The BOScoin Platform White Paper

Initial Version: 20161101 / Current Version: 20170430

Han-Kyul Park, Changki Park, Yezune Choi, Jake Hyunduk Choi

BOScoin, the Self-Evolving Cryptocurrency Platform

Abstract. *The BOScoin 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 called Owlchain, which consists of the Web Ontology Language and the Timed Automata Language. Trust Contracts aim 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. (2) The Congress Network is the decision making body in the BOScoin 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.*

1. Introduction

a. 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 has successfully supported over 180 million peer-to-peer transactions and now has a market capitalization of more than 10 billion dollars.

Following the success of Bitcoin, there have been numerous systems leveraging blockchain technology. There are hundreds of competing cryptocurrencies and according to a recent IBM report, more than 90% of banks are investing in blockchain technology[2]. Currency transactions are the most common applications of blockchain technology. 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

[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&

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.

Smart contracts have 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 contracts 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 smart contracts 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 smart contracts has inevitably led to a series of security vulnerabilities[6] and outright failed projects such as The DAO[7].

b. Proposal

Trust Contracts. BOScoin’s approach to the problem is to apply a domain-specific language which can be read easily by the average user and can demonstrate mathematically that the smart contract’s implementation is computationally decidable. Thus, with BOScoin we aim to develop a platform for *Trust Contracts:* securely executable contracts based on Owlchain technology.

Additionally, through BOScoin we attempt to solve a number of commonly recurring issues

[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

related to cryptocurrencies.

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. BOScoin 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 automatically 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. BOScoin sets aside a large public budget specifically for the development of the BOScoin ecosystem through these proposals.

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). BOScoin 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 freezing and confirmation rewards(rewards relative to the amount of coins locked away in a node) to maximize mining income.

Application Ecosystem. Decentralized currencies in many cases tend to become speculative islands with limited real applications. As we believe the value of a currency is intrinsically tied to how useful it is, the BOScoin team will release the coin with two ready-made apps that use BOScoin. The applications Stardaq and Delicracy have already been built and will not only increase the transactional value of the coin, but will also help acquire new users.

Features	**Bitcoin**	**Ethereum**	**BOScoin**
Coins	Bitcoin	Ether	BOScoin
Core Features	Financial Transactions (Bitcoin script)	Smart Contracts (Solidity, Serpent, etc)	Trust Contracts (OWL 2 profiles, SDLang, TAL)
Decision Making Process	Non-systematic	Non-systematic	Democratic Congress (One node = One vote)
Consensus Algorithm	Proof of Work	Current: Proof of Work Future: Casper(?)	Modified FBA(Federated Byzantine Agreement)
Transaction Speed	7 tx/sec	25 tx/sec	1,000 tx/sec (target)

Block Interval	10 minutes	15 seconds	5 seconds
Block Size	1 MB	Dynamic	Dynamic

Fig 1. Comparison of Cryptocurrencies

2. Trust Contracts

a. Overview

BOScoin aims to use the Owlchain technology which consists of the Web Ontology Language(OWL)[8] and Timed Automata Language(TAL). This architecture is designed to expand expressive power while retaining decidability to support secure and precise execution of contracts. These Owlchain based contracts on the BOScoin blockchain are called *Trust Contracts*.

Features	**Smart Contracts** (Ethereum)	**Ricardian Contracts** (R3CEV Corda)	**Trust Contracts** (BOScoin)
Programming Language	LLL, Serpent, Solidity	Ricardian Contract + Pure functions	Owlchain (OWL* + TAL*)
Decidability	Undecidable with gas(fee)	Undecidable (3rd party evaluation)	Decidable(TAL)
Blockchain type	Permission-less	Permission	Permission-less
Consensus	PoW*	Various	mFBA*
Contract Inference	None	None	OWL Reasoning
OWL*: Web Ontology Language TAL*: Timed Automata Language PoW*: Proof of Work mFBA*: modified Federated Byzantine Agreement			

