MULTICOIN CAPITAL

DPoS: 특징 & 트레이드오프

Myles Snider,

Tushar Jain, & Kyle Samani

멀티코인 캐피털은 세계 경제를 재편하는 토큰과 블록체인 프로젝트에 투자하는 철학을 토대로 활약하는 이론기반 크립토 펀드입니다. 자사는 블록체인 프로토콜, 프로젝트 팀, 시장 기회를 세밀하게 연구합니다. 이를 바탕으로 벤쳐캐피털식 투자를 진행하지만, 시장의 특수성을 이용하여 유동성 역시 확보합니다.

고지사항

본 보고서 발간 시점에 멀티코인 캐피털 매니지먼트 LLC 및 멀티코인 소속 직원들(이하 멀티코인), 본 보고서의 리서치에 기여하고 결과물을 공유받은 이들(이하 투자자) 모두 리포트 내에서 언급된 토큰을 매매하고자 하거나 이와 관련된 옵션을 보유하고 있을 수 있으며, 토큰 시세의 상승하락에 맞추어 이익을 실현하려는 입장을 취합니다. 본 보고서 발간 이후 투자자들은 다뤄졌던 프로젝트의 암호자산을 거래할 수 있습니다. 멀티코인은 본 보고서 내의 모든 정보를 정확하고 믿을만하다고 판단 정보원으로부터 확보합니다. 하지만 모든 정보는 있는 그대로 제시되어 어떤형식으로도 - 직접적으로 혹은 암시적으로 - 보장될 수 없습니다.

본 문서의 유일한 목적은 정보 제공이며, 특정 거래에 대해 공식적으로 확인하지 않습니다. 모든 시장 가격, 시장 데이터 및 기타 정보에 대한 완벽성과 정확성은 보증되지 않으며, 선별된 공개시장 정보를 기반으로 합니다. 해당 정보는 현 시점까지의 멀티코인의 관점을 반영하며, 별도의 통보 없이 변경될 수 있습니다. 멀티코인은 본 보고서에서 다루는 프로젝트에 대해 지속적으로 리포트를 발간할 의무를 갖지 않습니다. 본 리포트는 명시된 일자를 기준으로 작성되었으며, 이후 시장 혹은 경제 상황의 변화로 인해 그 신뢰성이 저하될 수 있습니다.

모든 투자는 가격 변동성, 불충분한 유동성, 원금의 완전한 손실 가능성 등의 상당한 리스크를 내포합니다. 본 보고서에서 멀티코인이 평가한 기초가치는 특정 토큰의 잠재적 기초가치에 대한 최선의 예측만을 반영하며 투자자를 위한 토큰 품질평가, 실적 요약, 투자전략 등을 의미하거나 시사하지 않습니다.

본 문서는 해당 토큰의 매수·매도와 관련된 청약 혹은 청약 권유를 포함하지 않습니다.

본 문서에 담겨진 정보는 향후 가능성을 예측하는 내용을 포함하고 있을 수 있으며 역사적인 사실을 다루는 것이 아님을 밝힙니다. 이와 같은 내용은 추후 잘못된 것으로 밝혀질 수 있으며, 부정확한 전제, 알려진 혹은 알려지지 않은 리스크, 불확실성 등을 포함하여 멀티코인이 통제할 수 없는 요인의 영향을 받을 수 있습니다. 투자자들은 본 문서에서 다루어지는 모든 암호자산에 대해서 금융, 법률 및 조세 전문가 등의 도움을 받아 독립적인 자가 실사를 수행해야 하며, 그 어떠한 투자 결정을 내리기 전에 앞서 관련 시장에 대한 독립적인 판단을 해야합니다.

주의: 여러 플랫폼들이 DPoS를 사용하긴 하지만 특정 기능들을 수정하였기에, 해당 문서에서는 비트쉐어, 스팀 그리고 EOS 에서 구현된 DPoS에 대해서 분석하였습니다. 그 중에서도, EOS 의 합의 알고리즘을 중심으로 분석 하였으며, EOS 에 대한 전체적인 분석과 가치 평가에 대한 글은 추후에 공개할 예정입니다.

