

# BOSCoreTechnicalWhitePaper

---

## NOTICE AND DISCLAIMER

----

PLEASE READ THE ENTIRETY OF THIS “NOTICE AND DISCLAIMER” SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER BOS FOUNDATION LTD. (THE FOUNDATION), ANY OF THE PROJECT TEAM MEMBERS (THE BOS TEAM) WHO HAVE WORKED ON THE BOS NETWORK (AS DEFINED HEREIN) OR PROJECT TO DEVELOP THE BOS NETWORK IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF BOS TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT <https://boscore.io> (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

All contributions will be applied towards the advancing, promoting the research, design and development of, and advocacy for an EOSIO ecosystem that supports more DApp and solve real-world problems through the usage of blockchain technology. The Foundation, the Distributor and their various affiliates would develop, manage and operate the BOS Network.

The Whitepaper and the Website are intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, the Distributor, and/or the BOS team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Foundation nor the Distributor is under any obligation to update or correct this document in connection therewith. Nothing in the Whitepaper or the Website constitutes any offer by the Foundation, the Distributor or the BOS team to sell any BOS (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the

future performance of the BOS Network. The agreement between the Distributor and you, in relation to any sale and purchase of BOS is to be governed by only the separate terms and conditions of such agreement.

By accessing the Whitepaper or the Website (or any part thereof), you represent and warrant to the Foundation, the Distributor, its affiliates, and the BOS team as follows:

- (a) in any decision to purchase any BOS, you have not relied on any statement set out in the Whitepaper or the Website;
- (b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);
- (c) you acknowledge, understand and agree that BOS may have no value, there is no guarantee or representation of value or liquidity for BOS, and BOS is not for speculative investment;
- (d) none of the Foundation, the Distributor, its affiliates, and/or the BOS team members shall be responsible for or liable for the value of BOS, the transferability and/or liquidity of BOS and/or the availability of any market for BOS through third parties or otherwise; and
- (e) you acknowledge, understand and agree that you are not eligible to purchase any BOS if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of BOS would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, New Zealand, People's Republic of China (but not including the special administrative regions of Hong Kong and Macau, and the territory of Taiwan), the Republic of Korea and the Socialist Republic of Vietnam).

The Foundation, the Distributor and the BOS team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation or the Distributor). To the maximum extent permitted by law, the Foundation, the Distributor, their affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of BOS should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the BOS token sale, the Foundation, the Distributor and the BOS team.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of BOS, and no virtual

currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of BOS and/or continued holding of BOS shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of BOS (the Terms and Conditions), which shall be separately provided to you or made available on the Website. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

No regulatory authority has examined or approved of any of the information set out in the Whitepaper or the Website. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

The information set out herein is only conceptual, and describes the future development goals for the BOS Network to be developed. The Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or the BOS team may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Whitepaper, and the Foundation, the Distributor as well as the BOS team expressly disclaims any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

The use of any company and/or platform names or trademarks herein (save for those which relate to the Foundation, the Distributor or its affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Whitepaper or the Website to specific companies and platforms are for illustrative purposes only.

The Whitepaper and the Website may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.

No part of the Whitepaper or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Foundation or the Distributor.

## Blockchain financial center building a trusted business ecosystem.

September 2018 V1

November 2019 V2

- [Background](#)
- [Overview](#)
- [Consensus Algorithm](#)
- [Interchain Communication](#)
- [Oracle](#)
- [Scaling Out Solution](#)
- [Post-Quantum Encryption Solution](#)
- [Scaling out Plan based on Zero-knowledge Proof](#)
- [Pegged Coin](#)
- [Accounts](#)
  - [Guaranteed Minimum Provision](#)
  - [Free Account Creation through Red Packet](#)
- [ThunderNode](#)
- [Enhanced Usability](#)
  - [Safer Random Number Scheme](#)
  - [Configurations on Chain](#)
  - [More Plugins](#)
  - [Producing Schedule according to Time Zone](#)
  - [P2P Self-Discovery](#)
- [Ecosystem Model](#)
  - [Issuance Method](#)
  - [Developer Incentives](#)
  - [Governance Model](#)
  - [Economic Model](#)
- [Conclusion](#)
- [References](#)

## Background

The emergence of EOS has brought a new paradigm to the blockchain. In just a few months since the main network was launched, the version has undergone dozens of upgrades, stability has been greatly improved, new functions have been gradually developed. The node team is also actively involved in building the EOSIO ecosystem. What is even more exciting is that EOS has attracted more and more development teams. There are already hundreds of DApp running on the EOS main network. market value in circulation far exceeds that of Ethereum, and the space for development is growing wider.

During the gradual development of the EOS main network, the BOS team has found some deviations from prior expectations. As the most competitive third-generation public chain, the BOS team looks forward to seeing more and more applications running on EOS. Developers will use EOS as their preferred platform for application development. But due to the limitations of the current EOS resource model, higher costs of usage have resulted from the creation of more user accounts and deployment of operating DApps. The key technology IBC required for the realisation of the millions of TPS described in the white paper has not been promoted. The main network has repeatedly experienced situations of insufficient CPU computing resources, which has intensified the urgency of its demand for cross-chain communication. In addition, due to the Pipeline-DPOS consensus algorithm adopted by EOSIO, a transaction requires nearly three minutes to ensure that it is finalised and immutable. Although performance in this regard is much better in comparison to Bitcoin and Ethereum, it also brings restrictions to many EOS application scenarios. Fast payment mechanisms can only be directed towards small transfers, large transfers require a certain waiting time to ensure that they cannot be changed, which limits the user experience with regards to payment services on the chain and under the chain.