Fig 2. Comparison of Blockchain-based Contracts

b. Background

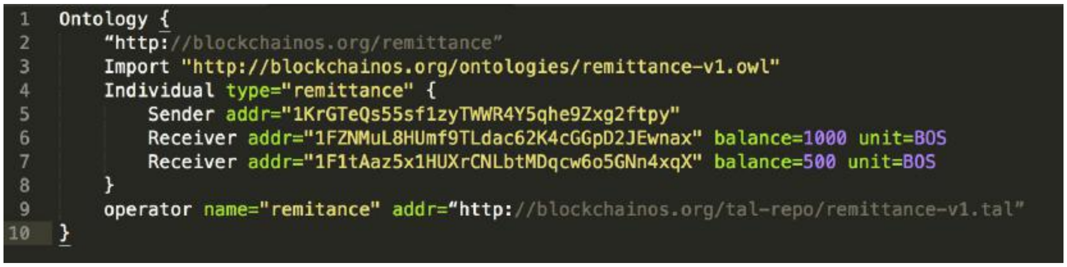
There are two primary approaches to developing contracts on the blockchain. One is through using a flexible programming language on a virtual machine, the other is to use a slightly less flexible but decidable domain-specific language. The BOScoin team decided to go with the later. Unlike cryptocurrencies based on virtual machines, as the inference engine is based on the semantic web technology, it is possible to infer information from the code before the contract is run. The contract is decidable and the outcome of the contract clearly known. This is a key concept in building a secure and sustainable currency with contract features. Although Ethereum attempted to solve this issue by using market mechanisms and applying a price to complexity, we believe that the stricter OWL and TAL approach will provide a more secure environment for contracts on the blockchain.

[8] *Web Ontology Language Reference*, https://www.w3.org/TR/owl-ref

c. Development

Building upon standard Web technologies such HTML, HTTP, RDF and OWL which were used to serve web pages, these technologies can be extended to share information in a way that can be predictably read by computers. Both OWL and RDF can be used to create unambiguous structured data taxonomies. Using these characteristics Ian Grigg proposed the concept of the Ricardian Contracts; contracts which are linked to every aspect of a payment system.[9] Despite, both OWL and RDF displaying similar characteristics, no RDF standards currently supports P-time completeness. Using reasoners, tools that infer logical consequences from a set of previously asserted facts or axioms, certain versions of the OWL standard promise P-time complexity. This means the amount of time it takes to run a contract can be pre-determined. This feature is a key reason why OWL was selected as the language to build trust contracts.

OWL DL(description logic) is a sublanguage of OWL, “designed to provide the maximum expressiveness possible while retaining computational completeness.”[9] OWL DL operates on a large dictionary of predefined vocabularies and taxonomies like the ISO20022 specification. As BOScoin specific features such as transactions will not be provided by the OWL dictionaries, these vocabularies and taxonomies need to be called from outside the contract. To solve this technical issue, we propose to create a designated namespace domain on the blockchain which can call non-standard primitive types(taxonomies) from the contract. Non-standard primitive types will be added conservatively in order to sustain the OWL’s decidability and taxonomic complexity features.



