BOSagora White Paper

Aug.2024

Table of Contents

Executive Summary

The BOSagora platform is a decentralized self-evolving public blockchain platform that is built on Smart Contracts and an embedded decision-making system called Congress Network.

(1) Smart 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.

Background

The blockchain was first conceptualized in Satoshi Nakamoto's white paper "Bitcoin: A Peer-to-Peer Electronic Cash System"[1] 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 a 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 an 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.[2]

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.

---

[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

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 our daily life by enabling meaningful projects with the expression of collective intelligence by an advanced democratic decision-making process.

Core Values and Key Attributes

Forward Thinking

Pioneering future realization: We aim to develop the first full-node Proof of Stake consensus algorithm blockchain platform with innovative technology development so 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 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. Additionally, BOSagora will be developing a "Decentralized Loyalty Point System," a business model that has high demand from ecosystem organizations and can be implemented by any company in the world, in order to activate the mainnet.

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.
Additionally, BOSagora will be developing a "Decentralized Loyalty Point System," a business model that has high demand from ecosystem organizations and can be implemented by any company in the world, in order to activate the mainnet.

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. A validator has the right to vote.

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 Commons Budget specifically for the development of the BOSagora ecosystem through these proposals. We will explain these further later in this paper.

Consensus Algorithm

Overview

The consensus algorithm is core to any decentralized blockchain. The algorithm attempts to answer the question, 'How can we prove with confidence that all distributed copies of block data hold exactly the same information?'

In response to this question, BOSagora originally created a solution using mFBA (Modified Federated Byzantine Agreement) which was FBA (Federated Byzantine Agreement) provided by SCP (Stellar Consensus Protocol) modified by adding Proof of Stake by requiring Validators to freeze 40,000 BOA.

However, during the testing process, we found that we need a long time and large human resources to support a vast number of validators due to the limitations of SCP. A large number of validators are an essential requirement for a truly decentralized blockchain. There is an urgent need for an alternative plan for mFBA that enables the support of a large number of validators more efficiently.

At the same time, in order to compete with other public blockchain platforms currently in operation, we need to quickly create network use cases. To this end, the versatility of blockchain algorithms and technical elements is essential.

In conclusion, in order for the BOSagora network to survive as a blockchain under the deepening competition situation, it is a ground task to launch a highly versatile network in a short period of time. For this reason, we decided to use a proven consensus algorithm that can support a large number of validators. It already has use cases that have been active for many developers and users.

Hence the change to use Gasper, which is a well-established and tested Proof of Stake (PoS) consensus algorithm, used in Ethereum's Beacon Chain since 1st December 2020.

Gasper

BOSagora now uses an algorithm known as Gasper. Gasper is a combination of Casper the Friendly Finality Gadget (Casper-FFG) and the LMD-GHOST fork choice algorithm. Gasper is an algorithm defining how validators (nodes that have the required stake and run a validator client) get rewarded or penalized depending on how they participate in proposing and attesting blocks. It also specifies which fork of the blockchain to build on when there are more than one.

See Gasper and Combining GHOST and Casper for more details on Gasper.

Casper FFG

Inspired by PBFT (Practical Byzantine Fault Tolerance) Casper was introduced by Buterin and Griffith in Casper the friendly finality gadget to define the concepts of justification and finalization.

Justification for a block is reached when it is attested by Validators with at least two-thirds of the frozen coins. A justified block is only considered finalized when the following justified block is added to the chain. Justification and finalization do not occur for every block (also often referred to as slot) but only for blocks at the epoch boundaries and are known as checkpoint blocks. Each epoch has up to 32 slots as sometimes the assigned validator is offline or does not complete the proposed block in time to be included in the chain.

By marking certain blocks as finalized other participants with partial information can still be fully confident that the blocks are part of the canonical chain of blocks.

LMD GHOST

A fork-choice rule where validators attest to blocks to signal support for those blocks. To prevent validators from voting in ways to attempt to break the protocol, like attesting to conflicting blocks, penalties are introduced for those that misbehave.

Features	Bitcoin	Ethereum	BOSagora
Coin	BTC	ETH	**BOA**
Core Features	Financial Transactions (Bitcoin Script)	Smart Contract (EVM)	**Smart Contract (EVM)**
Decision Making Process	Non-systematic	Non-systematic	**Congress Network (1validator = 1vote)**
Consensus Algorithm	PoW	Ethereum 1.0 : PoW Ethereum 2.0 : Gasper PoS	**Gasper PoS**
Block Size	1Mb	Dynamic	**Dynamic**

Fig 1. Comparison of Cryptocurrencies

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 within 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 proposal" 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

BOSagora 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” will ensure transparency and clarify responsibility by storing decision-making data in the blockchain. To maintain confidentiality, the hash of the voting data for data verification will be stored in the blockchain during the voting period. At the end of the voting period, the voting data will be stored in the blockchain, and the data will be verified with the recorded hash. Information about discussion and pre-evaluation will be stored on a separate server, and the information will be provided for participants to check at any time.

