BOSAGORA White Paper

Mar.2021

Executive Summary

The BOSAGORA platform is a decentralized self-evolving cryptocurrency that is built on Trust Contracts and an embedded decision-making system called the Congress Network. (1) Trust Contracts are securely executable contracts based on a protocol layer. We intend to provide an efficient, safely designed smart contract engine and provide an easy-to-develop language with many tools and popularity for easy adoption by developers. (2) The Congress Network is the decision making body in the BOSAGORA platform which solves governance issues arising in decentralized organizations. Through a clearly defined and automated governance system, we aim to continuously develop the community and software into a more anti-fragile ecosystem. The Congress Network follows the rule of one vote for one node. In other words, it promotes DAO where all node administrators have equal rights to vote without the delegation of voting rights or election of a delegate. (3) The Commons Budget is a BOA asset where a certain amount of BOA is accumulated whenever a block is created and 30% of the transaction fees are accumulated continuously. Its use is requested through a proposal in the Congress Network, and it is approved through the voting of the Congress Network. (4) T-Fi is a DeFi platform operated within the BOSAGORA platform. Based on a structure that connects blockchain to the real economy through lending, T-Fi promotes a broader concept of DeFi where fairness and publicness are guaranteed. T-Fi is an innovative business model that creates stable and high profits by converging the BOA coin with products of the real economy from all over the world.

Background

The blockchain was first conceptualized in Satoshi Nakamoto's white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008[1]. The technology was implemented the following year as the central technology behind Bitcoin. Bitcoin uses blockchain technology as a financial transaction ledger where individuals publicly record transfers of currency. Bitcoin was the first of its kind to use the blockchain to successfully solve the double-spending problem. Despite the absence of a centralized administrator, Bitcoin successfully supported 180 million P2P (peer-to-peer) transactions, and it is on its way to achieving market capitalization of over 1.1 trillion USD in 2021.

Following the success of Bitcoin, there have been numerous systems leveraging blockchain technology. There are hundreds of competing cryptocurrencies and according to a IBM report, more than 90% of banks are investing in blockchain technology. Currency transactions are the most common applications of blockchain technology[2]. However, some groups are also attempting to transfer and manage other kinds of digital assets using this technology, such as financial products and services, logistics information, property ownership, identity etc.

The cryptocurrency Ethereum gained a lot of traction in 2016 and aims to provide smart contracts on the blockchain: "A blockchain with a built-in fully fledged Turing-complete programming language that can be used to create 'contracts' that can be used to encode arbitrary state transition functions."[3]

The goal is to allow users to write any kind of program (or contract) onto the blockchain. Similar to Bitcoin, Ethereum uses the blockchain and a consensus mechanism to ensure that if a malicious node attempts to forge the content of the contract, the forged contract will eventually be removed from the blockchain. As Bitcoin ensures the integrity of the amount of Bitcoin being transferred between accounts, Ethereum must similarly ensure the integrity of the contract being executed.

The smart contract has the potential to be a paradigm shift in the development of decentralized applications. Programs that are not held on a centralized server, yet can run the same logic anywhere. Smart contract can be used to develop: decentralized marketplaces, currency exchange platforms, and projects like Golem[4] which aim to create a decentralized worldwide super-computer.

However, the freedom and flexibility provided by the Turing-complete language which Ethereum is based on is the cause for several serious problems. We believe that using a turing-complete language may be inappropriate for writing a smart contract as they are inherently undecidable.[5] Due to this undecidability issue, a smart contract based on a Turing-complete language will make it difficult to know what a smart contract will do before running it. Ethereum attempts to overcome this issue by applying a cost to computational work (gas), however the inherent issue of the language used to program and execute a smart contract has inevitably led to a series of security vulnerabilities[6] and outright failed projects.[7]

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [2] Leading the Pack in Blockchain Banking: Trailblazers Set the Pace, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&

[3] Vitalik Buterin, Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper

[4] Golem, https://golem.network

[5] Hodges, Andrew, Alan Turing: the enigma, London: Burnett Books, p. 111

[6] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on Ethereum smart contracts, https://eprint.iacr.org/2016/1007.pdf

[7] The DAO, https://slock.it/dao.html

Vision

Contribute to making a better world with blockchain technology as a project enabler.

Mission Statement

Building an open decentralized blockchain protocol that ensures the transparency of consensus algorithm and the clarity of contract, thereby enriching the blockchain ecosystem through enabling the meaningful projects with the expression of the collective intelligence by an advanced democratic decision-making process.

Core Values and Key Attributes

Forward Thinking

Pioneering future realization: We aim to develop a first full-node Proof of Stake and Federated Byzantine Agreement consensus algorithm blockchain platform with innovative technology development that anyone can experience speed and trust.

Fair

Mature democracy: Everyone can embody democracy that guarantees the highest level of fairness through free and inclusive decision-making with the advanced deliberative democratic decision-making tool.

Dependable

Clear transparency: To make it easier for anyone to see the entire project through transparency and to make decisions based on established procedures. (Community update, Technical advisory board, Github, Congress voting process)

ICO and the Original White Paper

BOSAGORA received a surprising response from 95 countries in May 2017 to achieve the 6902 BTC hard cap in just 17 hours. The result was achieved by the diverse technological and ecological blueprints pursued by the existing white paper. However, many similar projects have been announced over the past few years, and it has become difficult to gain exclusive status with technology development plans and ecosystem blueprints alone. Besides, competition in the blockchain platform market is getting even more intensive as the global giant is also signaling the launch of the blockchain platform. Under these circumstances, BOSAGORA should try to both pioneer new areas, where it could gain a more exclusive status to survive, and retain the framework and spirit of existing white papers to keep the promise with the participants of the Initial Coin Offering.

Since the ICO, regulations have changed along with numerous technological advancements. BOSAGORA team focuses on delivery adhering to the original white paper but at the same time, we must make amendments to reflect the changes in policies, technology and methodologies.

Accordingly, we will create a platform with more robust and up-to-date technology applied while keeping the promise of the value and vision embedded in the early white paper. The promise of the value and vision found in the original white paper should be maintained. In other words, fundamentals such as the formation of the Congress Network which all nodes participate in the decision-making, the provision of the Commons Budgets that can be utilized if the congress wants to, and the functions as a mainnet platform that supports various dapps and business partners should remain as it was written.

A distinct aspect of BOSAGORA's operating principles is that it can unleash collective intelligence because all nodes are involved in the decision-making process. In particular, thanks to the advanced form of mature decision-making capabilities of the BOSAGORA, various opinions will be aggregated into harmonized forms. Through this harmonious process of collective intelligence, it is ultimately what BOSAGORA seeks to improve its ecosystem.

Proposal

Anti-centralizing Consensus Algorithm

Cryptocurrencies like Bitcoin, that only use a proof-of-work (PoW) type consensus protocol, are affected by issues arising from the non-separation of economic and political incentives. By buying up more mining hardware, a user can attain more control of the blockchain(political) and also increase their mining income(economic). BOSAGORA overcomes this issue by using a consensus mechanism(explained in more detail below) that separates economic incentives from political ones. Attaining either political power or economical wealth requires an investment into the system. A user can either acquire more votes by increasing the number of nodes(one operational node equals one congressional vote) or a user can invest in confirmation rewards(rewards relative to the amount of coins locked away in a node) to maximize mining income.

Governance

Decentralized systems lack a systematic decision making process. There have been several cases in the cryptocurrency space, where this led to confusion and substantial financial losses. BOSAGORA constitutes a governance system whereby node operators referred to as the Congress Network can participate in creating and voting on proposals in order to continuously improve the software and ecosystem. System changing proposals that are voted on the Congress Network and are accepted, are considered to have reached a social consensus, and the changes in the proposal are applied to the network.

Another type of proposal is a funding proposal. These proposals are requests for funds from the Commons Budget and they are also voted upon by the Congress Network. BOSAGORA sets aside a large public budget specifically for the development of the BOSAGORA ecosystem through these proposals. We will explain further later in this paper.

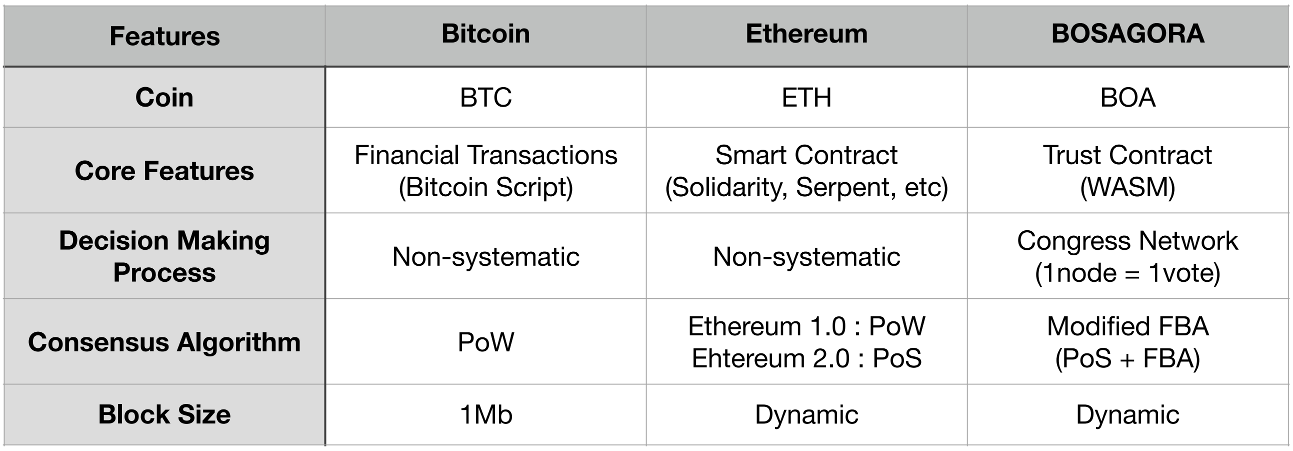
Trust Contracts. BOSAGORA team aims to implement Trust Contracts, which enable a safe, accurate, programmable and executable contract as in the original intention.

Rather than continuing what is not feasible, we will redefine "Trust Contracts", and will actively pursue the selecting the optimal direction and applying the suitable technology to improve the core protocol. This approach also considers adopting a methodology that uses flexible programming language on top of virtual machines and we are currently exploring WebAssembly as other industry players do. In the end, we intend to provide an efficient, safely designed smart contract engine and provide an easy-to-develop language with many tools and popularity for easy adoption by developers.

WebAssembly is a new type of code that can be run in a modern web browser. It provides new capabilities and offers significant performance benefits. “WebAssembly is a binary instruction format for a stack-based virtual machine. WebAssembly is designed as a portable target for compilation of high-level languages like C/C++/Rust, enabling deployment on the web for client and server applications.”

Running programs that are written in multiple languages on the web at near-native speeds using client applications was previously impossible. Running the codes on WebAssembly is similar to the actual hardware. With WebAssembly, developers can code in a variety of programming languages such as C++ and Rust, and they can expect to run the program in near-native performance. EOS also uses WebAssembly, and many blockchain platforms such as Ethereum, Tron and Cardano have already introduced or plan to introduce the virtual machines using WebAssembly.

Once the feasibility of the implementation plan has been studied and the solution has been discovered, technical and practical measures will be taken to complete the objectives and directions for the "Trust Contracts" presented in the original white paper.