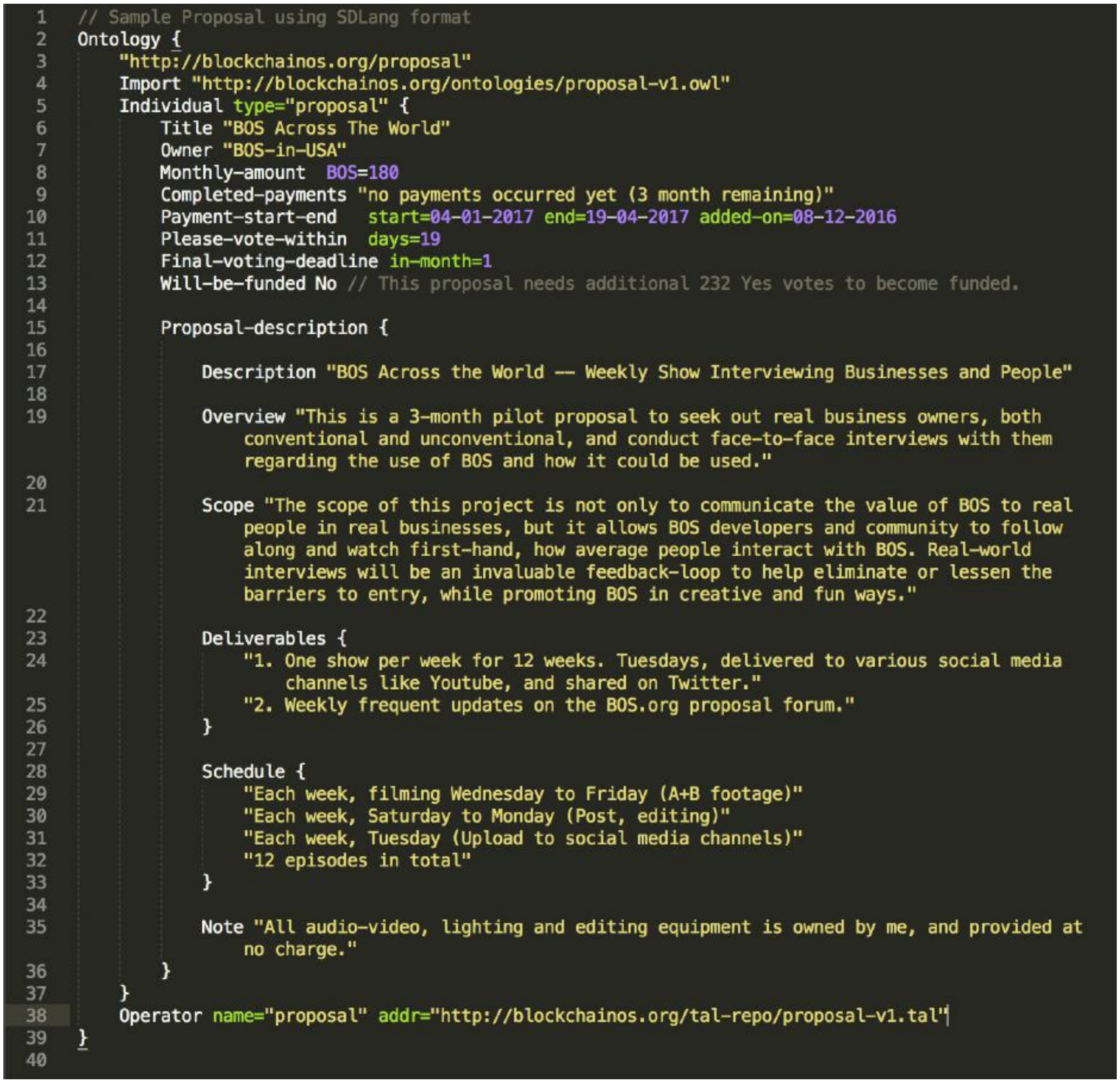
```
Ontology {
    “http://blockchainos.org/remittance”
    Import "http://blockchainos.org/ontologies/remittance-v1.owl"
    Individual type="remittance" {
        Sender addr="1KrGTeQs55sf1zyTWWR4Y5qhe9Zxg2ftpy"
        Receiver addr="1FZNMuL8HUmf9TLdac62K4cGGpD2JEwnax" balance=1000 unit=BOS
        Receiver addr="1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX" balance=500 unit=BOS
    }
    operator name="remitance" addr=“http://blockchainos.org/tal-repo/remittance-v1.tal”
}
```

Fig 3. BOScoin Transfer Example

Another issue with regards to Turing-complete contracts on blockchains is that Turing-complete languages are difficult to read by non-technical people. If ‘Code were law’, the code should be comprehensible to all the parties involved. Currently, currencies using Turing-complete languages for contracts can only be audited by those that can read code. By using the OWL standard and mapping the syntax to languages like SDLang[10], we aim to allow anyone to read and precisely comprehend what a contract is meant to do.