In addition to the abovementioned issues, there are many other potential improvements that have been actively discussed within the EOS community. As a result the BOS team believes that more experimentation should be done on EOS and more developers or teams rallied to participate in the building of the EOSIO ecosystem. Together, ecosystem participants will make efforts towards application of the blockchain towards different scenarios within different industries. BOS will become the first DPoS public chain that realizes decentralized cross-chain and has consensus. It is committed to using technology to create a trusted business ecosystem.

## Overview

The BOS Network is committed to providing users with easy-to-access and easy-to-use blockchain services, providing a more user-friendly infrastructure for DApp operations, working to support richer application scenarios, and actively promoting prosperity in trustless commerce. In addition to technical improvements, the BOS Network will also make attempts to improve in other areas. For example, in order to increase the level of participation of users in voting, estimator technology can be used to incentive accounts that meet certain predefined parameters. The incentives for BP (block producers) on the BOS Network will be adjusted according to the number of DApps on the chain, TPS, market value, liquidity and other indicators. Each BP incentive awarded is an encouragement for providing provision of more resources for the ecosystem. A resolution reached by a community referendum to the ecosystem. Changes to parameters on the BOS Network will be coded algorithmically executed as much as possible, to reduce human factors in within the process, keep the process on chain, and maintain fairness and transparency.

The codes of the BOS Network chain are fully contributed and maintained by the community. Each ecosystem participant can submit codes or suggestions. The related process will take reference from existing open source software projects, such as PEP (Python Enhancement Proposals).

In order to encourage the development of DApps in the BOS Network, the BOS Foundation will provide Token driven low-cost resource mortgage services for DApps in the BOS Network, reduce the operating costs of DApps in the initial development stage; in addition, it will also regularly provide BOS token incentives to developers who contribute on a regular basis in order to establish a mutually reinforcing community development trend.

## Consensus Algorithm

EOSIO uses a pipelined Byzantine Fault Tolerance system. For a block, Propose, Pre-Commit, Commit, Finalise [1] are required stages. The last unchangeable block will be marked by Last Irreversible Block (LIB). A transaction basically takes about 3 minutes (the theoretical minimum is 325 block time, that is, 162.5 seconds) to enter LIB, although the transaction reliability time is better than that of other digital assets such as BTC and ETH. However, there are still many limitations for many application scenarios. For example, in the payment scenario, because it is not immediately determined whether the success of transaction is successful at the endurable to be instantaneously determined, it takes a period of time to complete the transaction of the commodity, which adds a lot of restrictions to its practical use.

The long confirmation time for transactions due to DPOS BFT consensus algorithm, in which the acknowledgment information after all blocks are synchronised will only be broadcast when it is the turn of the relevant node. For example, in the case where BP1 is to produce block (the block is BLK<sub>n</sub>) and BP1 ~ BP21 take turns to produce the block, BP2 ~ BP21 will receive and verify BLK<sub>n</sub> one by one. However, all BPs can only wait till their turn to produce a block before they can send a confirmation message about BLK<sub>n</sub>.

After analysing the problem of the EOSIO consensus algorithm, in order to shorten the time required before a transaction becomes unchangeable, the BOS Network will use PBFT (Practical Byzantine Fault Tolerance [2]) instead of Pipelined BFT. In this way, BP is able to confirm the blocks immediately. The confirmation of blocks in real time enables the entire system to eventually to approach a near real-time consensus speed.

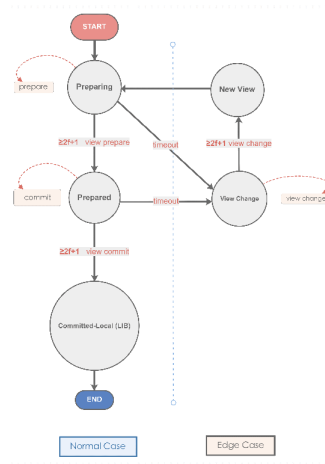
The consensus algorithm of the BOS Network is based on the PBFT theory, combined with the EOSIO code to improve, under the premise of ensuring Byzantine fault tolerance, the following changes will be made:

- 1. The mechanism of the Pipelined BFT's BP round outflow block is retained, and the synchronous clock and the block orders are strongly constrained similar to EOS.

- 2.Remove the logic of the Pipelined BFT Consensus section by removing the implicit confirm and (explicit) confirm sections from the original block to avoid conflicts with PBFT consensus results in edge cases.
- 3.Consensus communication mechanisms using existing p2p networks will use the PBFT mechanism to broadcast prepare and commit information and ensure communication costs are within acceptable limits.
- 4.The batch consensus is used to replace the requirement of consensus for each block in PBFT, and the ideal information of real-time BFT is approached and the network load is reduced through broadcasting the related information of multiple blocks at a time.

The status of the PBFT on the BOS Network is described as follows:

- **Pre-prepare**, indicating that after a block is produced, it is broadcasted to all other producing nodes in the network. It can be analogised to BP in EOSIO and broadcasting to the whole network.
- **Prepare** means that a producing node will broadcast the request to the entire network after receiving the request. It can't be analogised to the broadcasting of received information after all the nodes in EOSIO receive the block and verify successfully.
- **Commit** means that a producing node receives enough prepare messages for the same request and broadcasts the request to the entire network. It can be analogised to the node in EOSIO receiving enough prepare messages for the same block, and proposing a proposed lib message.
- **Committed-local** means that a producing node receives enough commit messages for the same request and completes the verification. It can be analogised to LIB promotion in EOSIO.
- **View** change means that a producing node loses the trust of other nodes for various reasons, the process of the whole system changes the producing node. Since EOSIO adopts the Pipelined BFT algorithm, all BPs are determined in advance by voting. Within one BP schedule, the order of the whole system is completely unchanged. When the network is in good condition and the producing node has not changed, it can be considered that there is no view change state. After the introduction of PBFT, in order to avoid the fork which may cause the consensus to become unable to advance, the view change mechanism is introduced. All unconsented information is discarded and consensus procedures are continually attempted until the consensus is made.
- **Checkpoint**, which refers to the recording of consensus evidence at a block height to provide a proof of security. This checkpoint is considered stable when there are enough producing nodes with the same checkpoint. The generation of checkpoints is done according to two major categories: one category consists of fixed block generation, and the other consists of special pointpoints that are structurally requires the provision of security proof, such as a block in which the block BP schedule changes.



