BOSAGORA 백서

2020.01.16

요약. BOSAGORA 플랫폼은 Trust Contracts와 의회 네트워크(Congress Network)라고 불리는 의사결정 시스템 위에서 작동하며, 스스로 진화하는 탈중앙형 암호화폐다. (1) Trust Contracts란 프로토콜 레이어에 기반하여 안전하게 실행되는 계약을 말한다. 우리는 효율적이고 안전하게 설계된 스마트 계약 엔진을 제공하고 개발자들이 쉽게 채택할 수 있도록 다양한 도구와 널리 사용되고 있는 프로그래밍 언어에 기반한 개발 환경을 제공할 계획이다. (2) 의회 네트워크는 분산형 조직에서 발생하는 거버넌스 문제를 해결하고, 시스템이 보다 탄탄한 생태계를 만들도록 계속적인 진화를 돕는 BOSAGORA 플랫폼의 의사결정 기관이다.

배경

블록체인은 2008년 Satoshi Nakamoto의 논문 “Bitcoin: A Peer-to-Peer Electronic Cash System”[1]에서 처음 개념화되었으며 다음 해에 Bitcoin의 핵심 기술로 구현되었다. Bitcoin은 개인들이 화폐 전송 정보를 공개적으로 기록하는 금융 거래 원장으로써 블록체인 기술을 사용한다. Bitcoin은 이중 지불 문제를 해결하기 위해 블록체인을 사용한 최초의 사례다. 중앙집권적인 관리자가 없음에도 불구하고 Bitcoin은 1억8천만건의 P2P(peer-to-peer) 거래를 성공적으로 지원했으며, 이제 1000억 달러 이상의 시가총액을 달성하고 있다.

Bitcoin의 성공에 뒤를 이어 블록체인 기술을 활용한 수많은 시스템이 나타났다. 수백 개의 암호화폐들이 현재 경쟁 중이며, IBM의 최근 보고서에 따르면 이제는 90% 이상의 은행들이 블록체인 기술에 투자하고 있다. 화폐 거래가 블록체인 기술의 가장 보편적인 응용 프로그램이지만, 이 외에도 금융 상품 및 서비스, 물류 정보, 재산 소유권, 신원 정보 등과 같은 다른 디지털 자산을 블록체인 기술을 사용하여 관리하려는 시도 또한 다양한 그룹에서 나타나고 있다.[2]

2016년, 암호화폐 Ethereum은 많은 관심을 받았다. 이더리움은 "임의의 상태변환 함수 구현에 사용될 수 있는 '계약'을 생성하는데 사용될 수 있는 본격적인 튜링-완전 프로그래밍 언어가 내장된 블록체인." 이며 블록체인에 Smart Contracts를 제공하는 것을 목표로 한다.[3]

목표는 사용자가 모든 종류의 프로그램 (또는 계약)을 블록체인에 쓸 수 있게 하는 것이다. Bitcoin과 마찬가지로, Ethereum은 블록체인과 합의 메커니즘을 사용하여 악의적인 노드가 계약 내용을 위조하려고 시도하면 위조 계약이 결국 블록체인에서 제거되도록 한다. Bitcoin은 계정 사이에서 전송되는 Bitcoin의 양을 완전하게 보장한다. 이와 비슷하게 Ethereum도 실행되는 계약의 무결성을 보장해야 한다.

Smart contracts는 탈중앙형 애플리케이션 개발의 패러다임 전환이 될 수 있는 잠재력을 가지고 있다. 프로그램이 중앙화된 서버에 올라가 있지 않더라도 어디서나 동일한 로직을 실행할 수 있다. Smart contracts는 탈중앙형 시장, 통화 거래 플랫폼, 탈중앙형 글로벌 슈퍼컴퓨터 개발을 목적으로 하는 Golem[4]과 같은 프로젝트에 사용될 수 있다.

그러나 Ethereum이 기반하고 있는 튜링-완전 언어가 제공하는 자유와 유연성은 몇 가지 심각한 문제들의 발생시키는 원인이다.[5] 우리는 튜링-완전 언어는 본질적으로 결정 불가능하기 때문에 Smart contracts 작성에 사용하는 것은 부적합하다고 생각한다. 이 결정 불가능성 문제 때문에, 튜링-완전 언어를 기반으로 한 smart contract는 smart contract가 실행되기 전에는 이것이 어떻게 작동될지 알 수 없다. Ethereum은 계산 작업에 대한 비용(가스)을 적용하여 이 문제를 극복하려고 시도했다. 하지만, Smart contracts을 개발하고 실행하는 데 사용되는 이 언어 자체에

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
[2] Leading the Pack in Blockchain Banking: Trailblazers Set the Pace, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN&
[3] Vitalik Buterin, Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper
[4] Golem, https://golem.network
[5] Hodges, Andrew, Alan Turing: the enigma, London: Burnett Books, p. 111

내재되어 있는 문제들은 어쩔 수 없이 일련의 보안 취약점[6]을 만들고 The DAO[7]와 같은 실패한 프로젝트들을 야기했다.

비전

프로젝트를 실현 가능하게 하는 블록체인 기술로 더 나은 세상을 만드는 데 기여한다.

미션

합의 알고리즘의 투명성과 계약의 명확성을 보장하는 개방된 탈중앙화 블록체인 프로토콜을 구축하고, 진보된 민주적 의사 결정 프로세스에 의한 집단지성의 실현으로 의미 있는 프로젝트를 가능하게 함으로써 블록체인 생태계를 풍요롭게 한다.

핵심 가치

진취적 사고

미래 개척: 우리는 누구나 속도와 신뢰를 경험할 수 있는 혁신적인 기술 개발로 최초의 완전한 풀-노드 지분 증명 및 Federated Byzantine Agreement 합의 알고리즘의 블록체인 플랫폼을 개발하는 것을 목표로 한다.

타당성

성숙한 민주주의: 누구나 진보된 숙의 민주주의 의사결정 도구를 통해 자유롭고 포괄적인 의사결정을 이루어 최고 수준의 공정성을 보장하는 민주주의를 구현한다.

신뢰성

명확한 투명성: 투명성을 통해 프로젝트 전체를 누구나 보다 쉽게 볼 수 있도록 하고 정해진 절차에 따라 결정을 내린다. (커뮤니티 업데이트, Technical advisory board, Github, 의회 투표 제도)

ICO와 초기 백서

BOSAGORA는 2017년 5월 95개국으로부터 17시간 만에 6902 BTC 하드캡을 달성한다는 놀라운 결과를 이끌어 내었다. 그 결과는 초기 백서가 추구하는 다양한 기술 및 생태학적 청사진에 의해 달성되었다. 하지만 지난 2년간 비슷한 사업이 많이 발표되었고 기술개발계획과 생태계 청사진만으로는 독점적 지위를 얻기 어려워졌다. 게다가 글로벌 거대기업들이 블록체인 플랫폼의 출시도 예고하고 있어 블록체인 플랫폼 시장의 경쟁은 더욱 치열해지고 있다. 이러한 상황에서, BOSAGORA 프로젝트는 생존을 위한 보다 독점적인 지위를 얻을 수 있는 새로운

[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

분야를 개척하고, ICO 참여자들과의 약속을 지키기 위해 초기 백서의 틀과 정신을 유지하도록 노력하려고 한다.

ICO 이후, 규제환경은 수많은 기술적 진보와 함께 변화해 왔다. BOSAGORA 팀은 초기 백서를 완수해야하는 목표에 초점을 맞추지만, 동시에 우리는 정책, 기술, 방법론의 변화를 반영하여 수정해야 한다.
이에 따라 우리 팀은 초기 백서에 녹아있는 가치와 비전의 약속을 지키면서 보다 탄탄하고 최신 기술을 반영한 플랫폼을 만들 것이다.

초기 백서의 중요한 가치와 비전의 약속은 지켜져야 한다. 즉, 의사결정에 모든 검증자가 참여하는 의회네트워크의 구성, 의회가 원할 경우 활용할 수 있는 공공예산의 제공, 각종 Dapp 및 비즈니스 파트너를 지원하는 메인넷 플랫폼으로서의 기능은 그대로 유지되어야 한다.

BOSAGORA의 플랫폼의 뚜렷한 특징은 모든 검증자가 의사결정 과정에 관여하기 때문에 집단지성을 발휘할 수 있다는 것이다. 특히 BOSAGORA의 성숙한 의사결정 도구 덕분에 다양한 의견이 조화로운 형태로 집약될 것이다. 이러한 집단지성의 조화로운 과정을 통해 궁극적으로 BOSAGORA 생태계 개선을 도모하는 것이 프로젝트의 최종 목표이다.

제안

중앙집중화 방지 합의 알고리즘. 작업 증명 유형의 합의 프로토콜만을 사용하는 비트코인과 같은 암호화폐들은 경제적 인센티브와 정치적 인센티브 분리되지 않음으로써 발생하는 문제를 겪고 있다. 더 많은 채굴(mining) 장비를 구입함으로써 사용자는 블록체인에 대한 통제력(정치적 측면)을 높이고, 또한 동시에 채굴 수입(경제적 측면)을 늘릴 수 있다. BOSAGORA은 경제적 인센티브와 정치적 인센티브를 분리하는 합의 메커니즘을 사용(아래에 자세하게 설명 됨)하여 이러한 문제를 극복한다. 정치 권력이나 경제적 재원을 얻으려면 시스템에 대해 투자를 해야한다. 사용자는 노드의 수를 늘려 투표수를 늘리거나 (운영중인 노드 1개는 의회 1표와 같음) 또는 사용자는 동결된 지분에 대한 보상 및 블록생성 보상(노드에 묶여있는 코인의 양에 비례해서 주어지는 보상)에 투자하여 마이닝 수입을 최대화할 수 있다. 부가적으로, 여기에 사용된 합의 프로토콜은 에너지 효율이 높고 더 빠르다.

거버넌스. 탈중앙형 시스템에는 시스템화된 의사 결정 프로세스가 결여되어 있다. 암호화폐 세계에서 의사결정 프로세스의 부재로 사람들에게 혼란을 주고 재정적으로 상당히 큰 손실이 생기는 등 여러가지 문제가 발생했던 사례들이 있었다. BOSAGORA는 지속적으로 소프트웨어와 전체 생태계를 개선하기 위해서, 의회 네트워크를 구성하는 노드운영자들이 제안을 작성하고 투표에 참여할 수 있는 의회 네트워크라고 하는 거버넌스 시스템을 구성했다. 시스템 변경 제안서는 의회 네트워크에서의 투표가 통과되면 사회적 합의에 도달한 것으로 간주하며, 제안서에 의해 변화된 내용은 네트워크에 자동으로 적용된다. 또 다른 유형의 제안서로는 자금 조달 제안서가 있다. 펀딩 제안서 제출 후 의회 네트워크의 투표에서 통과되면 공공예산을 사용할 수 있다. 이 공공예산의 사용처는 BOSAGORA 생태계의 발전을 위해 사용되어야 한다. 이것에 대하여 아래에 설명하도록 한다.

Trust Contracts. BOSAGORA 팀은 최초의 의도대로 안전하고 정확한 프로그램 가능하며 실행 가능한 계약을 가능하게 하는 Trust Contract의 개발을 목표로 한다.

실현 불가능한 것을 계속하기보다는 'Trust Contract'를 재정의하고, 최적의 방향 선정과 핵심 기능 개발을 위해 적절한 기술 적용을 적극적으로 추진하겠다. 또한 가상 머신 위에 유연한 프로그래밍 언어를 사용하는 방법론을 채택하는 것을 고려하고 있으며, 우리는 현재 다른 업계 경쟁사들과 같이 WebAssembly를 연구하고 있다. 결국, 우리는 효율적이고 안전하게 설계된 Smart contract 엔진을 제공하고 개발자들이 쉽게 채택할 수 있도록 많은 도구와 인기 있는 개발하기 쉬운 언어를 제공할 생각이다.