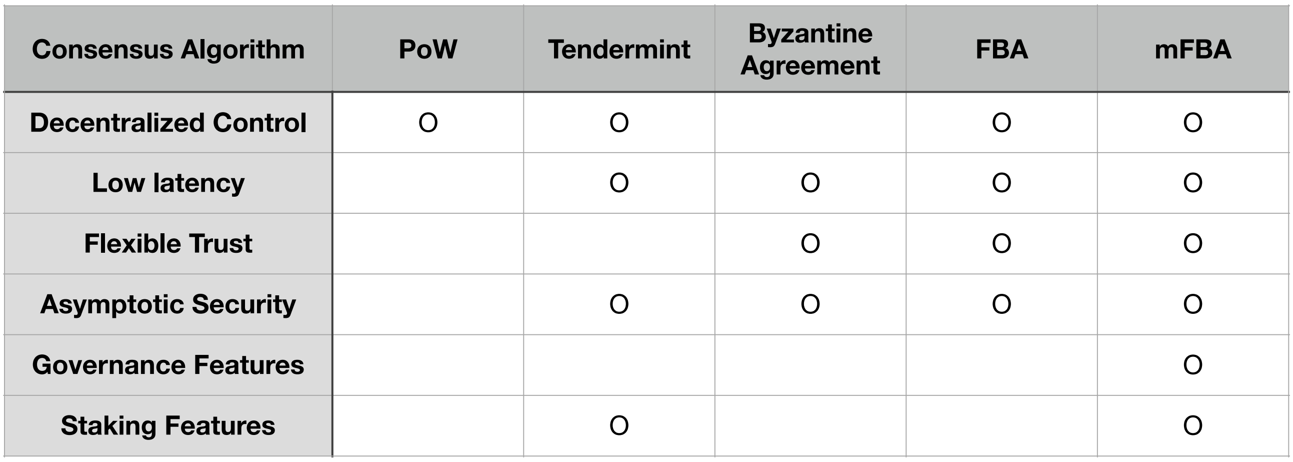
Features	Bitcoin	Ethereum	BOSAGORA
Coin	BTC	ETH	BOA
Core Features	Financial Transactions (Bitcoin Script)	Smart Contract (Solidarity, Serpent, etc)	Trust Contract (WASM)
Decision Making Process	Non-systematic	Non-systematic	Congress Network (1node = 1vote)
Consensus Algorithm	PoW	Ethereum 1.0 : PoW Ehtereum 2.0 : PoS	Modified FBA (PoS + FBA)
Block Size	1Mb	Dynamic	Dynamic

Fig 1. Comparison of Cryptocurrencies

Consensus Algorithm

Overview

The consensus algorithm is core to any blockchain based currency or system. The algorithm attempts to answer the question, ‘How can we prove with confidence that all distributed databases hold the same set of information?’
In response to this question, BOSAGORA uses a Modified Federated Byzantine Agreement (mFBA) consensus algorithm based on Stellar’s Consensus Protocol (FBA).[8]



Consensus Algorithm	PoW	Tendermint	Byzantine Agreement	FBA	mFBA
Decentralized Control	O	O		O	O
Low latency		O	O	O	O
Flexible Trust			O	O	O
Asymptotic Security		O	O	O	O
Governance Features					O
Staking Features		O			O

* Federated Bysantine Agreement
** Modified Federated Bysantine Agreement (BOSAGORA Protocol)

Fig 2. Comparison of Consensus Algorithms

Mazieres defines key features of the federated Byzantine Agreement Protocol:

- Decentralized control. Anyone is able to participate and no central authority dictates whose approval is required for consensus.
- Low latency. In practice, nodes can reach consensus at timescales humans expect for web or payment transactions—i.e., a few seconds at most.
- Flexible trust. Users have the freedom to trust any combination of parties they see fit. For example, a small non-profit may play a key role in keeping much larger institutions honest.
- Asymptotic security. Safety rests on digital signatures and hash families whose parameters can realistically be tuned to protect against adversaries with unimaginably vast computing power.
- Governance Features. Voting and features that are related to operating the congress are. additional features embedded into the protocol.

[8] David Mazieres, Stellar Consensus Protocol, https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Federated Byzantine Agreement Consensus Algorithm

Bitcoin's consensus mechanism and the traditional Byzantine agreement based protocols require a unanimous agreement by all participants of the network. However, the federated Byzantine agreement(FBA) does not require an unanimous agreement by all participants and additionally each node can choose which nodes to trust. This results in faster transactions without losing integrity of the financial network and allowing for organic growth of the network.

FBA implemented this type of non-unanimous consensus mechanism by grouping nodes into teams (also known as Quorums). When a transaction is made, the information is sent to all those in the group. Rather than waiting for the whole network to agree on the state of the data, if a node hears the same message from a sufficient number of trusted nodes, the node assumes the information is correct. The overlapping of nodes, or loose federation of nodes, results in different nodes that have different sets of teams to agree on the same transactions. This leads to a system-wide consensus, without requiring unanimous agreement for each transaction block.

In situations where nodes are in disagreement over a fraudulent transaction, there is a ballot system embedded into the system to overcome such issues. Further technical details regarding FBA can be found in Stellar's consensus protocol paper.

How is the modified federated Byzantine agreement(mFBA) algorithm different?

In addition to FBA, the BOSAGORA consensus protocol also applies a Proof of Stake feature for the maintenance of the governance system. Validators need to freeze 40,000 BOA within a node and forgo liquidity. The frozen coins in the node then act as both an economic incentive(Confirmation Rewards) to operate a node as well as collateral for the security and integrity of the information held in the node's blockchain. According to the pre-set rules, if the node is discovered to have forged the blockchain on the node, the frozen coins are forfeited to the Commons Budget.

BOSAGORA's DAO, the Congress Network

Overview

The Congress Network is the decision-making body for BOSAGORA consisting of fully-synchronized node operators. The Congress is a Decentralized Autonomous Organization (DAO), which is operated without regulation by a third-party or central organization. It enables effective and inclusive collaboration among the various project stakeholders to continuously enhance the software and the ecosystem. For example, decisions on a system upgrade or use of the Commons Budget can be made through proposal, review, and voting withing the Congress Network.

All node operators of BOSAGORA can join the Congress Network and participate in the collective decision-making process. The Congress Network enables its members to engage and contribute through proposals, discussion, voting, and reviewing issues of the project's common interest. The Congress Network adheres to the 1-node-to-1-vote rule. In other words, it seeks to become a DAO where all node administrators have the equal right to vote without delegation of the voting right or election of a delegate.

The Need

Blockchain projects must satisfy the needs of potential users. However, no matter how carefully they are designed, the directions of technology, people, and markets constantly change, and products must constantly adapt to such changes. Choosing when and how to change the network is critical to sustainability and growth.

In this process, however, communicating the interests and perspectives of every stakeholder in an agreement can be a painstakingly long process, resulting in centralized governance systems even for blockchain projects, which are about decentralization.

Even with the best intentions, a centralized decision-making process will inevitably leave out the comprehensive voices of the network. If members do not have a channel to participate and make changes about their problems, they have no other choice but to leave and move to another alternative, diminishing network effects. Establishing a DAO that is not centralized yet is inclusive and cooperative is an essential condition for a successful project.

Problems of collaborative decision-making

Poor decisions are caused by many reasons. Incomplete information, power dynamics, biases, and peer pressure make teams and communities reach poor decisions that are not inclusive of the best solution.

- Incomplete information: information about the topic that requires a decision may be incomplete. This information may be concrete facts about the topic or personal experiences of groups who are directly affected by this decision.
- Power dynamics: decisions are made by a small group of people without taking into account the opinions of others who are often most vulnerable to the consequences.
- Cognitive biases: subconscious (or conscious) biases prevent ideas from being evaluated on their merit
- Social Pressure: social or peer pressure prevents constructive feedback and dialogue

In particular, the decision-making process online is likely to become inefficient if there’s not an appropriate arbitration system..

Introduction of Congress Network

We propose a decentralized and collaborative decision-making institution, namely the BOSAGORA congress network, which is based on node operators.

The function of the Congress Network

The Congress Network will be an institution that carries out the following functions.

- Members can actively exchange ideas and communicate together
- Decisions can be reached on proposals to implement on BOSAGORA network

There are two subjects on which the Congress Network makes decisions.

•“System upgrade proposal” to make changes in the BOSAGORA platform

- This includes changes or improvements made to the technical function of the network. The Congress

Network’s decisions are implemented to set the direction of work for the foundation development team.

- “Commons Budget spending plan” to determine how to use the Commons Budget
  - The Congress Network can propose how to apply the Commons Budget, and can execute the proposed plan upon approval. Since the decision is made through DAO, proposals that benefit only a small group can be dismissed by a majority vote. In other words, proposals that benefit the entire BOSAGORA and holder community are more likely to be approved.

Characteristics of the Congress Network

BOSAGODA will overcome the problems of collective decision-making processes and establish a decision-making system that is more inclusive and efficient. To achieve this, “Votera”, an online decision-making tool, will be implemented. Votera has the following characteristics.

① **Anonymity:** In a democratic decision-making process, a mechanism that protects participants’ privacy is essential. This is because they are highly likely to be influenced by the majority if their identities are disclosed.
Votera guarantees anonymity for all participants in order to allow individuals to speak their minds freely in the Congress Network. No one is allowed to trace digital footprints of the members, create a dossier on individual behaviors or activities, or make personal contacts outside the network.

② **Flexibility:** Decision-making processes that are suitable for different circumstances can be added as needed. If an additional process is required as discussion takes place, additional activities can be performed in connection with it. Votera supports customization of such processes, including discussion, proposal review, voting, and so on.

③ **Convenience:** Votera provides a range of customizable functions. It provides templates that are optimized for each stage, including free discussion, prioritization, individual assessment on a particular result, and so on. This allows an autonomous organization to focus on a topic, and helps it to predict a situation where discussion takes place.

④ **Archiving:** Votera guarantees transparency by storing decision-making data in a block, and clarifies responsibilities. For efficiency, however, the blockchain contains a hash of the record that can verify the decision. The information on discussion, voting, and review will be stored in a separate server, and will be provided for the members to view at any time.

⑤ **Reporting function:** Votera provides a reporting function. Any member of the Congress can report other members who disturb the order of the decision-making process to impose necessary measures on them. This prevents the autonomy of DAO from degenerating into disorder.

Procedures of the Congress Network Activity

① Join the Congress Network

Anyone who fulfills the following conditions can become a member of the Congress:

- Freeze at least 40,000 BOA
- Operate a full node at a stable network speed (operate in a server or personal computer)

The members of the Congress can set nodes in two directions depending on their goals:

- Operating a greater number of nodes increases political influence (more voting power)
- Compiling and operating BOA tokens in one node reduces node operation costs.

② Create an activity

Any member can open an activity and start a discussion and decision-making process.
Currently, there are three types of activity template to choose from.

- Discussion: The members can share their opinions and develop ideas through brainstorming, etc.
- Voting: The members can develop choices and vote and make comments on them.
- Review: The members can participate in review products, decisions, etc. and participate in surveys.

We plan to provide additional functions and templates needed by users in the future.

③ Enter a guide

Activity creators should enter the information necessary for other members to understand the subject.

1. Link (optional): This can be generated in connection with an existing activity at the time of creating an activity. If a vote on a community rule has taken place, after some time a review activity can be connected regarding how well the implemented rule has been settling and whether there are other areas for improvement.
2. Name of activity
3. Objective and description
4. Deadline: By when should a decision on this subject be made?
5. Advanced setting (optional): The number of rights to speak to be distributed, type of ballet paper, rewards, and other conditions
6. Commission fees (optional): Creating an activity is free, but commission fees need to be paid in advance for a funding suggestion. (Please refer to the appendix for the commission fees system.)

④ Discuss

The members can write opinions and leave comments freely. Good opinions can be recommended, and it is possible to sort the opinions by recency or number of recommendations. Changes can be made to the contents of opinions except for the title; however, all participants can view the change log, which cannot be deleted. The members can leave comments on opinions, but comments cannot be deleted once created. If there are opinions or comments that violate the community rules, the members can hide them.

⑤ Vote

A vote is created in order to reach an agreement. The outcome of a member vote is recorded in the blockchain for further verification. However, a hash scheme is implemented so that the intermediate voting result cannot be disclosed until polls close. The vote result can be counted through deciphering only after polls close.

⑥ Inspect the vote

The date and time of each vote are saved, and if there are redundant votes from the same node, the latest vote is considered as the final result to guarantee one vote for one node.

⑦ Check the quorum for resolution

A quorum is the minimum number of people who must participate in a vote in order for a certain proposal to be executed in the platform. In the early stage, a quorum for resolution is set as one third of the total members; however, this can be adjusted later by reflecting the average participation rate.