Through observation of the existing EOS main network, the network delay between the global nodes is mostly within 1 second. According to the consensus algorithm of the PBFT of the BOS Network, consensus is projected to take 3 seconds to achieve immutability in most scenarios (pre-prepare, prepare, commit). Shortening the trusted time of a transaction from minutes to seconds will allow many scenarios to be implemented on the BOS Network.

## Interchain Communication

In the EOSIO technology white paper, interchain communication is used as a solution for high-concurrency and to construct flow channels between multiple chains. For the blockchain, TPS affects the throughput capacity of the entire blockchain system. The essential issue of cross-chain communication is to justify the credibility of transactions between various chains. Heterogeneous blockchain systems (such as EOS, ETH) have great differences in block generation speed, internal data structure, and consensus mechanism. Therefore, the implementation of heterogeneous decentralized cross-chain is relatively difficult. It is more practical to verify transactions between different chains based on EOSIO.

The basis for decentralized cross-chain communication is Light Weight Client and SPV/Simple Payment Verification. The Light Weight Client is a chain consisting of block heads, excluding the block bodies, so the Light Weight Client only takes up very little space. the SPV technology uses the merkle path to prove whether a transaction exists in a certain block [3].

The advantages of BOSCore cross-chain scheme are as follows:

1. Completely Decentralization. The Light Weight Client is implemented in the smart contract. When the correct starting block information is initialized, the contract can fully verify the validity of all subsequent blocks without relying on the trust of the relay or contract external information.
2. Light Weight. The Light Weight Client does not need to continuously synchronize all the block heads of the original chain, and only needs to synchronize a part of the segment of the blockchain to obtain a trusted block for verifying the transaction.



3. Fast Cross-chain Transactions. A cross-chain transaction takes less than 3 minutes from the generation to the conduction of corresponding transaction on the target chain.
4. Parallel Cross-chain Transactions. Different cross-chain transactions do not affect each other and can be executed in parallel, thus supporting a large number of concurrent transactions.
5. Safe. Due to the producer signature verification and strict logic check, the correctness of the Light Weight Client itself can be guaranteed and it cannot be maliciously attacked, so the authenticity of the transaction can be verified safely.

BOS provides a redemption channel with the EOS main chain based on the IBC scheme. EOS can be easily circulated between the BOS side chain and the EOS main chain, including other high-quality digital certificates on the EOS; similarly, BOS will advance to establish circulation channels with other EOSIO-based sidechains. And the entire EOSIO ecosystem begins to move into an ecological network. BOS will serve as a core circulation link to accelerate the development and evolution of the entire EOSIO ecosystem.

## Oracle

The oracle machine is a concept of Turing machine model. Due to the halting problem and mathematical incompleteness, you will get some unexpected results that a standard Turing machine. It is deterministic in the Turing machine, but the oracles in the blockchain are difficult to get theoretically defined characteristics. The reason is that the blockchain itself is built on fault-tolerant logic. It does not require certainty of input, and even allows deceptive behavior. This is also a fundamental difference between the oracles in the blockchain and the traditional oracles.

Facing the problem of untrusted oracles, simple deterministic computing models are not feasible. To this end, we try to introduce a game system model to solve these problems. In a nutshell, the oracle is not simply regarded as the system's information supply point, but it is regarded as the participants of the game and the information users to build a game model together. It also establishes a credible commitment by introducing a punishment mechanism and a multi-round arbitration mechanism. The information selection mechanism of multiple information providing data resources to reach Schelling point, thereby improving the credibility of the information. In addition, by introducing auditors and adding a joint reward and punishment mechanism, we construct The prisoner's dilemma in the role of information provider further guarantees credibility.

The design of some oracle services is based on the assumption that trusted data sources or authoritative data sources. Such assumptions are theoretically very risky and cannot guarantee the authenticity of data provided by such data sources. The principles of BOS 'oracle system from the beginning of construction are:

