The BOScoin White Paper

Initial Version: 20161101 / Current Version: 20170407

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

BOScoin, 스스로 진화하는 암호화폐 플랫폼

요약. BOScoin 플랫폼은 Trust Contracts와 Congress Network라고 불리는 의사결정 시스템 위에서 작동하며, 스스로 진화하는 탈중앙형 암호화폐다. (1) 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. (2) Congress Network는 분산형 조직에서 발생하는 거버넌스 문제를 해결하고, 시스템이 보다 탄탄한 에코시스템으로 계속 진화하도록 돕는 BOScoin 플랫폼의 의사결정 기관이다.

1. 도입

a. 배경

블록체인은 2008년 Satoshi Nakamoto의 논문 “Bitcoin: A Peer-to-Peer Electronic Cash System”에서 처음 개념화되었으며 다음 해에 Bitcoin의 핵심 기술로 구현되었다[1]. 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 10억 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[2]. 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.

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."[3]

[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

이며 블록체인에 Smart Contracts를 제공하는 것을 목표로 한다 :

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. 우리는 튜링-완전 언어는 본질적으로 결정 불가능하기 때문에 smart contracts 작성에 사용하는 것은 부적합하다고 생각한다[5]. 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 내재되어 있는 문제들은 어쩔 수 없이 일련의 보안 취약점[6]을 만들고 The DAO[7]와 같은 실패한 프로젝트들을 야기했다.

b. 제안

Trust Contracts. 이 문제에 대한 BOScoin의 접근 방식은 일반 사용자가 쉽게 읽을 수 있고 또한 구현된 smart contract가 계산적으로 결정가능한지 수학적으로 증명할 수 있는 도메인 특화 언어(domain-specific language)를 적용하는 것이다. 그래서 우리는 BOScoin을 통해 Trust Contracts-Owlchain 기술에 기반하여 안전하게 실행되는 계약-를 위한 플랫폼을 개발하는 것을 목표로 한다 :

추가적으로 BOScoin을 통해 우리는 암호화폐와 관련해 공통적으로 반복되는 문제들을 해결하려고 한다.

의사결정. 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. BOScoin은 지속적으로 소프트웨어와 전체 생태계를 개선하기 위해서, 의회 네트워크를 구성하는 노드운영자들이 proposal을 작성하고 투표에 참여할 수 있는 Congress Network라고 하는 거버넌스 시스템을 구성했다. 시스템 변경 제안서는 Congress Network에서의 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 Congress Network의 투표에서 통과되면 Commons Budget(공공 예산)을 사용할 수 있다.

---

[4] *Golem*, https://golem.network
[5] Hodges, Andrew*, Alan Turing: the enigma,* London: Burnett Books, p. 111
[6] N. Atzei, M. Bartoletti, T. Cimoli, *A survey of attacks on Ethereum smart contracts*, https://eprint.iacr.org/2016/1007.pdf
[7] *The DAO*, https://slock.it/dao.html

BOScoin은 이러한 제안들을 통해서 전체 보스코인 생태계의 개발을 위해 쓰일 수 있는 상당한 양의 공공 예산을 설정해 두었다.

중앙집중화 방지 합의 알고리즘. PoW유형의 합의 프로토콜만을 사용하는 Bitcoin과 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. BOScoin은 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 예치금 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.

어플리케이션 생태계. 많은 경우에 탈중앙형 화폐는 제한된 실사용처로 인해 투기의 온상이 되는 경향이 있다. 우리는 화폐 가치란 본질적으로 화폐가 얼마나 유용하게 쓰여지고 있는가 하는 사실과 연동되어 있다고 생각하기 때문에, BOScoin팀은 BOScoin을 사용하는 두 가지 어플리케이션을 출시할 예정이다. 이미 개발된 Stardaq 및 Delicracy 어플리케이션은 코인의 거래 가치를 높이는 것은 물론 새로운 사용자를 확보하는데도 도움이 될 것이다.