⑧ Pass the proposal

If the net percentage of positive votes exceeds the net percentage of negative votes by more than 10%, the proposal is approved.

⑨ **Execute the proposal**

The proposal is executed if the proposal is approved. If a proposal related to system upgrade is passed, the development team commences development according to the proposal (executing tasks related to a development plan, roadmap, security test, etc.). When a proposal on the Commons Budget is approved, the Commons Budget is allocated according to the details of the proposal Trust Contract. Even if a proposal is related to system upgrade, if expenses are incurred from proceeding with the development and implementing the details of the development, the proposal should take the form of a Commons Budget spending plan.

⑩ **Review/inspect**

After executing the proposal, the Congress Network and the foundation review whether appropriate tasks are being implemented according to the roadmap of the proposal. In the case of a proposal related to Commons Budget allocation, the expenses related to the review and inspection are compensated from the commission fees paid by the proposer.

Network Interactions

Transactions

When the user requests a transaction, the request is sent to the Congress Network. Concerning a simple BOA transfer, the user’s transaction is approved when the node confirms the block, after which the BOA is transferred to another wallet. If the transaction is based on a more complex Trust Contract, a predefined logic and procedure will be executed. A transaction fee is incurred for the transaction, and the amount of the fee can be adjusted by the Congress Network through a vote. The transaction fee is an incentive for verification and confirmation of the block, and is paid to the node’s administrator. It also acts as a protective mechanism against DoS attacks.

Proposals

Proposals are system changing plans or Commons Budget spending plans that are submitted to the Congress Network. Any member of the Congress Network can freely make a proposal. When a proposal is made, the net percentage of positive votes must exceed the net percentage of negative votes by more than 10% for the proposal to be approved. When the Commons Budget spending plan is approved, the requested coins are transferred to the proposer through the set procedures. Under some conditions, such as when the size of the proposal is large, the system can define a contract that requires a report on how the coins were spent.

Coin Freezing

Coin freezing is an action performed to verify the shares. To run a node and receive an incentive as an inspector, one must freeze coins. The frozen coins are used as collateral against an attempt to forge the blockchain. In other words, if a node tries to forge the blockchain, some of the frozen coins will be confiscated and sent to the Commons Budget account. It is also a mechanism to stimulate stabilization of coin price. A prior notification must be made two weeks in advance before cancelling coin freezing.

Reward System

The Congress Network has a unique incentive mechanism. The members of the Congress can maximize financial rewards by placing BOA coins in one node, or expand their voting rights by distributing BOA coins in multiple nodes (one vote is provided for one node).
Such deliberate distinction separates economic power and political power, and encourages distinction between motivation to participate in the decision-making process and economic motivation.
Bitcoin is experiencing difficulty concerning the concentration of Hash power since it relies on the work verification protocol. It allows a few giant miners to easily purchase a large volume of diggers. This can influence code change, and even threaten the integrity of the blockchain.

There are two ways for Congress Members to receive BOA rewards: confirmation rewards and transaction fees.

- **Confirmation Reward:** Confirmation rewards are given to a node when a block is confirmed. This reward is crucial in providing a financial incentive to operate a node and the reward is directly linked to the number of frozen coins in a node. The reward is issued relative to the proportion of frozen coins held in the node. Initially the block confirmation reward starts at 27 BOA per 5 seconds, and then it will decrease by 6.31% year on year over roughly 128 years. The rewards will be distributed to validators when a new block is created.
- **Transaction Fee:** Transaction fees are adjusted flexibly (see Appendix 3). Congress Nodes receive 70% of the collected transactions fee in a block, and 30% is sent to the Commons Budget. Transaction fees can be adjusted through the Congress.

Commons Budget

The Commons Budget is a BOA asset where a certain amount of is BOA accumulated whenever a block is created and 30% of the transaction fees are accumulated continuously. Its use is requested through a proposal in the Congress Network, and it is approved through voting by the Congress Network. If a proposal is approved by the Congress Network, the Commons Budget is transferred automatically according to the details of the proposal through the Trust Contract.

The Commons Budget can be used in various areas for the purpose of developing the ecosystem. For example, the Commons Budget can be spent on investment in a particular BM for BOA coin buy-back, bounty and marketing campaigns, initial expenses for projects/services to be introduced in the BOSAGORA ecosystem, and so on.

Token Distribution and Issuance

BOSAGORA Token Distribution

BOSAGORA has conducted an airdrop of BOA to BOS holders from Thursday, May 16th to September 30th, 2019 according to the snapshot taken on Friday, April 5th, 2019, 12:00:00 UTC. According to the snapshot, 542,130,130.1958463 BOS coins were in supply.

- 500,000,000 BOS is initial supply
- 41,420,159.8931463 BOS is BlockchainOS PF00 membership rewards issuance
- 709,970.3027000 BOS is BlockchainOS PF01 membership rewards issuance

After the finalization of BOA token airdrop, the distribution plan for BOA token will be the following:

Category			**Number of BOA**	**Share**
Innitial supply	Airdrop		247,595,031	5.09%
	Unclaimed	Burn	92,130,130	
		Marketing	30,000,000	0.61%
		Remain	82,404,969	1.66%
	Original Distribution	Foundation	40,000,000	0.81%
		Team Members	40,000,000	0.81%
		Bounty	10,000,000	0.20%
	Innitial supply total		542,130,130	
	1st Token Burn	BCOS PF	-42,130,130	
		Additional Token burn	-50,000,000	
	1st Token Burn Total		-92,130,130	
	Inicial circulating supply total		**450,000,000**	
Additional supply after CoinNet	Confirmation Rewards		2,700,000,000	54.54%
	Commons Budget		1,800,000,000	36.36%
Total			**4,950,000,000**	**100%**

Fig 3: BOA Coin Issuance Plan

The number of airdrop tokens for BOS holders is 247,595,031.305721. The number of unclaimed tokens after the finalization of airdrop is 204,535,098.694279.
From the total of 204,535,098.694279 of unclaimed tokens:

- 42,130,130.1958463 tokens are issued by Public Financing, which was never the intention of the BOS platform foundation, thus, it should be burned.
- 50,000,000 also will be burned. The foundation has decided to burn 50,000,000 BOA from the unclaimed tokens, which is 10% from the original issuance plan.
- 30,000,000 BOA will be reserved for marketing purposes and will be used for exchange listings and partnerships.
- 82,404,968.6942793 will remain unclaimed.

Therefore, the actual initial supply will be 450,000,000 BOA. The foundation will make a separate announcement regarding the token metrics when there are any changes.

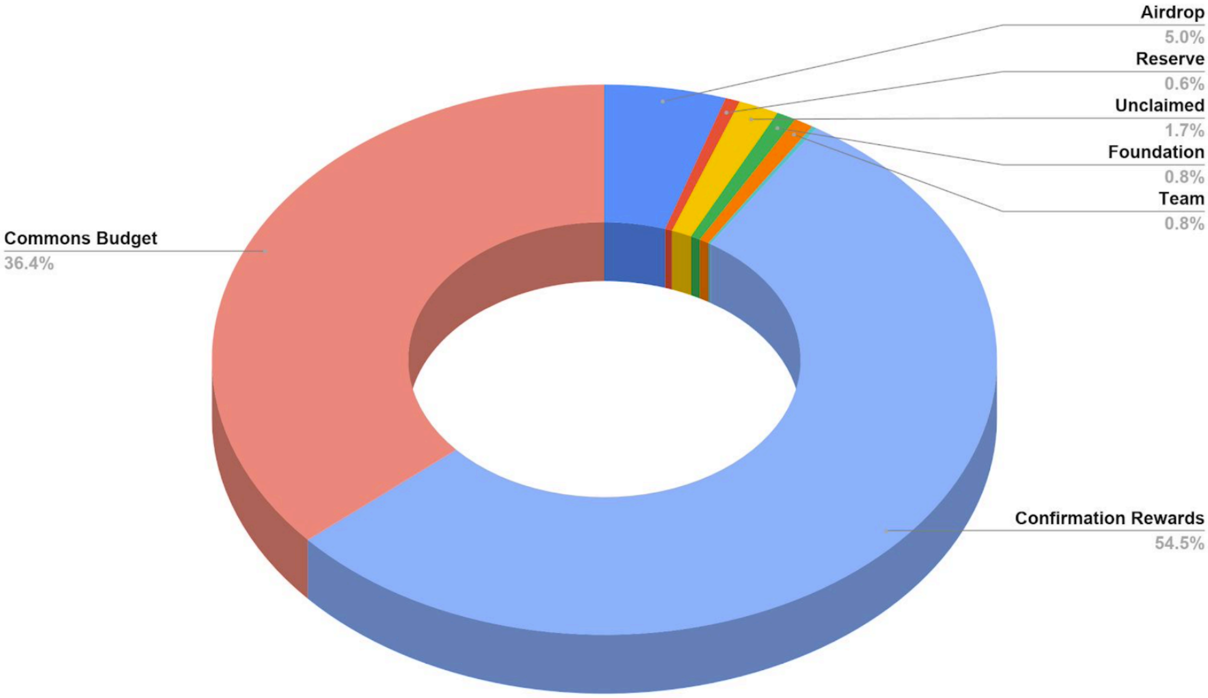


Fig 4: BOA Coin Issuance Plan

Issuance

New coins are issued in three ways; Initial Development Budget(0.45bil, 10%), confirmation rewards(2.7bil, 54%), and the Commons Budget(1.8bil, 36%). We aim to issue a total of 4.95 billion coins over the next 100 years. These values are subject to change.

- **Initial Development Budget:** Initial development coins are coins distributed prior to the Genesis block are intended to support the final development of the software. These coins are made up of airdrops and bounties. 450 million BOA are issued with the Genesis block.
- **Confirmation Rewards:** Confirmation rewards are financial rewards issued and evenly distributed to the nodes for every confirmed block. As the reward is distributed evenly, if the number of nodes increases the probability that a node will receive a reward decreases. This reward is relative to the number of coins frozen in a node. 2.7 billion BOA are issued through Confirmation rewards. Initially 27 BOA are issued per 5 seconds. The reward decreases every -roughly- one year by 6.31% over 128 years.
- **Commons Budget:** The Commons Budget holds BOA that can only be used by proposals that have passed the Congress Network. In order to create a sufficient budget for proposals, 50 Commons Coins are issued per 5 seconds for the first -roughly- six years. After the first six years the Commons Budget is maintained through the 30% commons fee on transactions fees.

After Coin Net is launched, block creation rewards and the Commons Budget will be generated. The complete token issuance chart is attached at the end of this document.

