

- Static Typing and Calling: Starcoin adopts static typing and static calling in its programming model, playing a crucial role in enhancing code stability and security. By eliminating the uncertainties and risks associated with dynamic calling, Starcoin provides a more stable and predictable environment for executing smart contracts.
- Preventing Security Vulnerabilities: Combining formal verification with static typing ensures that security vulnerabilities are identified and reduced at the earliest stages of development. This proactive approach to security is essential for maintaining the integrity and credibility of the Starcoin platform.

The integration of formal verification technology in Starcoin represents a significant advancement in the field of blockchain security. By providing developers with powerful tools to scientifically prove the security of their programs and adopting a static programming model, Starcoin sets a high standard for the security of the blockchain ecosystem. This commitment to security and stability makes Starcoin a reliable and trustworthy platform for users and developers, ensuring the inviolability of user assets and the overall security of the network.

4.3.5 Bootstrapped Economic Model

Sustainable Economics: The Bootstrapped Model Of Starcoin

Starcoin introduces a bootstrapped economic model, a forward-thinking approach to establishing a sustainable and stable financial ecosystem within its blockchain network. This model aims to ensure the continuous supply, fair distribution, and long-term economic stability of STC (Starcoin's native token).

Fixed Supply And Minting Process

- Unchanging Token Supply: In a key genesis transaction, the Starcoin genesis account minted all STC tokens and then securely locked them in a vault. Subsequently, the minting permission was irrevocably revoked. This decisive action guarantees the stability of STC's supply, eliminating the possibility of inflation through additional minting.
- Transparency and Predictability: By setting a total supply from the start and removing the ability to mint more STCs, Starcoin ensures the transparency and predictability of its economic model, fostering trust and stability within its ecosystem.

Linear Release And Distribution

- Linear Release Over Block Time: The STC tokens locked in the vault are released linearly over time, in sync with the blockchain's block time. This steady and predictable distribution mechanism contrasts sharply with the more aggressive or variable emission models in some other blockchain networks.
- Miner Rewards: Miners are rewarded for their contributions to the network, with STC tokens distributed from the treasury. Each block's reward is allocated to the miner responsible for creating that block. Notably, there is a delay of N blocks (initially set to 7) before these rewards are obtained, adding an extra layer of stability to the distribution process.

Feasibility Of The Bootstrapped Economic Model

- Miner Incentives and Ecosystem Growth: In the bootstrapped economic model, tokens are first distributed to miners and then gradually circulate within the broader ecosystem. This model supports the network's initial growth and development by incentivizing miners, who play a crucial role in maintaining and securing the blockchain.
- Self-sustaining Financial Model: A key goal of Starcoin's economic model is to sustain financial resources to fund future R&D investments and ongoing miner rewards. Achieving this milestone would indicate that Starcoin's economy has become self-sustaining, a significant achievement for any blockchain network.

Starcoin's bootstrapped economic model represents an innovative approach in blockchain economics, emphasizing long-term sustainability, predictable token distribution, and financial stability. By carefully designing its economic mechanisms, Starcoin not only incentivizes participation and growth but also lays the groundwork for establishing a self-sustaining, robust financial ecosystem within its blockchain network.

4.3.6 Use Stdlib To Manage Consensus

Stdlib: Facilitating Robust, Scalable Application Development In Starcoin

Starcoin's unique feature, Stdlib (Standard Library), plays a crucial role in its ecosystem by providing a secure and universal underlying framework that greatly aids developers in building scalable and robust applications.

Implementing Unified Protocol Standards Through Stdlib

- Comprehensive Standards Implementation: Starcoin has formally established a set of universal protocol standards through its Stdlib. These include secure token protocols, freely composable NFT (non-fungible token) protocols, and open Oracle protocols. The significance of these standards lies in their uniformity and compatibility, ensuring seamless interaction and integration within the Starcoin ecosystem.
- Simplifying Application Development: The standardization of these protocols in Stdlib enables developers to create inherently secure and interoperable applications, aligning with the core principles of blockchain technology.

Efficient Development With Out-Of-The-Box Components

- Ready-to-Use DAO and Configuration Management: Among the various components introduced in Stdlib are tools for DAO governance and on-chain configuration management. These components are designed to be reusable, significantly reducing the workload of blockchain developers.
- Simplifying Development with User-Friendly Tools: Starcoin's Stdlib also includes straightforward and easy-to-use tools like SafeMath for secure arithmetic operations and tools for floating-point calculations. These tools are not only user-friendly but also enhance the robustness of applications built on the Starcoin platform.

