Overview of White Paper 2.0 Part1

Written by BlockchainOS Dev Team
May 10 2018

백서 2.0을 발간한 이유

우리는 백서 1.0에서 미처 담지 못한 BOS팀과 BOScoin의 비전을 담기 위해 'BOScoin 백서 2.0'이라는 프로젝트를 시작하였습니다.

백서 2.0을 준비하며 자본주의 체제의 근본적인 문제점과 이를 극복하기 위한 각종 대안들을 연구하였고 그 끝에 암호화폐 경제체제의 한계를 극복 할 만한 새로운 전략이 필요하다는 판단이 들어 불가피하게 기존 전략을 수정할 수 밖에 없었습니다.

우리는 기존 암호경제의 ICO와 대비되는 Public Financing 이라는 새로운 개념을 중심으로 전략을 수정하였으며, 이와 함께 BOScoin 백서 1.0에서 미진했던 문제까지 함께 해결하고자 합니다.

백서 2.0 발간 계획

BOScoin 백서 2.0은 총 2개의 Part로 나눠 순차적으로 발간될 예정입니다.

Part 1

Part 1에서는 BOS팀이 풀고자 하는 문제와 그 해결책으로 '공공금융 (Public Financing, 이하 PF)' 개념 제안 중심으로 작성될 예정입니다.

우리는 Public Financing를 실행하기 위해 Congress Network의 투표를 이용하고자 하며, 투표의 익명성을 보장하고 시빌 어택 등을 방지하기 위해 최신 암호화 솔루션인 동형암호를 이용한 Congress Voting을 도입할 계획을 담았습니다.

Part 2

Part 2에서는 온라인 외에 오프라인 세계와 연결되는 고리로서 Generic Trust Third Party(이하 GTTP) 개념을 새롭게 제안할 예정입니다.

더불어 Public Financing, Commons Budgets, GTTP 모델, 경제참여자 보상 체계와 수정된 토큰발행 계획 등을 포함한 BOScoin 경제 모델을 제안할 예정입니다.

Public Financing

배경

우리는 현재 경제 체제의 문제점을 해결하기 위한 여러 대안 중 암호경제가 자본주의 신용창출 매커니즘을 활용하고 분배 문제를 해결하는데 있어서 가장 효과적이라고 평가했습니다.

다만, 기존 암호화폐의 발행량 고정에 따른 급격한 가격 변동성 문제를 해소하고 창출한 신용으로 획득한 부를 커뮤니티에 분배할 수 있는 새로운 전략으로 Public Financing이라는 체계를 도입하였습니다.

정의

Public Financing(이하 PF)은 BOScoin 커뮤니티에서 실물경제의 다양한 자산을 획득하기 위한 신용창출 수단으로 BOScoin을 추가 발행하는 것을 뜻합니다.

커뮤니티 스스로가 Congress Network를 통해 추가 발행을 제안, 검토, 투표 하며, 이렇게 결정한 내용이 Trust Contract를 통해 실행됩니다.

우리는 이러한 일련의 과정을 공공금융(Public Financing)이라고 정의하며, 2가지 측면에서 공공적(Public)이라고 말할 수 있습니다.

금융주권 확보

기존 금융기관에서 극소수 인원이 결정 하여 진행한 Project Financing이 아니라, 금융과 관련한 의사결정 권한이 모든 BOScoin 커뮤니티 구성원들의 합의에 의해 결정되는 신용 창출을 말합니다.

커뮤니티의 의지와 의사결정에 의한 신용창출 방식은 자본주의 체제 문제 중 하나인 금융주권 문제를 PF로 해결할 수 있다고 생각합니다.

부의 분배 문제 해결

Public Financing를 통해 창출한 신용으로 확보한 실물경제 자산을 Commons(공동의 것)으로 보며, Commons를 통해 발생한 부는 BOScoin 커뮤니티 공동의 것으로 보고 이를 분배하겠다는 뜻입니다.

우리는 자본과 기술에 의해 발생하는 노동 소득 감소 혹은 종말이라는 자본 주의 체제의 근본 문제를 PF로 해결할 수 있다고 믿습니다.

과정

PF는 커뮤니티 스스로가 Congress Network를 통해 BOScoin 추가 발행을 제안, 검토, 투표를 하며, 이렇게 결정한 내용은 Trust Contract로 통해 실행됩니다.

우리는 일정 규모의 PF를 Pilot 프로젝트를 진행하여 구체적이고 세부적인 PF 정책을 수립하고자 합니다.

이 Pilot 프로젝트를 통해 세부적인 Process와 추가 발행 관련 데이터를 커뮤니티에 제공하여 의사결정의 질을 높인 뒤 본격적인 Congress Network 투표 프로세스를 적용할 계획입니다.

Congress Voting

배경

우리는 백서 1.0을 작성할 당시 Congress Network의 의사 결정에 문제가 있음을 인식했고 이를 해결하고자 했습니다.

Congress Network의 투표과정은 보스코인을 많이 가진 이가 다수의 노드를 만들어 이를 통해 커뮤니티 의사 결정에 큰 영향력을 주는 구조가 될 수 있음을 인식했습니다.

커뮤니티에 참여하는 모든 회원이 동등한 권리와 참여의 기회를 부여 받고, 그들 모두의 이익을 증대시키는 방법이 무엇일지 고민했고, 우리는 네트워크상 모든 사람이 평등하게 대표성을 띠어야 하며, 사람당 하나의 투표권을 부여해야한다 판단했습니다.

하지만 그러기 위해서 네트워크가 각 회원에 대한 식별 정보를 수집하는 것은 프라이버시와 의사표시의 자유를 침해 할 수 있음을 인지했습니다.