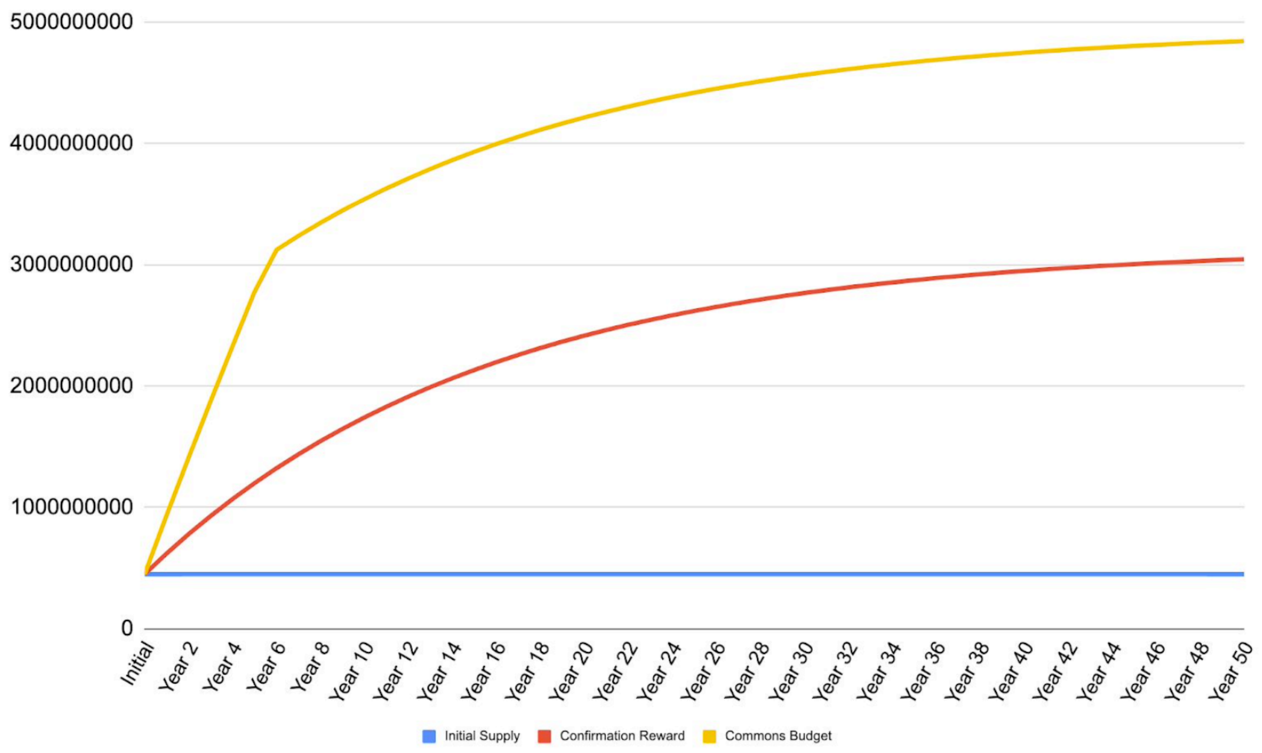


Fig 5: BOA Coin Issuance Schedule

Technology

Abstract

Bitcoin introduced the world to the idea of digital bearer's money. By implementing a virtual equivalent to cash, it laid the foundation for a multi-billion dollar industry where the properties of money are discussed and challenged.

The approach originally used is a timestamping server where inclusion of a batch of operations is based on expanded computing power. While providing very attractive properties, the usage of Proof-of-Work (PoW) turned out to be extremely energy inefficient. Additionally, the mining approach led to the development of specific hardware, centrally hosted in areas with lower energy cost, threatening the system with greater centralization. While alternatives have been developed for the latter, the mining approach is inherently wasteful.

We propose a construction where consensus is achieved at a low cost, in a self-contained system where penalties are applied to provably misbehaving actors. Such a self-contained system is usually referred to as "Proof-of-Stake" (PoS), although we provide our own definition of what that means.

We start by exploring the assumptions under which any system should operate to be safe, then define the properties we seek and how those compare to Bitcoin. Additionally, we explore the current state of the art development on PoS (most notably Ethereum's research) and PoS-specific attack.

I. Introduction

Proof-of-Work resource consumption

As mentioned in the Bitcoin white paper [Nak09] the main problem an electronic cash system face is double spend. While proof-of-work (PoW) was a powerful tool in democratizing the concept of electronic cash, it led to the development of special hardware and large, wasteful consumption of energy. As a result, mining operations have been largely centralized in areas offering cheap electricity. As of June 2018, it was estimated that around 74% of the hash-rate was operated by Chinese entities [KJL18]. Additionally, most of the specialized hardware (ASIC) is being developed in China, which makes the currency vulnerable to Chinese regulators.

Proof-of-Stake

There is not currently any replacement for PoW that exhibit the same properties. One contender is thought to be Proof-of-Stake (PoS). Many projects have explored the problem, starting from Peercoin in 2012 [KN12] with its "coin age" approach. Another well-established coin, NXT, uses an approach where the newly-created block data is used as a seed to decide on the next selector [NXT19]. The most prominent project working on a PoS system, Ethereum, has been planning to transition to PoS since its inception in 2014. Over the past few years, new projects have introduced the notion of "Delegated PoS" (DPoS), where nodes votes to delegate their voting power to a small subset of nodes.

One major difference between PoS and PoW protocol is that the former favors safety over liveness, resulting in protocols that can be stopped, but have instant finalization, while the latter provide guaranteed liveness and exponential safety. However, PoW does not provide

meaningful liveness: an attacker with enough resources could decide to produce empty blocks, effectively rendering the system useless. At the time of writing, the missing income would be marginal compared to the block reward, and could be easily compensated by external actors.

Nonetheless, regardless of any safety aspects any attack would likely result in the devaluation of the currency, which in many cases is a strong enough incentive to prevent attack. The blockchain community has fully embraced this, and game theory has been an essential part of the analysis of consensus protocol since day 1 [GTB19].

Scalability issues

Additionally to the inherent waste of resources that PoW system represent, blockchain scalability is a topic of active research. Even in the Bitcoin community, multiple factions have emerged: namely, Bitcoin has stayed with a 1 MB block limit (although Segregated Witness [SegWit] helped augment the capacity of the chain), while Bitcoin Cash has increased its block size to 32 MB. The argument in favor of small blocks is that only full nodes (nodes that verify the blockchains completely) are secure, while the others rely on other parts of the system (e.g. miners), and thus a personal computer should be able to run a bitcoin node. With 32 MB per block, at 1 block / 10 minutes (144 blocks per day), the amount of data that can be accepted is 4.6 GB daily, 138 GB monthly and 1,659 GB yearly.

One inherent requirement of a decentralized network is that a transaction has to be confirmed by a majority of the system to be considered accepted. Additionally, the more nodes that participate in the network, the more decentralized the network is, provided nodes are not controlled by colluding entities. Thus, a system which gains more users will put more stress on each node, leading to higher hardware and bandwidth requirements. On the other hand, when the number of nodes increases, every transaction will need to reach more nodes, increasing the time it takes for a transaction to be confirmed.

Instead of attacking this multi-objective optimization problem, we decided to follow the same track as Bitcoin core: building a layer(L2 / "Flash Layer") on top of the blockchain layer (L1 / "Settlement

Layer”), with slightly weaker rules, allowing to get most of the L1 safety while allowing transactions to be accepted by peers without needing to record them to L1 (and, by extension, forward them to all nodes). In doing so, we integrate some incentives for clients to use the scheme by default, and for nodes to accept such transactions.

The benefits of the Flash Layer solution are:

- Less data on the blockchain;
- Confirmation time is “almost instantaneous” if the protocol is followed;
- Users do not have to wait for a block for confirmation;
- Cheaper fee for the micro transactions that occur within the Flash Layer;

With the benefits, we expect that the built-in second layer solution will bring a secure and a low-cost dapp development environment. Additionally, one of the most important goal of BOSAGORA project, the separation of the political and the economic power will be realized with the Flash Layer solution.

Summary

In **Section II**, we will explore attacks on a PoS system.
In **Section III**, we introduce the foundations on our approach: the network model, source of randomness, and a scheme for validators to sign blocks in an efficient manner.
In **Section IV**, we introduce a consensus protocol where participants (“validators”) lock a specific amount (“stake”) in order to participate in the consensus protocol, and the incentive scheme is designed to encourage correct collaboration in the network.
In **Section V**, we describe our layer 2 approach and its integration with layer 1. This section will be developed further later.

II. Attacks on PoS

A few attacks and concerns on PoS have been discussed over the years. In this section, we will go over the basic definitions of such attack in an effort to enlighten the reader on challenges our protocol will face.

Short & long range attacks

We define short range attacks as attacks happening on clients that are less than N blocks behind the latest network-accepted block, while long range attacks are targeting clients more than N blocks behind the latest network-accepted block.
N is a parameter of the consensus protocol which can be explicitly chosen or derives from other factors. An example of an explicit definition of N can be found in Ethereum’s concept of weak subjectivity [VB14].

Due to the low computational cost associated with creating blocks, an adverse entity with access to past private keys could create a competing chain without much associated costs. As keys are essentially worthless after the coins they control have been moved, it would be economically viable for validators to sell their private keys after exiting the system.

Stake grinding attacks

Grinding attacks arise when part of the consensus algorithm depends on a random factor. Since the consensus protocol cannot rely on data it cannot verify (this would induce trust, and by extension a single point of failure), any randomness must be based on a known, predictable process, and data available to all participants, which is at odds with the traditional approach to randomness.

Since data is publicly available, attackers could attempt to influence it in a way that would be more favorable to them.

For example, a naive consensus protocol would have the following steps:

- Select a fixed set of n validators;
- Order this set in a predictable way (e.g. according to their public key);
- Every round, pick a validator to nominate a block;
- The validator selected has index Hash(previous_block) % n in the ordered set;

With such an approach, a validator would simply have to find a single suitable hash to be elected as the next round's validator. In the random oracle model, for n = 100, 1000 combinations would give a validator > 99.99% chances to be the next validator.

An approach that is often cited to solve such an issue is requiring blinded pre-commit. For example, validators would commit a hash during round R, and reveal the preimage of this hash on round R + 1. The random value (or seed for it) would then be the sum (or XOR, or hash of concatenation) of those preimages.

Nothing at stake attacks

Nothing at stake attacks were present in early design of PoS protocol.
When a validator is presented with two different blocks which are both valid candidates for the current chain, the most economically viable behavior would be to "vote" on both of them, since "voting" on a chain consumes no resources [VB14]. This led to consensus protocol adding penalization of such behaviors.
However, such penalties are inefficient if they are not combined with a mandatory lock-in period. If validators are able to move (sell) their stake at any time, including directly after voting on a block, it would be trivial for them to move their stake, then attempt to double spend a previously spend output from a block where they still had stake.
There would be no way to penalize such behavior, as the stake would already belong to another party.
For this reason, lock-in period are introduced.

III. Fundamentals

Network model

Out of all 3 available network models (Synchronous, Asynchronous, Partially synchronous), we position ourselves in the synchronous model [DLS88], as a result of SCP's requirement, which is a synchronous protocol.
A well-known result of consensus research is that no protocol can have liveness (ensuring that the network makes progress), safety (ensuring that all participants reach the same result) and fault tolerance (ensuring that the network can safely make progress if one or more nodes are not responding). This result

is called the FLP impossibility [FLP85] and is heavily referenced by the SCP paper, which chooses to favor safety over liveness. Fault tolerance, on the other hand, is a requirement for any system with open membership.

Source of randomness

Some parts of this paper, such as the signature scheme, rely on pseudo random data. Because randomness is by nature unpredictable, and hence cannot be verified for correctness, ensuring randomness in a distributed system faces needs to rely on seed data provided by all participants. A resulting challenge is ensuring no participant can gain an edge over any other participant by crafting or delaying its seed data.

This is achieved by using a hash and its preimage as seed data.

Upon enrollment, validators pick a random value, hash it n times, and commit the final value as their initial seed data. Every time a new seed data is required, validators can reveal the preimage of their last-published seed data, thus ensuring true randomness without the ability to manipulate data.

However, an issue arises when a validator willingly withhold data from the network. If publishing the data leads to a worse outcome than withholding it, then a node can choose to selectively withhold its preimage, either stopping the network or skewing the result. To avoid this pitfall, validators should regularly publish (and listening validator should support) enough seed data to survive a minor outage.

If sensible intervals are introduced in the consensus protocol, validators can be guaranteed that publishing their preimage ahead of time will not result in weakening the safety guarantees, and allowing them to cope with temporary downtime.

Enrollment process

When registering as a validator, a node broadcast the following data:

- **K** (UTXO key): A public key matching a frozen UTXO;
- **X** (random seed): The nth image of their private key;
- **n** (cycle length): the number of rounds a validator will participate in (currently fixed to (**freezing period** / 2)];
- **R** (signature noise): The initial nonce used for signing (see 3. Validator signature scheme);
- **S**: A signature for the message H(***K, X, n, R***) and the key **K**, using **R**.