Features	Bitcoin	Ethereum	BOScoin
Coins	Bitcoin	Ether	BOScoin
Core Features	Financial Transactions (Bitcoin script)	Smart Contracts (Solidity, Serpent, etc)	Trust Contracts (OWL 2 profiles, SDLang, TAL)
Decision Making Process	Non-systematic	Non-systematic	Democratic Congress (One node = One vote)
Consensus Algorithm	Proof of work	Current: Proof of work. Future: Casper(?)	Modified FBA(Federated Byzantine Agreement)
Transaction Speed	7 tx/sec	25 tx/sec	1,000 tx/sec (target)
Block Interval	10 minutes	13 seconds	5 seconds
Block Size	1 MB	Dynamic	Dynamic

Fig 1. 암호화폐 비교

2. Trust Contracts

a. 개요

BOScoin은 Web Ontology Language (OWL)[8]과 Timed Automata Language (TAL)로 구성된 Owlchain 기술을 사용하고자 한다. 이 아키텍처는 표현력을 확장하면서도 계약의 안전하고 정확한 실행을 지원할 수 있는 결정가능성을 유지하도록 설계되어 있다. 보스코인 블록체인 위에 만들어진 OWLchain에 기반한 계약을 Trust Contracts라고 한다.

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

Fig 2. 블록체인 기반 contracts 비교

b. 배경

블록체인에서 계약을 개발하는 데는 두 가지 기본 접근 방식이 있다. 하나는 가상머신 위에서 유연한 프로그래밍 언어를 사용하는 것이고, 다른 하나는 다소 덜 유연하지만 결정가능성을 가진 도메인 특화 언어(domain-specific language)를 사용하는 것이다. BOScoin팀은 두번째 방법을 선택했다. 가상머신에 기반을 둔 암호화폐와 달리, 추론 엔진은 시맨틱 웹 기술에 기반하므로 코드가 실행되기 전에 코드로부터 정보를 추론할 수 있다. 계약은 결정가능성을 가지고 있고, 계약의 결과는 분명히 확인된다. 이는 계약 기능을 가진, 안전하고 지속 가능한 통화를 구축하는 데 있어 핵심적인 개념이다. Ethereum은 시장 매커니즘을 사용하여 이 문제를 해결하려고 복잡성에 가격을 적용했지만, 우리는 더 엄격한 OWL 및 TAL 방식의 접근이 블록체인 기반의 계약을 개발하는데 있어서 보다 안전한 환경을 제공 할 것이라고 믿는다.

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

c. 개발

웹 페이지를 제공하는데 사용되는 HTML, HTTP, RDF 및 OWL과 같은 표준 웹 기술을 기반으로 개발할 때, 이 기술들은 컴퓨터가 예측 가능하게 해석할 수 있는 방식으로 정보를 공유하도록 확장될 수 있다. OWL과 RDF 모두 모호하지 않은, 구조화된 데이터 분류체계를 작성하는데 사용될 수 있다. Ian Grigg는 이러한 특성을 이용하여 지불 시스템의 모든 것과 연관된 계약인 Ricardian Contracts 개념을 제안했다[9]. OWL과 RDF가 비슷한 특성을 나타내지만, 현재 RDF 표준은 P-time 완전성을 지원하지 않는다. 그러나 이전에 제시된 사실 또는 공리의 집합에서 논리적인 결과를 추론하는 도구인 Reasoners를 사용하여 OWL 표준은 P-TIME 복잡성을 보장한다. 이것은 계약을 실행하는데 걸리는 시간을 사전에 결정할 수 있다는 것을 의미한다. 이 특성이 OWL을 Trust Contracts의 기반 언어로 선택하게 된 핵심 이유이다.