WebAssembly는 최신 웹 브라우저에서 실행할 수 있는 새로운 종류의 코드다. 이는 상당한 성능 이점을 제공한다. "WebAssembly는 스택 기반 가상 머신의 이진 명령 형식이다. WebAssembly는 C/C++/Rust와 같은 고도의 언어를 컴파일하기 위한 휴대용 타겟으로 설계되어 있어 클라이언트 및 서버 애플리케이션을 웹상에 배포 가능하게 한다."

웹 상에서 복수의 언어로 작성되는 프로그램을 클라이언트 애플리케이션을 사용하여 거의 네이티브에 가까운 속도로 실행하는 것은 이전에는 불가능했다. WebAssembly에서 코드를 실행하는 것은 실제 하드웨어와 유사하다. WebAssembly를 통해 개발자들은 C++, 러스트 등 다양한 프로그래밍 언어로 코딩할 수 있으며, 네이티브와 가까운 성능으로 프로그램을 실행할 수 있을 것으로 기대할 수 있다. 또한 EOS, Ethereum, Tron, Cardano와 같은 많은 블록체인 플랫폼 또한 WebAssembly를 사용하여 가상 머신을 도입하거나 도입할 계획을 가지고 있다.

도입 계획의 타당성을 연구하여 해결책이 발견되면, 본 백서에 제시된 "Trust Contract"의 목적과 방향을 완성하기 위한 기술적, 실용적 조치를 취할 것이다.

Features	Bitcoin	Ethereum	BOSAGORA
Coin	BTC	ETH	BOA
Core Features	Financial Transactions (Bitcoin script)	Smart Contracts (Solidity, Serpent, etc)	Trust Contracts (WASM)
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)
Block Size	1 MB	Dynamic	Dynamic

Fig 1. 암호화폐 비교

합의 알고리즘

개요

합의 알고리즘은 블록체인 기반 화폐 또는 시스템의 핵심이다. 알고리즘은 '모든 분산 데이터베이스가 동일한 정보 집합을 보유하고 있다는 것을 어떻게 증명할 수 있을까?'라는 질문에 답하려고 노력한다.

BOSAGORA은 이 질문과 관련해, Stellar의 합의 프로토콜(FBA)을 기반으로 한 수정된 FBA(mFBA) 합의 알고리즘을 사용하기로 했다.[8]

Consensus Algorithm	Proof of Work	Tendermint	Byzantine Agreement	FBA[1]	mFBA[2]
Decentralized Control	O	O		O	O
Low Latency		O	O	O	O
Flexible Trust			O	O	O
Asymptotic Security		O	O	O	O
Governance Features					O
Staking Features		O			O
[1] Federated Byzantine Agreement [2] Modified Federated Byzantine Agreement (BOSAGORA protocol)					

Fig 2. 합의 알고리즘 비교

Mazieres는 FBA 프로토콜의 핵심 기능을 다음과 같이 정의한다:

- 탈중앙 제어. 중앙 관리자의 허가 없이도 누구나 참여를 해서 합의를 이뤄낼 수 있다.
- 낮은 대기 시간. 노드는 실제로 인간이 웹 또는 지불 거래에 대해 대기하는 시간 (예 : 최대 몇초) 사이에 합의에 도달 할 수 있다.
- 유연한 신뢰. 사용자는 적합하다고 생각되는 조합을 자유롭게 선택 할 수 있다. 예를 들어, 작은 비영리 단체라도 더 큰 규모의 기관들이 신뢰를 유지하도록 하는데 중요한 역할을 담당할 수 있다.

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

- 점근적 보안(Asymptotic security). 보안은 전자 서명과 해시 패밀리에 의존하는데, 이 변수들은 방대한 컴퓨팅 파워를 가진 적(adversaries)으로부터 보호하기 위해 현실적으로 조정할 수 있다.
- 의사결정 기능. 투표 및 의회 운영과 관련된 투표 기능이 프로토콜에 추가기능으로 포함되어 있다.

Federated Byzantine Agreement 합의 알고리즘

Bitcoin의 합의 메커니즘과 전통적인 비잔틴 기반 프로토콜은 모든 네트워크 참여자가 만장일치로 동의해야 한다. 그러나 FBA는 모든 참여자가 만장일치로 합의할 것을 요구하지 않으며, 추가적으로 각 노드는 자신이 어떤 노드를 신뢰할 지 선택할 수 있다. 이는 금융 네트워크의 무결성을 잃지 않으면서 유기적 성장을 가능하게 하면서도 더 빠른 거래를 가능하게 한다.

FBA는 노드들이 팀(정족수(Quorum)라고도 함)으로 그룹을 구성함으로써 만장일치 없이도 합의할 수 있는 메커니즘을 구현했다. 거래가 이루어지면 그룹의 모든 사람들에게 정보가 전송된다. 전체 네트워크가 데이터 상태에 동의하기를 기다리는 대신, 노드가 신뢰할 수 있는 노드로부터 충분히 많은 횟수의 동일한 메시지를 듣는 경우, 해당 노드는 정보가 올바른 것으로 가정한다. 노드들이 중복되거나 느슨한 노드 연합이 발생하면 동일한 트랜잭션에 대해 동의하는 서로 다른 팀들을 갖는 서로 다른 노드들을 만들게 된다. 이는 각 트랜잭션 블록에 대해 만장일치의 동의 없이 시스템 전반에 걸친 합의를 이끌어낸다.

부정거래를 둘러싸고 노드가 서로 대립하는 상황이 발행하면 이를 극복하기 위한 투표 시스템이 시스템에 내장되어 있다. FBA에 관한 추가 기술적 세부 사항은 Stellar의 합의 프로토콜 문서에서 확인할 수 있다.

mFBA의 차이점

FBA 외에도 BOSAGORA 합의 프로토콜은 거버넌스 시스템의 유지 관리를 위해 지분 증명의 특성을 적용했다. 사용자는 검증자가 되기 위하여 40,000개의 BOA를 동결 해야 하며, 유동성을 억제하는 역할을 하는 댓가로 노드에 동결된 코인의 총 수에 비례하여 새로 발행된 BOA(블록생성 보상)을 받는다. 노드에 동결된 코인은 노드를 운영하는 데에 따른 경제적 인센티브를 제공하는 것과 동시에 노드의 블록체인에 보관된 정보의 보안 및 무결성에 대한 담보 역할을 한다. 사전 설정된 규칙에 따라, 노드가 블록체인을 위조한 것으로 밝혀지면 동결된 코인의 일부가 공공예산 계정으로 몰수된다.

의회(Congress) 네트워크

개요

의회 네트워크는 BOSAGORA의 민주적 의사결정 기관으로서, 각각의 풀-노드 운영자들로 구성된다. 의회는 소프트웨어와 생태계를 지속적으로 향상시키기 위해 다양한 프로젝트 이해관계자들 간의 효과적이고 포괄적인 협업을 가능하게 한다. 예를 들어, 소스 코드와 마케팅 자원의 개발은 시스템 내에서 제안, 결정, 구현될 수 있다.

BOSAGORA의 모든 노드 운영자는 의회 네트워크에 가입하여 집단 의사결정 과정에 참여할 수 있다. BOSAGORA 의회 네트워크는 구성원들이 프로젝트의 공통 관심사의 제안, 토론, 투표 및 검토를 통해 참여와 기여를 할 수 있도록 한다. 의회 네트워크는 1노드 대 1투표 규칙을 준수한다.

필요성

블록체인 프로젝트는 어느 제품과 마찬가지로 실제 사용자들의 요구를 충족시켜야 한다. 하지만 아무리 세심한 설계를 준비하더라도 기술, 사람, 그리고 시장의 방향성은 상시로 변하고 프로젝트는 이러한 변화에 꾸준히 적응해나갈 수 있어야 한다. 언제, 어떻게 네트워크를 진화시킬지를 결정하는 것이 지속가능성과 성장의 핵심인 것이다. 모든 이해관계자들의 의견과 관점을 하나의 합의로 이끌어 내는 것은 지극히 소모적인 과정이될 수 있다. 그렇기에 아무리 태생적으로 탈중앙화를 지향하는 블록체인 프로젝트라도 대부분 중앙화된 의사결정 시스템을 가지게 된다.

아무리 좋은 의도를 가졌더라도, 중앙화된 의사결정 프로세스는 결국 네트워크 전반적인 목소리를 수용할 수 없다. 그리고 멤버들이 느끼는 문제점을 알리고, 해결하는데 있어 참여할 수 있는 방도가 없다면 다른 프로젝트로 옮길 수 밖에 없을 것이며, 결국 네트워크 효과의 감소시킬 것이다. 포용적이며 협력적인 거버넌스는 성공적인 프로젝트의 필수조건이다.

집단 의사결정의 문제점

나쁜 의사결정은 여러 가지 이유에 의해서 발생할 수 있으며 그중에는 의사결정의 사회적이고 참여적인 성격 때문에 비롯되는 문제들이 포함된다. 불완전한 정보, 구성원간 역학관계, 인지 편향, 그리고 눈치보기로 인해 팀과 커뮤니티는 최선의 솔루션을 찾지 못할 때가 많다.

- 불완전한 정보: 결정을 내리기 위해 알아야 하는 이해관계자들의 입장이나 현장에 대한 정보가 충분하지 못한 경우.
- 역학관계(Power dynamics): 의사결정에 가장 취약하며 영향을 많이 받는 사람들의 의견을 제외한 소수 인원으로 내려진 의사결정. 논의를 독점하여 다른 사람들의 발언권 기회를 빼앗는 상황.
- 인지 편향(Cognitive Biases): 인지 편향(편견, 고정관념, 내집단 또는 외집단 편향 등의 다양한 심리 현상)으로 인해 객관적 판단을 흐리는 경우
- 사회적 압력: 동료의 눈치를 보거나 주변을 의식하는 등의 사회적 압력으로 인해 건설적인 피드백과 의사소통이 방해 받는 경우

오늘날 의사결정의 문제는 중재자의 부재로 인한 비효율성과 더불어 악화된다. 의사결정 과정을 통제하는 데 필요한 적절한 규칙이나 원활한 의사결정을 이끌어줄 퍼실리테이션(회의진행자)이 없어 참여자들의 서로 다른 의견들만 계속 늘어놓기만 하고 결론으로 나아가지 못한다.

의회 네트워크 개요

우리는 노드간의 숙의와 투표 시스템에 기반한 탈중앙화된 집단 의사결정을 제안한다. 이는 BOSAGORA 의회 네트워크라 칭한다.

기능

의회 네트워크는 다음과 같은 기능을 수행하는 플랫폼이 될 것이다:

- 멤버들 사이의 활발한 의견 공유와 소통
- BOSAGORA 네트워크에 구현하고자 하는 제안들에 대한 의사결정

BOSAGORA에는 크게 두 가지 유형의 제안이 있다.

- 시스템 제안은 BOSAGORA 플랫폼을 변경하는 제안이다. 네트워크의 기술적인 기능의 변경 또는 개선 등을 포함한다. 개발팀의 방향성은 의회 네트워크에서 만들어지는 결정을 반영할 것이다.
- 펀딩 제안은 공공예산에서 기금을 요청하는 제안이다. 이 기금은 블록체인 Dapp 프로젝트, 비 블록체인 영리 사업 투자, 그리고 비영리 단체를 위한 기부 등 BOSAGORA 생태계 확장을 위해 사용되어야 한다.

특징

집단 의사결정의 문제점을 극복하고 보다 포용적이고 효율적인 의사결정을 가능케 하기 위해 의회 네트워크는 다음의 기능을 탑재한다.

