BOSagora 백서

Nov.2022

목차

핵심 내용 요약

BOSagora 플랫폼은 탈중앙화되고 스스로 진화하는 퍼블릭 블록체인 네트워크로서, 스마트 컨트랙트와 블록체인 내의 의사결정 시스템인 의회 네트워크에 기반한다.

(1) 스마트 컨트랙트는 프로토콜 레이어상에서 안전하게 실행되는 계약이다. 우리는 효율적이면서도 안전하게 설계된 스마트 컨트랙트 엔진을 제공한다. 그리고, 개발자들이 쉽게 채택할 수 있도록 다양한 툴과와 대중성을 갖춘, 개발이 쉬운 프로그래밍 언어를 제공한다.

(2) 의회 네트워크는 분산형 조직에서 발생하는 거버넌스 문제를 해결하는 BOSagora 플랫폼의 의사결정 기관이다. 우리는 명확하게 정의되고 자동화된 거버넌스 시스템을 통해서 커뮤니티와 응용 소프트웨어를 발전시켜서, 어떤 환경에서도 성장할 수 있는 생태계를 만드는 것을 목표로 한다. 의회 네트워크는 “한 검증자 당 하나의 투표”라는 원칙을 따른다. 즉, 그 원칙은 DAO를 활성화시키게 되는데, 모든 검증자가 동등한 권리를 가지며 투표 권한의 이양이나 대의원 선출과 같은 방식를 거부하는 DAO의 사상을 반영한 것이다.

(3) 공공 예산은 BOA 화폐 자산으로서, 블록이 생성될 때마다 생성되며 트랙잭션들에 대한 수수료의 30%가 적립된다. 이것에 대한 사용은 의회 네트워크 상에서 제안과 표결을 통해서 진행된다.

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, 최고 1.2조 달러 이상의 시가총액을 기록한 바 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 스마트 컨트랙트를 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.

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

---

[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

비전

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 우리의 실생활을 풍요롭게 한다.

핵심 가치

진취적 사고

미래 개척: 우리는 누구나 속도와 신뢰를 경험할 수 있는 혁신적인 기술 개발로 최초의 완전한 풀-노드 지분 증명 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 달성하는 놀라운 결과를 이끌어 내었다. 그 결과는 초기 백서가 추구하는 다양한 기술 및 생태계 청사진에 의해 달성되었다. 하지만 지난 몇년간 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 위해 보다 독점적인 지위를 얻을 수 있는 새로운 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 준수해야 하는 목표에 초점을 맞추지만, 동시에 정책, 기술, 방법론의 변화를 반영하여 수정해야 한다.

따라서, 우리는 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 탈중앙화된 어플리케이션들(Dapps: Decentralized applications) 및 비즈니스 파트너를 지원하는 메인넷 플랫폼으로서의 기능은 그대로 유지되어야 한다.

BOSagora 플랫폼의 뚜렷한 특징은 모든 검증자가 의사결정 과정에 참여하기 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.

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 검증자들이 제안을 작성하고 투표에 참여할 수 있는 의회 네트워크라고 하는 거버넌스 시스템을 구성했다. 검증자는 투표 권한을 갖는다.

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 뒷 부분에서 설명하도록 한다.

합의 알고리즘

개요

합의 알고리즘은 모든 탈중앙 블록체인의 핵심이다. 합의 알고리즘은 다음과 같은 질문에 답하려고 노력한다. “모든 분산 데이터베이스가 동일한 정보 집합을 보유하고 있다는 것을 어떻게 증명할 수 있을까?”

원래 BOSagora는 이 질문에 관련해, SCP(Stellar Consensus Protocol)에서 제공되는 FBA를 수정한 mFBA(Modified Federated Byzantine Agreement) 알고리즘을 이용하여 블록체인을 개발했다. 그 알고리즘은, 검증자가 40,000 BOA를 동결하게 하면서 PoS(Proof of Stake)를 적용하는 방식으로 수정된 알고리즘이다.

그러나, 테스트 과정에서, SCP의 한계로 인해 많은 수의 검증자를 지원하기 위해서는 오랜 시간과 대규모 인적자원이 소요된다는 사실을 알게 되었다. 많은 수의 검증자는 진정으로 탈중앙화된 블록체인에서 필수적인 요구사항이다. 보다 효율적으로 다수의 검증자 지원을 가능케 하는 mFBA의 대체 방안이 절실히 필요하다.

또한 현재 가동중인 퍼블릭 블록체인 플랫폼들과 경쟁을 하기 위해서는 네트워크 사용 사례를 빠르게 만들어 가야 한다. 이를 위해서는 블록체인 알고리즘 및 기술요소들의 범용성이 필수적이다.

결론적으로, 심화되는 경쟁상황 아래 보스아고라 네트워크가 블록체인으로써 생존하기 위해서는 서둘러 범용성 높은 네트워크를 론칭하는 것이 지상 과제이다. 이러한 이유로 우리는 방향을 전환하여, 수많은 검증자를 지원할 수 있고, 기존에 많은 개발자 및 유저에게 활성화된 사용사례를 가지고 있는 검증된 합의 알고리즘을 사용하기로 하였다.

우리가 채택한 것은 Gasper 알고리즘이다. 그 알고리즘은 확실히 자리를 잡은 검증된 PoS 합의 알고리즘이며, 2020년 12월 1일부터 이더리움 비콘체인에서 사용되고 있다.

Gasper

BOSagora는 현재 Gasper 알고리즘을 사용한다. Gasper는 “Casper the Friendly Finality Gadget (Casper-FFG)”와 LMD GHOST 포크 선택 알고리즘을 조합한 알고리즘이다. 검증자는 지정된 BOA를 예치하고 검증자 클라이언트를 운영하는 노드이다. Gasper는 검증자가 블록을 제안하고 검증하는 과정에서 어떠한 방식으로 참여했는지를 확인하고 보상과 패널티 부과에 대해서 판단하는 알고리즘이다. 그리고, Gasper는 하나 이상의 블록체인 포크가 있을 때, 어떤 포크를 선택하여 블록을 만들지도 규정한다.