Procedures of the Congress Network Proposal

① Join the Congress Network

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

- Stake at least 40,000 BOA
- Operate a validator node at a stable network speed (operate on a server or personal computer)

In addition, the following cases will result in the loss of Congress Network qualifications.

- When the stake is reduced due to penalties for continuous network stability hazards and the deposit balance falls below 20,000 BOAs
- When a member conducts an act deemed inappropriate in the process of proposing and voting. See the "Reward System/Slashing" section below for details

② Create a proposal

Any member can open a proposal and start a discussion and decision-making process. A member can participate in three types of activities as follows for the proposal.

- Discussion: The members can share their opinions and develop ideas for the new proposal.
- Assessment: The members can assess the proposal in terms of its fitness in the case of a Commons Budget spending proposal and determine to proceed with the proposal.
- Voting: The members can vote for approval, rejection, or abstention on the proposal.

③ Enter the information of a proposal

A proposer should enter the information necessary for other members to understand the proposal. A proposer should deposit the required fees that are to prevent abusing the decision-making system. This fee must be paid according to the policy when registering a proposal. The required fee is automatically calculated for each type of proposal. The information necessary to create a proposal is as follows.

- Type of proposal
- Name of proposal
- Assessment period (only for Commons Budget spending proposal)
- Voting period
- Funding amount (only for Commons Budget spending proposal)
- Objective and description
- Relevant attached data

In order to improve the completeness of the proposal and to prevent it from abuse, the proposer shall deposit a fee when generating the proposal. The fee is 0.1% of the requested budget when proposing support for the Commons Budget, and 100BOA when proposing a system upgrade. The fee is non-refundable.

④ Discuss

Members can write opinions and leave comments freely on a proposal. Good opinions can be recommended, and it is possible to sort the opinions by recency or number of recommendations. The members can leave comments on opinions, but opinions and comments cannot be deleted or changed once created.

⑤ Vote

A vote is created in order to reach an agreement. Individual votes are stored directly on the blockchain by validators.

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 on 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 a system upgrade is passed, the development team commences development according to the proposal (executing tasks related to a development plan, roadmap,

security test, etc.). Even if a proposal is related to a system upgrade, if expenses are incurred from proceeding with the development and implementation, the proposal should take the form of a Commons Budget spending plan. If the proposal for the Commons Budget is approved, the proposer can withdraw the requested funds through the smart contract 24 hours after the end of voting. The foundation may reject Commons Budget expenditures within 24 hours from the closing time of voting in case of any fraud detected during the voting process.

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 Smart 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 Staking

Coin staking is an action performed to lock coins to be used as a stake in the PoS consensus. To run a node and receive an incentive as a validator, one must stake the required coins. These coins are used as collateral against an attempt to forge the blockchain. In other words, if a node tries to forge the blockchain it will pay penalties from the staking balance. To encourage the network to find and punish nodes requiring slashing, the whistleblower and proposer nodes are given a reward.

Reward System

There are two ways for Congress Members to receive BOA: Confirmation Rewards and transaction fees. Note that Confirmation Rewards are newly issued coins whereas transaction fees are just existing coins being taken from the transaction sender's account balance.

Confirmation Reward

Each epoch of 32 slots has a randomly chosen set of validators(Committee). Each slot is allocated a validator responsible to propose the contents of the block at that slot. If the validator is offline or is late in proposing the block then that slot will be marked as a missed slot and the validator will not receive the possible reward.

The chosen committee is responsible for attestations that vote for source and target checkpoints for Casper FFG and chain head block for LMD-GHOST. These attestations must be correct and timely to receive the full reward. In every epoch, there is a fixed allocation of possible rewards if the proposer and committee perform all their tasks perfectly. This fixed amount is calculated as 7 BOA coins every 5 seconds for the first year of the blockchain and is reduced by 1.347% each year after.

As the proposer and committee are randomly chosen, not all validators will get rewards for every block but will be rewarded when they complete their allocated tasks.

Slashing

Slashing only occurs for one of the following protocol violations:

① a misbehaving block proposer who proposes two different blocks at the same slot height

② an attester who publishes a vote with different source checkpoints for the same target checkpoint.

