Arichain: The Superorganism Network

Architected to be mass adopt blockchain technology
Low Entry barrier, High Performance and Scalability.

Ari Foundation

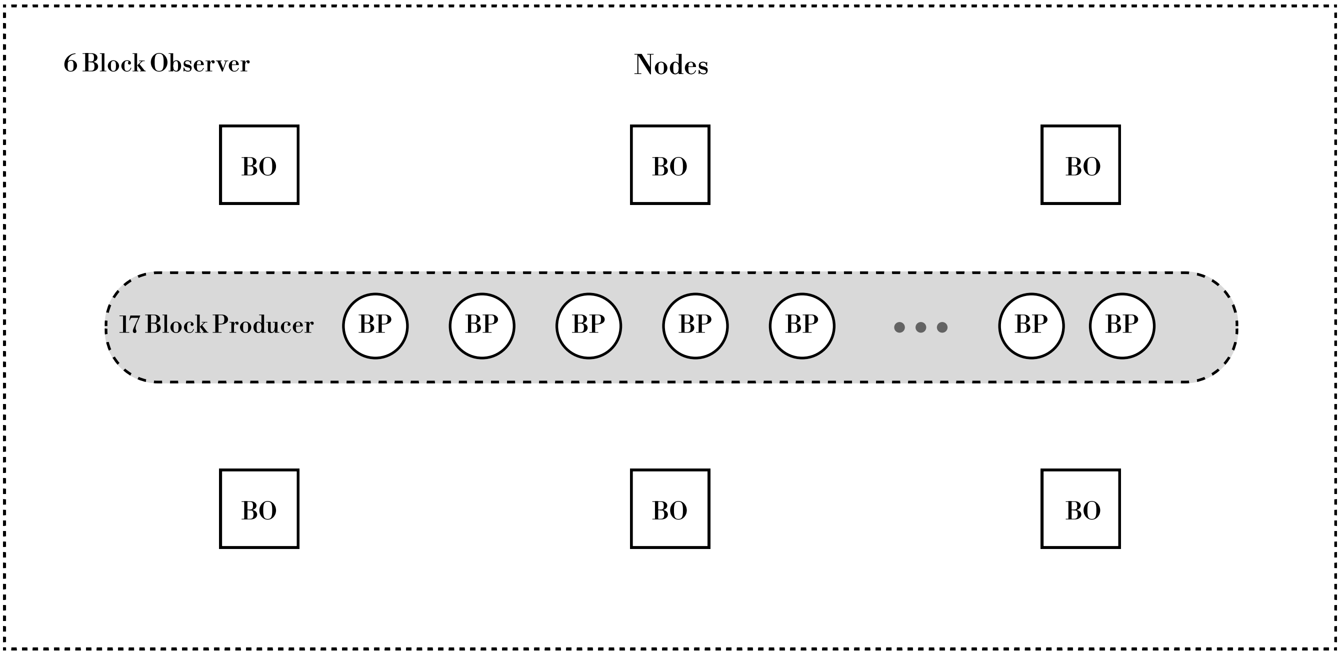
1. Abstract

In the highly competitive blockchain technology market, having a proprietary mainnet, using an effective consensus algorithm, and achieving high transaction processing speeds are crucial factors for gaining a competitive edge. ARICHAIN has made significant efforts to solve problems experienced with previous blockchain technologies and aims to build a faster and more secure mainnet. This includes improving the user interface and user experience on Linux/Windows operating systems.
To address the speed limitations of first-generation blockchains and the node security vulnerabilities in second-generation blockchain technologies, we have researched and developed the Delegated Random Proof of Stake (DRPoS) consensus algorithm.

This algorithm provides a more rational approach to improving specific block processing speeds from Block Producers (BP). Additionally, to resolve inefficiencies in redundant installations and excessive data storage issues, ARICHAIN offers access to the virtual machine environments of first and second-generation blockchains, providing a highly accessible environment for DApp developers.