Gasper에 대한 자세한 내용은 Gasper and Combining GHOST and Casper 사이트에 확인할 수 있다.

Casper FFG

Gasper는 PBFT (Practical Byzantine Fault Tolerance)에 영향을 받은 Buterin과 Griffith에 의해서 Casper the friendly finality gadget 논문에서 소개되었다. 그 논문은 타당성(justification)과 완결성(finalization)에 개념을 정의한다.

블록에 대한 타당성은 동결된 코인을 가진 검증자의 2/3가 검증했을 때 확보된다. 하나의 검증된 블록은 다음으로 검증된 블록이 체인에 추가될때 완결된 것으로 간주한다. 타당성과 완결성은 모든 블록(블록은 종종 슬롯(Slot)으로 해석됨)에 대해서 일어나는 것이 아니라 에폭(Epoch) 경계에 있는 체크포인트(Checkpoint) 블록에 대해서만 확인된다. 가끔 지정된 검증자가 오프라인이 되거나 제 시간에 제안된 블록을 완결해서 체인에 추가시키지 못하는 경우가 있기 때문에 각 에폭는 32개까지의 슬롯을 가진다.

특정한 블록은 완결된 상태로 만들어서, 다른 참여자들이 부분적인 정보만 가지고도 블록들이 정격체인(Canonical chain)의 일부라고 확실할 수 있다.

LMD GHOST

검증자들이 어떤 블록들을 검증하고, 그 블록들을 보증한다는 포크 선택 규칙이다. 검증자가 충돌이 일어나는 블록을 검증하는 것과 같은 방법으로 프로토콜을 무력하려는 시도를 막기 위해서, 그런 문제 행동에 대해서 패널티를 도입한다.

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

Fig 1. 암호화폐 비교

BOSagora의 DAO, 의회(Congress) 네트워크

개요

의회 네트워크는 BOSagora의 민주적 의사결정 기관으로서, 각각의 풀-노드의 검증자들로 구성된다. 의회 네트워크는 탈중앙화 자율조직(DAO)이므로, 써드 파티나 중앙단체의 규정에 통제받지 않고 운영된다. 의회 네트워크는 소프트웨어와 생태계를 지속적으로 향상시키기 위해 다양한 프로젝트 이해관계자들 간의 효과적이고 포괄적인 협업을 가능하게 한다. 예를 들어, 시스템 업그레이드나 공공예산의 사용은 의회 네트워크의 제안, 평가, 투표의 과정을 통해서 이루어질 수 있다.

노드를 운영하며 4만 BOA를 예치하면 검증자 권한이 부여된다. BOSagora의 모든 검증자는 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. 예치한 BOA 코인의 수에 따라 노드 내에 복수의 검증자를 등록할 수 있다. 4만 BOA 예치 시 마다 1검증자 등록권한이 부여된다. 의회 네트워크는 1검증자 당 1투표 규칙을 준수한다. 즉, 의회 네트워크는 모든 검증자가 투표권 이양이나 대리자 선거와 같은 경우 없이 동등한 권한을 갖고 투표하는 DAO를 추구한다.

필요성

블록체인은 잠재적인 사용자의 요구사항을 만족시켜야 한다. 그러나, 그것들이 아무리 면밀하게 설계된다고 해도 기술의 방향, 사람, 시장은 끊임없이 변하기 때문에 결과물은 지속적으로 그런 변화를 수용해야 한다. 언제 어떻게 BOSagora 네트워크를 바꿀 것인가를 결정하는 것은 지속성과 성장에 매우 중요하다.

이러한 과정에서, 합의 상에 있는 모든 이해당사자의 이익과 관점에 대해서 소통하는 것은 힘들고 긴 과정일 수 있고, 그 결과 탈중앙화가 핵심힌 블록체인 프로젝트에 중앙화된 거버넌스 시스템을 낳는 결과를 초래할 수 있다.

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

집단 의사결정의 문제점

나쁜 의사 결정은 여러가지 이유에 의해서 발생할 수 있다. 불완전한 정보, 역학관계, 인지 편향, 사회적 압력은 조직이나 커뮤니티가 잘못된 결정을 내리게 하는 원인이 되고, 그런 결정은 좋은 솔루션을 만들어내지 못한다.

- 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.
- 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

특히, 온라인 의사결정 과정은 중재 시스템이 없을 경우에 비효율적인 과정이 될 수 있다.

의회 네트워크의 개요

우리는 검증자 간의 숙의와 투표 시스템에 기반한 탈중앙화된 집단 의사결정을 제안한다. 이는 BOSagora 의회 네트워크라 칭한다.

의회 네트워크의 기능

의회 네트워크는 다음과 같은 기능을 수행하는 플랫폼이 될 것이다.

- 의회 구성원들 사이의 활발한 의견 공유와 소통
- BOSagora 네트워크에 구현하고자 하는 제안들에 대한 의사결정

의회 네트워크는 두가지 주제에 대해서 결정을 내린다.

- **BOSagora 플랫폼의 변경을 위한 “시스템 업그레이드 제안”**

  이것은 네트워크에 기술적인 기능의 변경이나 개선 등을 포함한다. 의회 네트워크의 결정에 따라 재단 개발팀의 개발 방향이 정해진다.

- **공공예산의 사용을 위한 “공공예산 기금 지원 제안”**

  의회 네트워크는 공공 예산에 기금을 요청하는 제안을 할 수 있고 제안된 계획이 승인되면 이를 집행할 수 있다. 이 결정은 DAO를 통해서 내려지고, 작은 조직의 이익만을 대변하는 제안은 다수결 투표에 의해서 거부될 수 있다. 즉, BOSagora와 커뮤니티 전체에 이익을 주는 제안이어야 승인 가능성이 높아진다.