프라이버시와 접근성을 동시에 보장하면서 블록체인에서 실존재를 수용할 수 있는 해결책을 마련하기 위해 방법을 모색했습니다.

정의

BOScoin은 Congress Network에 의한 민주적인 의사결정을 하기 위하여 익명성을 보장하면서, 동시에 개인 식별이 가능해 1인 1표를 부여할 수 있는 Voting System이 필요했습니다.

연구 끝에 '비밀키에 대한 접근을 필요로 하지 않고 암호화된 데이터에서 직접 연산을 할 수 있는' 동형암호가 가장 이상적이라고 판단하여 이를 이용한 Congress Voting System을 도입하였습니다.

구성 요소

Account

의회 멤버십 획득 시 생성된 멤버의 어카운트는 ID_A라는 공개주소로 표현됩니다.

의회 멤버십은 보스코인 멤버라면 누구든지 획득할 수 있지만 Sybil Attack 방지를 위해 유일성 검증 과정을 거쳐야 합니다.

유일성 검증 과정에서 어카운트는 프라이버시 보호를 위해 멤버와 유일성 검증 서버(Registry) 사이의 직접적인 연결성을 분리하고 유일성 검증 사실을 증명하는 토큰을 검증합니다.

이로 이해 한 멤버 당 하나의 토큰과 하나의 어카운트가 주어집니다.

어카운트는 블록체인 상에 형성되며 멤버는 토큰으로 자신의 유일성과 의회 멤버십을 증명할 수 있게 됩니다.

어카운트는 멤버에 대한 멤버십 인증에만 활용될 뿐 아무런 개인정보를 담고 있지 않으므로 개인정보가 유출될 염려가 없습니다.

Voting Program

특정 주제에 대해 투표가 진행하는 경우, 투표를 실행하기 위한 투표 프로그램이 생성됩니다.

즉 각 주제(어젠다) 마다 개별적인 투표 프로그램이 생성되며 각 투표프로그램은 ID_V라는 공개주소로 표현됩니다.

BallotStamp (투표지)

의회멤버십을 획득한 커뮤니티 멤버는 어카운트(ID_A)와 투표프로그램(ID_V)를 활용한 투표시스템을 통해 BallotStamp를 발급 받아 투표에 참여할 수 있습니다.

BallotStamp는 검증이 가능한 신뢰시스템에서 생성되지만 외부에서 BallotStamp와 멤버의 연계성을 유추할 수 없도록 생성되어 멤버의 프라이버시를 보호할 수 있습니다.

또한 같은 어카운트(ID_A)와 투표프로그램(ID_V)를 활용한 투표시스템은 한명의 멤버에게 매번 똑같은 BallotStamp를 발급하기에 Sybil Attack을 방지할 수 있습니다.

투표 과정

1. 특정주제와 관련된 투표 프로그램(ID_V) 생성

2. 투표에 참여할 멤버는 ID_A를 이용해 유권자 자격여부를 확인을 받으며 투표참가를 위한 시드를 요청함. 요청은 멤버 소유 개인키로 동형암호화한 상태로 전달됨

3. ID_A는 유권자 자격여부 확인 후, 유권자에게 동형암호화된 시드를 발급함

4. 유권자는 ID_V에 Ballot Stamp 발급 요청하며 동형암호화된 시드를 전달함

5. ID_V는 동형암호화된 Ballot Stamp를 생성해서 유권자에게 전달함 (각 ID_V는 각 유권자에 대해 오직 하나의 Ballot Stamp를 생성하며, 유권자가 여러번 Ballot Stamp를 신청하더라도 시스템은 매번 같은 Ballot Stamp만 주어짐)

6. 유권자는 개인키를 이용하여 Ballot Stamp을 해독하여 투표결과와 함께 ID_V에 전송함 (유권자는 투표기간 내 여러번 투표할 수 있지만, 마지막 투표만 최종 결과로 집계됨)

7. ID_V는 Ballot Stamp를 검증 후, 투표결과와 함께 저장함

8. 투표가 완료되면 집계가 실시 되며 모든 득표와 결과가 블록체인에 보관됨 (투표에 영향을 줄 수 있는 부분 집계는 공개 되지 않음)

결론

BOScoin은 글로벌 커뮤니티 화폐로서 실질 화폐의 지위를 가지는 암호화폐로 유통할 목적으로 프로젝트를 시작했었습니다.

그리고, 백서 2.0을 발간하면서 'Public Financing'이라는 신용창출 체계를 도입하여 기존 암호화폐들이 주권 화폐와 비교하여 신용창출 능력이 떨어지는 점을 보완하려고 합니다.

커뮤니티가 새로운 자산을 획득하고자 할 때, PF를 통해 신용을 창출하고 이를 통해 생성된 부를 커뮤니티에 분배함으로써 기존의 자본주의 체제의 근본적인 문제들을 해소하고자 합니다.

또한, 신용창출 과정에서 발생할 수 있는 부의 집중 문제를 해소하며, 모든 멤버들에게 평등하게 기회를 부여하기 위하여 사람 기준으로 투표권을 부여하되, 안심하고 참여할 수 있도록 동형암호를 이용한 Congress Voting을 도입할 것입니다.

우리는 Public Financing을 BOScoin이 글로벌 커뮤니티 화폐로서 실질 화폐의 지위에 도달하는데 중요한 방법 중의 하나로 생각하며, 보다 구체적인 연구 결과는 백서 2.0을 통해 공개할 예정입니다.

머지 않은 미래에 백서 2.0 Part1부터 순차적으로 커뮤니티에 공개하도록 하겠습니다.