After its registration is recorded, a validator is expected to start signing blocks immediately, as described in IV.1. The following are requirements the UTXO controlled by **X** must satisfy in order to qualify for enrollment:

- It has at least 40,000 coins;
- It did not default in the last **freezing period** blocks;

Validators signature scheme

Validators signal their commitment to a block by signing the hash of this block.
Signatures can be combined efficiently, so that in the best case scenario (all validators sign), the signature is

the combined signature of all validators, taking O(1) space.
The scheme used is based on Schnorr signatures, and is described below.
We define the following notations:

- H() is a hash function;
- Given the pair (k, K):
- k is a value in the group G of prime order P;
- K is the exponentiation of the base point B of the elliptic curve used by k;
- The pair (k, K) is used for the private/public key pair, respectively;
- The pair (r, R) is a unique random value and its exponentiation;

IV. Layer 1 Protocol

Cycle & Consensus rounds

We consider the consensus protocol as being a succession of simultaneous **cycles**, undertaken by each participant individually. Participants are called **Validators**, while observers of the consensus protocol are called **Nodes**. While every validator is a node, not every node is a validator.

Each cycle has a length (**n**) known at the beginning of the cycle. This length is expressed in terms of consensus round, with the output of each consensus round being a block, itself being primarily defined by the set of transactions being selected. Each round is expected to last in the range of (a few)minutes(to be defined by experimentation during testnet). Each round, the value of n decreases by one, and the cycle is over when the value reaches 0.

Cycles are dependent on the freezing capability of UTXO. A malicious actor would have a strong incentive to revert blocks right after it exited its validator capacity, if it was able to immediately trade the stake that was used for validation. As a result, the stake used for validation is frozen, and the **freezing period** is fixed to 14 days.

In order for a node to become a validator, and begin a cycle, it must complete the **enrollment process**. This is done by selecting a number of round n suitable for the entity, within the bounds defined in III.3, and propagating that message to existing validators.

Once that transaction is registered, a node immediately becomes a validator, collecting and propagating transactions. However, when a node originally enroll, it is not yet assigned a quorum set and is expected to be **passive** (sign blocks only when they reach the 50% threshold) until the next quorum balancing event happens.

Quorum balancing events happens once every 1 hour. When a quorum balancing event happens, the network is re-organized in a pseudo-random but predictable manner to ensure fairness in the reward process and prevent collusion between validators.

Towards the end of every round, nodes initiate a nomination process as defined by SCP [SCP16]. The leader selects a set of transactions and elects them according to the roles defined in the SCP paper. In the future, we aim to replace this nomination protocol by a protocol based on our source of randomness.

The result of the SCP round is a block that is signed by a majority of registered participants.

Preimage availability

Enrolled validators should always make sure their preimage is available to other nodes in a timely manner. As some aspects of validation / quorum balancing are dependent on preimages, any node that is not able to provide a preimage before it is needed (usually, the end of a consensus round). Validators can make their preimage available by broadcasting a message comprising of the preimage at a certain round and the round number, such as: (**P, Nx**), where **P** is the preimage and **Nx** is: **n - (rounds since enrollment)**.

Should the network miss a preimage, a node is said to have **defaulted**. Such node will not be able to re-enroll for consensus nor unfreeze their stake for a set period of time.

Nomination protocol

Nomination is the act of selecting a set of transactions as candidates for inclusion in the next block. Since multiple participants in the network might have a different set of transactions, this task is often relegated to a single node.
In Bitcoin, this node is the miner. In most other consensus protocol, there is a leader election who decides on the set of transactions. Currently, BOSAGORA relies on SCP's nomination protocol, which is based on a quorum leader election.

However, the presence of an unbiased source of randomness enables us to build a filter to make building a set of transactions more predictable, and more importantly, verifiable.

Such a change, while desirable, is left as a future improvement to the protocol.

Quorum balancing event

Quorum assignment is done to reduce the overhead of communication between nodes. Provided quorum assignment is essentially splitting the network into smaller, yet overlapping network, the main challenge is to provide a configuration which minimizes communication without compromising safety.

The quorum balancing event is currently being designed by our team and requires experimentation, and as such will be subject to changes in a later revision.

Reward allocation

Reward allocation follows the structure outlined previously in this whitepaper. A total of 27 coins are initially issued per 5 seconds, and distributed evenly to the validators when a new block is generated. A decreasing rate is applied over a fixed period.

V. Layer 2 Protocol

Flash Layer

The details of the realization of Flash Layer, which is an innovative solution for blockchain's issue of expandability, are roughly explained here. BOSAGORA can expand large numbers of people to active daily users through Flash Layer. Looking at the conventional blockchain projects, there are a couple of 2-layer solutions that can be used. One of the most popular realization cases is Bitcoin's lightning network. Our Flash Layer is built on the lightning network design, but adds the function of increased safety to it. Unlike Bitcoin's lightning network, our protocol is safe and never leads to accidental punishment and the consequent loss of funds. Flash Layer is built on the functional set supported by a script execution engine.

Opening a Flash Layer channel

For two users in the network to perform a transaction through Flash Layer, they need to have an open Flash channel between them. Indirect channel connection is also accepted. For example, if Alice opens a channel with Bob, and Bob opens a channel with Charlie, it is possible for Alice to make a payment to Charlie by routing a micro-transaction through Bob. These payment funds are safe in Flash Layer.

In order to open a new channel with another user, the two parties must agree on a common set of parameters. This can include the channel's capacity, separate commission fee for routing transactions, and the time lock that the funding contract will use as well as the Hashed Time-Lock contract time lock.

Once the parties agree on a set of parameters, this channel is built as one of the parties creates a multi-signature fund transaction that is posted in the blockchain. The output of this transaction can only be used pending the signatures from all participants of the contract.

When a fund transaction is confirmed in the blockchain, it is considered that a channel is open, and the parties can use this channel to make off-chain Flash Layer transactions.

Support for a script execution engine

In order to support Flash Layer, a script execution engine must support a series of "opcode" or system commands. These are required to set the conditions concerning when the funds can be spent, who can spend the funds, and under what time constraint the funds can be spent. The absolute time and relative time lock must be supported.

Off-chain transactions

Flash Layer uses a new status update mechanism built on the "Eltoo" update protocol layer in order to safely perform off-chain transactions without the potential for loss of funds.

Eltoo is the 2-layer payment channel's update and payment layer. It is a new and safe alternative to the penalty-based mechanism used in the lightning network found in Bitcoin.

Unlike the lightning network, Eltoo poses no risk of accidental loss of funds. Eltoo is an efficient update mechanism, and does not include security risks in the event of data leakage. Unlike lightning, where only 20,000 people participate, Eltoo allows for channel funding with an indefinite number of sponsors.

Eltoo requires a special opcode and signature support built into the BOSAGORA's execution engine.

The following is a simple overview of the design.

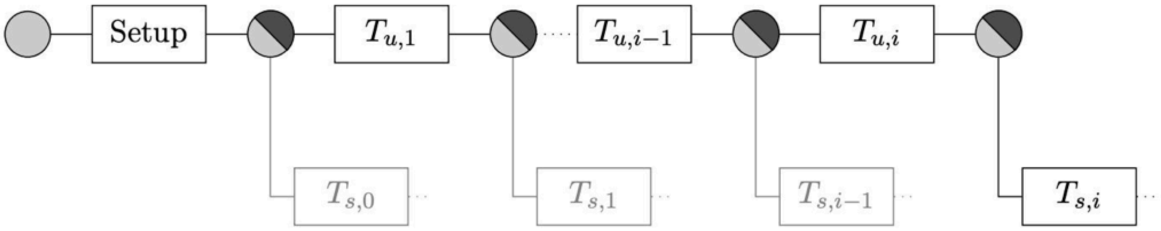


Fig 6. 2-Layer Protocol Design

Overview of the on-chain update protocol. The setting transaction initiates the protocol. Each update transaction, Tu,i, nullifies the payment transaction, Ts,i-1, (marked in a brighter color), which was previously negotiated until Ts,i is not nullified, and the contract is paid.

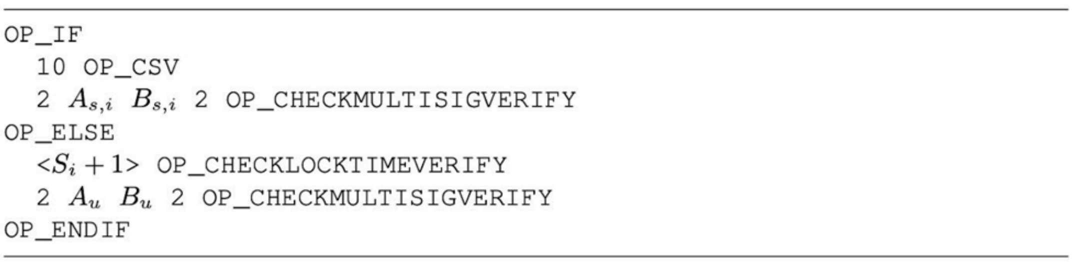
Channel status completion

There are generally two ways for the channel participant to confirm the channel status, by posting the status in blockchain and closing the channel. For cooperative closure of the channel, both participants must cooperate and sign the “closure” transaction. No matter how many off-chain transactions the participants make, there would be only two types of on-chain transactions, which are the funding transaction that opens a channel and the closing transaction that closes it.

Or, the participant can initiate a unilateral closure of the channel. In order to ensure safety, a unilateral closure is interrupted by a time limit. Through this, the other participant can take time to post the latest status in blockchain, effectively ending the unilateral closure with the latest status. In fact, this guarantees that there is no loss of funds apart from the commission fees paid for the unilateral closure.

Floating off-chain transaction

The Eltoo update and account balancing mechanism of Flash Layer must use a function called “floating transaction”. Using this function, it is possible to update the off-chain status of the payment channel by binding new update transactions to replace the previous update transaction.
The floating transaction requires realization of a new signature Hash mechanism and adding a new sequence number to the transaction structure.
The following is an example of an update transaction script.



```
OP_IF
  10 OP_CSV
  2 $A_{s,i}$ $B_{s,i}$ 2 OP_CHECKMULTISIGVERIFY
OP_ELSE
  <$S_i + 1$> OP_CHECKLOCKTIMEVERIFY
  2 $A_u$ $B_u$ 2 OP_CHECKMULTISIGVERIFY
OP_ENDIF
```

Fig 7. Off-chain transaction script example

It is a display script used in the update transaction. Before proceeding with signature verification, compare the lock time of the payment transaction with the script’s status number, Si+1 (it matches the transaction lock time after use).

Hashed time lock contract

The user intending to use Flash Layer may not always provide a channel directly to other users or stores. In this case, they can select a payment route through a third-party channel.

Through the hashed time limit contract, the user can send funds through an intermediate route without risking loss of funds. As a third-party channel is not a channel that can be trusted, use a time limit contract so that the user’s funds are delivered to the destination user or affiliate safely and on time.

Indirect payment routing

When the user wishes to perform a micro-transaction to another user who has directly opened a channel, the Flash Layer finds the most appropriate indirect route to the other user using algorithms. This is referred to as source-based routing.

The algorithms find the optimal path that involves the least intermediate channel hop. It then composes an “onion encryption packet”. This packet includes encrypted packet chains that include routing information for each Flash Layer note. Each middle packet is encrypted in uniquely generated keys that can only be used to decipher the target node. Using encryption warrants that the packet cannot be tampered with along the route. However, if unique keys are used, it is impossible to trace or inspect the packet by searching for a specific byte string for the specified key.

Once the packet starts to be routed in the network, a series of tasks is executed. The node receiving the packet deciphers its own payload, and uses the parameters designated in the payload to proceed with a new channel update signed by the users. After a successful execution, the node keeps routing the packet as the next target node.

Hashed Time-Locked Contracts must be used for signed channel updates. If the payment fails to reach the destination, the channel update may be returned safely, and there is no risk of losing funds in the channel.

Conclusion

The BOSAGORA team aims to overcome the technical and operational issues inherent in many cryptocurrencies. The incentive scheme and issuance plan is aimed towards creating value for the coin while deterring the centralization of power. The Modified Federated Byzantine Agreement algorithm will allow for low latency transactions while being more energy efficient. The Congressional System is aimed towards creating a more democratic and productive decision making process. Trust contracts will provide a decidable and approachable framework for creating and executing contracts on the blockchain. The BOSAGORA team will aim to achieve these goals while leveraging the security and integrity that can be gained through blockchain technology.