Voice (동등한 발언권): 목소리 크고 자기 과신에 찬 사람들은 토의를 독점하게 된다. 이런 사람들은 보통 사회적으로 권력층에 속해 있는 경우가 많고 다른 사람들의 의견을 묵살함으로써 실망스럽고 모두의 이해를 대표하지 못하는 (많은 사람들에게 영향을 미치지만 소수에 의해 정해진) 결과를 초래한다. 평등한 발언 기회의 원칙이 지켜질 수 있도록 의회 네트워크에서의 논의는 '발언권 (Voice)'에 기반한다.
발언권은 기여할 수 있는 능력이다: 멤버들은 논의에 참여하거나, 제안하거나, 결과를 평가함으로써 기여한다.
발언권은 토의에 참여하는 모두에게 평등하게 분배된다. 지나치게 길어지거나 비효율적인 논의와 트롤링을 방지하기 위해 발언 횟수가 제한된다. 특정한 활동 (논의, 투표, 평가)를 개시하는 시점에 각자에게 몇 개의 발언권을 부여할지 정한다.
주어진 발언권을 모두 소진한 멤버는 다른 멤버들에게 발언권 위임을 요청할 수 있다. 만약 누군가 커뮤니티 모두를 위해 가치있는 의견을 내고 있다고 여겨진다면, 당신은 그 사람에게 당신의 발언권을 위임할 수 있다. 이를 통해 탈중앙화된 큐레이션, 즉 강제로 다른 사람의 발언권을 박탈하지 않으면서 함께 가치있는 담론을 형성하는 것이 가능해진다.

AAID (Incognito): AAID는 의회와 생태계 멤버들의 프라이버시와 자격증명을 동시에 보장하기 위한 개념이다. 열린 참여를 증진하면서 프라이버시 노출 문제가 없는 플랫폼을 만들기 위해 적용된 AAID (Authenticated Anonymous IDentity;인증받은 익명 아이덴티티) 기술은 자격증명이 확인된 멤버에 대해 익명 계정을 생성하고, 각 활동에 참여할 때는 해당 익명 계정으로부터 그 활동 내에서만 유효한 일회용 아이덴티티를 발생시킴으로써 여러 활동들에 남겨지는 디지털 발자국(digital footprints)을 추적하는 것을 방지한다. 이 기술은, 비록 발생할 일이 거의 없는 경우이기는 하나 심지어 서버가 해킹당하는 상황에서도, 사용자들의 프라이버시를 완벽하게 보호한다. 편견은 제거하되 신뢰를 유지하고, 멤버들은 토의 과정에서 표현의 자유를 누린다.

멤버의 자격 인증과 관련하여서는, 네트웍와 AAID 서비스 제공자가 자격을 확인한 후, AAID 서비스 제공자가 확인 증명을 발행한다. 동형암호를 사용하여 AAID는 자격 증명(4만 보아 이상을 가진 노드 주소)에서 파생되어 생성되지만 연결관계가 드러나지 않게 된다.

이 기술은 토의와 리뷰에 적용된다. 시스템 자체에 지대한 영향을 끼치게 될 제안이나 펀딩 제안을 결정하는 투표의 경우엔 투표 기록의 검증 가능성이 강력한 익명성보다 우선순위를 가지므로 AAID가 적용되지 않는다.(검증 가능성을 위해서는 투표한 사람의 노드 주소가 필요하다.)

유연성 (적응적) : 문제를 해결하는데 정해진 공식이 없다는걸 알기에 의회 네트워크는 사용자별, 상황별 필요한 단계들과 기능을 제공한다. 상황에 알맞은 의사결정 흐름을 찾아내기 위해 프로세스는 실시간으로 조정이 가능하다. 토의, 리뷰 또는 투표를 진행하고, 연결된 활동을 언제든 추가해서 실시간으로 변동하는 우선순위에 대응할 수 있다.

Facilitated (효율성) : 주제에 대한 결과를 내는데 집중할 수 있게 의회 네트워크는 다양한 맞춤 기능이 탑재된 활동 템플릿을 제공해서 참여 인원들이 현재 단계를 예측 가능케 한다. 활발한 자유 토의든, 정해진 목록에서 우선순위를 정하든, 특정 결과에 대한 개별 평가를 내린다던지, 무엇을 하고, 언제 어떤 종류의 결과가 나올지 예측할 수 있어 집중력을 유지할 수 있다.

아카이빙 (투명성 & 책임성) : 투명성과 책임성은 좋은 의사결정에 필수적인 기반이다. 의회 네트워크는 가능한 많은 의사결정 데이터를 기록 보관할 것이다. 다만 블록 크기의 한계로 블록체인은 결정을 검증할 수 있는 기록의 해시를 담을 것이다. 토의, 투표 그리고 리뷰 정보는 별도의 서버에 저장해서 멤버들이 언제든지 내부 의사결정 기록을 열람할 수 있도록 제공할 것이다. 여기 또한 AAID가 적용 되기에 논의 내용 열람은 가능하지만 내용을 연결지어 개인들을 특정지을 수 없고, 사용자 스스로만이 자신이 참여한 기록을 모아 볼 수 있다.

절차

의회 네트워크 가입

누구나 다음 조건을 이행하면 의회 구성원이 될 수 있다:

- 안정적인 네트워크 속도에서 풀-노드 및 검증자 운영
- 최소 40,000 BOA 동결

노드는 의회 구성원이 실행하는 서버 또는 개인용 컴퓨터일 수 있다. 노드는 네트워크 속도가 안정적일 경우 가정이나 원격 위치에 배치할 수 있다. 의회 구성원들은 더 많은 노드를 운영함으로써 그들의 정치적 영향력을 증가시키거나, 동결된 BOA 토큰의 수를 증가시킴으로써 그들의 경제적 수익을 증가시키는 데 투자할 선택권을 가지고 있다.

활동 만들기

멤버들은 활동을 만듦으로서 논의와 의사결정을 진행할 수 있다. 현재는 3가지의 활동 템플릿이 있는데 이 중에서 사안에 따라 선택하면 된다. 신규 사업 기회, 시스템 변경, 또는 프로젝트에 대한 전반적인 설문조사 등, 의회 멤버들의 의견이 필요한 모든 의견을 다룰 수 있다.

- 논의: 멤버들은 브레인스토밍 등 서로의 의견을 나누고 발전시킬 수 있다.
- 투표: 멤버들은 선택지들에 대해 투표와 댓글을 달 수 있다.
- 리뷰: 멤버들은 제품, 결정 등을 리뷰하거나 설문조사에 참여할 수 있다.

사용하면서 사용자들이 필요 하는 추가 기능과 템플릿은 앞으로 추가할 수 있는 구조다.

모든 구성원들은 제안을 할 수 있다. 더 나은 제안의 질과 그 제안의 책임을 보장하기 위해서 수수료 체계를 향후 도입예정이다.

가이드

각 활동 마다 생성자는 다른 멤버들이 이해하고 참여할 수 있도록 필요한 정보를 입력해야한다.

1. 링크 (optional): 활동을 생성할 때, 이미 존재하는 활동에 연결 지어 만들 수 있다.만약 커뮤니티 규칙에 대한 투표가 진행되었다면, 시간이 어느정도 지난 뒤, 도입된 규칙이 얼마나 잘 자리잡고 있는지, 더 개선할 점이 있는지에 대해서 리뷰 활동을 연결 지을 수 있다.
2. 이름: 활동에 대한 레이블.
3. 목표와 설명: 이 활동의 주제, 목적과 배경을 입력해야 한다.
4. 마감일: 언제까지 이 주제에 대한 결론이 내려져야 하는가?
5. 고급 설정 (optional): 템플릿 마다 설정할 수 있는 기능들이 있다. 몇가지 예시로 분배할 발언권의 갯수, 투표용지 종류, 리워드 등이 있다.
6. 수수료 (optional): 활동 생성은 무료이지만 펀딩 제안의 경우, 투표 생선 전에 수수료를 지급해야한다. (수수료 체계는 향후 적용 될 예정)

논의

멤버들은 발언권을 사용해서 의견과 댓글을 쓸 수 있다. 의견은 추천을 받을 수 있고 최신 또는 추천 수로 의견을 나열 지어 볼 수 있다. 의견은 제목 이외 수정 가능하나, 수정의 기록은 다른 참여자들이 모두 볼 수 있고 삭제가 불가하다. 멤버들은 의견에 대해 댓글을 달 수 있지만 댓글은 삭제 불가하다.

만약 의견 또는 댓글 중 커뮤니티의 규칙에 어긋난다면 멤버들은 해상 콘텐츠를 뮤트 시켜 로컬 앱에서 숨길 수 있다.

투표

투표는 합의를 이루기 위해 생성된다. 투표의 결과가 BOSAGORA에 직접적인 영향을 미치기에, 추후에 검증 가능하도록 결과는 기록 되어야 한다.

검증 가능하지만 중간 결과는 마감 까지 알 수 없게 하기 위해서 우리는 검증자 해시 체인 구조(validator hash scheme)를 도입했다.

어떤 사람이 검증자가 되고 따라서 의회 구성원이 되면, 이 구성원은 자신만 알고 있는 임의의 번호를 선택해야 한다. 이 구성원은 임의의 숫자를 n번 해시 해야한다. n번 해시된 임의의 번호는 Hn-1로 나타낸다. n은 값을 찾기 위한 지표가 된다.

만약 검증자가 블록 높이가 500일 때 투표하기로 결정한다면, 이 검증자는 H1008의 약속을 한 것이다. 블록 높이가 100블록 거리인 600일 때 투표가 종료될 경우, 검증자는 자연스럽게 H908인 사전 이미지를 100으로 전송하게 된다. 사전 이미지로 H1008의 유효성을 검증하기는 쉽지만 H1008에서는 H908을 알아낼 수 없다.

H1008을 지분 증명 계층에 검증값으로 사용함하게되면 검증자는 이를 네트워크에 전달하지 않아 불이익을 받게 된다. 투표 시스템은 검증자들이 투표에 적절하게 참여할 수 있도록 인센티브의 계층을 추가함으로써 참여를 유도할 것이다.

검증자는 공약과 투표를 제출해야 하며, 투표는 H908에서 파생된 개인 키로 암호화된다. 예: H(H908||"Congress Network"|| vote ID)
투표가 마감되면 검증자는 H908을 대변하게 되며, 투표 서버는 제출 된 투표를 복호화하여 집계할 수 있게 된다.

투표 검수

투표 기간이 끝나면 투표 결과를 보관한다. 각 투표의 날짜와 시간이 저장되고 동일한 노드로부터 투표가 중복될 경우 마지막 투표만 최종 결과로 간주되어 1노드-1 투표의 특이성을 보장한다. 이 과정과 결과는 위에서 설명한 제도로 검증할 수 있다.

정족수

정족수는 어떤 제안이 플랫폼상에서 인정되기 위한 투표에 참여해야 하는 의회 네트워크 구성원의 최소 수이다. 의결 정족수는 초기 전체 구성원의 3분의 1로 정해지지만 평균 참여율을 반영해 추후 조정될 수 있다.

긍정 혹은 부정 표결 사이의 '순 백분율 차이'가 10%를 초과하면 제안서가 통과된다. 부정 표를 뺀 긍정 표가 총 유효표수의 10% 이상에 해당할 때 제안서는 반려된다.

적용

제안이 통과된 후, 해당 제안은 실행되어야 한다. 개발팀은 승인된 시스템 제안을 담당하며 필요할 때 개발계획, 로드맵, 보안테스트 등을 제공한다.
공공예산 제안은 서면계약에 따라 배분된다. 이후 Trust Contract가 구현됨에 따라 이를 관리하기 위해 블록체인 내 거래로 적용 될 것이다.

검토/감사

제안서 시행 후 의회 네트워크와 재단의 검토를 받게 된다. 제안서의 로드맵에 따라 예정된 검토가 있어야 한다. 검토 활동의 템플릿은 진행 중인 제안에 대한 이해 관계자들의 의견를 집계하기 위해 이용할 수 있다.
공공예산 제안의 경우, 검토 및 감사 비용은 제안자가 지불한 수수료에 의해 보상될 것이다.