OWL DL(description logic)은 OWL의 하위 언어로, "계산의 완전성을 유지보유하면서도 가능한 최대 표현력을 제공하도록 설계되었다."[9] OWL DL은 ISO20022 사양과 같이 사전 정의된 방대한 어휘 및 분류체계 사전 위에서 작동한다. 거래와 같이 보스코인에 특화된 기능은 OWL 사전에서 제공되지 않기 때문에, 이와 관련된 어휘 및 분류체계는 계약 외부에서 호출해야 한다. 이러한 기술적인 문제를 해결하기 위해, 블록체인 위에 사전 정의된 네임 스페이스 도메인을 생성하는 방법을 제안한다. 이 네임스페이스 도메인은 계약에서 비표준 기본 타입(분류체계)을 호출 할 수 있다. OWL의 결정가능성 및 분류학적 복잡성 기능을 유지하기 위해 비표준 기본 타입이 신중하게 추가될 것이다.

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

Fig 3. BOScoin 전송 예제

블록체인에 대한 튜링-완전 계약의 또 다른 문제는 튜링-완전 언어는 비전문가들이 읽기 어렵다는 것이다. '코드가 법'이라면 코드는 관련된 모든 당사자가 이해할 수 있어야 한다. 현재 계약용 튜링-완전 언어를 사용하는 통화는 코드를 읽을 수 있는 사람만 검사할 수 있다. 보스코인은 OWL 표준을 사용하고 SDLang[10]과 같은 언어에 문법을 매핑함으로써, 누구나 계약 내용을 읽고 그 계약이 의미하는 바를 정확하게 이해할 수 있게 하려고 한다.

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

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

        Proposal-description {

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

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

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

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

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

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

Fig 4. Trust Contract 예제

Timed Automata Language 개념은 Andrychowicz의 논문인 'Timed Automata에 의한 Bitcoin Contracts 모델링'[11]을 기반으로 한다. TAL은 Trust Contract에서 사용되는 프로그래밍 로직을 모델링하는 데 사용된다. OWL 및 TAL의 관계는 HTML과 Javascript의 궁합과 유사하다. OWL은 데이터 구조를 제공하고 TAL은 연산자처럼 작동한다. 프로그래밍 언어의 연산자는 더하기, 빼기 및 비교와 같은 특정 기능을 수행하는 구문이다. OWL은 정보를 제공하고 TAL은 컴퓨터에 데이터 처리 방법을 알려준다. TAL은 전역 시간 요소(global time factor)가 있기 때문에 다른 프로그래밍 언어와 약간 다르다. 즉,

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

계약을 실행하는 데 걸리는 시간을 사전에 테스트 할 수 있다. 가능한 모든 각각의 결과에 대해 사전에 자동화된 테스트를 실행함으로써 블록체인에서 버그 없는 계약을 구축할 수 있는 플랫폼을 제공할 수 있다.

위의 개념에 대한 자세한 내용은 기술 보고서에서 자세히 설명한다.

3. 합의 알고리즘

a. 개요

컨센서스 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.

BOScoin은 이 질문과 관련해, Stellar의 합의 프로토콜(FBA)[12]을 기반으로 한 수정된 FBA(mFBA) 합의 알고리즘을 사용하기로 했다.

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

Fig 5. 합의 알고리즘 비교

Mazieres는 FBA 프로토콜의 핵심 기능을 다음과 같이 정의한다[13].

- 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 몇

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

초) 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.
- 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.

b. Federate Byzantine Agreement 합의 알고리즘[14]

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.

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

FBA 외에도 BOScoin 합의 프로토콜은 거버넌스 시스템의 유지 관리를 위해 지분 증명의 특성을 적용했다. 사용자는 한 노드 내에 10,000개 단위로 BOScoins을 예치 할 수 있으며, 유동성을 억제하는 역할을 하는 댓가로 노드에 예치된 코인의 총 수에 비례하여 새로 발행된 BOScoin(예치금에 대한 이자와 유사함)을 받는다. 노드에 예치된 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 예치된 코인이 모두 Commons Budget 계정으로 몰수된다.

4. 의회(Congress) 네트워크

a. 개요

Congress 네트워크는 BOScoin의 민주적 의사결정 기관으로서, 각각의 풀노드 운영자들로 구성된다.

[14] Ibid.