Appendix 1: What is the Federated Byzantine Agreement?

In 2015, Professor David Mazieres, head of Stanford's Secure Computer Systems Group, introduced an alternative to pBFT called the Stellar Consensus Protocol, or Federated Byzantine Agreement(hereinafter FBA), a decentralized alternative to existing consensus protocols such as PoW or pBFT.

The consensus protocol is likely to require some extensions in order to make it fully decentralized and open. However, FBA has a proven track record of technical excellence and is unlikely to change. FBA, short for Federated Byzantine Agreement, powers Stellar, the 13th biggest cryptocurrency, with a market capitalization of over 900 million dollars.

Federated Byzantine Agreement can be described by the following:
A network consisting of quorums, and each quorum is a set of nodes sufficient to reach an agreement. FBA also introduces the concept of a quorum slice, the subset of a quorum that can convince one particular node of agreement. The consensus process is achieved via the quorums, and the collective agreement of the quorums is used as the final decision of the entire network despite byzantine failure.

Pros about FBA

There are two main features that FBA is suitable for BOSAGORA consensus protocol.

First, the confirmation of the transaction by the consensus protocol gets finalized in a few seconds. Unlike PoW, there is no mining process which means there should not be much computing power involved to reach an agreement. The agreement happens during the data passing within the voting process. Also, there is no need to validate every single node's data but validate the result of voting of the quorums. As a utility coin, the confirmation speed and low latency are critical to be utilized in a real-life environment.

Second, the membership mechanism of the network is open to the public. In FBA, there is no validator list chosen by someone or an organization. Rather, each validator decides which other validators they trust, and their list of trusted validators is called their quorum slice. The quorum slices of each validator overlap to form a quorum or network-wide consensus on a transaction. Because of the character of the FBA network, anyone can spin up a validator and participate in consensus if any other participating validator adds you to their quorum slice.

Like Bitcoin, we can expect validators joining and leaving the network without much impact on consensus. Currently, the Stellar network is the biggest network utilizing FBA. There is an argument that Stellar network is not yet as decentralized as, say, Bitcoin. But it is important to note that its construction inherently allows for growing decentralization (unlike PBFT) as more and more nodes are added to the network and new quorum slices form. Therefore, this will lead the entire network to a more decentralized network as we wanted.

Openness

Although FBA is pursuing an open network to the public, it still has its shortcomings. For example, to be a validator node, it should have its own quorum set, so the validating node per account can participate in the consensus process. However, if a new node attempting to join the network and declares itself as a validator then composes their own quorum set, but if the existing validators do not accept the new node into their quorum set, the decision of the new node will not be received by the other validators. This will lead the new nodes cannot participate in the decision process.

The SCP (Stellar Consensus Protocol) states that anybody can operate as a node and can join the Stellar network, which characterizes the network to be open. But this is only half correct. Although joining the network is open to anyone, to join the network and participate in the consensus process as a validator is limited. Currently, in the SCP network, to join as a validator, the existing validators must approve and accept the new node. In other words, everyone who wants to join the network needs permission from someone.

Appendix 2: Trust Contract

The original white paper explains trust contract as following:
"Trust Contracts are securely executable contracts based on a protocol layer called Owlchain, which consists of the Web Ontology Language and the Timed Automata Language. Trust Contracts are intended to overcome the issues regarding non-decidable smart contracts by using a more contained and comprehensible programming framework, which provides secure and decidable transactions of contracts."

The ultimate goal of this architecture is to be able to build a decidable contract, which ensures safe and accurate execution while maximizing its scalability.
To achieve the goal, the original white paper mentions two methodologies. One is through using a flexible programming language on a virtual machine, the other is to use a slightly less flexible but decidable domain-specific language. The original plan was going with the second option.

The initial development team(BlockchainOS) researched the inference engine based on semantic web technology. However, there was no result from the research nor discovery of method or technology to overcome the issue.

"An ontology is an explicit specification of a conceptualization. The term is borrowed from philosophy, where an ontology is a systematic account of Existence. In knowledge-based systems, what "exists" is exactly that the contents that can be represented. When the knowledge of a domain is represented in a declarative formalism, the set of objects that can be represented is called the universe of discourse. The set of objects and the describable relationships among them are reflected in the representational vocabulary with which a knowledge-based program represents knowledge. Thus, we can describe the ontology of a program by defining a set of representational terms."[9]

"An ontology is a formal, explicit specification of a shared conceptualization of a domain of interest."

The ontology has been researched and developed in artificial intelligence and the natural language processing field for a long time. It enables the computers to understand the information that is given from the relationships and definitions. On this basis, the computers will eventually infer the requested information.

However, building an ontology in the real-world takes a lot of effort and time. It is not only difficult for the decentralized general public to work on the meaning of the inference engine until the function of the inference engine is completed, but it is also limited in the use of the engine and verify the results according to the input value. And there is no commercialized technology that can make inference engines easy for different situations.

It's even more difficult to automate Time Automata Language-based verification by analyzing semantic source codes that are implemented in OWL. As the complexity of the source code increases, the number of states increases exponentially, making it almost impossible to verify. When OWL is used to write a contract, it will require the complex and detailed specification to produce a realistic contract and if the process of creating a predictable and realistic contract is too difficult to verify, it will be challenging to be used by the users.

[9] A Translation Approach to Portable Ontology Specifications: https://pdfs.semanticscholar.org/5120/f65919f77859a974fcc1ad08f72b2918b8ec.pdf

BOSAGORA team aims to implement Trust Contracts, which enable a safe, accurate, programmable and executable contract as in the original intention.

Rather than continuing what is not feasible, we will redefine "Trust Contracts", and will actively pursue the selecting the optimal direction and applying the suitable technology to improve the core protocol. This approach also considers adopting a methodology that uses flexible programming language on top of virtual machines and we are currently exploring WebAssembly as other industry players do. In the end, we intend to provide an efficient, safely designed smart contract engine and provide an easy-to-develop language with many tools and popularity for easy adoption by developers.

WebAssembly is a new type of code that can be run in a modern web browser. It provides new capabilities and offers significant performance benefits. “WebAssembly is a binary instruction format for a stack-based virtual machine. WebAssembly is designed as a portable target for compilation of high-level languages like C/C++/Rust, enabling deployment on the web for client and server applications.”[10]

Running programs that are written in multiple languages on the web at near-native speeds using client applications was previously impossible. Running the codes on WebAssembly is similar to the actual hardware. With WebAssembly, developers can code in a variety of programming languages such as C++ and Rust, and they can expect to run the program in near-native performance. EOS also uses WebAssembly, and many blockchain platforms such as Ethereum, Tron and Cardano have already introduced or plan to introduce the virtual machines using WebAssembly.

Once the feasibility of the implementation plan has been studied and the solution has been discovered, technical and practical measures will be taken to complete the objectives and directions for the "Trust Contracts" presented in the white paper.

[10] WebAssembly, https://webassembly.org

Appendix 3: BOA Network Commission Fees

Transaction fee

This commission fee is applied to all transactions regardless of the type.
In the earlier version of the white paper, the transaction fee was set at 0.01 BOA; however, it has been improved to change fluidly at the time of a network expansion. Accordingly, this will make flash transactions that are provided for the sake of expandability appear more attractive.

One option suggested for this is to apply the same formula as for data plans. However, according to our request that large-capacity payload (images, etc.) should not be saved in the chain, the data commission fee is designed to increase exponentially. On the other hand, the transaction fee does not follow the same pattern, but will be designed so as to increase linearly.

Considering that a basic transaction involving 2 inputs and 2 outputs would take about 2 * 40 (the size of "Output") + 2 * 132 (the size of "Input") = 342 bytes, the commission fee will be set at 0.01 BOA per 500 bytes.

This commission fee is a minimum commission fee. The user can freely set a higher value per type in order to encourage the inspector to prioritize the user's transaction. Such a prioritization option must be realized in the wallet, and AGORA will guarantee that the minimum commission fee be respected. This will be rendered by a simple selection of "Low" / "Moderate" / "High" that is adjusted according to the network status.

If the BOA reaches a market price that makes such commission fees too high, a protocol upgrade can be anticipated. Such a protocol upgrade simply indicates that AGORA starts to accept transactions that were previously rejected, so forward compatibility will be possible.

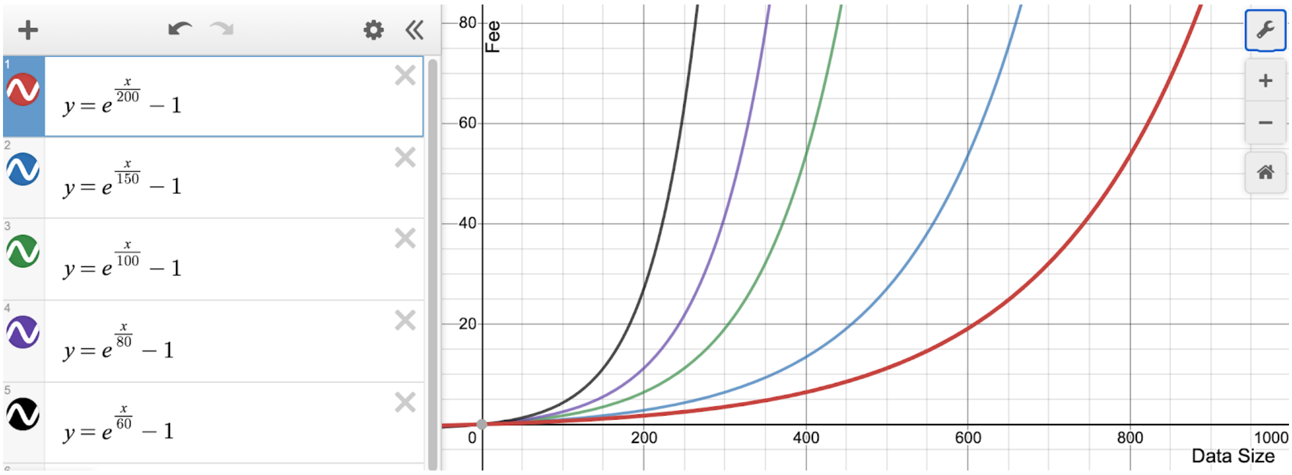
Data fees

A data commission fee is a commission fee that is charged in addition to the transaction fee for transactions involving data (e.g. application data, Votera, etc.). This is implemented to reflect the cost of data storage in the chain. The current formula is as follows.

$$e^{\frac{x}{200}} - 1$$

The main purpose of this formula is to prevent users from saving large items that may contain illegal contents such as images in the chain. Instead, users should focus on saving digest and evidence, and leave the storage space to the appropriate media.

The following shows the other values proposed for the indices for the purpose of comparison.



1 $y = e^{\frac{x}{200}} - 1$

2 $y = e^{\frac{x}{150}} - 1$

3 $y = e^{\frac{x}{100}} - 1$

4 $y = e^{\frac{x}{80}} - 1$

5 $y = e^{\frac{x}{60}} - 1$

Transaction substitution

A function that can substitute a transaction that is in the current transaction pool is provided to the user. This only influences transactions that are not confirmed, the opposite of the transactions externalized in the chain.

We wish for the user to be able to use this function to “cancel” a transaction or “modify” it in the case of an error (e.g. by sending UTXO to the user). To do this, we propose AGORA to accept substitute transactions which incur a commission fee of at least 15% higher than the conventional fee. However, this is not a parameter of the consensus, so it cannot be enforced on the network level.

Proposal commission fee

Funding proposals are a major element of BOSAGORA, and they are for development and expansion. However, in order to prevent the forming of unfair or reckless proposals, 1% of the funding amount at the time of proposal will be charged as the proposal commission fee. In addition, the proposer must provide the data fee and transaction fee required for the Congress members for the first vote (1 round) on the proposal.

The commission fee paid at the time of proposal will not be refunded, regardless of the approval or rejection of the proposal.
The commission fee will be used to compensate the experts for their contribution to the Congress members’ decision by providing good reviews and opinions on the proposal, and to cover the expenses incurred for contract and execution and displays of gratitude as a result of the proposal’s approval.