2. Consensus Algorithm

Trusted institutions such as central banks and public offices authenticate various types of value. However, if these entities cannot recognize such value, or in scenarios where such recognition fails, there is a risk of undermining the value of both tangible and intangible assets. Moving beyond these centralized and authoritative methods, a crucial aspect of current blockchain technology is the consensus algorithm, which democratically acknowledges value without a specific centralized authority, instead relying on the collective recognition of many individuals.



DRPoS (Delegated Random Proof of Stake)

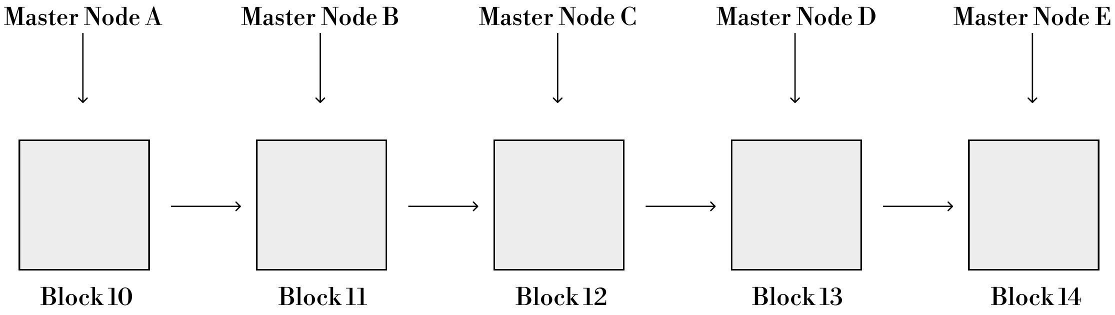
The block creation method in Bitcoin or Ethereum follows the first-generation PoW (Proof of Work) approach. Blocks are generated by finding a hash value of the block header, created by changing the nonce value through hash operations via GPU, that is smaller than the given bits value. This method requires high computational power equipment and has the drawback of high costs compared to the mining output.

To reduce these costs, several other Blockchain Mainnets like Quantum and NEO have devised a second-generation block creation method, PoS (Proof of Stake), where blocks are generated randomly and the probability of block generation gives priority to nodes with higher stakes. However, granting block generation priority to those with more stakes leads to the centralization of capital, distorting the essence of decentralization and posing a risk of a 51% attack.