사람들은 암호화폐가 탈중앙되고 자동화된 것이라고 말하지만 대부분의 경우 사실이 아니다. 코드와 블록체인에 저장된 정보 둘 다 영향을 받기 쉽게 되어 있다. 이러한 문제들을 극복하기 위해, BOScoin은 시스템을 완전히 탈중앙화하고 자동화하기 위한 Congress Network라는 의사결정 기구를 제안한다. 소스 코드 개발, 포크 및 마케팅 리소스는 시스템으로부터 충당될 수 있다.

b. 의회 네트워크의 역할

i. 의회 구성원

다음 기준을 충족하면 Congress member로 간주된다.

● 안정적인 네트워크 속도로 완전히 동기화된 노드(풀 노드) 운영

● 4 unit 이상의 예치 (하나의 예치 단위는 10,000 BOS)

● 투표에 참여

누구든지 Congress 구성원이 될 수 있다. 노드는 Congress 구성원이 운영하는 서버 또는 개인용 컴퓨터 일 수 있다. 네트워크 속도가 안정적이기만 하다면, 노드는 가정 또는 원격 서버에 배치될 수 있다.

Congress members는 그들의 정치적 영향력을 위해 더 많은 노드를 운영하는 것을 선택하거나 혹은 BOScoin 예치금을 늘림으로써 경제적 이익을 증가시키는 방향으로 투자하는 것을 선택할 수 있다.

ii. Users

사용자는 BOScoin 시스템의 수혜자이다. 그들은 거래를 시작하고, 제안서를 제출하고 BOScoins에 대한 이자(보스코인 예치에 대한 보상)를 얻는 세 가지 방법으로 BOScoin Network와 상호 작용할 것이다. 이러한 상호 작용은 아래 그림에 표시되어 있다.

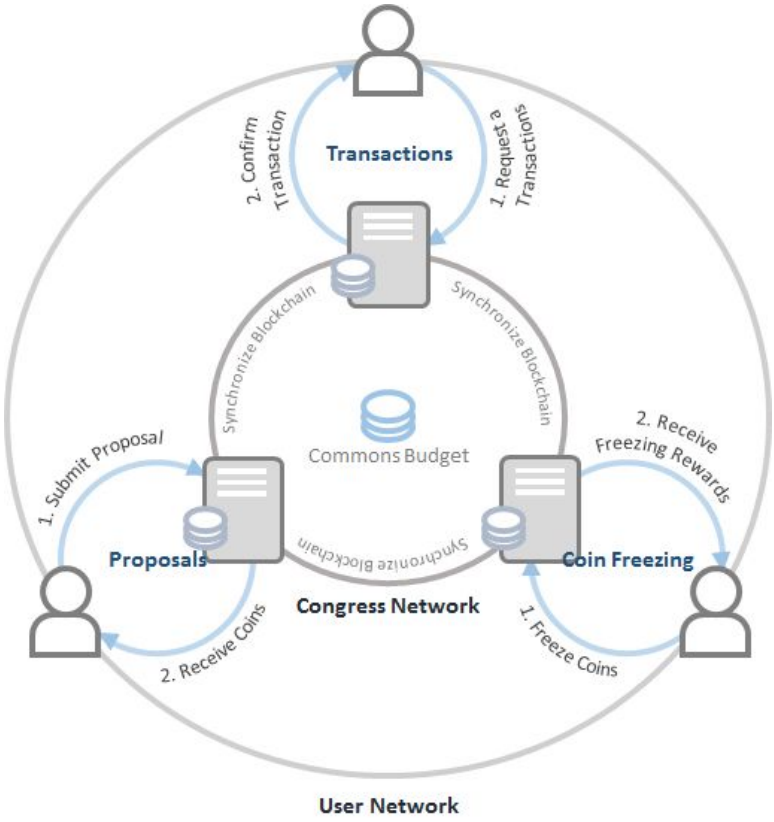

Fig 6. Congress Network와 사용자 Network 간의 상호 작용

c. 네트워크 상호작용

i. 거래

사용자가 트랜잭션을 요청하면 해당 요청은 Congress 네트워크로 전송된다. 간단한 BOScoin 전송에 대해서 이야기하자면, 노드가 (대략 5초마다) 블록을 확정하면 사용자의 트랜잭션이 승인되고 BOScoin이 다른 지갑으로 전송된다. 보다 복잡한 Trust Contracts라면 사전에 정의된 논리 및 절차가 실행될 것이다. BOScoin의 초기 단계에서 거래 수수료는 0.01 BOS로 고정되지만, 이 요금은 Congress 네트워크에서 투표를 통해 조정할 수 있다. 거래 수수료는 노드 운영자에게 경제적 인센티브로 작용하고 또한 DoS 공격에 대한 방어 메커니즘으로도 작용한다.