The goal is automatic processing through contracts in the decentralized status in the future. Until then, the BOSAGROA foundation must disclose expenditures to the Congress.

Appendix 4: BOA-nomics (T-Fi, True Finance)

Recently, cryptocurrency is establishing its position as an alternative currency thanks to the expansion of national currencies and the expansion of the digital ecosystem. It is expanding while solidifying the foundation with an influx of large funds from the conventional financial sector such as large-scale hedge funds, institutional investors, and insurance companies as it is used as a hedge for the decreasing return on investment in conventional finance, a hedge for excessive monetary supply, and a hedge for inflation.

As the foundation for cryptocurrency is becoming stronger, the expansion of cryptocurrency finance to the realm of the real economy is an essential element for the expansion of its base. In response to this, BOSAGORA plans to provide an environment where humanity can enjoy a service for safer and more convenient economic activity by using cryptocurrency. By connecting the traditional finance area where only legal tenders are used with cryptocurrency, we could like to achieve true finance (T-Fi: True Finance) through blockchain, taking one step closer to BOSAGORA's goal to make a better world.

BOSAGORA wants cryptocurrency to be implemented in the human economy in a more complete form. There are conditions that must be met in order to establish a true financial system that is complete with the implementation of cryptocurrency.

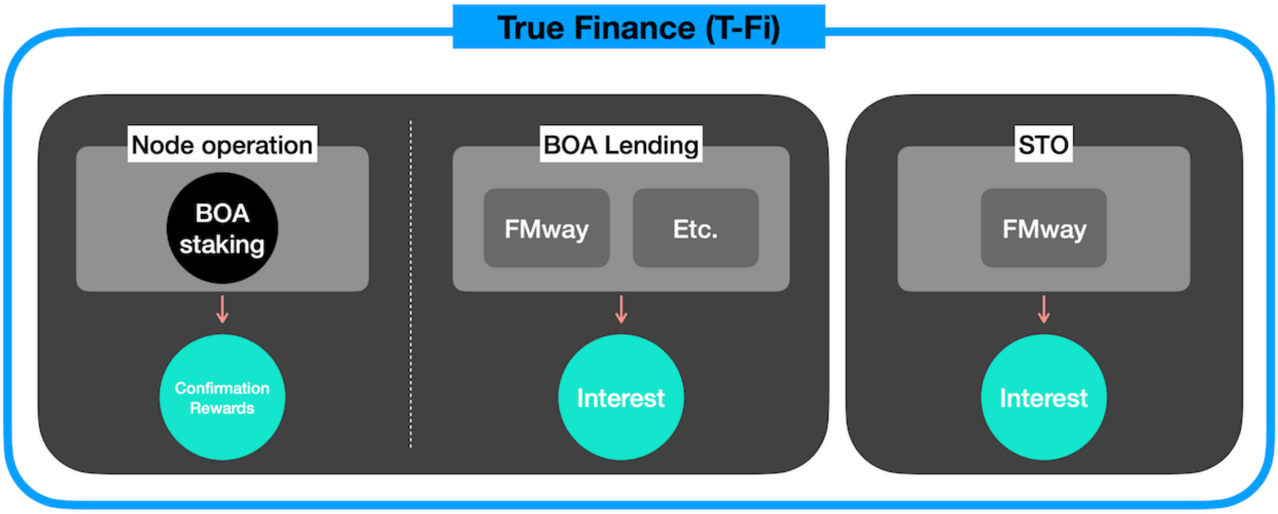
Accessibility
It must be able to approach various real economies that exist. It should be possible to participate in a range of areas where financial values can be created, including stock, real estate, share ownership, private equity funds, loans, and so on. Finance is an economic activity that creates profit by lending and borrowing funds based on trust. Most loan applicants in the real economy are people who need the legal tenders. Even though it may be possible to get a loan in cryptocurrency, it would be viable for them only if securitization to the legal tender is possible.

Perpetuality
For vitalization and expansion of the ecosystem, a reward that is remote from the nature of financial product must not be the motivation for participation. A model that creates profits from economic activity itself must be built. If nonessential and temporary rewards become the main motivation for participation, there is a risk that the number of participants will decrease drastically whenever the rewarded coin price fluctuates. There is also a risk that the ecosystem itself will be deformed. It is possible to keep the ecosystem healthy and sustain it perpetually when there are more participants who are motivated by the profits gained from the economic activity.

Through the next-generational economic business model T-Fi, BOSAGORA plans to build a true financial system in its complete form and expand the cryptocurrency finance to the realm of the real economy.

T-Fi is a DeFi platform operated within the BOSAGORA platform. T-Fi has a structure where blockchain is connected to the real economy through lending, and promotes a broader concept that guarantees fairness and publicness. T-Fi is an innovative busines model that creates more stable and higher profits by converging BOA coin and the real economy products of the world.

Structure of the T-Fi platform
There are three main ways to participate in T-Fi.



First, users can participate in it through BOA node operation consignment. Users who cannot operate nodes directly or users who possess less than 40,000 BOA can participate in the BOA node operation consignment service provided by T-Fi Labs and receive block creation rewards.

Second, users can participate in lending additionally after BOA consignment. For operation of a node, users can lend BOA that is frozen as staking (agreement on lending) and receive additional confirmed rewards. Users will receive a reward at a fixed rate at maturity depending on the lending product.

Third, users can participate through STO project investment. STO projects from the real economy partners who signed a strategic partnership with BOSAGROA will be launched for their respective country, and users can officially register and participate in the projects. Users can gain return on investments by participating directly using BOA, T-Fi's key currency.

Characteristics of T-Fi

First, it is an expanded concept of DeFi. T-Fi is an economic ecosystem that includes the real economy. However, a transparent and trustworthy environment is provided, utilizing the characteristics of T-Fi where all transactions are processed through contracts.

Second, it is fair and safe.
Since BOA of the expected interest rate indicated in the product information announcement is paid in connection with the real economy, fair allocation of profits are enabled without the risk of extortion using bug or contract vulnerabilities. In addition, the T-Fi Labs lending account uses the escrow function, meaning that each participant's asset stays in the wallet and can be withdrawn only through user verification. If there is no participant verification, no one can occupy or move lent assets.

Third, it is a platform that is open to anyone.
Since it is based on the real economy, anyone can easily understand the profit structure and participate in it. In addition, it is possible to participate in excellent overseas products without the restrictions posed by national borders. Various business models that exist in the world can participate in the T-Fi ecosystem and operate projects.

T-Fi's operating entity: T-Fi Labs

T-Fi Labs is a central institution that is in charge of technological, administrative, and legal areas to ensure normal operation of the T-Fi economy model. T-Fi Labs operates nodes for users and provides collaterals for lending assets, serving the role of connecting liquidated collateral assets to the real economy.

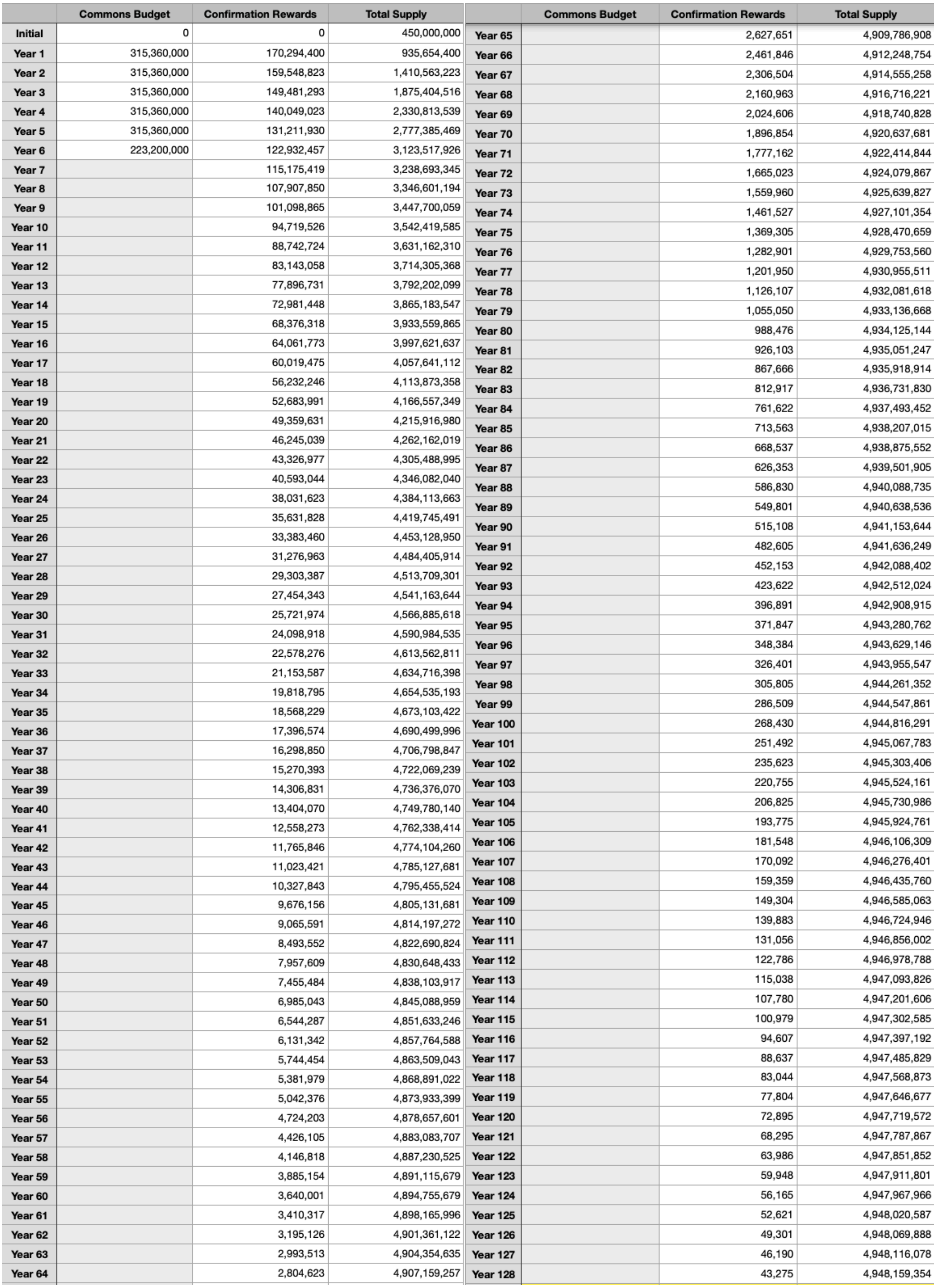
① Asset deposit function
To participate in the T-Fi staking and lending, the BOA holder can participate in staking and lending while possessing the asset in the user's wallet without a transfer of funds. However, since lending takes place in a certain period, the secret key for the lent asset is divided between the participant and T-Fi Labs to act as escrow. The T-Fi Labs provides the secret key only for withdrawals after maturity.

② Issuance and withdrawal of lending certificate token
The T-Fi platform issues a lending certificate token to users who lent BOA (e.g. FMT is issued when lending to FMway). The lending certificate token certifies the lent BOA and the right to future returns. When lending expires, the reward is paid and the lending certificate token is automatically withdrawn and incinerated.

③ Lending certificate token exchange
If the user needs to liquidate the lending before maturity, the user can transfer the lending certificate token via P2P on the lending certificate token exchange. Transferring a lending certificate token means transferring the principal of the lending, the fixed rate reward to be paid at maturity, and the right to airdrop.

Complete decentralization
Even though T-Fi is an economic ecosystem that includes the real economy, a transparent and trustworthy environment is provided utilizing the characteristics of T-Fi where all transactions are processed through contracts. For data generated outside of BOSAGORA's blockchain in the realm of the real economy, the objective is complete decentralization through transformation to on-chain through integration with the middleware Oracle project Chainlink.