의회 네트워크의 특징

BOSagora는 집단 의사결정의 문제점을 극복하고 보다 포용적이고 효율적인 의사결정을 가능케 할 것이다. 이를 달성하기 위해서, 온라인 의사결정 툴인 “보테라”를 구현할 것이다.

보테라는 의사결정 데이터를 블록에 저장함으로써 투명성을 보장하고, 책임소재를 명확히 할 것이다. 기밀성을 유지하기 위하여 투표 기간 동안에는 데이터 검증을 위한 투표 데이터의 해시를 블록에 저장할 것이다. 투표 기간이 종료되면 투표 데이터가 블록에 기록될 것이고, 기록되어 있는 해시를 통해 데이터가 검증될 것이다. 논의, 사전 평가에 대한 정보는 별도 서버에 저장될 것이고, 그 정보는 참여자가 언제든지 볼 수 있도록 제공될 것이다.

의회 네트워크 활동의 절차

① 의회 네트워크 가입

누구나 다음 조건을 이행하면 의회 구성원이 될 수 있다:

- 최소 40,000 BOA 예치
- 안정적인 네트워크 속도에서 검증자 노드 운영(서버나 개인 컴퓨터에서 운영됨)

또한, 아래와 같은 경우에는 의회 네트워크 자격이 상실된다.

- 지속적인 네트워크 안정성 위해 행위에 대한 페널티로 지분이 삭감되어 예치 잔고가 20,000 BOA 이하로 떨어지는 경우
- 제안과 투표 과정에서 부적절하다고 판단되는 행위를 할 경우. 자세한 사항은 아래 “보상구조/슬래싱(Slashing)” 섹션 참조

② 제안 만들기

의회 구성원 누구라도 제안을 만들어 의사 결정 과정을 시작할 수 있다. 의회 구성원은 만들어진 제안에 대하여 다음의 3가지 유형의 참여가 가능하다.

- 논의 : 제안에 대한 의견을 공유하고 아이디어를 발전시킨다.
- 평가 : 공공예산 기금 지원 제안의 경우, 제안의 적합도를 평가하여, 정식 제안으로 받아들일지 여부를 결정한다. 시스템 업그레이드 제안의 경우, 평가하기 단계는 생략된다.
- 투표 : 제안에 대해 찬성, 반대, 기권의 의사 표시를 할 수 있다.

③ 제안 정보 입력

제안 생성자는 다른 의회 구성원들이 이해하고 참여할 수 있도록 필요한 정보를 입력해야 한다. 어뷰징을 방지하기 위하여 제안 등록 시 정책에 따른 소정의 수수료를 납부하여야 하며, 납부하여야 할 수수료는 제안의 유형, 요청 금액 입력 시 자동으로 계산되어 제시된다. 제안을 생성하기 위하여 입력이 필요한 정보는 다음과 같다.

- 제안의 유형
- 제안의 타이틀
- 사전 검토 기간 (공공예산 기금 지원 제안의 경우)
- 투표 기간
- 요청 금액 (공공예산 기금 지원 제안의 경우)
- 사업목표 및 설명
- 관련 첨부 자료

제안의 완성도를 높이고 어뷰징을 방지하기 위해 제안자는 제안을 생성할 때 수수료를 입금하여야 한다. 제안 수수료는 공공예산 기금 지원 제안 시에는 요청 금액의 0.1%, 시스템 업그레이드 제안 시에는 100BOA이다. 제안 수수료는 환불되지 않는다.

④ 논의
의회 구성원은 의견이나 논평을 낼 수 있다. 좋은 의견은 추천을 받을 수 있고, 의견을 최신순이나 추천순으로 정리해 볼 수 있다. 의견은 제목 이외의 수정이 가능하나, 수정의 기록은 다른 참여자들이 모두 볼 수 있고, 삭제가 불가능하다. 의회 구성원은 의견에 대해 댓글을 달 수 있지만 댓글은 삭제 불가하다.

⑤ 투표
투표는 합의를 이루기 위해서 생성된다. 개별 투표는 검증자들이 직접 블록체인에 저장한다.

⑥ 투표의 검토
각 투표의 날짜와 시간을 저장하고, 만약 같은 검증자로부터의 투표가 중복될 경우, 마지막 투표만 최종 결과로 간주되어 1검증자-1투표의 정책을 보장한다.

⑦ 정족수 확인
정족수는 어떤 제안이 플랫폼상에서 실행되기 위해서, 투표에 참여해야 하는 의회 네트워크 구성원의 최소 수이다. 초기에 의결 정족수는 전체 멤버의 3분의 1로 정해지지만 평균 참여율을 반형해 추후에 조정될 수 있다.

⑧ 제안의 승인
투표 참여자의 찬성표 순백분율이 반대표 순백분율을 10%를 초과하면 제안이 승인된다.

⑨ 제안 실행하기
제안이 승인되면 실행에 옮겨진다. 만약 시스템 업그레이드에 대한 제안이 승인된다면 개발팀은 제안에 따라서 개발을 시작한다. 개발팀은 개발 계획, 로드맵, 보안 테스트 등의 작업을 수행하게 된다. 시스템 업그레이드에 대한 제안이라 하더라도 개발의 상세 내용을 개발, 구현하는 데 비용이 필요하다면 제안은 공공예산 지출 계획의 형태를 취해야 한다. 공공예산에 대한 제안이 승인되면, 제안자는 공공예산을 직접 인출할 수 있다.

⑩ 검토/감사
제안의 실행후에 의회 네트워크와 재단은 적절한 과업이 제안의 로드맵에 따라서 실행되었는지를 검토한다. 공공예산과 관련한 제안의 경우, 그 검토나 감사에 관련된 비용은 제안자가 지불한 수수료로 충당한다.