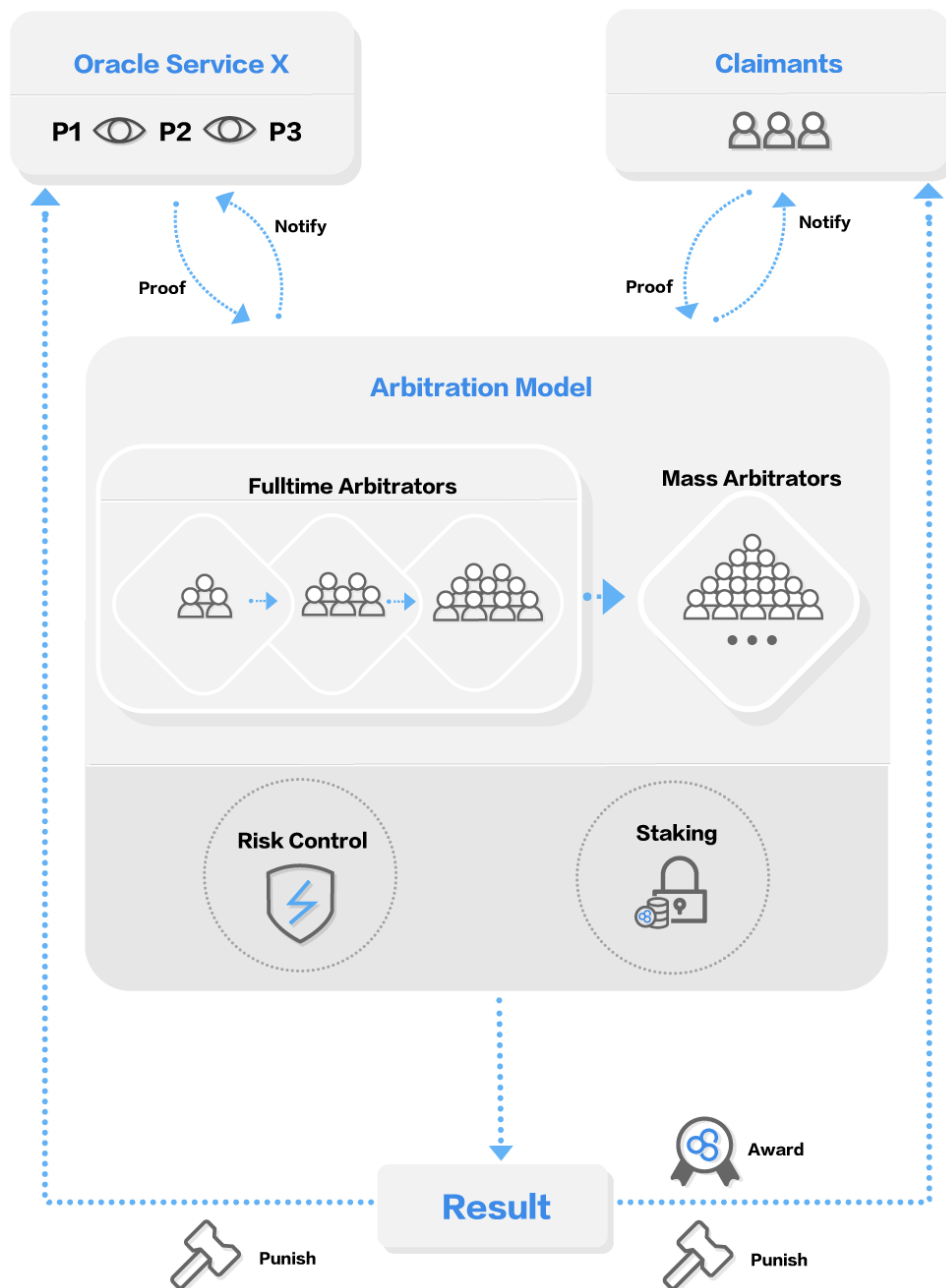
Not relying on each oracle machine data provider to provide real data, but admit its deficiencies.

And take them into consideration in order to achieve overall credibility in the game.

In this way, as long as the participants and the real world roles are mapped during the game, not only can we gain the credibility of the input data of the blockchain, but we can also output "trust" to the real world. In fact, this is more like a trusted platform based on blockchain, and its service display form is a oracle.

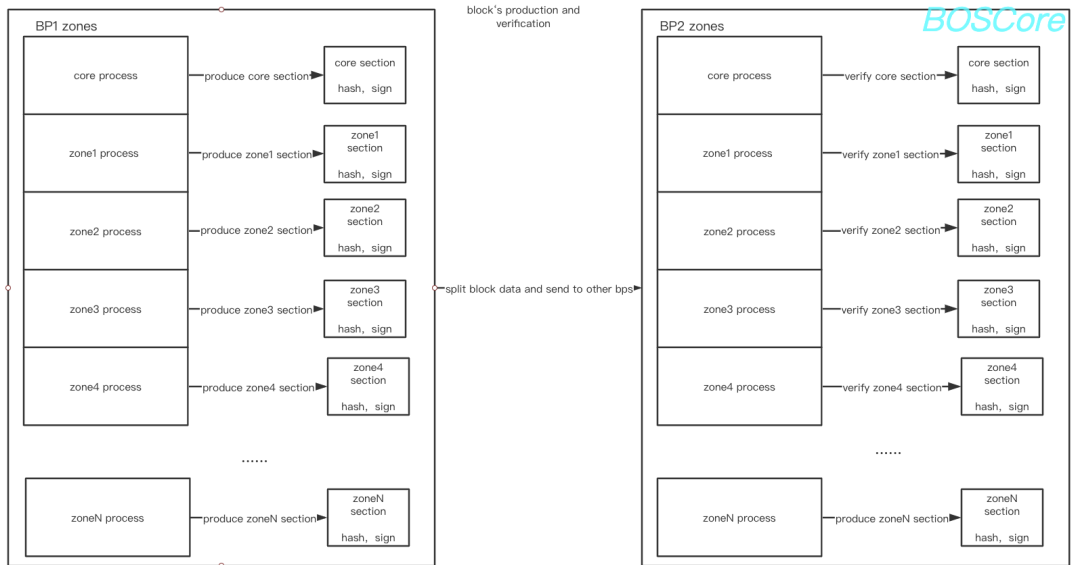
BOS oracle will extend the value of the blockchain from its monetary attributes to the construction of transactions and rules. This extension will solve or improve many real-world trust issues, thereby expanding the application boundary of the blockchain, and eventually Let blockchain technology land in scenarios other than transaction transfers.