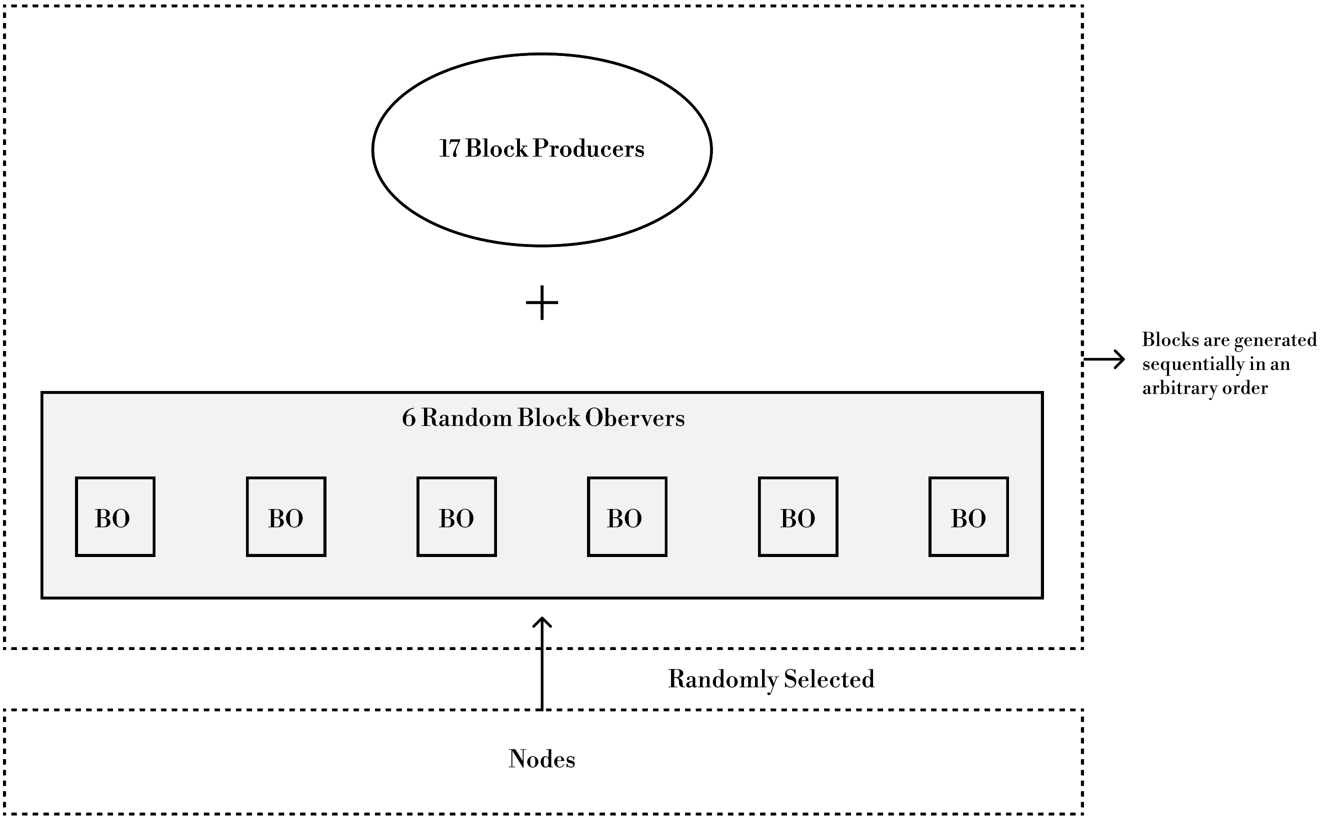
To address this issue, ARICHAIN has introduced the DRPoS (Delegated Random Proof of Stake) method, where 17 elected master Nodes (BPs) and 6 randomly selected Block Observers (BOs) together create blocks in random order to maintain the integrity of the entire blockchain.

Compared to the existing DPoS, which consists only of BPs, DRPoS strengthens blockchain integrity through a dual verification structure of BPs and BOs. BOs are randomly selected to participate in block creation alongside BPs, increasing the network's resistance to collusion or malicious attacks. This random selection of BOs prevents the concentration of influence in the block creation process and enhances the level of decentralization of the network.

Due to these advantages, Arichain's DRPoS consensus algorithm compensates for the limitations of the existing DPoS consensus algorithm, enabling the implementation of a more secure and decentralized blockchain network.