네트워크 상호작용

트랜잭션

사용자가 트랜잭션을 요청하면 의회 네트워크로 전송된다. 간단히 BOA 전송에 대해서 이야기하자면, 노드가 블록을 확정하면 사용자의 트랜잭션이 승인되고 BOA가 다른 지갑으로 전송된다. 만약 트랜잭션이 보다 복잡한 스마트 컨트랙트에 기반한 것이라면, 사전에 정의된 논리와 절차가 실행될 것이다. 각 트랜잭션에 대해서 트랜잭션 수수료가 발생하고 수수료는 의회 네트워크의 투표를 통해서 조정된다. 거래 수수료는 검증자에게 경제적 인센티브로 작용하고 또한 DoS 공격에 대한 방어 메커니즘으로도 작용한다.

제안서

제안서란 의회 네트워크에 제출되는 공공예산 사용 계획 또는 시스템 변경 계획을 의미한다. 의회 네트워크의 모든 구성원은 자유롭게 제안을 만들 수 있다. 제안이 이루어지고 제안서가 통과되기 위해서는 반드시 찬성 및 반대 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 예치(Coin Staking)

코인 예치는 PoS 합의 알고리즘에서 예치금으로 사용할 코인을 동결하는 과정이다. 노드를 실행하고 검증자로서 인센티브를 받기 위해서는, 운영자는 정해진 양의 코인을 예치해야 한다. 예치된 코인은 노드가 블록체인을 조작하려는 경우를 대비해 담보물로서 사용된다. 다시 말해, 노드가 블록체인을 조작하려고 하면, 그 노드는 예치 계좌에서 벌금을 지불하게 된다. 네트워크 스스로가 지분삭감(Slashing) 대상이 될 노드를 발견하고 처벌할 수 있도록 하기 위해서, 내부 고발자와 블록 제안자들은 보상을 받는다.

보상 구조

의회 구성원은 블록생성 보상, 거래 수수료의 두가지 방법으로 BOA 보상을 받을 수 있다. 블록생성 보상은 새롭게 생성되는 코인인 반면에 거래수수료는 기존에 발행된 코인으로서 트랜잭션 발신자의 계좌에서 인출된다.

블록생성 보상(Confirmation Reward)

에포크(epoch)는 32개 슬롯(Slot)으로 구성되어 있고, 매 에포크에는 임의로 선택된 검증자 그룹인 위원회(Committee)가 배정된다. 각 슬롯마다 블록의 내용을 구성하고 제안할 책임이 있는 검증자(Proposer, 제안자) 하나가 정해진다. 만약 이 검증자가 오프라인 상태이거나 블록 제안을 지연하면, 해당 슬롯은 놓친 슬롯으로 표시되고 검증자는 할당된 보상을 받지 못한다.

선택된 위원회는 Casper FFG에 대한 조상, 자손 체크포인트와 LMD-GHOST에 대한 체인 헤드 블록을 위한 투표를 하는 검증의 책임을 갖는다. 증명은 정확해야 하고 적절한 시간에 전체 보상을 받게 된다. 제안자와 위원회가 작업을 충실히 수행하면 매 에포크마다 정해진 량의 보상을 받게된다. 이 고정된 양은 첫 해에 매 5초당 7 BOA 코인씩 계산되고 이후부터는 매년 1.347%씩 감소된다.

제안자와 위원회는 임의로 선택되기 때문에 모든 검증자가 매 블록마다 보상을 받는 것은 아니고 제안자와 위원회에 속한 검증자가 주어진 작업을 완수하면 보상을 받게 된다.

슬래싱(Slashing)

슬래싱은 다음의 프로토콜 위반 사항에 대해서 발생한다.

① 악의적인 블록 제안자(Proposer)가 같은 슬롯 높이에 다른 블록을 제안하는 경우

② 증명자(Attester)가 자손 체크포인트에 대해서 서로 다른 조상 체크포인트에 대해서 투표하는 경우

③ 증명자가 다른 투표상에 존재하는 조상, 자손 체크포인트 관계를 감싸는 또 다른 투표를 하는 경우

슬래싱을 당하면 그 검증자는 즉시 검증자 풀에서 즉시 탈락된다.

거래 수수료(Transaction Fee)

거래 수수료는 유연하게 조정된다. 의회 검증자들은 블록당 총거래 수수료의 70%를 받고, 30%는 공공예산으로 보낸다. 거래 수수료는 의회를 통해 조정될 수 있다.

공공 예산

공공예산은 생태계의 발전을 목적으로 하는 다양한 영역에서 사용될 수 있다. 예를 들어, BOA 코인 환매, 바운티와 마케팅 캠페인, BOSagora 생태계에 진입하는 프로젝트나 서비스에 대한 초기 자금 지원 등등에 사용될 수 있다.

공공예산은 초기 약 5년간 총 18억BOA가 생성되고, 블록이 생성될 때마다 트랜잭션 수수료의 30%가 지속적으로 적립된다. 그것에 대한 사용은 의회 네트워크에서의 제안과 투표에 의해서 승인된다. 제안이 의회 네트워크에서 승인이 되면, 공공 예산의 스마트 컨트랙트를 통해서 제안의 세부 사항에 맞게 자동적으로 전달된다.

토큰 배분 및 발행

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, 유통량은 542,130,130.19558463 BOS 였다.

- 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:

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 재단이 의도한 바가 아니기에 소각되었다.
- 50,000,000 개의 토큰 또한 소각되었다. 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 보관하고 있으며 이는 거래소 상장 혹은 파트너쉽을 위해 사용하고 있다.
- 82,404,968.6942793 개의 토큰은 유보되어있다.