결론

의회 네트워크는 BOSAGORA 커뮤니티만을 위한 전용모델이 아니다. 우리는 의회 처럼 포용적이고, 효율적이며 투명한 협력 시스템이 함께 의사결정을 만들어 가야하는 다양한 조직들에게도 적용되길 기대한다. 다른 블록체인 프로젝트, 기업, 심지어는 정치에 있어서도 함께 더 나은 숙의 민주주의를 단계적으로 만들어 나갈 수 있다고 믿는다.

네트워크 상호작용

거래

사용자가 트랜잭션을 요청하면 해당 요청은 의회 네트워크로 전송된다. 간단한 BOA 전송에 대해서 이야기하자면, 노드가 블록을 확정하면 사용자의 트랜잭션이 승인되고 BOA가 다른

지갑으로 전송된다. 보다 복잡한 Trust Contracts라면 사전에 정의된 논리 및 절차가 실행될 것이다. BOSAGORA의 초기 단계에서 거래 수수료는 0.01 BOA로 고정되지만, 이 요금은 의회 네트워크에서 투표를 통해 조정할 수 있다. 거래 수수료는 노드 운영자에게 경제적 인센티브로 작용하고 또한 DoS 공격에 대한 방어 메커니즘으로도 작용한다.

제안서

제안서란 의회 네트워크에 제출되는 공공예산 사용 계획 또는 시스템 변경 계획을 의미한다. 제안이 이루어지고 제안서가 통과되기 위해서는 반드시 긍정 및 부정 투표 간의 '순 백분율 차이'가 10 %를 초과해야 한다. 자금과 관련된 제안서가 통과되면 요청된 코인은 제안자에게 전송된다. 어떤 경우, 예컨대 제안의 규모가 큰 경우에는 시스템에서 코인이 어떻게 사용되었는지에 대한 보고서를 요구하도록 정의할 수 있다.

코인 동결(Freezing)

코인 동결은 지분 증명 개념으로, 사용자가 검증자가 되기 위하여 코인을 동결할 수 있다. 동결된 코인은 블록체인 위조 시도 시 담보로 사용된다. 노드가 블록체인을 위조하려고 시도하면 동결된 코인의 일부가 몰수되어 공공예산 계정으로 보내진다. 또한 코인 가격 안정을 촉진하기 위한 메커니즘으로, 코인 동결을 취소하려면 2주 전에 사전 통보해야 한다. 이 개념은 이 백서의 기술 부분에서 추가적으로 다루어진다.

보상 구조

비트코인은 작업 증명 프로토콜에 의존하기 때문에 해시 파워 집중화 문제로 어려움을 겪고 있다. 소수의 거대채굴자들이 대량의 채굴기를 쉽게 구입할 수 있는데, 이것은 코드 변경에 영향을 미칠 수 있으며 또한 심지어 블록체인의 무결성을 위협할 수도 있다. 금전적 이득을 극대화하려는 사람들의 인센티브를 분리함으로써, 의사 결정 프로세스에 참여하기 위한 진입 장벽은 의사 결정 권한과 금전적 보상이 비례하는 시스템보다 상대적으로 낮게 되어 있다.
의회 구성원은 블록생성 보상, 거래 수수료의 두가지 방법으로 BOA 보상을 받을 수 있다.

- **블록생성 보상(Confirmation Reward)**: 블록이 확정되면 블록생성 보상이 해당 노드에 제공된다. 이 보상은 노드 운영자들에게 제공하는 핵심적인 인센티브다. 그리고 이 보상은 노드에 동결된 코인 수에 비례하여 지급된다. Bitcoin의 블록 보상과 마찬가지로 참여 노드 수가 증가하면 블록생성 보상을 받을 확률이 줄어든다. 동결된 코인에 대한 보상은 노드에 동결된 금액에 비례한다. 리워드는 5초당 평균 27 BOA코인으로 시작한다. 처음 블록생성 보상은 5초당 27 BOA에서 시작하며 대략 128년 동안 전년 대비 6.31%씩 감소한다.

- **거래 수수료(Transaction Fee)**: 거래 수수료는 0.01 BOA로 고정된다. 의회 노드들은 블록당 총거래 수수료의 70%를 받고, 30%는 공공예산으로 보낸다. 거래 수수료는 의회를 통해 조정할 수 있다.

공공예산(Commons Budget)

공공예산(Commons Budget)은 BOA가 보관되는 계좌이며, 의회 투표를 통과한 제안서에만 이체될 수 있다. 공공예산의 주된 역할은 초기 단계에서 코인 사용자의 수를 늘리는 것이다.

공공예산의 코인은 주로 두 개의 채널을 통해 축적된다; 첫 번째는 대략 6년 동안 5초당 50 BOA를 직접 발행하는 것이고, 두 번째로 거래 수수료의 30%가 축적되는 것이다. 이것은 BOSAGORA 플랫폼의 사용률을 획기적으로 높이기 위해 사용할 수 있는 자금을 보장해줄 것이다.
의회를 통과하는 제안은 어떤 것이라도 공공예산을 받을 수 있다. 제안의 한 사례를 들자면 BOSAGORA 플랫폼의 사용자 수를 늘리기 위해 무료로 코인을 사용자에게 배포하는 Airdrop 제안이 있을 수 있다. 다른 사례들로는 BOSAGORA 생태계 개발 자금 조달, 마케팅 캠페인 그리고 BOSAGORA 관련 밋업 개최 등이 있을 수 있다.

토큰 배분 및 발행

BOSAGORA 토큰 배분

BOSAGORA 팀은 2019년 4월 5일 금요일 12:00 UTC 기준의 스냅샷에 따라 2019년 5월 16일부터 9월 30일까지 BOS 홀더에 대한 BOA 에어드롭을 수행했다. 이 스냅샷에 따르면, 542,130, 130.19558463 BOS 코인이 유통량 이었다.

- 500,000,000 BOS 가 최초의 유통량
- 41,420,159.8931463 BOS 는 BlockchainOS PF00 멤버쉽 보상 발행
- 709,970.3027000 BOS 는 BlockchainOS PF01 멤버쉽 보상 발행

BOA 토큰 에어드랍 이후, BOA 토큰의 배분 계획은 다음과 같다:

Category			BOA	Share
Initial Supply	Airdrop for BOS holders		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%
		Members	40,000,000	0.81%
		Bounty	10,000,000	0.20%
	Initial supply total		542,130,130	
	Token burn	BCOS PF	42,130,130	
		Unclaimed	50,000,000	
	Initial supply total after burn		450,000,000	
Confirmation Rewards			2,700,000,000	54.54%
Commons Budget			1,800,000,000	36.36%
Total			4,950,000,000	100.00%

Fig 3 : BOA 코인 발행 계획

BOS 홀더들에게 지급된 에어드롭의 총량은 247,595,031.305721 개 이다. 에어드롭이 마무리 된 이후 남은 토큰의 수는 204,535,098.694279 개 이다.
이 남은 204,535,098.694279 개의 토큰은:

- 42,130,130.1958463 개의 토큰은 Public Financing를 통해 발행되었다. 이것은 재단의 의도한바가 아니며 소각되어져야 한다.

- 50,000,000 개의 토큰 또한 소각 대상이다. 재단은 남은 토큰 중 50,000,000 BOA 를 소각하기로 결정하였으며 이는 초기 발행계획의 약 10% 이다.
- 30,000,000 BOA 는 마케팅을 위하여 별도로 보관될것이며 이는 거래소 상장 혹은 파트너쉽을 위해 사용될 것이다.
- 82,404,968.6942793 개의 토큰은 유보되어있다.

결과적으로 최초 전체 유통량은 450,000,000 BOA가 된다. 재단은 토큰 메트릭에 변동 사항이 있을 경우 별도로 공지할 계획이다.

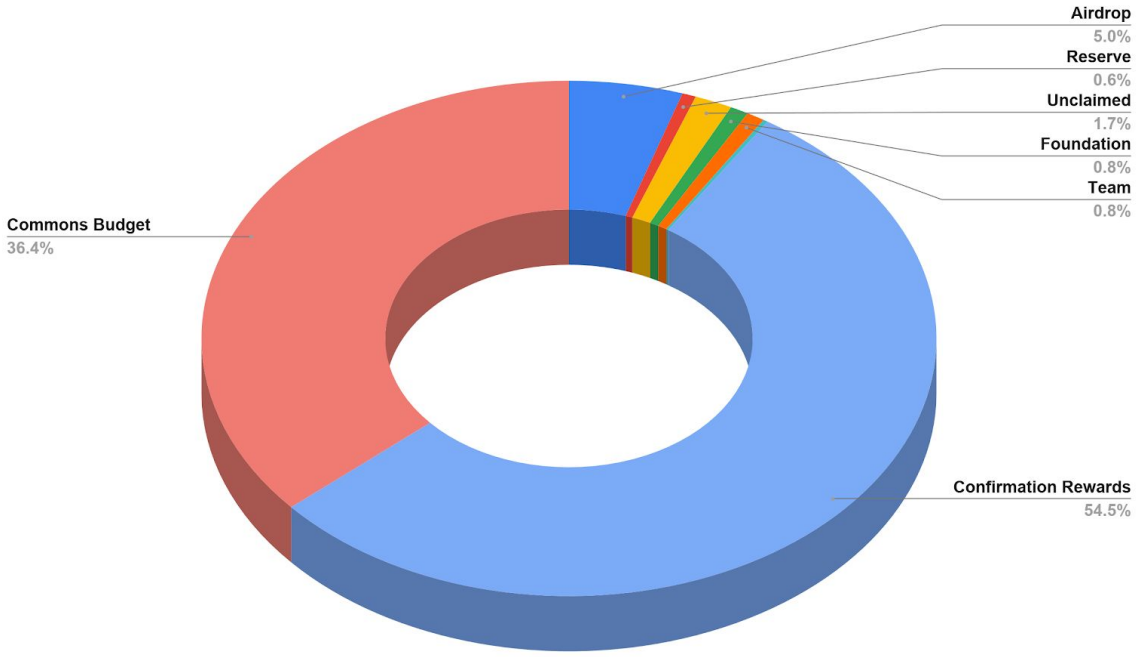

Fig 4 : BOA 코인 발행 계획

발행

새로운 코인은 네 가지 방법으로 발행된다; 초기 개발 예산(4.5억개, 10 %), 블록생성 보상(27억개, 54 %), 및 공공예산(18억개, 36 %). 우리는 앞으로 100 년간 총 49.5억개의 코인을 발행할 계획이다. 이 값은 변경될 수 있다.

- **초기 개발 예산 :** 초기 개발 예산은 Genesis 블록 이전에 배포되는 코인이며 소프트웨어 개발 완수를 지원하기 위한 것이다. 이 코인은 ICO 판매 및 포상금(bounty)으로 구성된다. 4.5억 개의 BOA코인이 Genesis 블록과 함께 발행된다.
- **블록생성 보상:** 블록생성 보상은 공평하게 노드에 지급되는 금전적 보상이다. 보상이 공평하게 분배됨에 따라, 노드의 수가 증가하면 한 노드가 보상을 받을 양이 감소할 수 있다. 이 보상은 노드에 동결된 코인 수에 비례한다. 27억 BOA가 블록생성 보상으로 발행된다. 처음에는 5초당 27 개의 BOA가 발행된다. 보상은 약 1년씩 128년 동안 6.31%씩 감소한다.

- **공공예산:** 공공예산은 의회 네트워크를 통과한 제안서에 지급할 BOA를 보유하고 있는 계좌다. 제안을 위한 충분한 예산을 만들기 위해 초기 약 5년 동안 5초당 50 공공 코인을 발행된다. 처음 5년 후에 공공예산은 거래 수수료에 대한 30 %의 공공 수수료를 통해 유지된다.

코인넷이 출시된 이후, 블록생성 보상과 공공예산이 생성될 것이다.

전체 토큰 발행 차트는 이 문서의 마지막에 첨부되어있다.

