Overview of White Paper 2.0 Part1

Written by BlockchainOS DEV Team

May 10 2018

Why we are publishing White Paper 2.0

We have decided to publish our ‘BOScoin White Paper 2.0' to include the vision of the BOS team and that had previously not been included in the first white paper.

In preparing the White Paper 2.0, we studied the fundamental problems of the capitalist system and various alternative propositions to combat those issues. In the end, we decided that a new strategy was needed to overcome the limitations of the cryptographic economy.

We have revised the strategy based on a new concept called ‘Public Financing’, which contrasts the existing ICO model. Through this, we hope to mitigate the problems which the first white paper lacked in addressing.

Plans for publishing White Paper 2.0

The BOScoin White Paper 2.0 will be published in two parts.

Part 1

In Part 1, the BOS team plans to introduce the concept of "Public Financing" as a solution to the current problems facing the cryptographic economy.

In implementing the PF concept, the Congress Network voting mechanism will be used in conjunction with a homomorphic encrypted password to provide anonymity of the vote and preventing Sybil attacks.

Part 2

In Part 2, we will propose the ‘Generic Trust Third Party (GTTP)’ concept as a means to link the offline world with online.

In addition, we will propose a BOScoin economic model that includes Public Financing, Commons Budgets, GTTP model, Economic Participant Compensation System and the modified token issuance plan.

Public Financing

Background

We have assessed that the cryptographic economy is the most effective way to tackle the issues facing our current economic system.The cryptographic economy utilizes capitalistic credit creation whilst solving the problem of wealth distribution.

However, sudden price volatility caused by fixed issuance of cryptographic currency remains a key problem. Public Financing is our new strategy to resolve this issue and a means to effectively distribute the generated credit back to the community.

Definition

Public Financing (hereinafter PF) is the issuance of BOScoin as a credit-generating means to acquire various assets of the real economy from the community.

The community itself suggests, reviews and votes on additional issuance through the Congress Network and this decision is processed through the Trust Contract.

We define this process as Public Financing, which we deem to be 'public' in two respects.

Securing financial sovereignty

As opposed to the conventional project financing model that is decided by a very small number of people at the top of the existing financial institutions, any finance related decision-making on BOScoin is determined by the consensus of its community members.

PF can solve the problem of financial sovereignty, a key flaw of the capitalist system, by a credit creation system driven by a community-based decision making process.

Solving the Wealth Distribution Problem

Real economic asset secured by the credit generated through public financing is seen as the Common Wealth. The wealth generated by the BOScoin community will be seen as such and will be distributed equally.

We believe that PF can solve the issues surrounding the reduction of human labour caused by technology and capital; a fundamental problem with the capitalist system.

Process

The PF will propose, review and vote on additional BOScoin issuance via the Congress Network and the decisions made by the community itself will be made through the Trust Contract.

We would like to establish a specific and detailed PF policy by conducting a pilot project of a certain size.

Through this pilot project, we plan to provide the community with a detailed process and additional issuance data in order to raise the quality of decision making. We will then proceed to implement the full Congress Network voting process.

Congress Voting

Background

When we wrote the first white paper, we recognized that there was a problem with the Congress Network's decision making process and wanted to address it.

We recognised that the current Congress Network's voting mechanism allowed a large number of BOScoin owners to create a number of nodes that could have a significant impact on the community’s decision-making process.

In order to provide equal rights and opportunities to participate whilst increasing the benefits to all members of the community, equal representation on the network should be given. We have concluded that to enable such representation, each participant should be given one single vote.

However, we also became aware that in order to do so, the network needed to collect identification information about each member which could violate privacy and freedom of expression rights.
We sought a way to create a solution that could accommodate real existence on the blockchain while ensuring both privacy and accessibility.

Definition

BOScoin needed a voting system on the Congress Network to ensure anonymity and demarcation, while at the same time allowing individual identification and granting one vote per person.

At the end of the research, we decided that the ideal design of the Congress Voting System is to base it on the use of a private key which directly interacts with encrypted data without requiring access to the private key itself.

Essential Elements

Account

Once the Congress Network membership is obtained, the member account represented by the ID_A public address.
Congress membership can be obtained by any BOScoin member but they must undergo a verification process to prove their uniqueness in order to prevent a Sybil Attack.
During the verification process, the account isolates the direct connectivity between the member and the Uniqueness Verification Server (Registry) for privacy protection and validates the token to prove the uniqueness.
Following this process one token and one account will be assigned to the member.
The account is formed on the blockchain and the member is able to prove their uniqueness and Congress Network membership with their token.
The account will be used only for membership verification and will not contain any personal information, eliminating the risk of a leak.

Voting Program

If a vote is on a specific subject, a voting program will be created to execute that specific vote.
Thus Individual voting programs are created for each subject (agenda), and each voting program is represented by a ID_V public address.

BallotStamp

Community members who have obtained membership in the Congress Network can vote by issuing a BallotStamp through the voting system using an ID_A member account and voting program (ID_V).
BallotStamp is generated from a verifiable trust system, but it is generated in a manner which does not infer a BallotStamp's association with its members, thus protecting the privacy of its members.
Voting systems using the same ID_A account and voting program (ID_V) issues the same Ballotstamp everytime which means it can prevent Sybil Attacks.

Voting Process

1. Create a voting program (ID_V) related to a specific subject
2. The voting members will use their ID_A to confirm their voter eligibility and request a seed for voting. Requests are sent with the member's private key that has gone through homomorphic encryption.
3. ID_A issues an homomorphically encrypted seed to voters after verifying their eligibility.
4. The voter requests the ID_V to issue a BallotStamp and delivers the homomorphically encrypted seed.
5. ID_V generates and sends the homomorphically encrypted BallotStamp to voters (each ID_V creates only one BallotStamp for each voter, even if the voter submits multiple BallotStamps, the system gives the same Ballot Stamp each time)
6. Voters use their private key to decrypt the BallotStamp and send it to the ID_V along with the voting results (voters can vote multiple times during the voting period, but only the last vote counts as the final result)
7. ID_V verifies BallotStamp and saves it with voting results
8. When voting is completed, all votes will be aggregated an and results will be stored on the blockchain (partial aggregations that may affect the votes are not disclosed)

Conclusion

BOScoin started the project as a global community currency with the aim of distributing it as a currency with real money status.

By publishing White Paper 2.0, we are introducing a credit-generating system called 'Public Financing', which aims to compensate the shortfall of credit generating capabilities of existing cryptographic currencies compared to sovereign currencies.

When a community wants to acquire new assets, we want to eliminate the fundamental problems of the existing capitalist system by creating credit through PF and distributing the generated wealth back to the community.

In addition, Congress will introduce Congress Voting with the same private key to eliminate the concentration of credit creation, give equal voting rights to all members and allow them to participate with ease.

We consider Public Financing to be one of the key features to propel BOScoin to be recognised as the universal money for the unbanked and as a global community currency. A more detailed report of our research will be disclosed on our White Paper 2.0.

We will be sequentially releasing the contents of our White Paper 2.0 to the community in the near future.