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

Category			Number of BOA	Share
Initial supply	Airdrop		247,595,031	5.09 %
	Unclaimed	Burn	92,130,130	
		Marketing	30,000,000	0.61 %
		Remain	82,404,969	1.66 %
	Original Distribution	Foundation	40,000,000	0.81 %
		Team Members	40,000,000	0.81 %
		Bounty	10,000,000	0.20 %
	Initial supply total		542,130,130	
	1st Token Burn	BCOS PF	-42,130,130	
		Additional Token	-50,000,000	
	1st Token Burn Total		-92,130,130	
	Initial circulating supply total		**450,000,000**	
Additional supply	Confirmation Rewards		2,700,000,000	54.54 %
	Commons Budget		1,800,000,000	36.36 %
Total			**4,950,000,000**	**100 %**

Fig 2. 보아토큰 배분 및 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 검증자의 필수 작업을 올바르게 수행한 검증자에게 지급되는 금전적 보상이다. 만약 검증자가 온전하게 작업을 수행하지 못하면 할당된 BOA는 패널티의 형태로서 회수되어 공공예산의 계좌로 보내지면서 전체 발행량은 정해진대로 유지된다. 27억 BOA가 블록생성 보상으로 발행된다. 처음에는 5초당 7 개의 BOA가 발행된다. 보상은 약 1년씩 128년 동안 1.347%씩 감소한다.

- **공공 예산**

  공공예산은 의회 네트워크를 통과한 제안서에 지급할 BOA를 보유하고 있는 계좌다. 제안을 위한 충분한 예산을 만들기 위해 5초당 50개의 공공예산용 코인을 발행하여, 결과적으로 약 5년간 총 18억개의 코인을 발행한다. 또한, 트렌젝션 수수료의 30%도 공공예산에 적립된다.

메인넷이 출시된 이후, 블록생성 보상과 공공예산이 생성될 것이다. 전체 토큰 발행 차트는 이 문서의 마지막에 첨부되어있다.