ii. 제안서

제안서란 Congress 네트워크에 제출되는 Commons Budget 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.

iii. 코인 예치(Freezing)

코인 예치는 PoS의 개념으로, 사용자가 코인을 예치하면 그 대가로 그들은 예치된 코인의 수와 코인이 예치된 시간에 비례하여 이자를 받는다. 이 이자를 예치 보상금이라고 한다. 사용자는 10,000 BOS 단위의 코인을 한 유닛으로 예치할 수 있다. 예치된 코인은 블록체인 위조 시도 시 담보로 사용된다. 노드가 블록체인을 위조하려고 시도하면 예치된 코인의 일부가 몰수되어 Commons Budget 계정으로 보내진다. 또한 코인 가격 안정을 촉진하기 위한 메커니즘으로, 코인 예치를 취소하려면 2주 전에 사전 통보해야 한다.

d. 보상 시스템

Congress Network에는 독특한 인센티브 메커니즘이 있다. Congress members는 하나의 노드에 보스코인을 예치하여 경제적 보상을 극대화하거나, 여러 노드 (1 노드는 1표와 동일)를 실행하여 투표 권한을 늘려 투표권을 극대화 할 수 있다.

이러한 의도적 구분은 경제 권력과 정치 권력의 분리와 유사한 개념으로써, 의사결정에 참여하고픈 동기와 경제적 동기를 구분하도록 장려한다.

Bitcoin은 PoW 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.

Congress 구성원이 BOScoin 보상을 받는 세 가지 방법이 있다. 예치 보상금, 블록생성 보상금, 거래 수수료.

- **예치보상금(Freezing Reward) :** Congress 멤버는 코인을 동결하면 (코인을 동결한) 일반 지갑 사용자와 동일하게 이자를 받는다. 첫해부터 총 5,400개의 BOScoins이 각각의 예치된 유닛에 균등하게 분배되고 이 freezing reward는720 블록 (약 1시간마다)마다 발행된다. 분배되는 총 금액은 59년 동안 매년 5.00%씩 감소한다.

- **블록생성 보상금(Confirmation Reward) :** 블록이 확정되면 블록생성 보상금이 해당 노드에 제공된다. 이 보상은 노드 운영자들에게 제공하는 핵심적인 인센티브다. 그리고 이 보상은 노드에 예치된 유닛 수에 비례하여 제공된다. Bitcoin의 블록 보상과 마찬가지로 참여 노드 수가 증가하면 블록생성 보상을 받을 확률이 줄어든다. 프리징 리워드는 노드에 저장된 금액에 비례한다. 리워드는 블록당 평균 18 보스코인으로 시작한다.

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

  처음의 블록 컨펌 리워드는 한 블록 당 18 BOS에서 시작하며 대략 128년 동안 전년 대비 6.31%씩 감소한다.

- **Transaction Fee:** 거래 수수료는 0.01 BOScoin으로 고정된다. Congress Nodes는

블록당 총거래 수수료의 70%를 받고, 30%는 Commons Budget으로 보낸다. 거래 수수료는 Congress를 통해 조정할 수 있다.