[9] *OWL Web Ontology Language*, https://www.w3.org/TR/owl-features/

[10] Simple Declarative Language, https://sdlang.org/



```
// Sample Proposal using SDLang format
Ontology {
    "http://blockchainos.org/proposal"
    Import "http://blockchainos.org/ontologies/proposal-v1.owl"
    Individual type="proposal" {
        Title "BOS Across The World"
        Owner "BOS-in-USA"
        Monthly-amount  BOS=180
        Completed-payments "no payments occurred yet (3 month remaining)"
        Payment-start-end   start=04-01-2017 end=19-04-2017 added-on=08-12-2016
        Please-vote-within  days=19
        Final-voting-deadline in-month=1
        Will-be-funded No // This proposal needs additional 232 Yes votes to become funded.

        Proposal-description {

            Description "BOS Across the World -- Weekly Show Interviewing Businesses and People"

            Overview "This is a 3-month pilot proposal to seek out real business owners, both
                conventional and unconventional, and conduct face-to-face interviews with them
                regarding the use of BOS and how it could be used."

            Scope "The scope of this project is not only to communicate the value of BOS to real
                people in real businesses, but it allows BOS developers and community to follow
                along and watch first-hand, how average people interact with BOS. Real-world
                interviews will be an invaluable feedback-loop to help eliminate or lessen the
                barriers to entry, while promoting BOS in creative and fun ways."

            Deliverables {
                "1. One show per week for 12 weeks. Tuesdays, delivered to various social media
                    channels like Youtube, and shared on Twitter."
                "2. Weekly frequent updates on the BOS.org proposal forum."
            }

            Schedule {
                "Each week, filming Wednesday to Friday (A+B footage)"
                "Each week, Saturday to Monday (Post, editing)"
                "Each week, Tuesday (Upload to social media channels)"
                "12 episodes in total"
            }

            Note "All audio-video, lighting and editing equipment is owned by me, and provided at
                no charge."
        }
    }
    Operator name="proposal" addr="http://blockchainos.org/tal-repo/proposal-v1.tal"
}
```

Fig 4. Trust Contract Example

The Timed Automata Language concept is based off of Andrychowicz's paper, 'Modeling Bitcoin Contracts by Timed Automata'[11]. TAL will be used to model the programming logic used in a Trust Contract. The HTML and Javascript pairing is similar to OWL and TAL. OWL provides the structure of the data and TAL acts as an operator. Operators in programming languages are constructs that do a certain function, such as adding, subtracting and comparisons. OWL provides the information, and TAL tells the computer what to do with the data. TAL is slightly different to other programming languages as there is a global time factor. This means contracts can be tested for how long they take beforehand. By running

[11] 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

automated tests on all the different possible outcomes beforehand, we can promise a platform with bug-free contracts on the blockchain.

The details of the above concepts are further explored in the technical paper.

3. Consensus Algorithm

a. 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, BOScoin uses a Modified Federated Byzantine Agreement(mFBA) consensus algorithm based on Stellar’s Consensus Protocol(FBA)[12].

Consensus Algorithm	Proof of Work	Tendermint	Byzantine Agreement	FBA[1]	mFBA[2] (BOScoin protocol)
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
[1] Federated Byzantine Agreement [2] Modified Federated Byzantine Agreement					

Fig 5. Comparison of Consensus Algorithms

Mazieres defines key features of the federated Byzantine Agreement Protocol[13]:

- 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.

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

[13] Ibid.

- 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.

b. Federated Byzantine Agreement Consensus Algorithm[14]

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.

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

In addition to FBA, the BOScoin consensus protocol also applies a Proof of Stake feature for the maintenance of the governance system. Users can freeze coins in units of 10,000 BOS within a node and forgo liquidity in return for newly issued BOScoin(similar to interest on savings) based on the total number of frozen coin in the node. The frozen coins in the node then act as both an economic incentive 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.