Strengthening Consensus Management With Stdlib

- Secure, Scalable Framework: By incorporating these tools and standards into Stdlib, Starcoin provides a secure, scalable framework for consensus management. This framework enables developers to build applications that are both reliable and capable of evolving with the network.
- Reducing Complexity in Application Creation: Stdlib offers standardized, interoperable components and user-friendly tools, reducing the complexity traditionally associated with blockchain application development. This ease of use is key to attracting more developers to the Starcoin ecosystem.

The use of Stdlib to manage consensus in Starcoin represents an innovative approach to blockchain development. By providing a full suite of standardized protocols, reusable components, and developer-friendly tools, Stdlib not only enhances the security and scalability of applications but also simplifies the development process. The strategic use of Stdlib indicates that Starcoin is a developer-centric, future-oriented platform capable of supporting a wide range of applications and use cases in the blockchain domain.

4.3.7 State Billing

In public blockchain networks, the challenge of state explosion is a critical issue. As block data grows over time, accumulating more information, efficient data management becomes crucial. Starcoin adopts an innovative state billing strategy to address this issue, aiming to optimize data storage and ensure the sustainability of the network.

Challenges Of State Explosion

- Growing Data Accumulation: Public chains face the challenge of continually increasing block data, known as state explosion. This phenomenon leads to an ongoing accumulation of data, much of which may no longer be actively accessed or used but still needs to be stored and synchronized across all nodes. This situation results in significant resource wastage and inefficiency.
- Need for Efficient Data Management: The continuous growth of blockchain data necessitates a solution that can manage this expansion without impacting network performance and scalability.

Starcoin's Survival-Of-The-Fittest Strategy

- Preserving Valuable Data: Starcoin's state billing method is akin to a survival-of-the-fittest strategy for blockchain data. It aims to gradually accumulate and preserve valuable user data while eliminating less relevant or outdated information. This approach ensures that only data with intrinsic value remains in the network.
- Avoiding Unlimited State Expansion: By implementing state billing, Starcoin effectively addresses the issue of unlimited state expansion. This method helps avoid unnecessary data accumulation, maintaining a lean and efficient state.

Benefits Of State Billing

- Resource Optimization: State billing helps optimize the use of network resources. By removing outdated and low-value data, the storage and synchronization burden on nodes can be alleviated.
- Enhanced Network Performance: With a more streamlined state, the overall performance and scalability of the Starcoin network are improved. This approach ensures the network remains flexible to accommodate future growth and data demands.

Starcoin's state billing method is an effective solution to address the state explosion problem in public blockchains. By prioritizing the retention of valuable data and eliminating redundancy, Starcoin not only optimizes resource usage but also ensures the long-term sustainability and efficiency of the network. This strategy underscores Starcoin's commitment to maintaining a robust and scalable blockchain infrastructure that can adapt to the evolving needs of users and the broader blockchain ecosystem.

5 STARCOIN'S ECONOMIC MODEL

Overview of STC Token and Its Uses

https://starcoin.org/en/overview/economy_whitepaper/



STC Token: The native token of the Starcoin network, STC, has a total issuance of 3,185,136,000. It serves several purposes within the Starcoin ecosystem:

- Paying transaction GAS fees.
- Paying state space fees (post-activation of the state billing mechanism).
- Voting in on-chain governance.
- As the on-chain ecosystem matures, STC is expected to have an increasing number of applications.

Genesis Token Distribution And Management

Initial Minting and Distribution: At genesis, all STCs were minted and deposited into the treasury. The genesis account, responsible for this minting, then revoked its minting rights to ensure no further issuance of STCs.

Allocation of STCs: The initial distribution included:

- 5% to the Starcoin Foundation for early investors.
- 8% and 7% for ecological construction and core project development respectively, released over three years.
- Treasury withdrawal rights locked in the DAO, subject to on-chain governance for future withdrawals.

Block Rewards And Incentives For Miners

Reward Mechanism: Block rewards in Starcoin are based on a linear release model over time. The reward for each block is calculated using the current epoch's block time target, with the base block reward and base block time target being adjustable through on-chain governance.

Incentives for Reporting Uncle Blocks: To encourage the reporting of uncle blocks, Starcoin provides additional rewards to miners who include uncle block headers in their blocks.

Starcoin's economic model is designed to maintain a sustainable and balanced ecosystem, with its tokenomics and governance structure facilitating broad participation and secure growth within the network.

6 TEAM

Starcoin Foundation: Guiding Excellence and Innovation



The Starcoin Foundation is an independent standard-setting body responsible for overseeing and advancing the Starcoin platform and its flourishing ecosystem. As the guardian of the Starcoin protocol and brand, the Foundation's role extends beyond supervision. It is the driving force behind the adoption and collaboration strategies that elevate Starcoin to a global focus. The Foundation's work aims to expand the Starcoin community, influence legislative and commercial standards, and uphold stakeholder responsibilities at all levels.