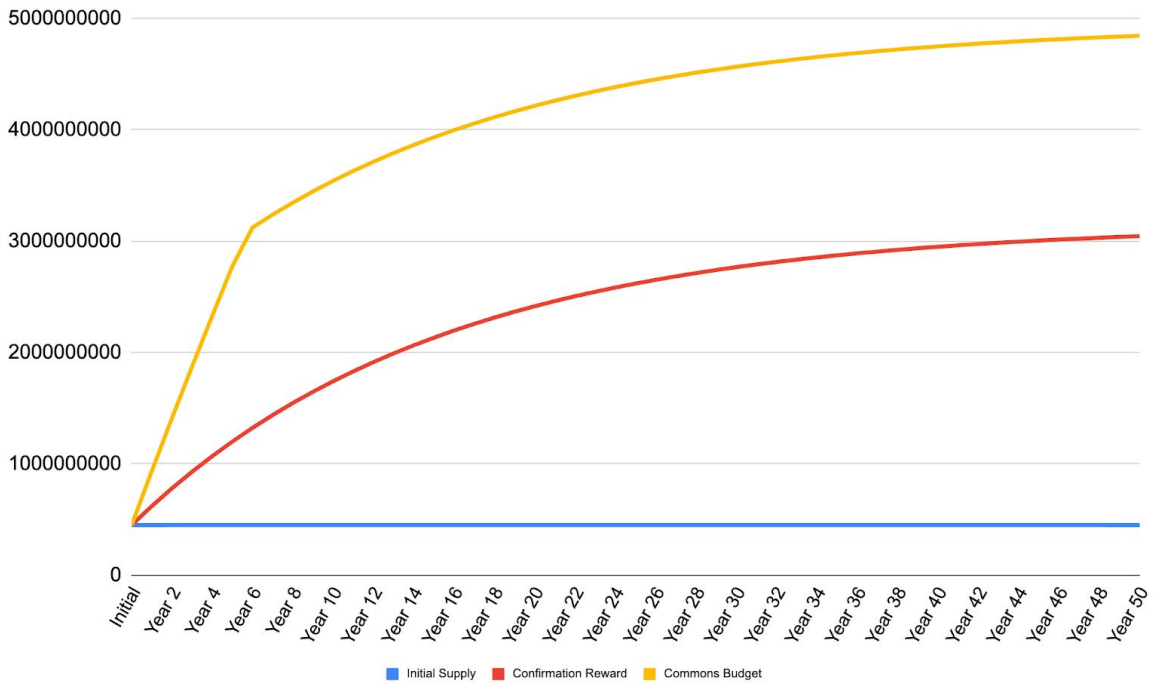

Fig 5 : BOA 코인 발행 계획

기술

요약

비트코인은 전세계에 디지털화 된 돈에 대한 아이디어를 소개했다. 현금에 대응하는 가상의 기술을 구현함으로써 돈의 속성이 논의되고 도전받는 수십억 달러 규모의 산업의 토대를 마련했다.

최초로 사용된 접근방식은 강력한 컴퓨팅 능력에 기초하여 일련의 작업을 포함하는 타임스탬프 서버를 사용하는 것이었다. 이것은 매우 매력적인 특성을 제공하지만 작업 증명(PoW)의 사용은 매우 비효율적인 것으로 드러났다.
또한, 채굴 회사의 운영으로 인해 에너지 비용이 낮은 지역에서 중앙 집중식으로 운영되며 특정 하드웨어의 개발로 이어져 시스템을 더욱 중앙 집중화시킬 위험이 있다.
이를 위한 대안이 개발되고 있지만, 작업 증명 접근은 본질적으로 낭비적이다.

우리는 낮은 비용으로, 또한 잘못된 행동을 하는 참여자들에게 벌칙이 적용되는, 독자적인 시스템에서 합의를 이루는 방식을 제안한다. 이것이 무엇을 의미하는지 우리만의 정의가 있지만, 일반적으로 이러한 시스템을 "지분 증명(Proof-of-Stake)"이라고 부른다.

우리는 어떠한 시스템이든 안전하도록 작동해야 하는 대전제 하에 여러 가설을 연구하고, 우리가 찾는 특징들이 비트코인과 어떻게 비교되는지를 정의하는 것부터 시작한다. 또한, 우리는 지분 증명(가장 주목할 만한 것은 Ethereum의 연구)과 지분 증명에 특화된 각종 공격에 대한 최신 연구 개발 현황을 탐구한다.

I. 개요

작업 증명의 자원 소모

비트코인 백서[Nak09]에서 언급되어 있듯, 전자 현금 시스템이 직면하는 주된 문제는 이중 지불이다. 작업증명(PoW)은 전자 현금 개념을 민주화하는 강력한 도구였지만, 전문 하드웨어(ASIC)의 개발과 대량의 낭비적인 에너지 소비로 이어졌다. 그 결과, 채굴장의 운영은 주로 값싼 전기를 제공하는 지역에 집중되었다. 2018년 6월 기준으로, 해시율의 약 74%가 중국 기업[KJL18]에 의해 운영된 것으로 추정되었다. 게다가, 대부분의 전문 하드웨어(ASIC)는 중국에서 개발되고 있어, 이는 중국 규제당국에 취약하다.

지분 증명

아직까지 최선의 해결책을 가진 작업증명의 대체품은 없다. 하나의 대안은 지분 증명(PoS)이라 할 수 있다. 2012년 피어코인(Peercoin)[KN12]을 시작으로 '코인 시대'를 맞아 많은 프로젝트가 이 문제를 연구했다. 또 다른 잘 알려진 코인인 NXT는 새로 생성된 블록 데이터를 시드로 사용하여 다음 선택을 결정하는 접근방식을 사용한다[NXT19]. 지분증명 시스템을 연구하고 있는 가장 두드러진 프로젝트인 Ethereum은 2014년 부터 지분증명으로 이전할 계획을 세우고 있다. 지난 몇 년 동안, 새로운 프로젝트들은 "위임된 지분 증명(Delegated PoS)"라는 개념을 도입했다. 여기서 사용자들은 노드 중 매우 소수에게만 본인의 투표권을 위임한다.

지분 증명 프로토콜과 작업 증명 프로토콜의 주요한 차이점 중 하나는 전자가 가용성보다 안전성을 선호하기 때문에 프로토콜은 중지될 수 있지만 즉각적인 완결화가 이루어지는 반면 후자는 가용성 및 사용성의 안전을 보장한다는 것이다. 그러나 작업 증명의 경우 충분한 해시파워를 가진 공격자가 빈 블록을 생산하기로 결정하여 시스템을 효과적으로 쓸모 없게 만들 수 있으므로 가용성조차 보장이 되지 않는다. 그러므로 지분 증명의 가용성이 완벽하지 못한 이유로 받지 못한 보상은 블록 생성 보상에 비해 미미하여 외부의 참여자들로 부터 보정이 쉽게 이루어진다.

그럼에도 불구하고, 어떤 공격을 통해서든 안전성의 저하는 화폐 가치의 하락을 초래할 가능성이 높으며, 많은 경우 공격을 예방하기에 충분한 동기가 된다. 블록체인 커뮤니티는 이를 충분히 수용해 왔으며, 게임 이론은 암호화폐 세상의 기원부터 합의 프로토콜 분석의 필수적인 부분이었다. [GTB19].

확장성 문제

지분 증명 시스템이 나타내는 자원의 본질적인 낭비 외에도, 블록체인 확장성은 활발한 연구의 주제다. 비트코인 커뮤니티에서도 비트코인은 1MB의 블록 한계(Segregated Witness[SegWit]가 체인 용량을 늘리는데 도움이 되었음에도 불구하고)를 유지했고 비트코인 캐쉬(BCH)는 블록 크기를 32MB로 늘렸다. 소형블록에 찬성하는 주장은 전체 노드(블록체인을 완벽하게 검증하는 노드)만 보안이 되는 반면, 다른 노드들은 시스템의 다른 부분(채굴자 등)에 의존하기 때문에 개인용 컴퓨터로도 비트코인 노드를 실행할 수 있어야 한다는 것이다. 블록당 32MB로 블록당 1개/10분(하루 144개 블록)으로, 수용할 수 있는 데이터의 양은 매일 4.6GB, 매월 138GB, 연간 1659GB이다.

분산형 네트워크의 독특한 요구사항 중 하나는 거래가 이루어진 것으로 간주되기 위해서 시스템의 다수에 의해 확인되어야 한다는 것이다. 또한, 네트워크에 참여하는 노드가 많을수록 네트워크는 더 분산된다. 또한, 노드가 특정 주체에 의해 관리되지 않아야 한다. 따라서, 사용자가 지속적으로 늘어날 수록 각 노드에는 더 많은 스트레스를 줄 것이고, 더 높은 하드웨어와 대역폭 요구로 이어질 것이다. 반면 노드 수가 증가하면 모든 트랜잭션은 더 많은 노드에 도달해야 하므로 트랜잭션 확인에 걸리는 시간이 증가한다.

이러한 여러가지 문제점을 동시에 해결해야하는 최적화 문제를 공략 하는것 보다, 블록체인 계층(L1 / "합의 계층") 위에 두번째 계층(L2 / "플래시 계층")를 구축해, 조금 더 유연한 환경을 구축한 상태에서, L1의 이점인 안전성을 효과적으로 얻을 수 있도록 하는 동시에, L1에 모든 데이터를 기록할 필요 없이 피어에서 트랜잭션을 수락하도록 할 수 있다(확장하면 모든 노드로 전달). 우리는 클라이언트가 이 환경을 우선적으로 사용하고, 노드가 이와 같은 트랜잭션을 조건없이 받아들이도록 하는 보상 체계를 구축한다.

2계층을 사용함으로써 얻는 이점은:

- 블록체인 데이터를 줄이고;
- 프로토콜의 여건이 허락하는 한 컨펌 시간이 “거의 즉각적" 이며;
- 사용자들은 컨펌이 되기를 기다리지 않아도 된다;
- 또한 플래시 계층 상 이루어지는 마이크로 트랜잭션들은 더 저렴한 사용료의 혜택을 누릴 수 있다;

이러한 이점으로 인해, 우리는 자체적으로 내장된 플래시 계층 솔루션이 안전하고 저비용의 Dapp 개발 환경을 가져올 것으로 기대한다. 또한 플래시 계층 솔루션을 통하여 BOSAGORA 프로젝트의 가장 중요한 목표 중 하나인 경제적 인센티브와 정치적 인센티브의 분리를 실현할 수 있을 것이다.

요약

II 장에서는, 우리는 지분 증명 시스템에 대한 공격을 연구할 것이다.
III 장에서는, 네트워크 모델, 난수의 근거, 검증자가 효율적인 방법으로 블록에 서명할 수 있는 계획 등, 우리의 접근방법의 기초들을 소개한다.
IV 장에서는, 우리는 네트워크 참여자("검증자")가 합의 프로토콜에 참여하기 위해 특정 금액("지분")을 잠그는 합의 프로토콜을 도입하고, 네트워크에서 정확한 협력을 장려하기 위한 보상제도를 설명 한다.
V 장에서는, BOSAGORA 프로토콜의 2계층 접근방식과 1계층과의 통합을 설명한다. 이 장은 추후 개발의 진척에 따라 추가 기술될 것이다.

II. 지분 증명에 대한 공격

몇 년 동안 지분 증명에 대한 몇 가지 공격과 우려가 논의되어 왔다. 본 장에서는, 우리의 프로토콜이 직면하게 될 도전들인 공격의 기본적 정의를 검토한다.

Short & long range 공격

우리는 Short range 공격을 마지막 네트워크-수용 블록 뒤에 있는 N 블록 이하의 클라이언트에서 발생하는 공격이라고 정의하고, Long range 공격은 마지막 네트워크-수용 블록보다 뒤쳐진 N 블록 이상의 클라이언트를 대상으로 정의한다.
N은 명시적으로 선택되거나 다른 요소에서 파생될 수 있는 합의 프로토콜의 매개변수다. N에 대한 명시적 정의의 예는 Ethereum의 약한 주관적 의존(weak subjectivity)에서 찾을 수 있다 [VB14].