[14] Ibid.

4. Congress Network

a. Overview

The Congress Network is the decision-making body for BOScoin consisting of individual fully-synchronized node operators. Although people refer to cryptocurrencies as decentralized and autonomous, in many cases, this is not true. Both the code and the information on the blockchain are vulnerable to influence. In order to overcome these issues, BOScoin proposes a decision-making body called the Congress Network to fully decentralize and automate the system. Development of the source-code, forks, and even marketing resources can be allocated from within the system.

b. Congress Network Roles

i. Congress members

You will be regarded as a Congress member if you meet the following criteria:

- Run a fully-synchronized node at stable network speeds
- Freeze at least four units (one frozen unit is 10,000 BOS)
- Participate in voting

Anyone can become a Congress member. A node could be a server or a personal computer that a Congress member runs. The node can be located at home or a remote location, as long as network speeds are stable.

Congress Members have the choice to either invest in increasing their political influence through running more nodes or increasing their economic return through increasing the BOScoin frozen.

ii. Users

Users are the beneficiaries of the BOScoin system. They will interact with the BOScoin Network in three ways: by initiating transactions, submitting proposals and earning interest on BOScoins (coin freezing). These interactions are displayed in the figure below.

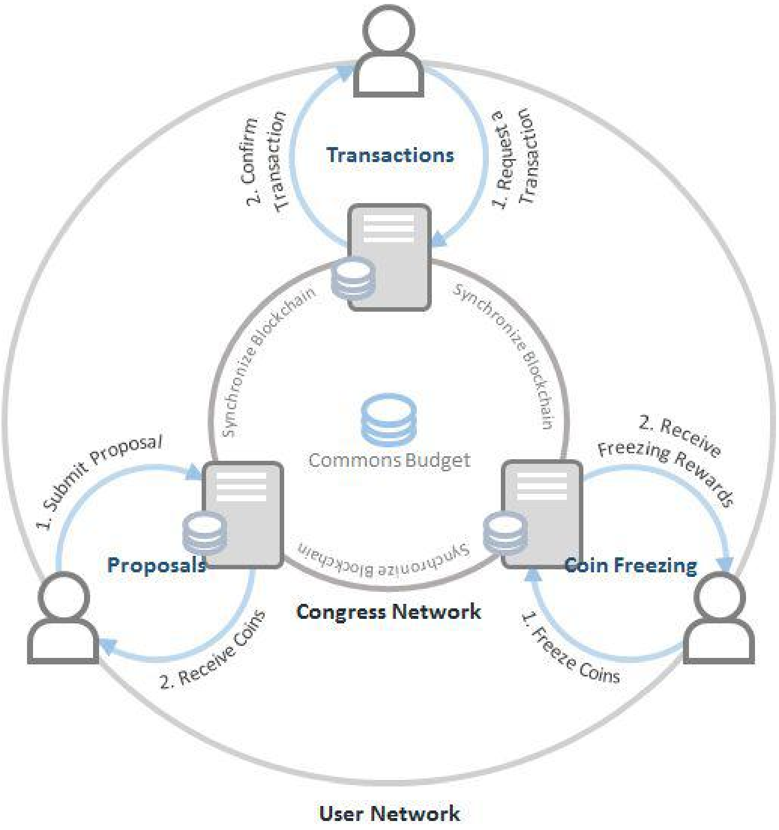


Fig 6. Interactions Between the Congress Network and User Network

c. Network Interactions

i. Transactions

When a transaction of digital assets is requested by a user, the request is sent to the Congress Network. For a simple transfer of BOScoin, when a node confirms the block –roughly every 5 seconds– the user's transactions will be confirmed, and the BOScoin will be transferred to another wallet. For more complex Trust Contracts, the pre-defined logic/procedures will also be carried out. In the initial stage of BOScoin, transaction fees will be fixed at 0.01 BOS. The fixed transaction rate can later be adjusted by the Congress Network through the voting process. Transaction fees act as an economic incentive for node operators and also as a defense mechanism against DoS attacks.