Appendix 5: Coin issuance schedule



	Commons Budget	Confirmation Rewards	Total Supply
Initial	0	0	450,000,000
Year 1	315,360,000	170,294,400	935,654,400
Year 2	315,360,000	159,548,823	1,410,563,223
Year 3	315,360,000	149,481,293	1,875,404,516
Year 4	315,360,000	140,049,023	2,330,813,539
Year 5	315,360,000	131,211,930	2,777,385,469
Year 6	223,200,000	122,932,457	3,123,517,926
Year 7		115,175,419	3,238,693,345
Year 8		107,907,850	3,346,601,194
Year 9		101,098,865	3,447,700,059
Year 10		94,719,526	3,542,419,585
Year 11		88,742,724	3,631,162,310
Year 12		83,143,058	3,714,305,368
Year 13		77,896,731	3,792,202,099
Year 14		72,981,448	3,865,183,547
Year 15		68,376,318	3,933,559,865
Year 16		64,061,773	3,997,621,637
Year 17		60,019,475	4,057,641,112
Year 18		56,232,246	4,113,873,358
Year 19		52,683,991	4,166,557,349
Year 20		49,359,631	4,215,916,980
Year 21		46,245,039	4,262,162,019
Year 22		43,326,977	4,305,488,995
Year 23		40,593,044	4,346,082,040
Year 24		38,031,623	4,384,113,663
Year 25		35,631,828	4,419,745,491
Year 26		33,383,460	4,453,128,950
Year 27		31,276,963	4,484,405,914
Year 28		29,303,387	4,513,709,301
Year 29		27,454,343	4,541,163,644
Year 30		25,721,974	4,566,885,618
Year 31		24,098,918	4,590,984,535
Year 32		22,578,276	4,613,562,811
Year 33		21,153,587	4,634,716,398
Year 34		19,818,795	4,654,535,193
Year 35		18,568,229	4,673,103,422
Year 36		17,396,574	4,690,499,996
Year 37		16,298,850	4,706,798,847
Year 38		15,270,393	4,722,069,239
Year 39		14,306,831	4,736,376,070
Year 40		13,404,070	4,749,780,140
Year 41		12,558,273	4,762,338,414
Year 42		11,765,846	4,774,104,260
Year 43		11,023,421	4,785,127,681
Year 44		10,327,843	4,795,455,524
Year 45		9,676,156	4,805,131,681
Year 46		9,065,591	4,814,197,272
Year 47		8,493,552	4,822,690,824
Year 48		7,957,609	4,830,648,433
Year 49		7,455,484	4,838,103,917
Year 50		6,985,043	4,845,088,959
Year 51		6,544,287	4,851,633,246
Year 52		6,131,342	4,857,764,588
Year 53		5,744,454	4,863,509,043
Year 54		5,381,979	4,868,891,022
Year 55		5,042,376	4,873,933,399
Year 56		4,724,203	4,878,657,601
Year 57		4,426,105	4,883,083,707
Year 58		4,146,818	4,887,230,525
Year 59		3,885,154	4,891,115,679
Year 60		3,640,001	4,894,755,679
Year 61		3,410,317	4,898,165,996
Year 62		3,195,126	4,901,361,122
Year 63		2,993,513	4,904,354,635
Year 64		2,804,623	4,907,159,257
Year 65		2,627,651	4,909,786,908
Year 66		2,461,846	4,912,248,754
Year 67		2,306,504	4,914,555,258
Year 68		2,160,963	4,916,716,221
Year 69		2,024,606	4,918,740,828
Year 70		1,896,854	4,920,637,681
Year 71		1,777,162	4,922,414,844
Year 72		1,665,023	4,924,079,867
Year 73		1,559,960	4,925,639,827
Year 74		1,461,527	4,927,101,354
Year 75		1,369,305	4,928,470,659
Year 76		1,282,901	4,929,753,560
Year 77		1,201,950	4,930,955,511
Year 78		1,126,107	4,932,081,618
Year 79		1,055,050	4,933,136,668
Year 80		988,476	4,934,125,144
Year 81		926,103	4,935,051,247
Year 82		867,666	4,935,918,914
Year 83		812,917	4,936,731,830
Year 84		761,622	4,937,493,452
Year 85		713,563	4,938,207,015
Year 86		668,537	4,938,875,552
Year 87		626,353	4,939,501,905
Year 88		586,830	4,940,088,735
Year 89		549,801	4,940,638,536
Year 90		515,108	4,941,153,644
Year 91		482,605	4,941,636,249
Year 92		452,153	4,942,088,402
Year 93		423,622	4,942,512,024
Year 94		396,891	4,942,908,915
Year 95		371,847	4,943,280,762
Year 96		348,384	4,943,629,146
Year 97		326,401	4,943,955,547
Year 98		305,805	4,944,261,352
Year 99		286,509	4,944,547,861
Year 100		268,430	4,944,816,291
Year 101		251,492	4,945,067,783
Year 102		235,623	4,945,303,406
Year 103		220,755	4,945,524,161
Year 104		206,825	4,945,730,986
Year 105		193,775	4,945,924,761
Year 106		181,548	4,946,106,309
Year 107		170,092	4,946,276,401
Year 108		159,359	4,946,435,760
Year 109		149,304	4,946,585,063
Year 110		139,883	4,946,724,946
Year 111		131,056	4,946,856,002
Year 112		122,786	4,946,978,788
Year 113		115,038	4,947,093,826
Year 114		107,780	4,947,201,606
Year 115		100,979	4,947,302,585
Year 116		94,607	4,947,397,192
Year 117		88,637	4,947,485,829
Year 118		83,044	4,947,568,873
Year 119		77,804	4,947,646,677
Year 120		72,895	4,947,719,572
Year 121		68,295	4,947,787,867
Year 122		63,986	4,947,851,852
Year 123		59,948	4,947,911,801
Year 124		56,165	4,947,967,966
Year 125		52,621	4,948,020,587
Year 126		49,301	4,948,069,888
Year 127		46,190	4,948,116,078
Year 128		43,275	4,948,159,354

Reference

The BOSAGORA White Paper, https://bosagora.io/ WebAssembly, https://webassembly.org/

A Translation Approach to Portable Ontology Specifications: https://pdfs.semanticscholar.org/5120/f65919f77859a974fcc1ad08f72b2918b8ec.pdf

The DAO, https://slock.it/dao.html

David Mazieres, Stellar Consensus Protocol, https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Andrychowicz, Dziembowski, Malinowski and Mazurek, Modeling Bitcoin Contracts by Timed Automata, Lecture Notes in Computer Science Formal Modeling and Analysis of Timed Systems, 7-22, 2014, https://arxiv.org/pdf/1405.1861v2.pdf

David Mazieres, Stellar Consensus Protocol, https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Decentralized Prediction Market, https://www.augur.net/

Evan Duffield, Daniel Diaz, Dash: A PrivacyCentric CryptoCurrency, https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

Golem, https://golem.network
Hodges, Andrew, Alan Turing: the enigma, London: Burnett Books

Ian Grigg, The Ricardian Contract, First IEEE International Workshop on Electronic Contracting (WEC) 6th July 2004, http://iang.org/papers/ricardian_contract.html

Leading the Pack in Blockchain Banking: Trailblazers Set the Pace, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&

N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on Ethereum smart contract, https://eprint.iacr.org/2016/1007.pdf

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

Simple Declarative Language, https://sdlang.org/

38

The DAO, https://slock.it/dao.html

Using Decentralized Governance: Proposals, Voting, and Budgets, https://dashpay.atlassian.net/wiki/display/DOC/Using+Decentralized+Governance%3A+Prop osals% 2C+Voting%2C+and+Budgets

OWL Web Ontology Language, https://www.w3.org/TR/owl-features/
OWL Web Ontology Language Reference, https://www.w3.org/TR/owl-ref
Vitalik Buterin, Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper

De Filippi, P. & Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3). Retrieved March 18, 2018 from https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentrali sed- infrastructure

Ehrsam F. (2017) Blockchain Governance: Programming our future. Retrieved March 18, 2018 from https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d 74

Albert O. Hirschman. 1970. Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.Cambridge, MA: Harvard University Press. Retrieved March 18, 2018

Duncan L. (2017) Thoughts on Governance and Network Effects. Medium. Retrieved March 18, 2018 from https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98

Surowiecki J. (2005) The Wisdom of Crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations. Anchor. Retrieved March 18, 2018
Homomorphic Encryption Standardization homepage, Retrieved March 18, 2018 from http://homomorphicencryption.org/introduction/

Bernhard D., Warinschi B. (2014) Cryptographic Voting — A Gentle Introduction. In: Aldini A., Lopez J., Martinelli F. (eds) Foundations of Security Analysis and Design VII. Lecture Notes in Computer Science, vol 8604. Springer, Cham, Retrieved March 18, 2018 from https://link.springer.com/chapter/10.1007/978-3-319-10082-1_7

B. Thiyaneswaran, S. padma. (2012) Iris Recognition Using left and right Iris feature of the Human Eye for Biometric Security system.

39

IJCA, vol 50 No. 152. Retrieved March 18, 2018
from http://www.gjimt.ac.in/wp-content/uploads/2017/11/Vijay-Kumar-Sinha_Enhancing-Iris-Securi ty-by-Detection-of-Fake-Iris_Paper.pdf

Zyskind, Nathan, Pentlend (2016) Decentralizing Privacy: Using Blockchain to Protect Personal Data. Retrieved March 18, 2018
from https://enigma.co/ZNP15.pdf

Fujioka A., Okamoto T., Ohta K. (1993) A practical secret voting scheme for large scale elections. In: Seberry J.,

Zheng Y. (eds) Advances in Cryptology — AUSCRYPT '92. AUSCRYPT 1992. Lecture Notes in Computer Science, vol 718. Springer, Berlin, Heidelberg. Retrieved March 18, 2018 from https://link.springer.com/chapter/10.1007/3-540-57220-1_66

Çetinkaya O., Doganaksoy A. (2007) A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, Availability Reliability and Security 2007. ARES 2007. The Second International Conference on, pp. 432-442, 10–13 April 2007. Retrieved March 18, 2018 from http://ieeexplore.ieee.org/document/4159833/

Dash: Using Decentralized Governance: Proposals, Voting, and Budgets, https://dashpay.atlassian.net/wiki/display/DOC/Using+Decentralized+Governance%3A+Prop osals%2C+Voting%2C+and+Budgets

Understanding Dash Governance https://docs.dash.org/en/stable/governance/understanding.html

Dmytro Kaidalov, Andrii Nastenko, Oleksiy Shevtsov, Mariia Rodinko, Lyudmila Kovalchuk, Roman Oliynykov (2016) A Review of the Dash governance system https://api.zotero.org/groups/478201/items/BJUUEE9Q/file/view?key=Qcjdk4erSuUZ8jvAah5 9Asef

Bingsheng Zhang, Roman Oliynykov, Hamed Balogun (2017) A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence https://www.lancaster.ac.uk/staff/zhangb2/treasury.pdf?utm_content=buffer7118a&utm_medi um=social&utm_source=twitter.com&utm_campaign=buffer

[Nak09] Satoshi Nakamoto. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[KJL18] Ben Kaiser, Mireya Jurado, Alex Ledger. (2018). The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. arXiv:1810.02466v1 [cs.CR]

[KN12] Sunny King, Scott Nadal. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. https://peercoin.net/whitepapers/peercoin-paper.pdf

40

[Poe15] Andrew Poelstra. (2015). On Stake and Consensus. https://download.wpsoftware.net/bitcoin/pos.pdf

[NXT19] NXT Contributors. Version from 2018-07-02 15:03. https://nxtwiki.org/wiki/Whitepaper:Nxt#Nxt.E2.80.99s_Proof_of_Stake_Model

[VB14] Vitalik Buterin. (2014-11-25). Proof of Stake: How I Learned to Love Weak Subjectivity. https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

[DLS88] Cythia Dwork, Nancy Lynch, Larry Stockmeyer. (1988). Consensus in the Presence of Partial Synchrony. https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf

[SCP16] David Maziere. (2016). The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[GTB19] https://arxiv.org/pdf/1902.10865.pdf