서문

블록체인에서 확장성은 쉽게 확보할 수 있는 성질이 아니다. 지난 몇 년간 비트코인 및 이더리움을 비롯한 많은 프로젝트들이 거래속도와 플랫폼의 거래처리량을 높이려는 시도를 지속적으로 해오는 것만 보아도 알 수 있다.

이 난제는 확장성 트릴레마로 쉽게 이해할 수 있다. 확장성 트릴레마는 Vitalik Buterin과 Trent McConaghy에 의해서 처음으로 구체화되었다. 확장성 트릴레마는 모든 노드가 모든 거래를 검증할 수 있는 블록체인 시스템이 추구하는 블록생성의 탈중앙화(DBP), 안전성, 확장성 중 두가지만 달성할 수 있음을 지적한다.

이 3가지 요소는 아래와 같이 각각 정의될 수 있다:

- 블록생성의 탈중앙화는 블록 생성자의 숫자로 측정될 수 있다.
- 안전성은 네트워크의 생기성이나 거래 오더링에 영향을 미칠 수 있는 비잔틴 공격 행위를 하는데 소요되는 비용으로 측정된다. 한가지 알아야 할 점은, 안전성이 암호학적 서명의 무결성 혹은 개인키로부터 공개키를 파생시키는 제 3자의 능력을 의미하는 것은 아니다.
- 확장성은 단위 시간동안 시스템이 처리할 수 있는 거래의 숫자로 측정될 수 있다.

이더리움, 디피니티(Dfinity), 폴카닷(Polkadot), 그리고 카데나(Kadena)와 같은 프로젝트들은 확장성 트릴레마를 샤딩, 새로운 합의 알고리즘 등을 비롯한 다양한 기술들로 *해결하려는* 시도를 하고 있다. 그러나 아직까지도 이를 해결한 프로젝트는 존재하지 않는 실정이다. 만에 하나 확장성 트릴레마를 해결했다고 하더라도, 시장이 크게 관심을 주지 않을 가능성 또한 존재한다. 다만, 사용자들이 특정 서비스를 사용할 때는 안전성 혹은 블록 생성에 대한 탈중앙화를 일정 부분 희생하더라도 더 높은 성능과 사용자 친화적인 서비스를 제공하는 블록체인을 선택할 가능성 또한 상당히 높다.

탈중앙화의 가치는 그 누구도 데이터베이스의 정보를 바꿀 수 없다는 점에 있다. 탈중앙화의 정도가 높아질 수록, 정보의 변경도 어려워진다. 블록체인에서 구동되는 서비스는 그 종류마다 다른 수준의 보안성이 요구된다. 검열저항성이 주목적인 비트코인의 경우에는 주권을 보호하기 위해 설계되었다. 즉, 비트코인은 거대 국가 및 조직에 의한 공격을 견뎌낼 수 있도록 설계되었다. 그러나 대부분의 dApp(탈중앙화 어플리케이션)은 이 정도 수준의 탈중앙화를 필요로 하지 않는다. dApp 은 플랫폼 수준 정도의 보호가 필요하다. 플랫폼 수준의 보안성을 가진 서비스란 한 주체가 중앙적으로 통제하지 않으면서 중립적이고 글로벌한 데이터베이스를 의미한다.

DPoS는 소수의 '알려지고 일정 부분 신뢰를 받는(semi-trusted) 주체'들에게 블록생성권한을 집중시킴으로써 작업증명 (PoW)과 지분증명(PoS) 기반의 블록체인보다 훨씬 높은 확장성을 가진다. 해당 보고서에서는 DPoS 의 특징과 트레이드 오프에 대해서 알아보고자 한다.