# BOS.Oracle Game Model

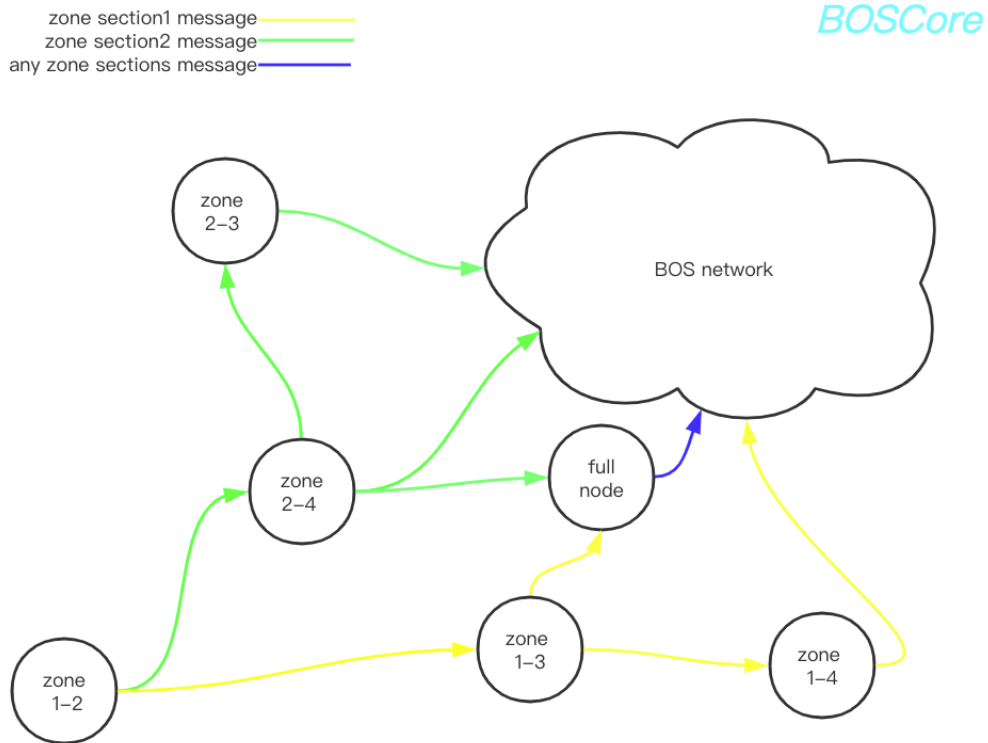


## Scaling Out Solution

BOS is actively promoting and exploring broader Scaling out solution. Abstractly speaking, the smart contracts running on the blockchain are relatively independent of high-probability events. Therefore, it is feasible to divide different smart contracts from a global perspective for concurrent execution. so the Scaling out solution based on isolated calculation was proposed. This solution will redefine the roles and block structure of the nodes in the network, in order to leverage on horizontal Scaling out to improve the overall BOS chain loading capability.



The concept of "zone" is introduced in the solution. Transactions between each computational zone are processed in parallel, and block generation and execution are performed simultaneously. The BOS mainnet will become the "core computational zone", which will take charge of the account and token systems. Relevant data will be synchronized to each zone.



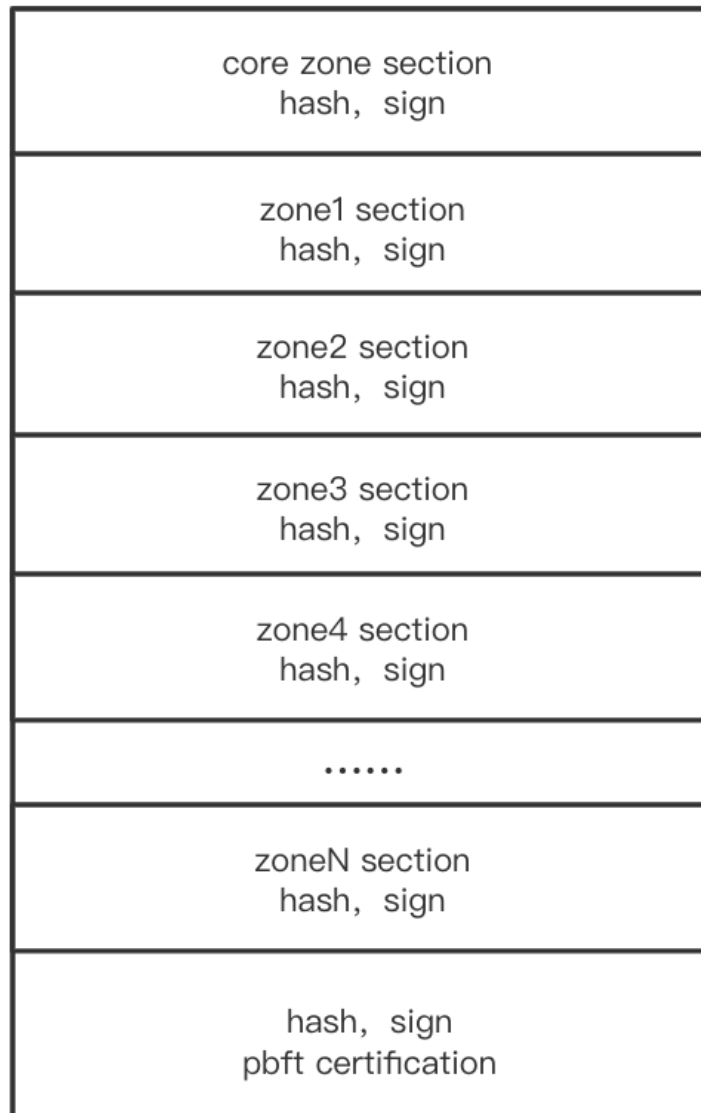
There are three types of network node: BP node, broadcast node and data node: BP nodes are responsible for signing and executing the transactions concurrently. Broadcast nodes can accelerate data synchronization. Data nodes can be configured to verify the different sections within the block. This will realize consensus security and maintain its anti-attack characteristics on the premise of ensuring decentralization.