ii. Proposals

Proposals are system changing plans or Commons Budget spending plans that are submitted to the Congress Network. When a proposal is made, the 'net percentage point difference' between the positive and negative votes must exceed 10% for the proposal to be passed. For a funding proposal if the proposal passes, the requested coins will be sent to the proposer. 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.

iii. Coin Freezing

Coin Freezing is a Proof of Stake concept where if a user locks-in their coins and in return they will receive interest based on the number of coins frozen and the length of time the coins are stored. This interest is called the Freezing Reward. Users can freeze coins in units, which are sets of 10,000 BOS. Frozen coins are used as collateral in case of attempted forgery of the blockchain. If a node attempts to forge the blockchain, a portion of the frozen coins are confiscated and sent to the Commons Budget. Additionally the system requires two weeks prior notice to unfreeze coins, as a mechanism to promote price stability.

d. Reward System

Within the Congress Network, there is a unique incentive mechanism. Congress members can either choose to maximize financial rewards, by freezing BOScoin in one node or increase their voting power by running multiple nodes (one node equals one vote).

This deliberate division incentivizes the separation of economic motives from decision-making motives similar to the separation of economic and political power concept.

Bitcoin suffers from the hash power centralization issue, due to its reliance on a Proof of Work consensus protocol. A small number of major miners can easily buy up large amounts of mining hardware, which allows them to influence changes in code and even threaten the integrity of the blockchain. By separating the incentives of those that wish to optimize financial gain, the barriers to entry to participate in the governance process is comparatively lower than a system that equates decision making power with financial rewards.

There are three ways for Congress Members to receive BOScoin rewards: the freezing reward, confirmation rewards, and transaction fees.

- **Freezing Reward:** Congress Members receive the same amount of interest as normal wallet users when coins are frozen. Starting from the first year, a total of 5,400 BOS is distributed equally to each unit of frozen BOScoins. This freezing reward is issued every 720 blocks(roughly one hour). The total amount that is distributed decreases by 5.00% year on year over 59 years.
- **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 Units in a node. Similar to the block reward in Bitcoin, as the number of participating nodes increases, the probability of winning the confirmation reward decreases. The reward is issued

relative to the proportion of frozen units held in the node. Initially the reward starts with a network-wide average of 18 BOScoins per block.

$$confirmation\ reward\ = 18 \times \frac{Number\ of\ Frozen\ Units}{Average\ of\ Total\ System\ Frozen\ Units}$$

Initially the block confirmation reward starts at 18 BOScoins per block, and it will decrease by 6.31% year on year over roughly 128 years.

- **Transaction Fee:** The transaction fee is a fixed 0.01 BOScoins. 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.

e. Decision Making Process

The idea of an integrated decision-making process within the currency was inspired by Dash coin[15] where the masternodes[16] vote to make decisions. In BOScoin there are largely two type of proposals. There are System Proposals and Funding Proposals. System Proposals are proposals that automatically change the code of the BOScoin platform and Funding Proposals are proposals that request for funds from the Commons Budget. Anyone with a wallet can make a proposal, which is then reviewed every third Monday of the month by 24:00 GMT. These proposals are then voted on by the Congress members by the fourth Monday of the month by 24:00 GMT. If the ‘net percentage point difference’ between the positive and negative votes exceed 10%, the proposal is passed. There is the option for a neutral vote to signal that the Congress member participated in the decision-making process and votes can also be changed any time before the final due date.

For Funding Proposals, in order to increase the chances of a proposal being passed, it is possible to provide collateral with the proposal. Proposals that provide more than 1,000,000 BOS become Significant Proposals. Voting participation is especially important for Significant Proposals and so if a Congress member does not vote on a Significant Proposal, they are penalized by having the freezing feature disabled for their node for two weeks. Disabling the coin freezing feature means the node will forgo all the benefits from freezing coins and will not be able to freeze any coins for two weeks.

f. Commons Budget

The Commons Budget is an account where BOScoins are held and can only be transferred by proposals that are passed through the Congress. The main role of Commons Budget is to expedite the growth of the coin users during the early stages. Coins in the Commons Budget are mainly accumulated through two channels; the first is the direct issuance of 50 BOS coins

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

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

per block for roughly 6 years and secondly from 30% of the transaction fee. Out of all issued coins, Commons Budget make up the largest proportion of coins. This will ensure funds are available to growth hack the adoption of BOScoin.