블록 생성과 관련된 낮은 계산 비용 때문에 과거 개인 키에 접근하는 악의적인 누군가는 관련 비용 없이 경쟁 사슬을 만들 수 있다. 그들이 통제하는 코인이 옮겨진 후에는 키가 본질적으로 가치가 없기 때문에, 검증자들은 시스템에서 투자금을 회수한 후에 개인 키를 판매하는 것이 경제적인 관점에서 가능할 것이다.

지분 그라인딩(Stake grinding) 공격

그라인딩 공격은 합의 알고리즘의 일부가 난수 인자(random factor)에 의존할 때 발생한다. 합의 프로토콜은 검증할 수 없는 데이터에 의존할 수 없기 때문에(이는 신뢰를 유도할 수 없고, 단일 실패 지점을 확장함) 임의의 난수성은 모든 참여자가 이용할 수 있는 알려진 예측 가능한 프로세스 및 데이터에 기초해야 하며, 이는 난수성에 대한 전통적인 접근법과 상충된다.
데이터를 공개적으로 사용할 수 있기 때문에, 공격자들은 그들에게 더 유리한 방식으로 영향을 미치려고 시도할 수 있다.

예를 들어, 취약한 합의 프로토콜은 다음과 같은 단계를 가진다:

- 정해진 n 검증자의 집합을 선택;
- 예측 가능한 방법으로 해당 집합을 정열 (예: 그들의 공개키 기준으로 정열);

- 매 라운드 마다, 특정 검증자를 선택하여 블록 생성을 할당;
- 선택된 검증자가 인덱스 해시(이전 블록) % n 을 정열된 집합 안에 가지고 있음;

위와 같은 접근방식에서, 검증자는 단지 다음 라운드의 검증자로 선출될 적절한 해시를 하나만 찾으면 될 것이다. 난수 오라클 모델에서 n = 100, 1000 조합은 검증자가 99.99%를 초과하여 다음 검증자가 될 기회를 제공한다.

그러한 문제를 해결하기 위해 종종 인용되는 접근법은 무조건적인 사전 커밋을 요구하는 것이다. 예를 들어, 검증자는 라운드 R 동안 해시를 커밋하고 라운드 R + 1에서 이 해시의 사전 이미지를 공개한다. 그러면 난수 값(또는 그것에 대한 시드)은 그러한 사전 이미지의 합계(또는 XOR, 또는 연결의 해시)가 될 것이다.

무 이해(Nothing at stake) 공격

지분 증명 프로토콜의 초기 설계에는 어떠한 위험 공격도 없었다.
검증자가 현재 체인의 유효한 후보인 두 개의 다른 블록을 제시하면, 가장 경제적으로 실행 가능한 행동은 체인의 "투표"가 자원을 소비하지 않기 때문에 두 블록 모두에 대해 "투표"하는 것이다[VB14]. 이것은 그러한 행동들에 대한 벌칙을 추가하는 합의 프로토콜로 이어졌다.
그러나 이러한 벌칙은 강제적인 동결 기간과 결합되지 않으면 비효율적이다. 만약 검증자들이 어떤 블록에 투표한 후 바로 그들의 지분을 이동(판매)할 수 있다면, 해당 지분을 이동시키는 것은 간단하기 때문에 쉽게 할 수 있는 행동이다. 그리고 그들이 여전히 지분을 가지고 있는 블록에서 이전에 소비했던 잔고에서 이중 지불(double spending)을 시도할 것이다.
이미 지분이 이동 되어버렸기 때문에 이와 같은 행위를 처벌할 방법은 없을 것이다. 이 때문에, 강제 동결 기간이 도입된다.

III. 기술적 제반

네트워크 모델

사용 가능한 세 가지 네트워크 모델(동기식, 비동기식, 부분적 동기식) 중 우리는 동기식 프로토콜인 SCP의 요건에 따라 동기식 모델[DLS88]을 채택했다.
합의 알고리즘 연구의 잘 알려진 결과는 어떤 프로토콜도 가용성(네트워크가 멈추지 않도록 보장), 안전성(모든 참여자가 동일한 결과에 도달하도록 보장) 및 내결함성(하나 이상의 노드가 응답하지 않을 경우 네트워크가 안전하며 멈추지 않도록 보장)을 가질 수 없다는 것이다. 이 결과는 FLP 불가능[FLP85]이라고 불리며, 가용성보다 안전성을 취하기로 선택한 SCP 논문에 중요하게 언급된다. 반면에 내결함성은 오픈 멤버십을 가진 모든 시스템이 필수적으로 가져야하는 요건이다.

난수의 근거

서명 체계와 같은 본 문서의 일부 부분은 의사 난수(pseudo-random) 데이터에 의존한다.
난수성은 본질적으로 예측할 수 없기 때문에 정확성을 검증할 수 없다. 그러므로 분산시스템의 경우 난수성을 보장하기 위해서 모든 참여자가 제공하는 시드 데이터에 의존할 필요가 있다.
결과적으로 어떤 참가자도 시드 데이터를 조작하거나 지연시킴으로써 다른 참가자에 비해 우위를 확보할 수 없도록 장치를 하는 것이 과제다.

이것은 해시와 그 사전 이미지를 시드 데이터로 사용함으로써 달성된다.

등록 시 검증자는 난수 값을 선택하고 n회 해시 처리 후 최종 값을 초기 시드 데이터로 커밋한다. 새로운 시드 데이터가 필요할 때마다 검증자는 마지막에 사용된 시드 데이터의 사전 이미지를 공개할 수 있으므로 데이터를 조작할 수 없는 진정한 난수성을 보장할 수 있다.

그러나 검증자가 스스로 네트워크로부터 데이터를 보류할 때 문제가 발생한다. 데이터를 게시하는 것이 데이터를 보류하는 것보다 더 나쁜 결과를 초래하는 경우, 노드는 네트워크를 중지하거나 결과를 왜곡하여 사전 이미지를 선택적으로 보류하도록 선택할 수 있다. 이러한 위험을 피하기 위해, 검증자는 간헐적인 중단 사태를 발생 시키지 않기 위해 충분한 시드 데이터를 정기적으로 게시해야 한다(그리고 그것을 리스닝 검증자가 지원해야 한다).

합의 프로토콜에 합리적인 간격이 도입될 경우 검증자는 사전 이미지를 미리 공표하는 것이 안전 보장의 약화 및 일시적인 다운타임이 일어하는 결과를 가져오지 않도록 보장할 수 있다.

등록 과정

검증자가 되기 위해 등록 할 경우, 노드는 다음과 같은 데이터를 게시해야한다:

- K (UTXO 키): 동결된 UTXO와 매치되는 공개키;
- X (난수 시드): 비밀키의 n번째 이미지;
- n (사이클 길이): 검증자가 참여하게 될 라운드 넘버 (현재는 다음으로 고정 (**동결 기간** / 2)];
- R (서명 노이즈): 서명을 위한 최초의 논스값 (3. 검증자 서명 구조 참고);
- S: 메세지 H(*K, X, n, R*)를 위한 서명과 R을 사용하는 키K

등록이 기록된 후 검증자는 IV 장 1에 설명된 대로 즉시 블록에 서명하기 시작할 것으로 예상된다.

다음은 등록 자격을 갖추기 위해 X에 의해 제어되는 UTXO가 충족해야 하는 요건이다:

- 최소 40,000 코인이 동결되어있어야 한다;
- 마지막 **동결 기간(freezing period)** 블록에서 디폴트가 나지 않았어야 한다;

검증자 서명 구조

검증자는 이 블록의 해시에 서명함으로써 해당 블록에 대한 보장을 한다.
서명을 효율적으로 조합할 수 있으므로, 최선의 시나리오(모든 검증자 서명)는 해당 서명이 모든 검증자의 결합 서명이 될것이며 이 경우, O(1) 공간을 차지한다.
사용되는 구조는 Schnorr 서명에 기초하며, 아래와 같다.

우리는 다음과 같은 표기법을 정의한다:

- H() 는 해시 함수이다;
- (k, K) 가 주어져 있다:
- k는 프라임 오더 P의 그룹 G에 있는 값이다;
- K는 k가 사용하는 타원곡선의 기준점 B를 지수화한 것이다;
- 쌍(k, K)은 각각 개인/공개 키 쌍에 사용된다;
- 쌍(r, R)은 고유한 랜덤 값이며 또한 그것을 지수화한 것이다;

IV. 블록체인 계층 프로토콜

사이클 & 합의 라운드

합의 프로토콜은 각 참가자가 개별적으로 수행하는 동시에 일어나는 사이클의 연속이라 할 수 있다. 참가자를 검증자(validator)라고 하고, 합의 프로토콜의 관찰자를 노드(node)라고 한다. 모든 검증자가 노드인 반면, 모든 노드가 검증자는 아니다.

각 사이클은 사이클의 시작 부분에 알려진 길이(n)를 가진다. 이 길이는 합의 라운드 단위로 표현되며, 각 합의의 결과는 새로운 블록이며, 이 블록은 주로 선택된 거래의 집합에 의해 정의된다. 각 라운드는 몇 분(테스트넷 기간 동안 여러가지 시험을 통해 결정될 것이다.) 범위내에서 유동적으로 일어날 것으로 예상된다. 라운드당 n의 값은 1씩 감소하며, 값이 0에 이르면 사이클이 끝난다.

사이클은 UTXO의 동결 여부에 따라 달라진다. 악의적인 행위자는 검증에 사용된 지분을 즉시 교환할 수 있다면 검증자로서 역할을 종료한 직후 블록을 되돌릴 강력한 동기를 부여받을 것이다. 이에 따라 검증에 사용되는 지분은 동결(freezing)되고, 최소 동결기간(**freezing period**)은 14일로 정한다.

노드가 검증자가 되고 하나의 사이클을 시작하려면 **등록 과정**을 완료해야 한다. 이는 III.3에서 정의한 범위 내에서 해당 단위에 적합한 다수의 원형 n을 선택하고 기존 검증자에게 메시지를 전파함으로써 이루어진다.

등록 과정 트랜잭션이 완료되면 해당 노드는 즉시 검증자가 되어 트랜잭션을 수집하고 전파한다. 그러나 노드가 처음 등록할 때는 아직 정족수 집합이 할당되지 않았으며, 다음 정족수 조정 이벤트가 발생할 때까지 **수동적(passive)**(반드시 50% 임계값에 도달할 때만 서명 블록)이 될 것으로 예상된다.

정족수 조정 이벤트는 1시간마다 한 번씩 일어난다. 정족수 조정 이벤트가 발생했을 때, 네트워크는 의사 난수(pseudo-random)에 의해 또한 예측 가능한 방식으로 재조직되어 보상 절차의 공정성을 확보하고, 검증자 간의 유착을 방지한다.

모든 라운드가 끝날 때마다 노드는 SCP [SCP16]에 의해 정의된 지명 프로토콜 프로세스를 시작한다. 리더는 SCP 문서에 정의된 역할에 따라 트랜잭션 집합을 선택하고 결정한다. 향후, 우리는 난수의 근거에 기초한 프로토콜로 이 지명 프로토콜을 대체하는 것을 목표로 한다.

SCP 라운드 결과는 등록된 참가자 대다수가 서명한 블록이 될것이다.

사전 이미지 유효성

등록된 검증자는 항상 자신의 사전 이미지를 다른 노드에서 적시에 사용할 수 있도록 해야 한다. 검증/정족수 조정의 일부 요건들은 사전 이미지에 따라 달라지기 때문에, 사전 이미지를 제공할 수 없는 노드(일반적으로 합의 라운드의 종료)가 필요하다. 검증자는 다음과 같은 특정 라운드의 사전 이미지와 해당 라운드 번호로 구성된 메시지를 전송함으로써 사전 이미지를 이용할 수 있다: (P, Nx) 여기서 P는 사전 이미지, Nx는 n - **(등록 이후 라운드)**.