③ an attester which publishes a vote that surrounds or is surrounded by another of its votes in relation to source and target checkpoints.

If slashing occurs then the validator is ejected from the validator pool immediately.

Transaction Fee

Transaction fees are adjusted flexibly. 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 Congress.

Commons Budget

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 BOA coin buy-back, bounty and marketing campaigns, initial expenses for projects/services to be introduced in the BOSagora ecosystem, and so on.

1.8 billion BOA will be generated as the Commons Budget in the first 5years, and 30% of the transaction fees will be sent to the Commons Budget as well whenever a block is created. 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 Smart Contract.

Token Distribution and Issuance

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 the 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 the tokens will be the following:

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

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

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

Category			Number of BOA	Share
Initial 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 %
	Initial 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	
	Initial circulating supply total		**450,000,000**	
Additional supply	Confirmation Rewards		2,700,000,000	54.54 %
	Commons Budget		1,800,000,000	36.36 %
Total			**4,950,000,000**	**100 %**

Fig 2. Token distribution and issuance plan

Issuance

New coins are issued in three ways; Initial Development Budget(0.45 billion, 10%), Confirmation Rewards (2.7 billion, 54%), and the Commons Budget (1.8 billion, 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 before the Genesis block, intending 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 distributed to honest validators who perform their required tasks. If the Validators do not perform perfectly then some of the allocated BOA is held back in the form of penalties and will be sent to the Commons Budget to keep the total supply as specified. 2.7 billion BOA are issued through Confirmation Rewards. Initially, 7 BOA are issued per 5 seconds. The reward decreases every year by 1.347% over 128 years.
- **Commons Budget:** The Commons Budget holds BOA that can only be used by proposals that have passed the Congress Network. To create a sufficient budget for proposals, 50 coins are issued per 5 seconds until 1.8 billion are issued within about five years. And 30% of the transaction fee is also sent to Commons Budget.

After MainNet is launched, block Confirmation Rewards and the Commons Budget will be generated. A table with 128 years of coin issuance is attached at the end of this document.