Any proposal which passes through the congress can access coins from the Commons Budget. An example of a proposal is an Airdrop proposal; geo-socially distribute free coins to users in order to increase the number of BOScoin users. Other examples can include funding the development of the BOScoin eco-system, marketing campaigns and organizing BOScoin related meetings.

5. Ready-made Application Ecosystem

Many cryptocurrencies offer examples of how to use and build applications on their platform. However, few have delivered working applications utilizing currency. Although it is difficult to fully understand how much of a cryptocurrency's value is made up of transactional value and how much is made up by speculative value, BOScoin's goal is to increase the transactional value of the currency relative to its competitors. In the long-run the core-value of a currency is its usefulness.

Through ready-built applications such as Stardaq and Delicracy released with the currency, users will have sophisticated services available immediately within the BOScoin ecosystem.

a. Stardaq

Stardaq is an international celebrity popularity prediction market. A celebrity's popularity is represented as an index and users can place bets on whether the popularity of the celebrity will rise or fall. The bets can only be placed with BOScoins.

b. Delicracy

Delicracy is a collective decision making tool that can be implemented in any organization. All users can participate in the decision-making process by placing bets on a set of proposals, similar to the Augur prediction market[17]. The proposal with the most bets is passed. This type of system can help promote transparency and participation for decision-making processes in organizations large and small.

These applications serve as outlets to spend BOScoins and also serve as channels for Airdropping free coins. Appropriately using these tools can help grow the ecosystem by introducing new users.

6. Technical Roadmap

[17] Decentralized Prediction Market, https://www.augur.net/

The following is a technical roadmap defining the key milestones.

Milestones→ **↓Modules**		**M1** **Alpha**	**M2** **Genesis**	**M3** **Nebula**	**M4** **Sirius**
Consensus	P2P	Protocol specification & Implementation	Unit & Acceptance Test		
	mFBA Consensus	FBA : Key Design Implementation	mFBA : Key Design Implementation	mFBA Optimization	
	Data Store	Store specs & SQLite Store implementation	MessagePack History		Blockchain backup & restore using ISP(AWS, Azure)
Trust Contracts	Ontologies & Rule(TAL)	Remittance : Send & Receive Tokens based on Trust Contracts		Governance Trust Contracts & Multisig Tx Specification	Multisig Tx Implementation
		Import and define basic BOScoin Ontologies	Construct Core Ontologies	Construct Key Governance Ontologies	
			Governance System Specifications	Proposal & Vote Implementation	Automated Proposal Implementation
	Inference Engine	Formal Specification and Key Design Elements	Reasoner Integration with Blockchain	Reasoner Optimization	
UX	CLI & Web Interface	CLI design & Implementation	Web UX design		
	Wallet	Wallet Formal specification	UX design Application PoC Test		Android & iOS SPV Wallets
	RPC & REST API		Blockchain Explorer		

Fig 7. Implementation Roadmap

7. Coin Issuance

New coins are issued in four ways; Initial Development Budget(0.5bil, 10%), confirmation rewards(1.8bil, 36%), freezing rewards(0.9bil, 18%) and the Commons Budget(1.8bil, 36%). We aim to issue a total of 5.0 billion coins over the next 100 years. These values are subject to change.