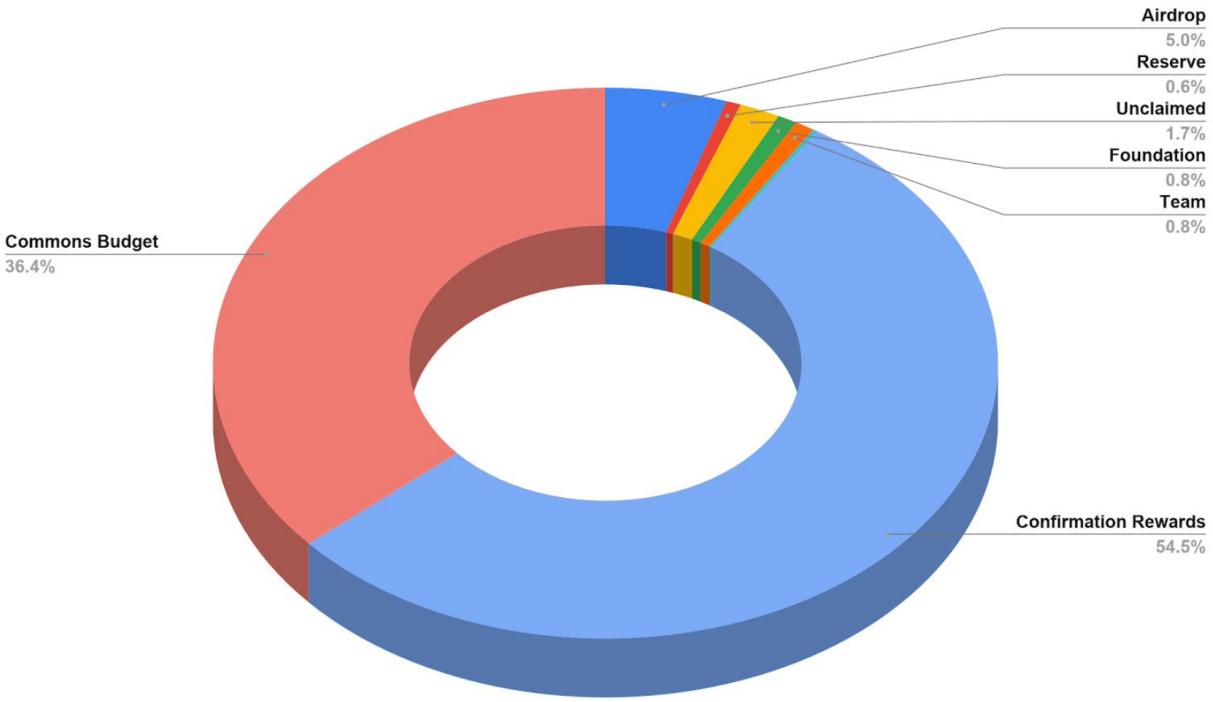

Fig 3: 보아코인 발행 계획

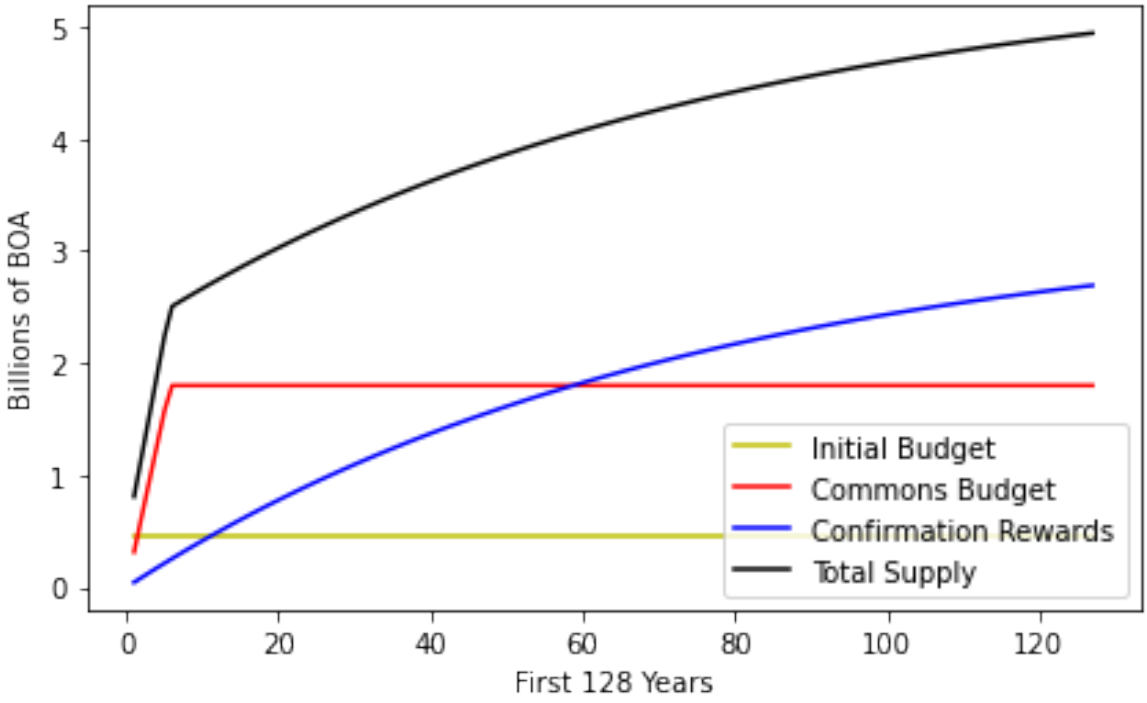

Fig 4: 누적 보아코인 발행 계획

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. Gasper 지분증명 알고리즘은 에너지 효율성이 높으면서도 빠른 트랜잭션을 가능하게 한다. 의회 시스템은 보다 민주적이고 생산적인 의사 결정 프로세스를 창출하기 위한 것이다. 스마트 컨트랙트는 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: 블록생성보상 및 공공예산 계획 수정

1. 서론

현재 우리는 보스아고라의 메인넷의 출시를 앞두고 있습니다. 발행계획이 작성된 것은 약 5년전이고 현재의 상황과 많이 다릅니다. 우리는 보아생태계의 지속적인 성장을 위해서 발행계획을 수정하고 보완하는 것에 대한 필요성을 인식하게 되었습니다. 우리는 여기에서 기존의 **블록생성보상 발행계획에 대한 문제점**을 확인하고 그것을 해결할 수 있는 **적절한 발행계획과 정책**을 제시하겠습니다. 또한 **공공예산의 안전한 사용 정책**도 제안하겠습니다.

2. 기존의 발행계획

보아 코인은 블록생성보상과 공공예산으로 추가 발행됩니다. 블록생성보상에 대한 발행계획은 5초당 27개의 BOA 가 발행되며 약 1년씩 128년 동안 6.31% 씩 감소합니다. 128년 동안 총 2,700,000,000 BOA가 발행됩니다.
공공예산의 발행계획은 5초당 50개의 BOA 가 발행되며 5년동안 총 1,800,000,000 BOA 가 발행됩니다.
두 가지 발행계획에 대한 보아 재단의 정책을 좀 더 자세히 알아 보겠습니다.

3. 블록생성보상의 발행 계획

3.1. 블록생성보상의 기존 발행계획

먼저 블록생성보상의 년간 발행량과 그 해의 년간 이자율(APR)을 계산하면 [표 1] 과 같습니다.

첫 해 5초당 발행량 (BOA)	27
1년간 감소율 (%)	6.31

년	5초당 발행량	1년 발행량	발행량 누적	검증자의 수에 따른 년간이자율(APR) (%, 소수점 이하 절사)			
				1,000	2,000	5,000	10,000
1	27.00	170,294,400	170,294,400	426	213	85	43
2	25.30	159,548,823	329,843,223	399	199	80	40
3	23.70	149,481,293	479,324,516	374	187	75	37
4	22.20	140,049,023	619,373,539	350	175	70	35
5	20.80	131,211,930	750,585,469	328	164	66	33
6	19.49	122,932,457	873,517,926	307	154	61	31
7	18.26	115,175,419	988,693,345	288	144	58	29
8	17.11	107,907,850	1,096,601,194	270	135	54	27
9	16.03	101,098,865	1,197,700,059	253	126	51	25
10	15.02	94,719,526	1,292,419,585	237	118	47	24

[표 1] 기존 블록생성보상 계획과 검증자의 수에 따른 이자율(APR)

향후 10년 동안의 년간 이자율(APR)을 먼저 계산해 보겠습니다. 년간 이자율은 검증에 참여한 검증자의 수에 따라서 달라집니다. 년간 발행되는 코인의 수는 정해져 있고 그것을 검증자가 나누어 가지기 때문입니다. 검증자의 수가 많아지면 년간이자율은 줄어들게 됩니다. 즉, 년간이자율에 영향을 주는 것은 블록생성보상과 검증자의 수입니다.
예치 금액이 40,000 BOA이고, 네트워크에 1,000개의 검증자가 가동중 일 때 년간 이자율이 426%입니다. 그리고 2,000개의 검증자가 가동중 일 때 년간 이자율은 213%입니다.
이 값은 [표 2] 에서 제공되는 주요 다른 플랫폼들의 년간이자율에 비해서 아주 높은 값입니다.

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

정보제공 - https://www.stakingrewards.com

[표 2] 주요 플랫폼들의 년간 이자율

3.2. 블록생성보상의 수정된 발행 계획

블록생성보상이 높을 경우 검증자로 참여하고자 하는 강한 동기부여가 됩니다. 그러나 블록생성보상이 과도하게 높을 경우 코인 가치가 심각하게 훼손되는 등의 인플레이션 효과가 발생하게 됩니다. 재단은 검증자 참여를 위한 충분한 동기부여가 되면서도 너무 과하지 않은 적정한 인플레이션율을 찾기 위해 [표 4]와 같이 다양한 시뮬레이션을 진행해 왔습니다. 그리고 블록생성보상이 5초당 7개의 BOA가 발행되며 약 1년씩 128년 동안 1.347% 씩 감소하도록 수정했을 때 인플레이션과 리워드가 적절하게 유지되어 네트워크가 지속적으로 성장할 수 있을 것이라는 판단을 하게 되었습니다.