네트워크가 사전 이미지를 놓치면 노드가 **디폴트(defaulted)**되었다고 한다. 해당 노드는 합의를 위해 재등록하지 못하며 일정 기간 동안 그들의 지분을 동결할 수 없게 된다.

지명(nomination) 프로토콜

지명이란, 다음 블록에 포함시킬 후보로 일련의 트랜잭션들을 선택하는 행위를 말한다.
네트워크상에 복수의 참가자가 서로 다른 트랜잭션 집합을 가질 수 있기 때문에, 이 행위는 종종 단일 노드에서 처리 된다.
비트코인에서는 이 노드가 채굴자다. 대부분의 합의 프로토콜들은, 트랜잭션의 집합을 결정하는 리더를 선출하는 과정이 있다. 현재 BOSAGORA는 정족수 리더 선출에 기반을 둔 SCP의 지명 프로토콜을 사용한다.
그러나, 공정한 결과를 보장하는 난수의 근거가 있으므로 일련의 트랜잭션을 보다 예측가능하고, 더 중요한 것은 검증가능하게 만들기 위한 필터를 구축 할 수 있게 해준다.

이 같은 방향은 바람직하다 판단되며 우리 프로토콜의 향후 개선 목표라 할 수 있다.

정족수 조정 이벤트

노드 간의 통신 오버헤드를 줄이기 위해 정족수를 정의한다. 정족수 배정은 본질적으로 네트워크를 더 작지만 서로 겹치게되는 네트워크로 분할하는 것이다. 이 과정에 있어서 중요한 목표는 보안성을 훼손하지 않고 통신을 최소화하는 구성을 제공하는 것이다.

정족수 조정 이벤트는 현재 설계하고 있으며 앞으로 많은 실험이 필요하다. 따라서 추후 최종적인 방안을 결정하여 제안할 것이다.

보상 배분

보상 배분은 앞서 이 백서에 기술된 구조를 따른다. 초기에는 5초당 총 27개의 코인이 발행되며, 새로운 블록이 생성되면 검증자들에게 지분에 따라 공평하게 배포된다. 앞서 기술한대로 이 보상율은 일정 기간 별로 지속적으로 감소한다.

결론

BOSAGORA팀은 다양한 암호화폐에 내재된 기술 상의 그리고 운영 상의 문제를 극복하는 것을 목표로 한다. 인센티브 제도 및 발행 계획은 권력의 중앙집중화을 억제하면서 코인의 가치를 창출하는 것을 목표로 한다. mFBA 알고리즘은 에너지 효율성이 높으면서도 빠른 트랜잭션을 가능하게 한다.
의회 시스템은 보다 민주적이고 생산적인 의사 결정 프로세스를 창출하기 위한 것이다. Trust Contract는 블록체인 위에서 계약을 생성하고 실행하는데 있어 결정가능성과 접근가능성을 가진 프레임워크를 제공할 것이다. BOSAGORA팀은 블록체인 기술을 통해 얻을 수 있는 보안성 및 무결성을 활용하면서 위와 같은 목적을 달성하는 것을 목표로 하고 있다.

Appendix 1 : Federated Byzantine Agreement 란 무엇인가

2015년 스탠포드의 보안 컴퓨터 시스템 그룹(Stanford's Secure Computer Systems Group) 총책임자인 데이비드 마지에레스(David Mazieres) 교수는 기존에 사용되고 있던 합의 프로토콜들인 PoW, pBFT 등의 대안으로 스텔라 합의 프로토콜(Stellar Consensus Protocol), 혹은 Federated Byzantine Agreement(FBA)를 제안하였다.

합의 프로토콜은 완전히 분산되고 개방되도록 하기 위해 일반적으로 다른 영역에서 포기하는 부분이 생긴다. 그러나 FBA는 기술적 우수성이 입증되었고 이는 앞으로도 그럴것으로 보인다. FBA는 Federated Byzantine Agreement의 줄임말로서 9억 달러 이상의 시가총액을 가지고 13번째로 큰 암호 통화인 Stellar가 기반기술로 사용 하고 있다.

Federated Byzantine Agreement 는 다음과 같이 정의 할 수 있다:
정족수들로 구성되는 네트워크로, 각 정족수는 합의에 도달할 수 있을 만큼 충분한 노드 집합이다. FBA는 또한 정족수 조각(quorum slice)의 개념을 도입하는데, 정족수 조각은 특정 노드를 설득할 수 있는 정족수의 하위 집합이다. 정족수를 통해 합의 과정이 이루어지며, 정족수의 집합적 합의는 비잔틴 합의 실패(byzantine failure)를 극복하기 위해 전체 네트워크의 최종 결정으로 사용된다.

FBA의 장점

FBA가 BOSAGORA 합의 프로토콜에 적합하다는 두 가지 주요 특징이 있다.

첫째, 합의된 프로토콜에 의한 트랜잭션의 컨펌이 몇 초 안에 확정된다. PoW와는 달리, 합의에 도달하기 위해 많은 컴퓨팅 능력이 필요하게 되는 채굴(mining) 과정이 없다. 이 합의는 투표 과정 내에서 자료가 서로 전달되는 동안 이루어진다. 또한 모든 노드의 데이터를 검증할 필요는 없고, 정족수의 투표 결과만 확인하면 되므로 효율적이다. 유틸리티 코인으로서, 컨펌 속도와 낮은 대기 시간은 실생활 환경에서 활용되기 위해 매우 중요하다.

둘째, 이 네트워크는 누구나 구성원으로 참여할 수 있도록 개방되어있다. FBA에는 누군가 또는 조직에 의해 선택된 검증자 목록이 없다. 오히려 각 검증자는 자신이 신뢰하는 다른 검증자를 결정하고, 신뢰할 수 있는 검증자의 목록을 **정족수 조각**이라고 한다. 각 검증자의 정족수 조각이 중복되어 거래에 대한 정족수 또는 네트워크 전체의 합의를 형성한다. FBA 네트워크의 특성 때문에, 다른 참여 검증자가 당신을 정족수 조각에 추가한다면 누구라도 검증자로서 등록시키고 합의에 참여할 수 있다.

비트코인과 마찬가지로, 우리는 검증자들이 합의에 큰 영향을 미치지 않고 네트워크에 등록하고 또한 탈퇴 하는것을 기대할 수 있다. 현재 스텔라 네트워크는 FBA를 활용한 최대 네트워크다. 스텔라 네트워크가 비트코인만큼 아직 분산되어 있지 않다는 주장이 있지만 네트워크에 점점 더 많은 노드가 추가되고 새로운 정족수 조각이 형성되기 때문에 PBFT와는 달리, 본질적으로 분산성을 증가시킬 수 있다는 점에 주목해야 한다. 따라서, 이와같은 특성은 전체 네트워크를 우리가 원하는 대로 더 분산된 네트워크로 이끌 것이다.

개방성

FBA는 대중에게 개방적인 네트워크를 추구하고 있지만 여전히 단점을 가지고 있다. 예를 들어 검증자 노드가 되려면 해당 계정의 유효성 확일을 위하여 자체적인 정족수 집합이 설정되어 있어야 합의 과정에 참여할 수 있다. 그러나 네트워크에 가입하려는 새로운 노드가 자신을 검증자로 선언하고 스스로 검증자로 선언하는 경우 자체 정족수 집합을 구성하지만 기존 검증자가 해당 노드를 정족수 집합으로 받아들이지 않으면 기존의 다른 검증자가 새 노드의 결정을 수신하지 못하게 된다. 이는 결과적으로 새로운 노드가 의사결정 과정에 참여할 수 없게 한다.

SCP(Stellar Consensus Protocol)는 누구나 노드를 운영할 수 있으며, Stellar 네트워크에 누구나 가입할 수 있다고 기술하고 있다. 그러나 이것은 절반만 옳다. 네트워크 가입은 누구에게나 열려 있지만, 네트워크에 가입하고 검증자로서 합의 과정에 참여하는 것은 제한적이다. 현재 SCP 네트워크에서 검증자로 참여하려면 기존 검증자가 새 노드를 승인해야 한다. 즉, 네트워크에 가입하고자 하는 모든 사람은 누군가의 허가가 필요하다.

Appendix 2 : Trust Contracts

초기 백서에서 Trust Contract에 대해 다음과 같이 설명하고 있다 :
"Trust Contracts란 Owlchain이라 불리는 프로토콜 레이어에 기반하여 안전하게 실행되는 계약을 말한다. Owlchain은 Web Ontology Language와 Timed Automata Language로 구성된다. Trust Contracts는 Owlchain이라 불리는 결정가능성을 가진 프로그래밍 프레임워크에 기반하여 안전한 계약을 보장하며 기존 스마트 컨트랙트의 결정불가능성(non-decidable)으로부터 발생되는 문제들을 극복한다."

이 아키텍처의 궁극적인 목표는 안전하고 정확한 실행을 보장하는 동시에 확장성을 극대화하는 데 있어 결정가능한(decideable) 계약을 구축하는 것이다.
이 목표를 달성하기 위해, 초기 백서는 두 가지 방법론을 언급한다. 하나는 가상 머신에서 유연한 프로그래밍 언어를 사용하는 것이고, 다른 하나는 그에 비해 덜 유연하지만 특정 도메인의 언어를 사용하는 것이다. 초기 계획은 후자의 방향으로 결정되어 있었다.

초기의 개발팀은 시맨틱 웹 기술을 바탕으로 추론 엔진을 연구하였으나 성과가 없었고. 또한 이 문제를 극복할 수 있는 방법이나 기술 연구의 결과가 없었다.

"온톨로지(Ontology)는 개념의 명시적 규격이다. 이 용어는 시스템적으로 존재한다는 철학적인 뜻에서 차용되었다. 온톨로지(Ontology)는 존재에 대한 체계적인 설명을 가능케 하는 철학 지식 기반 시스템, 즉 "존재한다" 라는 것을 정확하게 나타낼 수 있는 방법이다. 도메인에 대한 지식이 특정한 형태를 갖추어 표현될 때, 표현할 수 있는 대상의 집합을 논의 영역(universe of discourse)이라 한다. 대상의 집합과 그들 사이의 설명 가능한 관계는 지식 기반 프로그램이 지식을 나타내는 표현 어휘에 반영된다. 따라서, 일련의 표현 용어를 정의함으로써 프로그램의 온톨로지를 설명할 수 있다."[9]

"온톨로지는 특정 영역에서 공유할 수 있는 개념화의 공식적이고 명시적인 규격이다."

온톨로지는 오랫동안 인공지능과 자연어 처리 분야에서 연구 개발되어 왔다. 이는 컴퓨터가 관계와 정의로부터 주어진 정보를 이해할 수 있게 해준다. 이를 근거로, 컴퓨터는 결국 요청된 정보를 추론하게 될 것이다.

하지만 현실 세계에서 온톨로지를 구축하는것, 즉 세상의 사물에 대한 관계를 정립한다는 것에는 많은 노력과 시간이 필요하다. 탈중앙화된 일반 대중이 추론 엔진의 기능이 완성될 때까지 추론 엔진의 의미에 대해 작업하는 것은 어려울 뿐만 아니라, 엔진의 사용에도 한계가 있고 입력 값에 따라 결과를 검증하는 것도 어렵다. 그리고 현재 추론 엔진을 여러 상황에 쉽게 사용할 수 있는 상용화된 기술은 존재하지 않는다.

또한, OWL에서 구현된 의미론적인 소스 코드를 분석하여 Time Automata Language 기반 검증을 자동화하기는 더욱 어렵다. 소스 코드의 복잡성이 증가함에 따라 검증 대상 수가 기하급수적으로 증가하여 검증이 거의 불가능하다. OWL을 계약서 작성에 사용할 경우,

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

복잡하고 상세한 사양을 요구하게 되며, 예측 가능하고 현실적인 계약서를 작성하는 과정이 너무 어려워서 검증하기 어렵다면 이용자로 하여금 해당 기술을 사용하도록 장려할 수 없다.