	Initial Development Budget	**Confirmation Rewards**	**Freezing Rewards**	**Commons Budget**
BOScoins	500,000,000	1,800,000,000	900,000,000	1,800,000,000
Share	10%	36%	18%	36%
Decrease Rate	-	6.31% per 6,311,520 blocks	5.00% per 6,311,520 blocks	-
End of Issuance	Genesis Block	Year 2145	Year 2076	Year 2023

Fig 8. Issuance Summary

- **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 ICO sales and bounties. 500 million BOScoins are issued with the Genesis block.
- **Confirmation Rewards:** Confirmation rewards are financial rewards issued randomly to a node for every confirmed block(every 5 seconds). As the reward is distributed randomly, if the number of nodes increase the probability that a node will receive a reward decreases. This reward is relative to the number of units frozen in a node(refer to section 4d). 1.8 billion BOScoin are issued through Confirmation rewards. Initially 18 BOScoins are issued per block. The reward decreases every 6.31 million blocks–roughly one year– by 6.31% over 128 years.
- **Freezing Rewards:** Freezing rewards are distributed relative to the number of BOScoin units frozen in a node and are issued every 720 blocks(roughly one hour). Initially the total amount is 5,400. The reward decreases by 5.00% over every 6.31 million blocks–roughly 1 year – over 59 years. The freezing reward acts as an important incentive for congress members to increase the number of coins frozen in one node and disincentivize the centralization of decision making.
- **Commons Budget:** The Commons Budget holds BOScoins 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 block for the first 35 million blocks–roughly five years. After the first five years the

Commons Budget is maintained through the 30% commons fee on transactions fees.

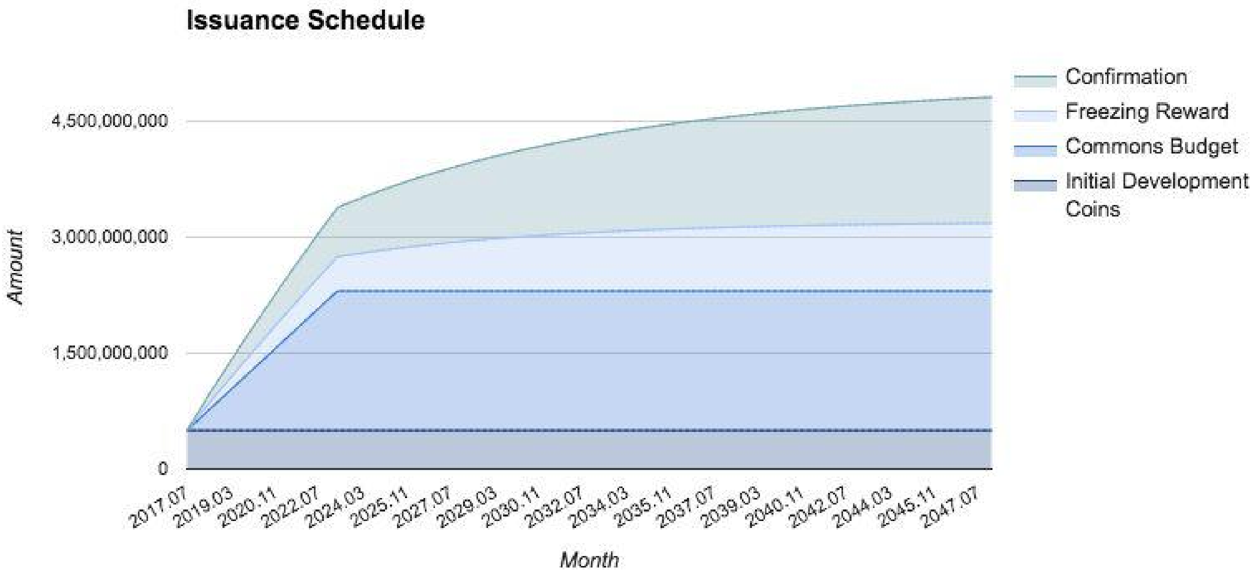


Fig 9. Coin Issuance Plan

8. Conclusion

The BOScoin 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 BOScoin team will aim to achieve these goals while leveraging the security and integrity that can be gained through blockchain technology.

Works Cited

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 contracts*, 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/

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+Proposals%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