[표 3] 에서 10,000개의 검증자가 가동되면 APR이 10%를 유지하는 것을 볼 수 있습니다. 또한 초기 1,000개 의 검증자의 경우는 상당히 높은 값인 110% 입니다. 이것은 많은 검증자들의 참여를 유도하기에 충분한 값입니다.

따라서 우리가 선택할 수 있는 가장 적절한 블록생성보상에 대한 발행계획은 다음과 같습니다.

5초당 7 개의 BOA 가 발행되며 약 1년씩 128년 동안 1.347% 씩 감소합니다.
블록생성보상에 대한 총 발행량은 약 2,700,000,000 BOA 입니다

메인넷 론칭시에는 재단이 블록생성보상율을 결정해 적용하지만, 의결권이 있는 의회가 구성된 이후에는 의회가 스스로 제안과 투표를 통하여 블록생성보상율을 조정할 수 있습니다.

5초당 발행량 (BOA)	7
1년간 감소율 (%)	1.347

년	5초당 발행량	1년 발행량	발행량 누적	전체 검증자의 수에 따른 년간이자율(APR) (%, 소수점 이하 절사)			
				1,000	2,000	5,000	10,000
1	7.00	44,150,400	44,150,400	110	55	22	11
2	6.91	43,555,694	87,706,094	109	54	22	11
3	6.81	42,968,999	130,675,093	107	54	21	11
4	6.72	42,390,206	173,065,300	106	53	21	11
5	6.63	41,819,210	214,884,510	105	52	21	10
6	6.54	41,255,906	256,140,416	103	52	21	10
7	6.45	40,700,189	296,840,604	102	51	20	10
8	6.37	40,151,957	336,992,561	100	50	20	10
9	6.28	39,611,110	376,603,671	99	50	20	10
10	6.20	39,077,549	415,681,220	98	49	20	10

[표 3] 적정 블록생성보상 계획과 검증자의 수에 따른 이자율(APR)

3.3. 초기의 높은 인플레이션에 대한 대응책

초기 발행량은 450,000,000 BOA 입니다. [표 3] 에서 보는 바와 같이 수정된 발행계획에서도 매년 초기 발행량과 비슷한 량이 신규로 발행되는 높은 인플레이션이 유지되고 있습니다. 따라서 재단에서는 재단이 보유하고 있는 40,000,000개의 BOA코인을 이용하여 1,000개의 검증자로서 참여하고 여기서 발생하는 블록생성보상을 소각할 계획입니다.
만약 2,000개의 검증자가 가동되고, 이중 1,000개의 검증자가 재단소유의 BOA로 가동될 경우 연간 최대 약 22,000,000개의 BOA코인이 소각될 것입니다. 이 정책으로 인해 초기의 과도한 인플레이션을 방지할 수 있을 것입니다.

4. 공공예산의 사용계획

공공예산은 블록생성보상에 비해서 단기간 발행되지만 그 발행량이 크기 때문에 많은 분들이 과도한 인플레이션을 우려하고 있습니다. 그러나 공공예산은 생태계의 발전을 목적으로 하는 다양한 영역에서 사용될 계획입니다. 예를 들어, BOA 코인 환매, 바운티, 마케팅 캠페인, BOSagora 생태계에 진입하는 프로젝트나 서비스에 대한 초기 자금 지원 등등에 사용될 수 있습니다. 그리고 공공예산은 의회 네트워크에서의 제안과 투표에 의해서 승인이 되어야만 사용이 가능합니다. 따라서 공공예산은 발행량보다 제안과 투표를 통해 적절한 곳에 사용될 수 있도록 의회구성원들이 적극적으로 참여하여 제안을 검토하고 투표하는 것이 더 중요합니다.

이러한 이유로 재단은 공공예산이 좀 더 신중하게 사용될 수 있도록 하기 위해서 의회구성원의 수가 2,000이 되기 전까지는 공공예산의 사용을 보류하도록 할 계획입니다. 이 사용계획을 통해 공공예산이 보다 많은 의회구성원의 적극적 참여와 세심한 검토를 거친 후 반드시 필요한 사업에 투자될 수 있도록 할 것입니다.

5. 결론

재단은 과도하게 높게 계획된 블록생성보상율을 적절하게 수정하고 재단소유의 BOA 코인을 이용하여 발생된 블록생성보상을 소각함으로써 인플레이션을 억제할 계획을 가지고 있습니다.
또한 재단은 공공예산이 많은 의회구성원의 검토와 논의를 거쳐 사용될 수 있도록 의회구성원의 수가 2,000이 되기전까지는 공공예산의 사용을 보류하도록 할 예정입니다.

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

[표 4] 블록생성 보상 발행량 및 검증자 수에 따른 연간 이자율 시뮬레이션

Appendix 2: 수수료

가스 수수료

네트워크를 안정된 상태로 유지하기 위하여, 실행된 연산에 대한 수수료인 가스 수수료는 연산을 착수한 계정에게 주어진다. 즉, 대량의 트랜잭션으로 시스템에 부하를 주는 행위는 많은 비용을 발생시킨다. 그리고, 할당된 가스가 결국에는 모두 소모되기 때문에, 스마트 컨트랙트가 무한 루프나 연산 능력을 낭비하는 것을 방지할 수 있다.

기본 수수료(Base Fee)

가스당 최소 비용은 고정되지 않고, 네트워크의 부하에 상태에 의해서 시간에 따라서 변경될 수 있다. 기본 수수료는 공공예산 계좌로 보내진다.

팁(Tip)

블록 제안자가 트랜잭션을 블록에 포함시키도록 인센티브를 주기 위해서 단위 가스당 팁을 추가할 수 있다. 전체 수수료에 이 부분은 검증자에게 주어진다. 검증자는 블록을 생성하면서, 블록 제안자로서 어떤 트랜잭션을 포함할지를 결정한다.