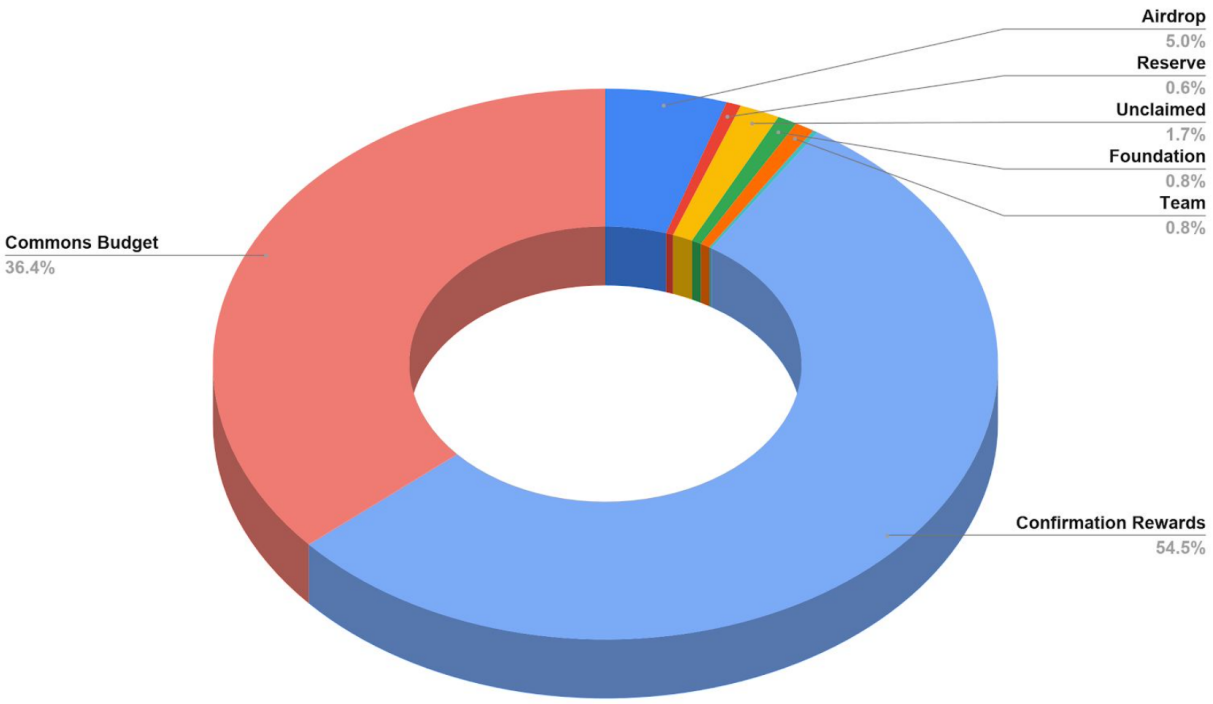

Fig 3: BOA Coin Issuance Plan

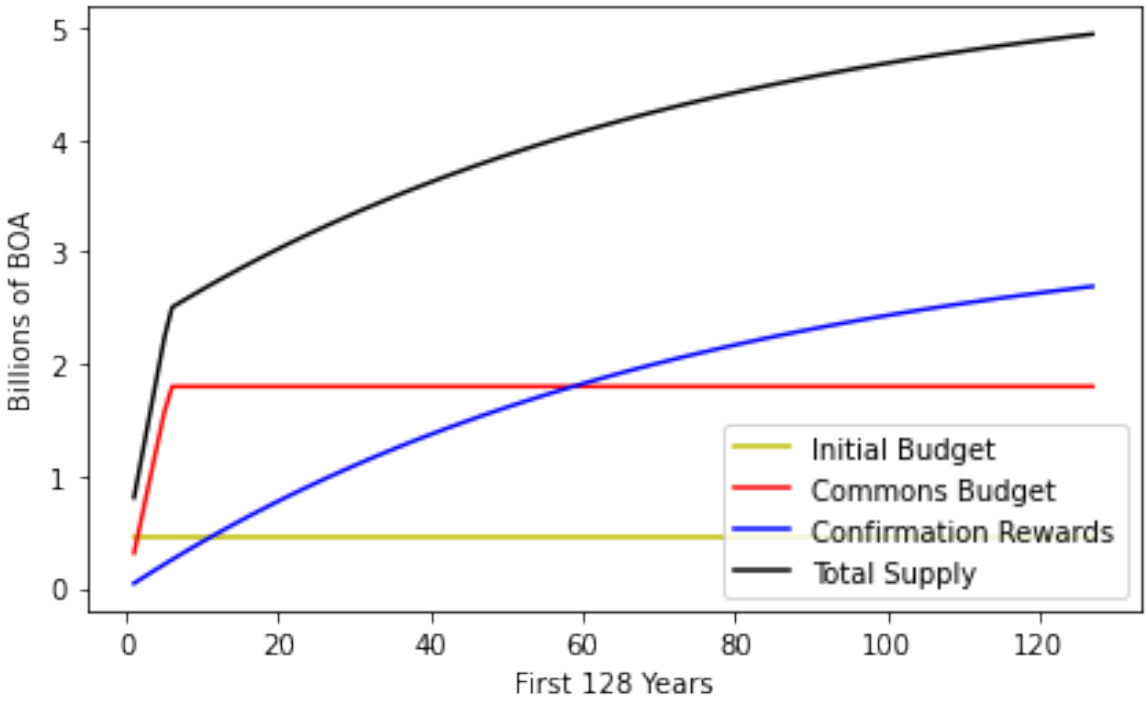

Fig 4: Cummulative coin issuance

Conclusion

The BOSagora team aims to overcome the technical and operational issues inherent in many cryptocurrencies. The incentive scheme and issuance plan are aimed toward creating value for the coin while deterring the centralization of power. The Gasper Proof of Stake algorithm will allow for low latency transactions while being more energy efficient. The Congress system is aimed at creating a more democratic and productive decision-making process. Smart 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: Change of Confirmation Rewards and Commons Budget plan

1. Background

Currently, BOSagora is nearing the launch of its MainNet. What needs to be noted, however, is that the issuance plan was published five years ago and a lot has changed since then. As a result, we've recognized the need to make an amendment and improve the issuance plan in order to maintain sustainable growth of BOA ecosystem. Below, we identified **the issue with the previous Confirmation Reward issuance plan**, and the more **reasonable issuance plan and policy** are provided to resolve the issue presented. Also, we suggested **a policy for the safe usage of Commons Budget**.

2. Previous Issuance Plan

New BOA coins are issued through Confirmation Rewards and Commons Budget. For Confirmation Rewards, 27 BOA are issued per 5 seconds initially and the reward decreases every -approximately- one year by 6.31% over 128 years. 2.7 billion BOA are issued through Confirmation Rewards. As for the Commons Budget, 50 coins are issued per 5 seconds and 1.8 billion BOAs are issued over 5 years. A closer look at the BOSagora Foundation's policy on the issuance plan is as follows;

3. Confirmation Rewards Issuance Plan

3.1. Previous Confirmation Rewards Issuance plan

Below is a table of the amount of new BOA being issued as Confirmation Rewards with estimated APR for each year.