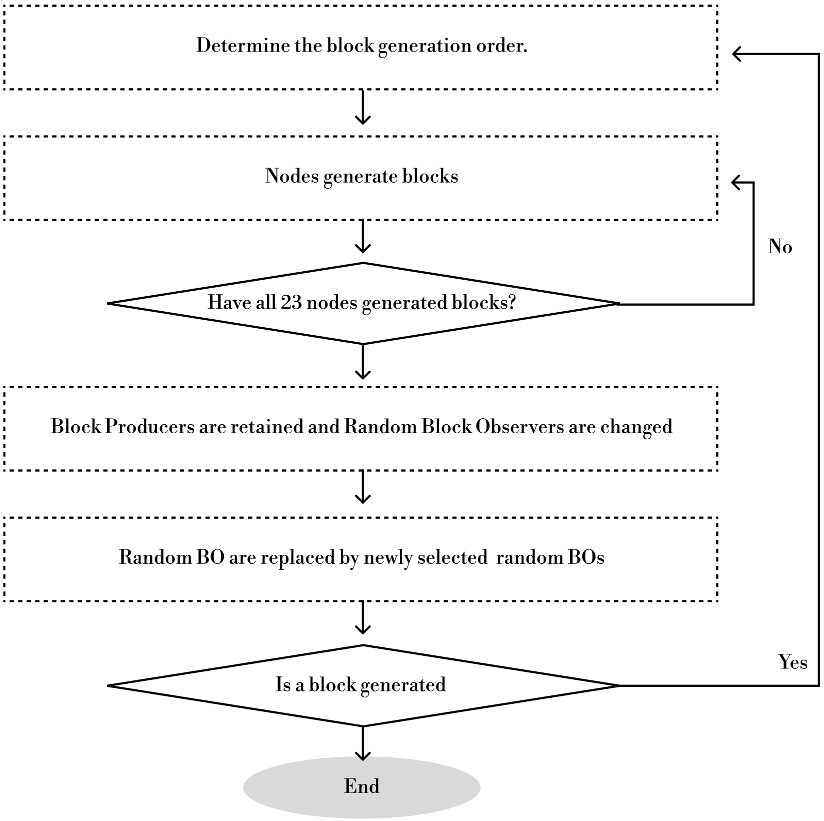


[Figure 2. Arichain Block Generation]

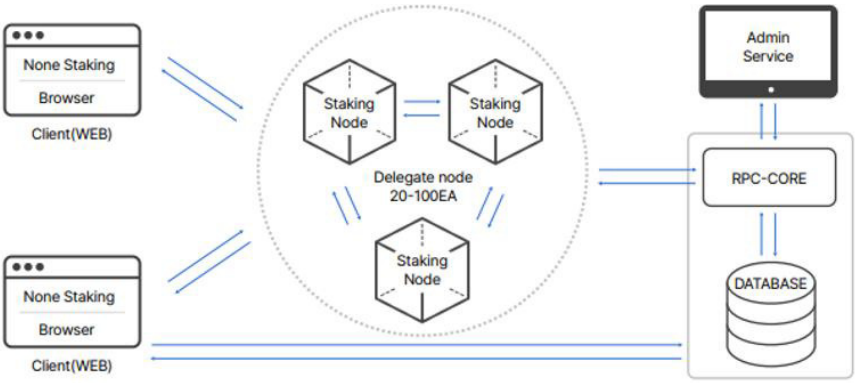


[Figure 3. DRPoS Algorithm

Figure 2 and Figure 3 depict the improved block generation structure according to the DRPoS algorithm. Referring to these, the present invention involves selecting a random number of nodes (BO) among the general nodes and having these nodes (BO) collaborate with the master nodes (BP) to generate blocks in random order.


Determine the block generation order.
Nodes generate blocks
Have all 23 nodes generated blocks?
No
Block Producers are retained and Random Block Observers are changed
Random BO are replaced by newly selected random BOs
Is a block generated
Yes
End

[Figure 4. Block Generation Flow]



[Figure 5. Arichain System Architecture]