전체 수수료

수수료 = 가스 개수 x (기본 수수료 + 팁)

결제 트랜잭션

코인을 한 계좌에서 다른 계좌로 전송하는 트랜잭션의 경우, 21,000개의 가스가 수수료로 지불된다. 이런 수수료는 전송하는 측의 계좌에서 빠져나가게 된다.
예를 들어, Bob이 Alice에게 100 BOA를 지불하는데, 기본 수수료가 90 Gwei이고 10 Gwei의 팁이 추가된다면, Bob의 계좌에서는 다음의 계산에서 보여지는 만큼의 Gwei가 감소된다:
100_000_000_000 + (21_000 * (90 + 10))
= 100_000_000_000 + 2_100_000
= 100_002_100_000 Gwei
= 100.0021 BOA
그리고, Alice의 계좌는 100 BOA 만큼 증가된다.

스마트 컨트랙트

트랜잭션이 스마트 컨트랙트에 대한 호출을 포함한다면, 연산을 위해서 사용되는 가스가 트랜잭션 소유자에게 부과된다. BOSagora 블록체인은 확고하게 정착된 EVM(Ethereum Virtual Machine)을 사용하여 스마트 컨트랙트를 실행한다. 이더리움 옐로우 페이퍼의 부록 G 부분에서 다양한 연산들에 대한 가스 소모량에 대한 상세한 내용을 확인할 수 있다.

Appendix 3: 코인 발행 일정

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

68		17,796,086.55	4,224,315,273.37	99		11,688,094.15	4,671,658,832.60
69		17,556,373.27	4,241,871,646.64	100		11,530,655.52	4,683,189,488.12
70		17,319,888.92	4,259,191,535.56	101		11,375,337.59	4,694,564,825.72
71		17,086,590.02	4,276,278,125.58	102		11,222,111.80	4,705,786,937.51
72		16,856,433.65	4,293,134,559.23	103		11,070,949.95	4,716,857,887.47
73		16,629,377.49	4,309,763,936.71	104		10,921,824.26	4,727,779,711.72
74		16,405,379.77	4,326,169,316.49	105		10,774,707.28	4,738,554,419.01
75		16,184,399.31	4,342,353,715.79	106		10,629,571.98	4,749,183,990.98
76		15,966,395.45	4,358,320,111.24	107		10,486,391.64	4,759,670,382.62
77		15,751,328.10	4,374,071,439.34	108		10,345,139.95	4,770,015,522.57
78		15,539,157.71	4,389,610,597.05	109		10,205,790.91	4,780,221,313.48
79		15,329,845.26	4,404,940,442.31	110		10,068,318.91	4,790,289,632.39
80		15,123,352.24	4,420,063,794.55	111		9,932,698.65	4,800,222,331.04
81		14,919,640.69	4,434,983,435.24	112		9,798,905.20	4,810,021,236.24
82		14,718,673.13	4,449,702,108.37	113		9,666,913.95	4,819,688,150.19
83		14,520,412.60	4,464,222,520.97	114		9,536,700.62	4,829,224,850.80
84		14,324,822.64	4,478,547,343.61	115		9,408,241.26	4,838,633,092.06
85		14,131,867.28	4,492,679,210.89	116		9,281,512.25	4,847,914,604.31
86		13,941,511.03	4,506,620,721.92	117		9,156,490.28	4,857,071,094.59
87		13,753,718.88	4,520,374,440.80	118		9,033,152.36	4,866,104,246.95
88		13,568,456.28	4,533,942,897.08	119		8,911,475.79	4,875,015,722.74
89		13,385,689.18	4,547,328,586.26	120		8,791,438.21	4,883,807,160.96
90		13,205,383.94	4,560,533,970.20	121		8,673,017.54	4,892,480,178.50
91		13,027,507.42	4,573,561,477.62	122		8,556,192.00	4,901,036,370.50
92		12,852,026.90	4,586,413,504.52	123		8,440,940.09	4,909,477,310.58
93		12,678,910.09	4,599,092,414.61	124		8,327,240.63	4,917,804,551.21
94		12,508,125.18	4,611,600,539.79	125		8,215,072.70	4,926,019,623.91
95		12,339,640.73	4,623,940,180.52	126		8,104,415.67	4,934,124,039.57
96		12,173,425.77	4,636,113,606.28	127		7,995,249.19	4,942,119,288.76
97		12,009,449.72	4,648,123,056.01	128		7,887,553.18	4,950,006,841.94
98		11,847,682.44	4,659,970,738.44				

Reference

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

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

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

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

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

Golem, https://golem.network
Hodges, Andrew, Alan Turing: the enigma, London: Burnett Books

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

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

N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on Ethereum smart contract, https://eprint.iacr.org/2016/1007.pdf

Using Decentralized Governance: Proposals, Voting, and Budgets, https://wiki.terracoin.io/view/Using_Decentralized_Governance:_Proposals;_Voting;_and_Budgets
Vitalik Buterin, Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper

De Filippi, P. & Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3). Retrieved March 18, 2018 from https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

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

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

Duncan L. (2017) Thoughts on Governance and Network Effects. https://medium.com/aragondec/thoughts-on-governance-and-network-effects-f40fda3e3f98

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

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

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

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

Zyskind, Nathan, Pentlend (2016) Decentralizing Privacy: Using Blockchain to Protect Personal Data. https://enigma.co/ZNP15.pdf

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

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

Çetinkaya O., Doganaksoy A. (2007) A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, Availability Reliability and Security 2007. http://ieeexplore.ieee.org/document/4159833/

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

Bingsheng Zhang, Roman Oliynykov, Hamed Balogun (2017) A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence https://www.lancaster.ac.uk/staff/zhangb2/treasury.pdf

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

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

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

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

[NXT19] NXT Contributors. https://nxtwiki.org/wiki/Whitepaper:Nxt#Nxt.E2.80.99s_Proof_of_Stake_Model

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

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

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