			Confirmation Rewards / 5s (BOA, 1st yr)			27
			Decrease in rewards each year (%)			6.31
Year	Issuance (BOA/5s)	Issuance (BOA/year)	Cumulative issuance (BOA)	APR by the number of participating validators (%, truncated)		
				1,000	2,000	5,000	10,000
1	27.00	170,294,400	170,294,400	426	213	85	43
2	25.30	159,548,823	329,843,223	399	199	80	40
3	23.70	149,481,293	479,324,516	374	187	75	37
4	22.20	140,049,023	619,373,539	350	175	70	35
5	20.80	131,211,930	750,585,469	328	164	66	33
6	19.49	122,932,457	873,517,926	307	154	61	31
7	18.26	115,175,419	988,693,345	288	144	58	29
8	17.11	107,907,850	1,096,601,194	270	135	54	27
9	16.03	101,098,865	1,197,700,059	253	126	51	25
10	15.02	94,719,526	1,292,419,585	237	118	47	24

[Table 1] Previous Confirmation Reward issuance plan and APR by the number of validators

First, APR is calculated over next 10 years. Since there is a fixed amount of BOA being issued per year and the amount is distributed to validators, APR depends on the number of participating validators. APR decreases as the number of participating validators increases. Simply put, APR is affected by Confirmation Rewards and the number of participating validators.
If the amount of staked BOA is 40,000 and the number of validators operating on the network is 1,000, APR is calculated to be at 426%. And if there are 2,000 validators operating, APR is at 213%.
These numbers are very high in comparison to interest rates offered by other major platforms shown in [Table 2].

Platform	APR
Ethereum	4.56%
Solana	6.79%
Cardano	13.79%
Avalanche	9.02%
BNB Chain	5.1%
Polkadot	14.81%
Tron	3.15%
Polygon	13.48%

Source - https://www.stakingrewards.com

[Table 2] APR from other major platforms

3.2. Amendment to Confirmation Rewards Issuance Plan

Although a high Confirmation Reward provides a strong motivation to partake as a validator, it can also lead to an inflation effect that can cause coin devaluation among other things. The foundation has been running simulations in various ways as shown in [Table 4], to find the optimal inflation rate at which enough motivation can be provided to encourage validator participation. We concluded that if 7 BOA are issued per 5 seconds with the rewards decreasing every year by 1.347% over 128 years, inflation and rewards can be properly maintained for the network's continual growth.

APR remains at 10% with 10,000 participating validators as seen in [Table 3]. In addition, APR is still very high at 110% with initial 1,000 validators. This number should be sufficient enough to attract many to participate as validators.

Therefore, the most appropriate Confirmation Reward plan that the foundation can choose is as follows;

7 BOA are issued per 5 seconds decreasing every year by 1.347% over 128 years.
Total BOA being issued through Confirmation Rewards are 2,700,000,000.

Although the foundation decides and applies Confirmation Rewards at the MainNet launch, the rewards can be amended by the Congress Network through proposals and voting after the Congress Network with voting rights is established.

Confirmation Rewards / 5s (BOA, 1st yr)	7
Decrease in rewards each year (%)	1.347

Year	Issuance (BOA/5s)	Issuance (BOA/year)	Cumulative issuance (BOA)	APR by the number of participating validators (%, truncated)			
				1,000	2,000	5,000	10,000
1	7.00	44,150,400	44,150,400	110	55	22	11
2	6.91	43,555,694	87,706,094	109	54	22	11
3	6.81	42,968,999	130,675,093	107	54	21	11
4	6.72	42,390,206	173,065,300	106	53	21	11
5	6.63	41,819,210	214,884,510	105	52	21	10
6	6.54	41,255,906	256,140,416	103	52	21	10
7	6.45	40,700,189	296,840,604	102	51	20	10
8	6.37	40,151,957	336,992,561	100	50	20	10
9	6.28	39,611,110	376,603,671	99	50	20	10
10	6.20	39,077,549	415,681,220	98	49	20	10

[Table 3] Optimal Confirmation Reward issuance plan and APR by the number of validators

3.3. Counter-measure for Initial High Inflation

The Initial supply is 450,000,000 BOA. As indicated in [Table 3], inflation still remains high for the amended issuance plan - the amount of new BOA issued through Confirmation Rewards each year almost equals that of the initial supply. Therefore, the foundation plans to run 1,000 validators using 40,000,000 BOA in possession and burn the Confirmation Rewards earned from it.
If there are 2,000 validators operating on the network with 1,000 Foundation validators, a maximum amount of 22,000,000 BOA per year will be burned. This policy will prevent initial high inflation.