After adopting the multi-zone parallel scheme, the block structure needs to be adjusted to achieve the purpose of reducing network traffic and faster consensus. The

new block structure will contain the data of each computational-zone, different section will be verified separately.

block structure

*BOSCore*



To ensure the trustworthiness of data, BOS will introduce a new trusted query function. In summary, credible data query not only needs to provide the target data, but also needs to provide sufficient evidence. The data on chain will be restructure into MVCC record structure. Each change will increase the version number of the data record by one, while retaining the previous data history. In this design mode, given the height of a transaction, we can quickly queried corresponding to that height of the global state. A Merkle Tree data proof based on the state can be generated.

The horizontal scaling out plan will be implemented simultaneously with the multi-threaded solution. With decentralization and data security, the horizontal and vertical Scaling out of computing resources will be achieved, thereby laying a solid foundation for achieving the goal of one billion users.

## Post-Quantum Encryption Solution

With the development of quantum computer technology and the realization of quantum hegemony, general-purpose quantum computers are no longer the holy grail. Quantum computer will bring a series of profound changes in the foreseeable future. The collapse of asymmetric cryptosystems based on large number decomposition and discrete logarithm is one of the most significant features in the transformation. The ECDSA signature algorithm currently used by BOS is also hacked, so we will introduce a new anti-quantum encryption system to solve the above challenges.

Among the many quantum-resistant cryptosystems, The lattice cryptosystem will be chosen as the main architecture for BOS quantum-resistant cryptography. NTRU (including encryption and signature) will be the main encryption system. FrodoKEM and Spincs+ will be taken as the backup encryption system.

Considering that the lattice encryption system has not been theoretically completed and the international post-quantum cryptographic standard is under development. BOS will keep the capability to support multiple cryptographies. Meanwhile, the lattice-based cryptographic signature system can also facilitate the construction of quantum-safe anonymous coins. This design will give the maximum scalability for BOS, while preserve the maximum support for multi-cryptosystem and dramatically reduce the risk from failure of single cryptosystem.

## **Scaling out Plan based on Zero-knowledge Proof**

For the blockchain, TPS that affects the overall capability of entire blockchain system and determines the boundaries of the application quantity. In addition to promoting multi-threaded and multi-computation zone Scaling out solutions, based on the research and accumulation of the knowledge for Zero-knowledge Proof, BOS will also consider Scaling out solutions based on it.

Considering the smart contract execution plan are determined and limited, so we can improve and optimize the existing zero-knowledge proof solution to meet the functional requirements, meanwhile, according to the characteristics of different contracts, the compute-intensive contracts can be executed in zone-knowledge proof mode, and the others can be executed in the normal VM scheme. In this way, the computational efficiency can be maximized.

## **Pegged Coin**

In order to enrich the economic ecosystem of the entire chain, in addition to using the IBC mechanism to establish a distribution channel with the EOSIO main network, the BOS Network will also adopt the “Notary Schemes” to map BTC and ETH to the native chain of the BOS Network in conjunction with the world’s top exchanges. Through this

trusted channel, both BTC and ETH can easily achieve cross-chain circulation on the BOS Network. This means that for DApps running on the BOS Network, while supporting EOSIO ecosystem digital assets, digital assets under other consensus algorithms can also be supported. In addition, this method can also be used as a solution to improve the liquidity of some coins with low TPS.

The BOS Network will provide a mechanism for issuing 1:1 secondary pegged virtual tokens for different digital passes and authenticate the identity of trusted intermediaries through BP multi-signatory mechanism. Every trusted intermediary needs to stake a certain quantity of BOS. Organizations or companies with sufficient strength and credibility can apply for “notary” status. When 25 of the top 30 BPs are passed, the secondary pegged virtual currency can be issued.

## **Accounts**

### **Guaranteed Minimum Provision**

Since the EOS main network came online, for ordinary token holders, it is often the case that a transfer fails due to insufficient staked resources. In this case, the only option for users is to ask others for help, which results in poor user experience and intensifying entry barriers.

For a chain, the growth of an active user population will promote the development of the chain, and also promote the development of DApps on the chain, this is vital to the entire ecosystem. In order to solve this problem, the BOS Network implements an improvement. The free resource quota allocated to each user can be adjusted through the parameters of the native blockchain, which is equivalent to a social security system on the BOS Network. In this way, the basic daily transfer needs of most users can be met, thus, there is no need to worry about the inability to use the chain functions due to the lack of initial resource stake. For users with greater usage requirements, resource usage beyond the minimum amount of coverage still needs to be delegated.

### **Free Account Creation through Red Packet**

For the EOSIO main network, account creation costs pose a problem that cannot be ignored. The BOS Network is aimed at enriching the DApp usage on the chain, so it also provides a solution to the cost of creating accounts for users. Referring to the example of handing out a red packet in real life, the BOS Network will build a community-developed “red packet DApp” and will continue to provide a certain amount of free account creation opportunities through the BOS Foundation. Other DApp project parties or organisations can easily create accounts for users free of charge

through red packets. The red packet DApp-related functions can be accessed through the official website or through the access points provided by each BP.

## ThunderNode

By improving the consensus mechanism, the reliable time of a transaction on the BOS chain can be shortened to less than 3s. This time is still somewhat different from the centralized system. Therefore, in order to meet the needs of such a semi-centralized system, BOS will provide a node that can achieve millisecond-level confirmation, called ThunderNode.