e. 의사결정 구조

BOScoin 내에 통합되어 있는 의사 결정 프로세스에 대한 아이디어는, 대시 코인[15]이 사용하고 있는 방식 즉 마스터 노드들[16]이 투표를 통해 결정하는 절차에서 영감을 받았다. BOScoin 내에서는 크게 두 가지 유형의 제안서가 있다. 하나는 시스템에 관련된 제안이고 다른 하나는 자금 조달에 관한 제안이 있다. 시스템 제안서는 BOScoin 플랫폼의 코드를 변경하고자 하는 제안이고, 펀딩 제안서는 Commons Budget 사용하고자 하는 제안서다. 누구나 제안서를 작성할 수 있으며, 매월 셋째 월요일 24:00 GMT까지 검토를 받는다. 그리고 이 제안서에 대해 Congress 구성원들이 네 번째 월요일 24:00 GMT까지 투표한다. 긍정 혹은 부정 표결 사이의 '순 백분율 차이'가 10%를 초과하면 제안서가 통과된다. Congress 구성원이 의사 결정 과정에 참여했다는 의사만 표현하는 중립 표결 선택권이 있으며 최종 마감일까지 언제든지 표를 변경할 수 있다.

펀딩 제안서에 대해 이야기하자면, 제안서가 통과될 확률을 높이기 위해 제안서에 담보를 넣는 것이 가능하다. 1,000,000 BOS 이상의 코인을 요구하는 제안서는 중요 제안서로 분류된다. 중요 제안서 투표에 참여하는 것은 특히 더 중요하기 때문에 Congress 구성원이 중요 제안서에 대해 투표를 하지 않으면 노드가 2주 동안 예치 기능이 비활성화시되는 페널티를 받는다. 코인 예치 기능이 비활성화되면 노드가 코인을 예치한데 따른 모든 혜택을 받지 못하고 2주 동안 코인을 예치할 수 없게 된다.

f. 공공예산(Commons Budget)

공공예산(Commons Budget)은 BOScoin이 보관되는 계좌이며, Congress 투표를 통과한 제안서에만 이체될 수 있다. Commons Budget의 주된 역할은 초기 단계에서 코인 사용자의 수를 늘리는 것이다. Commons Budget의 코인은 주로 두 개의 채널을 통해 축적된다; 첫 번째는 대략 6년 동안 블록당 50BOS를 직접 발행하는 것이고, 두 번째로 거래 수수료의 30%가 축적되는 것이다. 발행된 모든 코인 중 Commons Budget이 가장 많은 부분을 차지한다. 이것은 BOScoin 사용률을 획기적으로 높이기 위해 사용할 수 있는 자금을 보장해줄 것이다.

Congress를 통과하는 제안은 어떤 것이라도 Commons Budget을 받을 수 있다. 제안의 한 사례를 들자면 BOScoin 사용자 수를 늘리기 위해 무료로 코인을 사용자에게 배포하는 Airdrop 제안이 있을 수 있다. 다른 사례들로는 BOScoin 생태계 개발 자금 조달, 마케팅 캠페인 그리고 BOScoin 관련 미팅 개최 등이 있을 수 있다.

5. 사전 개발된 어플리케이션 생태계

많은 암호화폐들이 그들의 플랫폼 위에 application을 사용하고 구축하는 방법에 대한 예제를

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

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

제공하지만, 그들의 통화로 작동하는 어플리케이션을 제공한 암호화폐는 별로 없다. 암호화폐의 가치가 거래의 가치로 구성되는 정도와 투기적 가치로 구성되는 정도를 완벽하게 파악하기는 어렵지만, BOScoin의 목표는 경쟁 업체와 비교하여 통화의 거래 가치를 높이는 것이다. 장기적으로 볼 때 통화의 핵심 가치는 통화의 유용성이다.

코인과 함께 공개되는 Stardaq 및 Delicracy와 같은, 이미 개발된 어플리케이션을 통해 사용자는 BOScoin 생태계 내에서 즉시 사용할 수 있는 세련된 서비스를 만나게 될 것이다.

a. Stardaq

Stardaq은 유명인 인기 예측 시장이다. 유명 인사의 인기는 지수로 표시되며 사용자는 유명 인사의 인기가 상승하거나 하락할 것인지 여부에 대해 배팅을 할 수 있다. 베팅은 오직 보스코인으로만 가능하다.

b. Delicracy

델리크라시는 어느 조직에나 적용될 수 있는 집단의사결정시스템이다. 어거(Augur)의 예측 시장[17]과 비슷하게, 사용자들은 제시된 안들에 대해 베팅을 함으로써 의사결정 과정에 참여할 수 있다. 가장 많은 베팅을 받은 제안이 선정되는 것이다. 이러한 방식의 시스템은 크고 작은 조직들에서 의사결정과정의 투명성과 참여를 증대시키는데 도움이 될 것이다.