Blockchain Communication

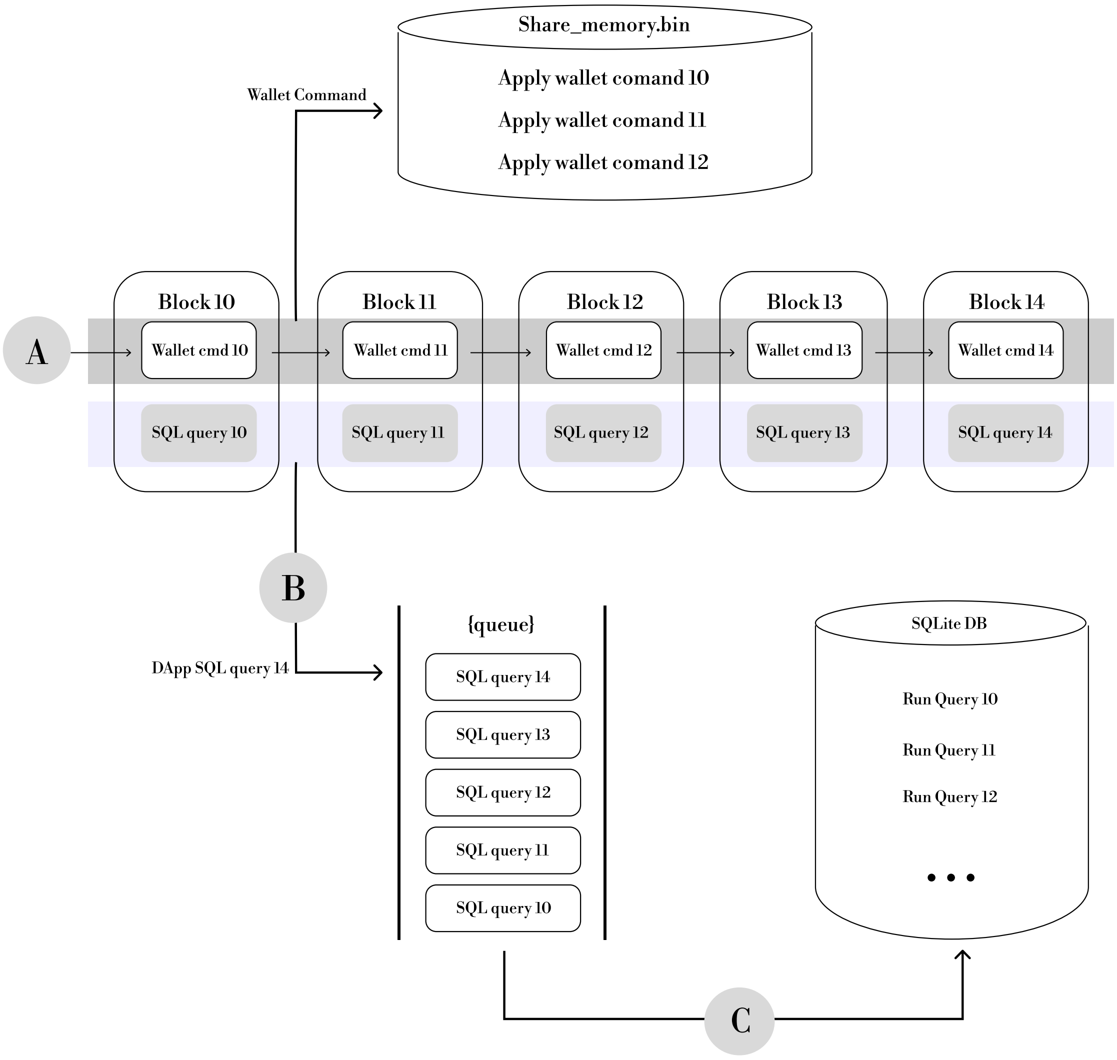
Arichain is designed to facilitate communication between blocks. During block production rounds, each node supports the validation of blocks and transactions. This allows for optimization of verification time and bandwidth by generating blocks with minimal overhead compared to using hash links, which is typical in block creation methods. With 23 block producers generating blocks every 3 seconds in a round, it takes a confirmed 69 seconds to determine irreversibility. This facilitates proving that transactions were not skipped or reordered, ensuring they are processed sequentially.

3. Smart Contract

In traditional blockchain mainnets, executing smart contracts involves writing program code, uploading contract transactions to the mainnet server, and compiling them, which incurs significant development time and complexity.
However, in Arichain, DApp developers can easily develop by simply calling APIs provided by the mainnet in their development environment. This provides DApp developers with a fast and stable development environment, greatly aiding the expansion of the mainnet ecosystem.

DApp Development Environment

DApp developers perform recording and querying on the blockchain using their Arichain Node.js Web API. As a result, they can save blockchain space by not compiling and loading source code binaries onto the blockchain. This also improves efficiency by avoiding the duplication of similar codes.



[Figure 6. Arichain Blockchain Architecture]

In determining the superiority of blockchain technology, the ability to accommodate and retrieve data as the volume of data increases, as well as the ability to process large amounts of data quickly and efficiently, are important validation criteria for Arichain technology.

When reviewing technical whitepapers, it is crucial to focus on key factors that can enhance the value of DApps. This includes support for fast data and API calls, creating a secure environment, convenience in development, fast transaction speeds, enhanced security, ease of debugging nodes, and accessibility of blockchain nodes, among others. Arichain leverages state-of-the-art technology detailed in this technical whitepaper to gain a competitive edge over other DApps. Our DRPoS consensus model stands unmatched in providing DApps with the fastest speeds, highest levels of security, scalability, and decentralization.