Similar to Lightning Networks, most of ThunderNode's transactions are done within a local network, and ThunderNode will ensure that transactions are visible on the BOS Network and cannot be changed. Once the user decides to use a certain ThunderNode, they need to lock part of the balance tokens. This part of the balance can only be used in the ThunderNode. When one decides not to use ThunderNode, the remaining locked BOS can be unlocked and restored to normal use. Once a user chooses to use the ThunderNode and locks a certain number of tokens, he or she needs to send the registration on the BOS Network and wait for it to take effect before he or she can start using it.

The role of being an operator of ThunderNode is completely open to competition. There are no hard restrictions. Users can also choose in accordance with their own needs. ThunderNode providers can obtain token remuneration through charging a certain service fee.

## Enhanced Usability

### Safer Random Number Scheme

At present, the known random number schemes in EOSIO are basically combined with multiple predictable fields, such as blockid, timestamp, etc. as part of a random seed, and then combined with the user side, DApp side or directly generated by the DApp offline. This type of solution involves certain security risks, cannot reduce the dependence on the credibility of the DApp side, and cannot avoid some replay attacks (such as `INLINE_ACTION` form). In response to the above problem, the BOS Network enables the `block_extension` feature and provides the `bpsig_action_time_seed` scheme. `bpsig_action_time_seed` not only prevents replay attacks, but also requires the signature private key signature of the BP node to be signed, and saves the generated seed into `block_extension` for other nodes to verify.



Combined with `bpsig_action_time_seed`, a safer random number scheme involving users, nodes, and DApp parties can be built.

`bpsig_action_time_seed` is generated as follows:

```
1 bpsig_action_time_seed = sign(BP_Sign_Key, F(block_timestamp, 0.5) +  
  global_action_sequence)
```

Note:

- `BP_Sign_Key`: The purpose of signing with a BP private key is to prevent others from a speculative calculation.
- `F`: The down integral function of `block_timestamp` by 0.5, and the BP adjustment timestamp is lowered to make the probability of speculation.
- `Global_action_sequence`: global action auto-increment flag, used to prevent `INLINE_ACTION` attacks.

## Configurations on Chain

Some design details of EOSIO are not precise enough, and the black and white list configuration is a good example of this. Due to the black and white list configuration problem, at least two frozen accounts are invalidated.

The BOS Network will put such public configuration information, such as black and white lists, on chain. BP will be valid after multi-signature, to avoid the failure of the configuration at some points due to other reasons and cause losses. The BOS Network will not only focus on the development of important features, but will also achieve more with regard to basic details.

## More Plugins

For the need to monitor the specific transaction situation of an account, the solution is more complicated for the current EOSIO, and is often implemented through the kafka plugin. This is another feature that is really needed for DApp, wallets or exchanges. For functional points that are generally required, the BOS Network will support it. The BOS Network has a built-in Notify Plugin that provides a similar method to the History Plugin, enabling a low-cost, fast access to account monitoring services.

In addition, the BOS Network will integrate the excellent plugins in the community to reduce the cost of compilation and make it easier for developers to use.

## Producing Schedule according to Time Zone

EOSIO currently uses the lexicographic order of the BP account name to produce blocks. From the observed effects of actual operations, this often leads to multiple small forks: the last 2–4 blocks cannot be broadcast to the next block BP in time. In order to reduce the network delay between two BPs, the BOS Network will use the time zone order to produce blocks, reduce the physical distance and avoid network jitters that cause small forks.

The BOS Network plans to build a network that uses dedicated lines to interconnect each node in addition to the normal connection network to ensure higher quality and low latency transmission of block data.

## **P2P Self–Discovery**

In the implementation of EOSIO, the connection with those nodes depends on the static configuration of the configuration file. When a new node joins, only published information can be obtained from other regions, but the published information cannot be ensured to be comprehensive and up–to–date, which will result in some node connection channels being biased and reduce the quality of the entire network.

The BOS Network has been enhanced to address this, and the configurations can set a node's status to be open to self–discovery. And subject to the overall limit of the maximum number of connections, even if only one of each team's nodes has self–discovery configured, it will help establish a higher level of interoperability quality network between the nodes on the BOS Network in. In order to reduce risks, a node only obtains connectable node information from existing nodes in the configuration file, and does not automatically create connections without restriction.

## **Ecosystem Model**

### **Issuance Method**

The Distributor which issues and sells BOS shall be an affiliate of the Foundation. The initial supply of BOS is 1 billion. The breakdown is as follows:

- 100 million will be used to do eco–airdrop
  - 50 million directly airdropped to EOS mainnet accounts
  - 50 million will be airdropped based on the transaction volumes of DApps and BP teams
- 100 million for strategic partner fund
  - which will be used to invest in quality projects based on BOS and cover cost of the BOS's operations

- 400 million used to incentivize the ecosystem, specifically, to subsidize payments and transactions on BOS chain
- 200 million left for the BOS team, which will be unlocked over a 4-year schedule;
- 200 million for private sale investors.
  - Private sale will be in four rounds
  - 50 million will be up for sale in each round

The annual inflation is 2%:

- 1% for BP rewards
- 0.8% for developer rewards
- 0.2% for governance incentives.

In particular, it is highlighted that BOS:

- (a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any affiliate;
- (b) does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of its affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to the BOS Network, the Foundation, the Distributor and/or their service providers;
- (c) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;
- (d) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment;
- (e) is not a loan to the Foundation, the Distributor or any of its affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of its affiliates, and there is no expectation of profit; and
- (f) does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of its affiliates.