BOSAGORA 팀은 최초의 의도대로 안전하고 정확한 프로그래밍이 가능하며 실행할 수 있는 계약을 가능하게 하는 Trust Contract의 개발을 목표로 한다.

실현 불가능한 것을 계속하기보다는 'Trust Contract'를 재정의하고, 최적의 방향의 선정과 핵심 기능 개발을 위해 적절한 기술 적용을 적극적으로 추진하겠다. 또한 가상 머신 위에 유연한 프로그래밍 언어를 사용하는 방법론을 채택하는 것을 고려하고 있으며, 우리는 현재 다른 업계 경쟁사들과 같이 WebAssembly를 연구하고 있다. 결국, 우리는 효율적이고 안전하게 설계된 Smart contract 엔진을 제공하고 개발자들이 쉽게 채택할 수 있도록 많은 도구와 인기 있는 개발하기 쉬운 언어를 제공할 생각이다.

WebAssembly는 최신 웹 브라우저에서 실행할 수 있는 새로운 종류의 코드다. 이는 상당한 성능 이점을 제공한다. "WebAssembly는 스택 기반 가상 머신의 이진 명령 형식이다. WebAssembly는 C/C++/Rust와 같은 고도의 언어를 컴파일하기 위한 휴대용 타겟으로 설계되어 있어 클라이언트 및 서버 애플리케이션을 웹상에 배포 가능하게 한다."

웹 상에서 복수의 언어로 작성되는 프로그램을 클라이언트 애플리케이션을 사용하여 거의 네이티브에 가까운 속도로 실행하는 것은 이전에는 불가능했다. WebAssembly에서 코드를 실행하는 것은 실제 하드웨어와 유사하다. WebAssembly를 통해 개발자들은 C++, 러스트 등 다양한 프로그래밍 언어로 코딩할 수 있으며, 네이티브와 가까운 성능으로 프로그램을 실행할 수 있을 것으로 기대할 수 있다. 또한 EOS, Ethereum, Tron, Cardano와 같은 많은 블록체인 플랫폼 또한 WebAssembly를 사용하여 가상 머신을 도입하거나 도입할 계획을 가지고 있다.

도입 계획의 타당성을 연구하여 해결책이 발견되면, 본 백서에 제시된 "Trust Contract"의 목적과 방향을 완성하기 위한 기술적, 실용적 조치를 취할 것이다.

Appendix 3 : 코인 발행 일정

	블록생성 보상	발행량	공공예산	전체 발행량
초기	0	450,000,000	0	450,000,000
Year 1	170,294,400	620,294,400	315,360,000	935,654,400
Year 2	159,548,823	779,843,223	315,360,000	1,410,563,223
Year 3	149,481,293	929,324,516	315,360,000	1,875,404,516
Year 4	140,049,023	1,069,373,539	315,360,000	2,330,813,539
Year 5	131,211,930	1,200,585,469	315,360,000	2,777,385,469
Year 6	122,932,457	1,323,517,926	223,200,000	3,123,517,926
Year 7	115,175,419	1,438,693,345		3,238,693,345
Year 8	107,907,850	1,546,601,195		3,346,601,195
Year 9	101,098,865	1,647,700,060		3,447,700,060
Year 10	94,719,526	1,742,419,586		3,542,419,586
Year 11	88,742,724	1,831,162,310		3,631,162,310
Year 12	83,143,058	1,914,305,368		3,714,305,368
Year 13	77,896,731	1,992,202,099		3,792,202,099
Year 14	72,981,448	2,065,183,547		3,865,183,547
Year 15	68,376,318	2,133,559,865		3,933,559,865
Year 16	64,061,773	2,197,621,638		3,997,621,638
Year 17	60,019,475	2,257,641,113		4,057,641,113
Year 18	56,232,246	2,313,873,359		4,113,873,359
Year 19	52,683,991	2,366,557,350		4,166,557,350
Year 20	49,359,631	2,415,916,981		4,215,916,981
Year 21	46,245,039	2,462,162,020		4,262,162,020
Year 22	43,326,977	2,505,488,997		4,305,488,997
Year 23	40,593,044	2,546,082,041		4,346,082,041
Year 24	38,031,623	2,584,113,664		4,384,113,664
Year 25	35,631,828	2,619,745,492		4,419,745,492
Year 26	33,383,460	2,653,128,952		4,453,128,952
Year 27	31,276,963	2,684,405,915		4,484,405,915
Year 28	29,303,387	2,713,709,302		4,513,709,302
Year 29	27,454,343	2,741,163,645		4,541,163,645
Year 30	25,721,974	2,766,885,619		4,566,885,619
Year 31	24,098,918	2,790,984,537		4,590,984,537
Year 32	22,578,276	2,813,562,813		4,613,562,813

Year 33	21,153,587	2,834,716,400		4,634,716,400
Year 34	19,818,795	2,854,535,195		4,654,535,195
Year 35	18,568,229	2,873,103,424		4,673,103,424
Year 36	17,396,574	2,890,499,998		4,690,499,998
Year 37	16,298,850	2,906,798,848		4,706,798,848
Year 38	15,270,393	2,922,069,241		4,722,069,241
Year 39	14,306,831	2,936,376,072		4,736,376,072
Year 40	13,404,070	2,949,780,142		4,749,780,142
Year 41	12,558,273	2,962,338,415		4,762,338,415
Year 42	11,765,846	2,974,104,261		4,774,104,261
Year 43	11,023,421	2,985,127,682		4,785,127,682
Year 44	10,327,843	2,995,455,525		4,795,455,525
Year 45	9,676,156	3,005,131,681		4,805,131,681
Year 46	9,065,591	3,014,197,272		4,814,197,272
Year 47	8,493,552	3,022,690,824		4,822,690,824
Year 48	7,957,609	3,030,648,433		4,830,648,433
Year 49	7,455,484	3,038,103,917		4,838,103,917
Year 50	6,985,043	3,045,088,960		4,845,088,960
Year 51	6,544,287	3,051,633,247		4,851,633,247
Year 52	6,131,342	3,057,764,589		4,857,764,589
Year 53	5,744,454	3,063,509,043		4,863,509,043
Year 54	5,381,979	3,068,891,022		4,868,891,022
Year 55	5,042,376	3,073,933,398		4,873,933,398
Year 56	4,724,203	3,078,657,601		4,878,657,601
Year 57	4,426,105	3,083,083,706		4,883,083,706
Year 58	4,146,818	3,087,230,524		4,887,230,524
Year 59	3,885,154	3,091,115,678		4,891,115,678
Year 60	3,640,001	3,094,755,679		4,894,755,679
Year 61	3,410,317	3,098,165,996		4,898,165,996
Year 62	3,195,126	3,101,361,122		4,901,361,122
Year 63	2,993,513	3,104,354,635		4,904,354,635
Year 64	2,804,623	3,107,159,258		4,907,159,258
Year 65	2,627,651	3,109,786,909		4,909,786,909
Year 66	2,461,846	3,112,248,755		4,912,248,755
Year 67	2,306,504	3,114,555,259		4,914,555,259
Year 68	2,160,963	3,116,716,222		4,916,716,222
Year 69	2,024,606	3,118,740,828		4,918,740,828

Year 70	1,896,854	3,120,637,682		4,920,637,682
Year 71	1,777,162	3,122,414,844		4,922,414,844
Year 72	1,665,023	3,124,079,867		4,924,079,867
Year 73	1,559,960	3,125,639,827		4,925,639,827
Year 74	1,461,527	3,127,101,354		4,927,101,354
Year 75	1,369,305	3,128,470,659		4,928,470,659
Year 76	1,282,901	3,129,753,560		4,929,753,560
Year 77	1,201,950	3,130,955,510		4,930,955,510
Year 78	1,126,107	3,132,081,617		4,932,081,617
Year 79	1,055,050	3,133,136,667		4,933,136,667
Year 80	988,476	3,134,125,143		4,934,125,143
Year 81	926,103	3,135,051,246		4,935,051,246
Year 82	867,666	3,135,918,912		4,935,918,912
Year 83	812,917	3,136,731,829		4,936,731,829
Year 84	761,622	3,137,493,451		4,937,493,451
Year 85	713,563	3,138,207,014		4,938,207,014
Year 86	668,537	3,138,875,551		4,938,875,551
Year 87	626,353	3,139,501,904		4,939,501,904
Year 88	586,830	3,140,088,734		4,940,088,734
Year 89	549,801	3,140,638,535		4,940,638,535
Year 90	515,108	3,141,153,643		4,941,153,643
Year 91	482,605	3,141,636,248		4,941,636,248
Year 92	452,153	3,142,088,401		4,942,088,401
Year 93	423,622	3,142,512,023		4,942,512,023
Year 94	396,891	3,142,908,914		4,942,908,914
Year 95	371,847	3,143,280,761		4,943,280,761
Year 96	348,384	3,143,629,145		4,943,629,145
Year 97	326,401	3,143,955,546		4,943,955,546
Year 98	305,805	3,144,261,351		4,944,261,351
Year 99	286,509	3,144,547,860		4,944,547,860
Year 100	268,430	3,144,816,290		4,944,816,290
Year 101	251,492	3,145,067,782		4,945,067,782
Year 102	235,623	3,145,303,405		4,945,303,405
Year 103	220,755	3,145,524,160		4,945,524,160
Year 104	206,825	3,145,730,985		4,945,730,985
Year 105	193,775	3,145,924,760		4,945,924,760
Year 106	181,548	3,146,106,308		4,946,106,308

Year 107	170,092	3,146,276,400		4,946,276,400
Year 108	159,359	3,146,435,759		4,946,435,759
Year 109	149,304	3,146,585,063		4,946,585,063
Year 110	139,883	3,146,724,946		4,946,724,946
Year 111	131,056	3,146,856,002		4,946,856,002
Year 112	122,786	3,146,978,788		4,946,978,788
Year 113	115,038	3,147,093,826		4,947,093,826
Year 114	107,780	3,147,201,606		4,947,201,606
Year 115	100,979	3,147,302,585		4,947,302,585
Year 116	94,607	3,147,397,192		4,947,397,192
Year 117	88,637	3,147,485,829		4,947,485,829
Year 118	83,044	3,147,568,873		4,947,568,873
Year 119	77,804	3,147,646,677		4,947,646,677
Year 120	72,895	3,147,719,572		4,947,719,572
Year 121	68,295	3,147,787,867		4,947,787,867
Year 122	63,986	3,147,851,853		4,947,851,853
Year 123	59,948	3,147,911,801		4,947,911,801
Year 124	56,165	3,147,967,966		4,947,967,966
Year 125	52,621	3,148,020,587		4,948,020,587
Year 126	49,301	3,148,069,888		4,948,069,888
Year 127	46,190	3,148,116,078		4,948,116,078
Year 128	43,275	3,148,159,353		4,948,159,353

Reference

The BOSAGORA White Paper, https://bosagora.io/

WebAssembly, https://webassembly.org/

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

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

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

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

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

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

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

Golem, https://golem.network

Hodges, Andrew, Alan Turing: the enigma, London: Burnett Books

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

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

N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on Ethereum smart 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

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. Retrieved March 18, 2018 from https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74

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

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

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

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

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

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

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

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

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

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

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

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

Dmytro Kaidalov, Andrii Nastenko, Oleksiy Shevtsov, Mariia Rodinko, Lyudmila Kovalchuk, Roman Oliynykov (2016) A Review of the Dash governance system
https://api.zotero.org/groups/478201/items/BJUUEE9Q/file/view?key=Qcjdk4erSuUZ8jvAah59Asef

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

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

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

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

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

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

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

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

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

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