4. Plan for Commons Budget

Although the Commons Budget is generated in a short period compared to the Confirmation Rewards, it has raised concerns for high inflation due to the fact the amount being issued is substantial. However, the Commons Budget will be used in various areas for the purpose of flourishing the ecosystem. For example, the Commons Budget can be spent on BOA coin buy-back, bounty, marketing campaigns,

initial expenses for projects/services to be a part of the BOSagora ecosystem, and so on. In addition, any use of the Commons Budget requires approval through proposal and voting by the Congress Network. Thus, it is more important that the members of Congress remain active participants in assessing proposals and casting votes for applying the Commons Budget for appropriate use than the amount of Commons Budget being issued.

With this consideration, the Foundation plans to suspend the use of the Commons Budget until the number of Congress Members reaches 2,000 in order to guarantee careful spending of the Commons Budget. This plan will ensure the Commons Budget is spent on necessary businesses with proactive participation and careful reviews by Congress Members of a sizable number.

5. Conclusion

The Foundation plans to suppress inflation by 1) optimizing the Confirmation Rewards rate that has been previously set at an exceedingly high rate and 2) burning Confirmation Rewards generated by using BOA in possession.

In addition, the Foundation plans to suspend the use of the Commons Budget until the number of Congress Members reaches 2,000 in order for the Commons Budget to be utilized through discussions and reviews by a sizable number of Congress Members.

Issuance/5s (decrease rate each year)	Year	Issuance (BOA/5s)	Issuance (BOA/year)	Cumulative issuance (BOA)	APR by the number of participating validators (%, truncated)			
					1,000	2,000	5,000	10,000
27BOA (6.31%)	0		450,000,000	450,000,000				
	1	27.00	170,294,400	620,294,400	426	213	85	43
	2	25.30	159,548,823	779,843,223	399	199	80	40
	3	23.70	149,481,293	929,324,516	374	187	75	37
	4	22.20	140,049,023	1,069,373,539	350	175	70	35
20BOA (4.7%)	0		450,000,000	450,000,000				
	1	20.00	126,144,000	576,144,000	315	158	63	32
	2	19.06	120,215,232	696,359,232	301	150	60	30
	3	18.16	114,565,116	810,924,348	286	143	57	29
	4	17.31	109,180,556	920,104,904	273	136	55	27
10BOA (2.2%)	0		450,000,000	450,000,000				
	1	10.00	63,072,000	513,072,000	158	79	32	16
	2	9.78	61,684,416	574,756,416	154	77	31	15
	3	9.56	60,327,359	635,083,775	151	75	30	15
	4	9.35	59,000,157	694,083,932	148	74	30	15
7BOA (1.347%)	0		450,000,000	450,000,000				
	1	7.00	44,150,400	494,150,400	**110**	**55**	**22**	**11**
	2	6.91	43,555,694	537,706,094	**109**	**54**	**22**	**11**
	3	6.81	42,968,999	580,675,093	**107**	**54**	**21**	**11**
	4	6.72	42,390,206	623,065,300	**106**	**53**	**21**	**11**
5BOA (0.7%)	0		450,000,000	450,000,000				
	1	5.00	31,536,000	481,536,000	79	39	16	8
	2	4.97	31,315,248	512,851,248	78	39	16	8
	3	4.93	31,096,041	543,947,289	78	39	16	8
	4	4.90	30,878,369	574,825,658	77	39	15	8
3BOA (0%)	0		450,000,000	450,000,000				
	1	3.00	18,921,600	468,921,600	47	24	9	5
	2	3.00	18,921,600	487,843,200	47	24	9	5
	3	3.00	18,921,600	506,764,800	47	24	9	5
	4	3.00	18,921,600	525,686,400	47	24	9	5

[Table 4] Simulation: APR by Confirmation Rewards issuance amount and the number of participating validators

Appendix 2: Fees

Gas Fees

To help keep the network secure a fee for executed computation, known as gas, is charged to the account initiating the computation. This means that it is costly to try and overload the system with huge volumes of transactions. It also safeguards against smart contract code which enters infinite loops or resource-wasting computations as the allocated gas will eventually run out.

Base Fee

The minimum cost per unit of gas is not fixed but can dynamically change over time depending on the network load. These base fees will be sent to the Commons Budget.