The contributions in the token sale will be held by the Distributor (or its affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale. To the extent a secondary market or exchange for trading BOS does develop, it would be run and operated wholly independently of the Foundation, the Distributor, the sale of BOS and the BOS Network. Neither the Foundation nor the Distributor will create such secondary markets nor will either entity act as an exchange for BOS.

## Developer Incentives

To decentralize development of the core protocol, 0.8% of annual inflation will be distributed to BOS core code developers.

Every 3 months, the top 50 block producers nominated by the community will vote on and rank 40 winners to get the awards:

- The top 10 will share 40% (4% each)
- Individuals ranked 11 to 20 will share 30% (3% each)
- The last 20 share the remaining 30% (1.5% each)

The quarterly reward distribution will be preceded by releasing by a one-week public disclosure of the 40 nominated candidates. In case of reasonable objections by the community, the list will be re-evaluated. Each reward list will be recorded on chain.

As BOS continues to develop, developer rewards will be appropriately adjusted by the community to accelerate for the evolution of BOS.

## **Governance Model**

In the process of the ecosystem development of the chain, each chain in the future can be understood as a “state”. Each chain will have its own unique governance model. Different governance models will lead each chain in different directions and cause competition among the chains, allowing the developers and users choose the best model through the operation of the free market.

The governance model of the BOS Network advocates “Code is the law.” Ensuring the smooth development of DApps will be the highest priority for the BOS Network. The BOS Network issues an additional 0.2% per year for governance organisations or volunteers who help BOS holders to initiate arbitration/voting (for the avoidance of doubt, the right to vote is restricted solely to voting on features of the BOS Network; it does not entitle BOS holders to vote on the operation and management of the Foundation or its affiliates, or their assets, and does not constitute any equity interest in the Foundation or its affiliates). Anyone in the BOS Network can initiate arbitrations. The more support a proposal gets, the more reliable it is. If the arbitration takes effect, the initiator can receive 2000 BOS as governance incentives.

There are two types of decision or arbitration for the BOS Network: 1. Decided by the agreement of no less than 15 BPs. 2. Community referendum. There is no only one arbitration institution in the governance of the BOS Network. But more independent organisations or individuals are encouraged to participate in the process of determining network features. They can obtain community incentives for effective solutions or suggestions.

Note: The effective standard (for example, no less than N BPs agree that the arbitration will take effect) may change with the ecosystem development of the BOS

Network, and any changes must also be voted in accordance with current governance rules.

## Economic Model

The BOS Network is a very meaningful attempt at establishing the free market economy of the blockchain world. Due to the excessive intervention of the central bank in the market and the inability to maintain independence, the digital token industry as represented by Bitcoin attempts to solve the unresolved issue of real economy through the hypothesis of a rational man about the concept of a completely free market. When one looks back at the history of modern economics, governance and freedom, fairness and efficiency are always found within the process of competition and rebalancing of the status quo. From the classical school that pursues the free market, to the Keynesian school that emphasises government intervention, and then to the Austrian school that stresses returning to the market, no one school will become universally accepted, or will remain in a stable state forever.

The BOS Network hopes to balance the advantages and disadvantages of the BTC free market and the current over-governance of EOS through commercial development, while leveraging the advantages of efficiency and decentralisation to truly realize the commercialisation of the blockchain technology.

The inter-chain communication functions supported by the BOS Network will affect the operation of the entire blockchain industry. All kinds of digital assets can link traditional isolated digital assets into a network through inter-chain communication. Including BTC, ETH, EOS or other certificate assets can be traded and transferred on the BOS Network. The BOS Network can be understood as a free port of digital currency. The fast trading system brought via the BOS Network will give it a very impressive throughput. In addition, low account creation costs will attract merchants and applications from all over the world to join in the ecosystem, thus prospering the entire BOS Network ecosystem and then consequently feeding back into the EOSIO ecosystem.

When a user holds ETH, BTC and EOS at the same time, the user can import the above tokens into the BOS Network through the cross-chain channel, and create BOS-ETH, BOS-BTC, and BOS-EOS on the chain. The team calls such assets BOS assets. That refers to, assets brought by users into the free port of the BOS Network. Users can conduct consumption, investment, entertainment and other activities in the free port of the BOS Network. DApp developers can provide various services for users. In the process of service, BOS assets can be traded or transferred in different accounts of the BOS Network. Holders of BOS assets can circulate assets from the BOS Network back to the original BTC, ETH, and EOS chains through chain-chain communication at any time.

As a medium of exchange, BOS is expected to become the base pricing unit for the infrastructure platform for the entire Freeport. When multiple assets interact through

the BOS Network, BOS will play the role of the carrier of value as British pound and the US dollar have done in the past.

Historically, the Bank of England exchanged the full amount of gold with the British pound for the first time. The combination of the Roman law-based laws and the formation of a good business atmosphere attracted the best resources of the world at the time and finally made London the International Financial Centre. The BOS Network will likewise create a historic blockchain business center through the building of a sound infrastructure and establishment of a good business atmosphere.

## Conclusion

BOSCore is a DPoS public chain dedicated to building a trusted business ecosystem with technology that covers 1 billion users. From the perspective of the evolution of the blockchain, in addition to being the preferred public chain for commercial landing, BOSCore can also be used as a circulation chain for various heterogeneous chain tokens and as a free port in the blockchain world. The BOS Network comes from the community and will better develop through the joint efforts of the community.

## References

- [1] [ DPoS BFT — Pipelined Byzantine Fault Tolerance ]  
(<https://medium.com/eosio/dpos-bft-pipelined-byzantine-fault-tolerance-8a0634a270ba>)
- [2] [ Practical Byzantine Fault Tolerance ](<http://pmg.csail.mit.edu/papers/osdi99.pdf>)
- [3] [ Chain Interoperability ]  
(<https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf>)