Core Responsibilities

- Promoting Platform Adoption: The Foundation's core mission is to accelerate the adoption of the Starcoin platform. The team is dedicated to supporting a diverse community comprised of users, developers, and enthusiasts – a community that is integral to the implementation and realization of Starcoin's innovative potential.
- Supporting the Starcoin Ecosystem: To fulfill its duties, the Starcoin Foundation has established a governance board and a professional executive team. Community managers are often recruited from within the Starcoin community, playing a key role in ensuring tight connections and engagement among the user base.

Balancing Internal Focus With External Collaboration

- Inclusive and Forward-looking Approach: The Foundation's work is both broad and deep. It is committed to promoting cooperation within the wider blockchain industry, actively participating in advancing blockchain technology, and fostering integration with other compatible systems.
- Shaping Global Blockchain Discourse: Beyond technological advancements, the Foundation also plays a significant role in shaping the global dialogue on blockchain. By fostering this dialogue, the Foundation ensures that blockchain technology is not only usable by everyone but also understandable by all, paving the way for broad understanding and adoption of blockchain technology.

The Starcoin Foundation plays a crucial role in guiding the project towards realizing its vision. Combining internal expertise with external collaboration, the Foundation has a unique advantage in leading Starcoin into the future, ensuring its technology is widely adopted, understood, and valued.

Westar Labs

The Incubation Center Behind Starcoin's Technological Innovation Westar Labs is a vital technology incubator for the Starcoin project, playing a central role in promoting innovation and development within the blockchain ecosystem.

7 STARCOIN'S DEVELOPMENT TIMELINE

Roadmap:

2018 - 2020

Foundations And Launch

1. End of 2018: Publication of the first Starcoin whitepaper, laying the foundation for a scalable blockchain.
2. 2019-2020: Key developments including the adoption of the Move language (Q4 2019) and the release of Starcoin v0.1 (April 9, 2020).

2021

Milestones

1. March 27, 2021: Release of Starcoin v1.0.0.beta.
2. May 18, 2021: Launch of the Starcoin mainnet.
3. June 24, 2021: Introduction of the first Move Dapp and on-chain governance DAO.
4. September 2021: Release of the Starcoin NFT spec and the launch of Cyberrare, the first NFT marketplace.

2022**Ecosystem Practices**

1. January 2022: Launch of Arm Wrest War (AWW), a Play 2 Earn game.
2. March 2022: Introduction of FAI, a stablecoin protocol by Bfly Finance; launch of Starswap, a general-purpose DEX; and implementation of Fai Liquidation.
3. April 2022: Establishment of the first cross-chain bridge connecting Starcoin and Ethereum; launch of Bfly, an algorithmic currency protocol.
4. July 2022: Launch of the first Lending Protocol, fly, on the mainnet.
5. Q3-Q4 2022: Developments in DAO & governance, Layer1 & Layer 2 infrastructure, and the Move ecosystem.

2023**Innovating For The Future****enhancing pow consensus**

1. PoW consensus algorithm improvement strengthens consensus security.
2. Parallel-Chain Architecture
3. Economic Proof of Work

increasing transaction performance

1. We are increasing Layer 1 TPS by transaction parallel execution, etc.
2. P2P network optimization improves network performance (e.g., RPC optimization, scoring mechanism).
3. Network hole punching
4. Support QUIC protocol for performance
5. Light node, implemented as web assembly
6. RPC on p2p network
7. Incentive on p2p network

lowering validator threshold

1. Provide offline import and export block function, and improve block import speed.
2. Provide offline import and export snapshot data function and export support incremental export.
3. Provide asynchronous write and batch read interfaces to improve DB read and write speed.
4. Optimize accumulator write speed, and improve online synchronization block speed.
5. Provide snapshot sync on p2p and block WriteSet sync
6. Provide prune uncle block decrease storage size

improving the application development environment

1. Introducing and supporting new features of Move.
2. Provide U256 type to improve the convenience of dapp development.
3. Cookbook improvement to help developers quickly understand Starcoin development.
4. Using local node accounts to deploy contracts in remote nodes, facilitating developers to deploy mpm quickly provides integration test function, and mpm integration test provides custom parameters and deploys function, which is convenient for dapp developers to test.
5. Provide useful move data struct like HashMap and BigVector to improve the convenience of dapp development

This timeline encapsulates Starcoin's journey from its initial conceptualization to its current state and future plans. Each milestone reflects the project's commitment to innovation, scalability, and community-driven development. As Starcoin progresses, it continues to focus on enhancing its infrastructure, expanding its ecosystem, and solidifying its position in the blockchain industry.

The roadmap for 2023 and beyond promises further advancements, keeping Starcoin at the forefront of blockchain technology development.