Tip

To give more incentive for the block proposer to include a transaction then a tip per unit of gas can be added. This part of the fee goes to the Validator who is building the block as this block proposer has the choice of which transactions to include.

Total Fee

fee = gas units * (base fee + tip)

Payment Transaction

A transaction that sends a quantity of coin units from one account to another requires 21,000 units of gas to be paid for in fees. These fees are taken from the sender's account balance.
For example, if Bob pays Alice 100 BOA and the base fee is 90 Gwei and a tip is added for 10 Gwei:
Bob's account will be reduced by the following amount of Gwei:
100_000_000_000 + (21_000 * (90 + 10))
= 100_000_000_000 + 2_100_000
= 100_002_100_000 Gwei
= 100.0021 BOA
and Alice will have her account increased by 100 BOA

Smart Contracts

When a transaction includes calls to Smart Contracts then the gas used for the computations within are also charged to the transaction owner. As BOSagora blockchain utilizes the well-established EVM (Ethereum Virtual Machine) for executing smart contracts you can check Appendix G of the Ethereum Yellow Paper for details of how the quantity of gas is calculated for various operations.

Appendix 3: Coin issuance schedule

Year	Commons Budget	Confirmation Rewards	Total Supply	Year	Commons Budget	Confirmation Rewards	Total Supply
Initial	0	0	450,000,000.00	34		28,221,131.85	3,460,794,862.72
1	315,360,000.00	44,150,400.00	809,510,400.00	35		27,840,993.20	3,488,635,855.92
2	315,360,000.00	43,555,694.11	1,168,426,094.11	36		27,465,975.02	3,516,101,830.94
3	315,360,000.00	42,968,998.91	1,526,755,093.02	37		27,096,008.34	3,543,197,839.28
4	315,360,000.00	42,390,206.50	1,884,505,299.52	38		26,731,025.10	3,569,928,864.38
5	315,360,000.00	41,819,210.42	2,241,684,509.94	39		26,370,958.20	3,596,299,822.58
6	223,200,000.00	41,255,905.65	2,506,140,415.59	40		26,015,741.39	3,622,315,563.97
7		40,700,188.60	2,546,840,604.19	41		25,665,309.35	3,647,980,873.32
8		40,151,957.06	2,586,992,561.25	42		25,319,597.64	3,673,300,470.96
9		39,611,110.20	2,626,603,671.45	43		24,978,542.66	3,698,279,013.61
10		39,077,548.55	2,665,681,220.00	44		24,642,081.69	3,722,921,095.30
11		38,551,173.97	2,704,232,393.96	45		24,310,152.85	3,747,231,248.15
12		38,031,889.65	2,742,264,283.62	46		23,982,695.09	3,771,213,943.23
13		37,519,600.10	2,779,783,883.72	47		23,659,648.18	3,794,873,591.42
14		37,014,211.09	2,816,798,094.80	48		23,340,952.72	3,818,214,544.14
15		36,515,629.66	2,853,313,724.47	49		23,026,550.09	3,841,241,094.23
16		36,023,764.13	2,889,337,488.60	50		22,716,382.46	3,863,957,476.69
17		35,538,524.03	2,924,876,012.63	51		22,410,392.79	3,886,367,869.48
18		35,059,820.11	2,959,935,832.74	52		22,108,524.80	3,908,476,394.28
19		34,587,564.33	2,994,523,397.07	53		21,810,722.97	3,930,287,117.25
20		34,121,669.84	3,028,645,066.91	54		21,516,932.53	3,951,804,049.78
21		33,662,050.95	3,062,307,117.86	55		21,227,099.45	3,973,031,149.23
22		33,208,623.12	3,095,515,740.98	56		20,941,170.42	3,993,972,319.65
23		32,761,302.97	3,128,277,043.95	57		20,659,092.85	4,014,631,412.50
24		32,320,008.22	3,160,597,052.17	58		20,380,814.87	4,035,012,227.38
25		31,884,657.71	3,192,481,709.88	59		20,106,285.30	4,055,118,512.68
26		31,455,171.37	3,223,936,881.24	60		19,835,453.63	4,074,953,966.31
27		31,031,470.21	3,254,968,351.45	61		19,568,270.07	4,094,522,236.38
28		30,613,476.31	3,285,581,827.76	62		19,304,685.48	4,113,826,921.86
29		30,201,112.78	3,315,782,940.54	63		19,044,651.36	4,132,871,573.22
30		29,794,303.79	3,345,577,244.33	64		18,788,119.91	4,151,659,693.13
31		29,392,974.52	3,374,970,218.85	65		18,535,043.93	4,170,194,737.06
32		28,997,051.15	3,403,967,270.00	66		18,285,376.89	4,188,480,113.96
33		28,606,460.87	3,432,573,730.87	67		18,039,072.87	4,206,519,186.82
68		17,796,086.55	4,224,315,273.37	99		11,688,094.15	4,671,658,832.60