이들 서비스들은 무료 코인을 배포하는 채널 역할을 하는 동시에 보스코인을 사용하는 매장 역할을 할 것이다. 이러한 도구를 적절하게 사용하면 새로운 사용자를 유입시킴으로써 생태계를 성장시키는 데 도움이 될 것이다.

이러한 응용 프로그램은 BOScoin을 사용하는 사용처이기도 하고, 무료로 코인을 배포하는 채널로도 사용된다. 이러한 도구를 적절히 사용하면 새로운 사용자를 유입시켜 생태계 전체를 성장시키는 데 도움이 될 수 있다.

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

6. 기술 로드맵

다음 표는 주요 일정을 정의한 기술 로드맵이다.

Milestone → ↓ Module	M1		M2		M3		M4
P2P	Protocol specification & Implementation	ALPHA	Unit & Acceptance Test	GENESIS		NEBULA	
mFBA Consensus	Key design Implementation		Test App				
Remittance	Address design UTXO Pattern Send & Receive coin				Multisig Tx Specs		Multisig Tx Implementation
Data Store	Store specs & SQLite Store implementation		MessagePack History				Blockchain backup & restore using ISP(AWS, Azure and google)
CLI & Web Interface	Web design & implementation		Web UX design				
Trust Contract Proposal & Vote			Trust Contract design		Proposal & Vote implementation		
Simple payment verification wallets (Mobile)	Wallet Formal specification		UX design Application PoC Test				Android & iOS Wallet
Inference Engine			Formal spec. and key design elements available		Reasoner integration with Blockchain		Constructing Basic Ontology
Trust Contract Modeler					Formal spec. and key design elements available		App Deployment & Demo Site
RPC & REST API			Blockchain Explorer				

Fig 7. 구현 로드맵

7. 코인 발행

새로운 코인은 네 가지 방법으로 발행된다; 초기 개발 예산(5억개, 10 %), 블록생성 보상(18억개, 36 %), 예치금 보상(9억개, 18 %) 및 Commons Budget(18억개, 36 %). 우리는 앞으로 100 년간 총 50억개의 코인을 발행할 계획이다. 이 값은 변경될 수 있다.

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

Fig 8. 발행 요약

- **Initial Development Budget:** 초기 개발 코인은 Genesis 블록 이전에 배포되는 코인이며 소프트웨어 개발 완수를 지원하기 위한 것이다. 이 코인은 ICO 판매 및 포상금(bounty)으로 구성된다. 5억 개의 BOScoin이 Genesis 블록과 함께 발행된다.

- **Confirmation Rewards:** Confirmation rewards는 발행된 블록(5 초마다)에 대해 무작위로 노드에 지급되는 금전적 보상이다. 보상이 무작위로 분배됨에 따라, 노드의 수가 증가하면 한 노드가 보상을 받을 확률이 감소한다. 이 보상은 노드에 예치된 유닛 수에 비례한다 (섹션 4d 참조). 18억 BOScoin은 블록생성 보상으로 발행된다. 처음에는 블록 당 18 개의 BOScoin이 발행된다. 보상은 약 631만 블록 (약 1년) 씩 128년 동안 6.31%씩 감소한다.

- **Freezing Rewards:** 예치금에 대한 보상은 노드에 예치된 BOScoin 유닛의 수에 비례하여 분배되며 720 블록 (약 1 시간)마다 발급된다. 초기의 총 금액은 5,400이다. 보상금은 631만 블록(대략 1 년)마다 59년 동안 5.00 %씩 감소한다. 예치금에 대한 보상은 Congress 구성원들이 한 노드에 예치하려는 코인 수를 늘리도록 유도하고, 의사 결정의 중앙집중화에 대한 동인을 꺾기 위한 중요한 인센티브로 작용한다.