Furthermore, our API architecture provides an efficient, economical, and user-friendly processing environment. We continuously improve and incorporate our technology through ongoing development of the latest advancements.

4.Node Operating(Staking)

Staking serves as a foundational aspect of Arichain, enabling network security and consensus through the DRPoS (Delegated Random Proof of Stake) mechanism. By participating in staking, both BP and BO play a crucial role in maintaining and safeguarding the network, ensuring long-term stability, performance, and success. The DRPoS chain relies on economic value rather than computational power, providing a more energy-efficient and scalable system.

DRPoS (Delegated Random Proof of Stake) represents a fourth-generation approach that enhances the existing method. In this mechanism, 17 elected master nodes (BP) and randomly selected 6 (BO) collaborate to generate blocks in random order to maintain the integrity of the entire blockchain. This approach supplements the previous method and aims to provide a more robust and secure network infrastructure.

In the DRPoS system, token holders stake their tokens to vote for BP or act as BO to generate new blocks, thereby contributing to the health and growth of the Arichain ecosystem for developers and users.

Arichain incentivizes BP, BO, and token holders who vote (stake) for BP through gas fee rewards and inflation rewards for newly issued ARI tokens. Newly issued ARI tokens are distributed to BP and BO annually at a fixed rate, and once block verification is completed, fees and inflation rewards are distributed to BP and BO. BP retains a portion of the rewards as commission, while the remainder is distributed to BO and the delegators.

Some of the generated block rewards and transaction fees are allocated to the storage fund. As time passes, the storage capacity that nodes must maintain increases significantly. From the perspective of a full node, which must retain all blocks from the genesis block to the current one, time and storage capacity are directly proportional. Therefore, to ensure the long-term sus tainability of the blockchain, there needs to be an economic incentive capable of accommodating extensive storage, even as time progresses. As a result, Arichain aims to create a storage fund to provide appropriate storage rewards to nodes participating in the network in the future.

System Requirements for Node Operations

Node	CPU	RAM	HDD	N/W
BP	16core	128gb	1tb	1tb
BO	2core	8gb	128gb	100mb

Node reward & penalty

Details are as follows.

Annual Inflation Reward, AIR:

$$\text{AIR} = \text{TotalSupply} \times \text{InflationRate}$$

TotalSupply: Total token supply of Arichain (e.g.,500 million ARI)
InflationRate: Annual inflation rate (1.5%)

Storage Fund Allocation, SFA:

$$\text{SFA} = \text{AIR} \times 0.1$$

Block Producer Inflation Reward (BPIR):

$$\text{BPIR} = (\text{AIR} - \text{SFA}) \times 0.7$$

Delegator Reward (DR):

DR = BPIR × 0.9
Individual Delegator Reward = DR × (Individual Delegator's Votes) ÷ (Total Votes from All Delegators)

Block Producer Actual Inflation Reward (BPAIR):

BPAIR = BPIR × 0.1
Individual BP Actual Inflation Reward = BPAIR × (Individual BP's Votes) ÷ (Total Votes from All BPs)

Block Observer Inflation Reward (BOIR):

BOIR = (AIR - SFA) × 0.3
Individual BO Inflation Reward = BOIR ÷ (Total Number of BOs)

Transaction Fee Reward (TFR):

TFR = Total Transaction Fees Included in the Block

Block Producer Total Reward (BPTR):

BPTR = Individual BP Actual Inflation Reward + Total Transaction Fees from All Blocks Validated

Block Observer Total Reward (BOTR):

BOTR = Individual BO Inflation Reward + Total Transaction Fees from All Blocks Validated

In this reward formula, 10% of the annual inflation reward is allocated to the storage fund. The storage fund is used to securely preserve blockchain data in the long term and compensate node operators for their storage costs.
The introduction of the storage fund is expected to increase the long-term sustainability of the Arichain network and provide node operators with stable rewards. Additionally, it is expected to enhance the trust of users by ensuring the integrity and availability of blockchain data.
The inflation rewards for BP and BO are calculated based on the remaining inflation rewards after allocating to the storage fund.