69		17,556,373.27	4,241,871,646.64	100		11,530,655.52	4,683,189,488.12
70		17,319,888.92	4,259,191,535.56	101		11,375,337.59	4,694,564,825.72
71		17,086,590.02	4,276,278,125.58	102		11,222,111.80	4,705,786,937.51
72		16,856,433.65	4,293,134,559.23	103		11,070,949.95	4,716,857,887.47
73		16,629,377.49	4,309,763,936.71	104		10,921,824.26	4,727,779,711.72
74		16,405,379.77	4,326,169,316.49	105		10,774,707.28	4,738,554,419.01
75		16,184,399.31	4,342,353,715.79	106		10,629,571.98	4,749,183,990.98
76		15,966,395.45	4,358,320,111.24	107		10,486,391.64	4,759,670,382.62
77		15,751,328.10	4,374,071,439.34	108		10,345,139.95	4,770,015,522.57
78		15,539,157.71	4,389,610,597.05	109		10,205,790.91	4,780,221,313.48
79		15,329,845.26	4,404,940,442.31	110		10,068,318.91	4,790,289,632.39
80		15,123,352.24	4,420,063,794.55	111		9,932,698.65	4,800,222,331.04
81		14,919,640.69	4,434,983,435.24	112		9,798,905.20	4,810,021,236.24
82		14,718,673.13	4,449,702,108.37	113		9,666,913.95	4,819,688,150.19
83		14,520,412.60	4,464,222,520.97	114		9,536,700.62	4,829,224,850.80
84		14,324,822.64	4,478,547,343.61	115		9,408,241.26	4,838,633,092.06
85		14,131,867.28	4,492,679,210.89	116		9,281,512.25	4,847,914,604.31
86		13,941,511.03	4,506,620,721.92	117		9,156,490.28	4,857,071,094.59
87		13,753,718.88	4,520,374,440.80	118		9,033,152.36	4,866,104,246.95
88		13,568,456.28	4,533,942,897.08	119		8,911,475.79	4,875,015,722.74
89		13,385,689.18	4,547,328,586.26	120		8,791,438.21	4,883,807,160.96
90		13,205,383.94	4,560,533,970.20	121		8,673,017.54	4,892,480,178.50
91		13,027,507.42	4,573,561,477.62	122		8,556,192.00	4,901,036,370.50
92		12,852,026.90	4,586,413,504.52	123		8,440,940.09	4,909,477,310.58
93		12,678,910.09	4,599,092,414.61	124		8,327,240.63	4,917,804,551.21
94		12,508,125.18	4,611,600,539.79	125		8,215,072.70	4,926,019,623.91
95		12,339,640.73	4,623,940,180.52	126		8,104,415.67	4,934,124,039.57
96		12,173,425.77	4,636,113,606.28	127		7,995,249.19	4,942,119,288.76
97		12,009,449.72	4,648,123,056.01	128		7,887,553.18	4,950,006,841.94
98		11,847,682.44	4,659,970,738.44				

Reference

The BOSagora White Paper, https://BOSagora.io/

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

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

Using Decentralized Governance: Proposals, Voting, and Budgets, https://wiki.terracoin.io/view/Using_Decentralized_Governance:_Proposals;_Voting;_and_Budgets
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-decentralised-infrastructure

Ehrsam F. (2017) Blockchain Governance: Programming our future. https://fehrsam.xyz/blog/blockchain-governance-programming-our-future

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. https://medium.com/aragondec/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, 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 Bio-metric Security system.

IJCA, vol 50 No. 152. http://www.gjimt.ac.in/wp-content/uploads/2017/11/Vijay-Kumar-Sinha_Enhancing-Iris-Security-by-Detection-of-Fake-Iris_Paper.pdf

Zyskind, Nathan, Pentlend (2016) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 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. http://ieeexplore.ieee.org/document/4159833/

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

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

[Nak09] Satoshi Nakamoto. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. White paper https://bitcoin.org/bitcoin.pdf

[KJL18] Ben Kaiser, Mireya Jurado, Alex Ledger. (2018). The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. https://arxiv.org/pdf/1810.02466.pdf [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

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

[NXT19] NXT Contributors. 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

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