- **Commons Budget:** Commons Budget은 Congress Network를 통과한 제안서에 지급할 BOScoin을 보유하고 있는 계좌다. 제안을 위한 충분한 예산을 만들기 위해 첫 번째 3500만 블록 (약 5 년) 동안 블록 당 50 Commons Coins를 발행된다. 처음 5 년 후에 Commons Budget은 거래 수수료에 대한 30 %의 commons 수수료를 통해 유지된다.

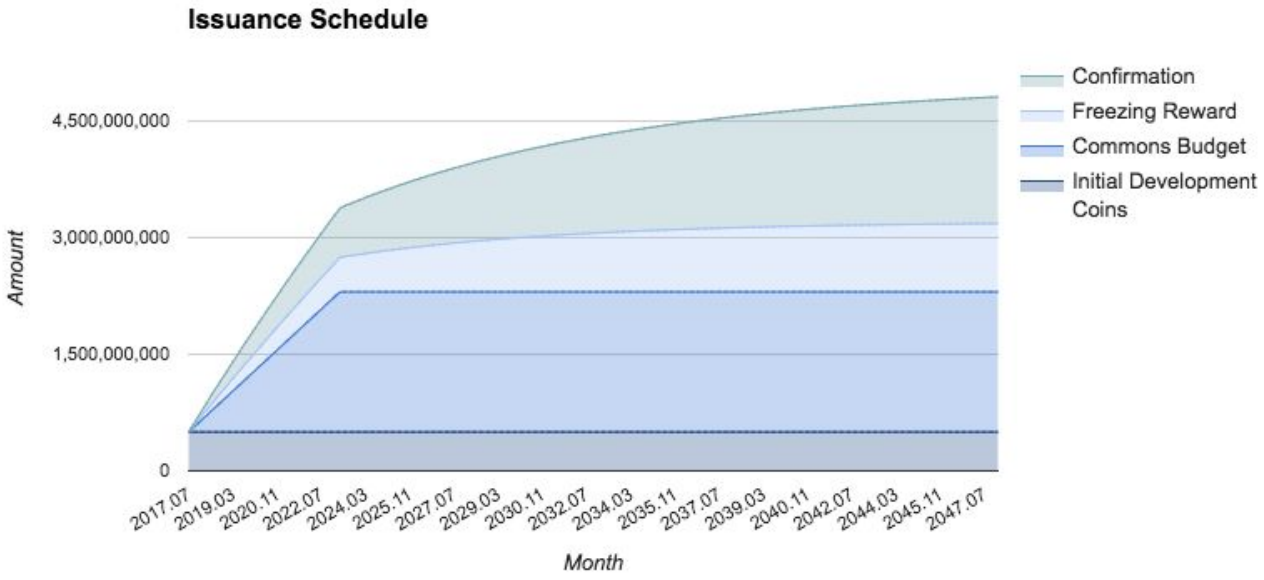

Fig 9. 코인 발행 계획

8. 결론

BOScoin팀은 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. Congress 시스템은 보다 민주적이고 생산적인 의사 결정 프로세스를 창출하기 위한 것이다. Trust Contract는 블록체인 위에서 계약을 생성하고 실행하는데 있어 결정가능성과 접근가능성을 가진 프레임워크를 제공할 것이다. BOScoin팀은 블록체인 기술을 통해 얻을 수 있는 보안성 및 무결성을 활용하면서 위와 같은 목적을 달성하는 것을 목표로 하고 있다.

Works Cited

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

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

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

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

Golem, https://golem.network

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

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

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

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

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

Simple Declarative Language, https://sdlang.org/

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

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

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

OWL Web Ontology Language Reference, https://www.w3.org/TR/owl-ref

Vitalik Buterin, *Ethereum Whitepaper*, https://github.com/ethereum/wiki/wiki/White-Paper