The reward and penalty structure in Arichain serves to incentivize Block Producers (BP) and Block Organizers (BO) to fulfill their responsibilities in block validation and contribute efforts to the network's activation. Transaction fee rewards are proportional to network usage, motivating BPs and BOs to process more transactions and enhance the efficiency of the blockchain.

The reward and penalty structure are delicately parameterized considering these factors. Validators receive relatively large rewards when given the opportunity to create blocks. Essentially, the system provides more rewards as validators actively engage in the network. In summary, the requirements to become a validator within Arichain aim to maintain participation as accessible as possible while ensuring a stable and robust network.

The reward and penalty system serve as mechanisms that guide the blockchain network towards security enhancement. Rewards should be designed to encourage honest and diligent participants to continue contributing to the network. Conversely, penalties should be in place to deter or swiftly remove participants who may harm the network. However, caution is needed to ensure that overly strict penalties do not create psychological barriers that hinder participation.
Penalties for non-participation ensure that the punishment is not overly punitive, balancing potential rewards with temporary operational pauses, such as short node downtime. However, direct threats to consensus activate strict rules to apply robust penalties.

If a BP or BO is offline or fails to participate in block creation, they will not receive rewards for that period. In the case of block creation failure, BPs are penalized with a deduction of 0.03% of the staked amount for each failure, while BOs face a deduction of 0.01% of the staked amount per failure. If more than 5% of the staked assets are slashed, both BP and BO qualifications are revoked.

Double Signing:
If BP and BO sign two or more different blocks for the same height, 5% of the total staked tokens are immediately slashed, and the BP qualification is automatically revoked.
Improper Block Creation or Validation::
If BP and BO create or validate blocks containing invalid transactions, they face penalties such as slashing. If confirmed, 5% of the total staked tokens will be slashed, and the BP/BO qualification will be automatically revoked.

5. Conclusion

Arichain: Inclusive Innovation Towards Decentralization
Blockchain technology holds the potential to revolutionize our society, yet its possibilities are still limited by issues of mass adoption and accessibility. Many projects remain technically innovative but are confined to areas understandable and usable only by a select few experts. Arichain aims to tackle these challenges head-on and build a true decentralized ecosystem where everyone can participate freely.

At the core of Arichain is the DRPoS (Delegated Random Proof of Stake) consensus algorithm. We recognize the limitations of existing DPoS systems and have introduced the Block Observer (BO) system, randomly selecting nodes to participate in block creation. This decentralizes the power concentrated among a few Block Producers (BP) and allows more participants to contribute to network decisions. DRPoS achieves both security and decentralization, laying the foundation for Arichain to become a trusted blockchain platform.

However, technical innovation alone is not enough. Arichain values user-friendliness and accessibility. We are developing intuitive and simple user interfaces to enable anyone to easily participate in the Arichain network, even without specialized knowledge, and providing educational materials and guidelines is one of Arichain's important tasks. We believe that the true value of technology lies in how it enhances people's lives.

Furthermore, Arichain pursues the value of inclusivity. We hope that people from diverse backgrounds and perspectives can participate in the Arichain ecosystem. To achieve this, we are building a fair and transparent governance system and actively listening to the community's opinions. Decision-making in Arichain is based on the consensus of the entire community rather than the influence of a few. We are confident that this inclusive approach will lead to the healthy development of Arichain in the long run.

Moreover, Arichain aims to bring about tangible changes in real life. We believe that decentralized technology can innovate in various fields such as finance, healthcare, and education. To this end, Arichain encourages the development of dApps that can be applied in real-life scenarios and promotes blockchain mainstreaming through partnerships. Our vision is not just to gain technological superiority but to lead positive changes throughout society via blockchain.

Arichain challenges the entry barriers and inequality of opportunities that have dominated the blockchain industry so far. Through innovation spanning technology, community, and the real world, we aim to create a decentralized future for all. Inclusivity and accessibility are the core values of Arichain.

The lens through which we envision the future of the chain. Our journey has just begun. Let's create a new world together with Arichain, where everyone is free, fair, and empowered.