권한위임 지분증명 (DPoS)

DPoS 합의 알고리즘은 2013년 Dan Larimer에 의해 탄생했다. 원래 DPoS는 Dan Larimer의 첫 번째 블록체인 프로젝트 비트쉐어(Bitshares)에 적용하기 위한 목적으로 개발되었다. 그는 이를 일부 수정하여 그의 두 번째 블록체인 프로젝트 스팀(Steem)에 적용하였고, 이를 한 단계 더 발전시켜 약 1년의 시간을 투자한 EOS에 적용했다. Larimer가 DPoS 를 개발하고 꾸준히 발전시켜나가는 동안, 다수의 타 프로젝트들도 각자에 맞는 방식으로 수정하여 DPoS를 도입했다. 현재 DPoS를 사용하고 있는 프로젝트들은 아래와 같다:

- EOS, BitShares, Steem, Golos, Ark, Lisk, PeerPlays, Nano(전 Raiblocks), Tezos
- Cosmos/Tendermint, Cardano 등 일부 타 프로젝트들은 DPoS를 일부 차용한 합의알고리즘을 사용

DPoS에서 네트워크 토큰 홀더들은 각자의 토큰을 블록 생성자 선출 투표권으로 사용할 수 있다. 유권자의 투표권은 본인의 지분에 따라 영향력을 행상할 수 있으며 가장 많이 득표한 상위 후보자들이 블록 생성자로 선출된다. 또한, 유권자는 본인이 직접 투표하지 않고 투표권을 다른 사람에게 양도("프록시")할 수도 있다. **DPoS는 토큰 홀더의 참정권을 도입한 리퀴드 민주주의이자 대의 민주제**이며, 전통적인 조직의 위계질서를 디지털 버전으로 형식화함으로써 완벽히 투명하게 조직을 운영할 수 있도록 한다. 이 문서의 범주를 벗어나면 민주주의 및 기업 구조 모두 문제점이 있겠지만, DPoS가 경쟁력을 가지는 이유는 프로토콜이 본질적으로 오픈 소스라는 것이다. 이는 네트워크 내 일부가 과반수가 내린 결정에 동의하지 않으면 언제든 포크하여 새로운 체계를 만들어 낼 수 있다는 것을 의미한다. 민주주의, 기업 등 기존 조직에서 이와 같이 하는 것은 불가능하다. 이처럼 DPoS 는 많은 전통적인 거버넌스 모델에서 그 아이디어를 차용했으며, 훨씬 더 유동적이고 투명하다.

DPoS에서는 투표로 블록 생성자를 선출할 수도, 제명할 수도 있다. 이는 블록 생성자들이 악의적인 행동을 하면 평판과 수익을 잃게함으로써 좋은 행동을 하도록 유인하는 시스템이다. 추가적으로, 슬래싱(slashing) 조건은 생각보다 간단히 권한위임 지분 증명에 적용될 수 있다. 대부분의 기존 지분증명(PoS)은 사용자로 하여금 본인의 네트워크 지분과 비례하여 블록을 생성할 수 있는 권한을 부여한다. 반면, DPoS에서는 블록 생성자를 선출하는 투표에 대한 영향력이 각 사용자들의 네트워크 지분과 비례한다. 블록 생성자 본인들은 큰 지분을 필요로 하지는 않지만 사용자들로부터 득표하기 위해 경쟁해야만 한다.

DPoS는 블록체인 전체를 구동하는 합의 알고리즘 뿐만 아니라, 차일드 체인, 사이드 체인, 프라이빗 체인 등에도 다양하게 사용될 수 있다. DPoS는 이더리움의 플라즈마 체인에서 사용될 수도 있으며 패리티(Parity) 팀이 개발한 권한증명(PoA) 합의 매커니즘과 많은 유사점을 공유한다. 또한, 코스모스 존(Cosmos zone)에 구축한 블록체인들과 같이 어플리케이션에 특화한 체인들을 위한 솔루션으로도 사용될 수 있다.

DPoS에 대해 더 자세한 설명은 비트쉐어측에서 작성한 이 문서와 이 문서를 참조할 수 있으며, Larimer의 백서에서도 찾아 볼 수 있다.

DPoS의 특징 및 트레이드오프

DPoS의 핵심 구성 요소는 아래와 같다:

블록 생성자

기타 지분증명 방식의 블록체인들이 그렇듯, DPoS 또한 블록 생성에 있어 해시 계산을 하는 채굴자들이 등장하지 않는다. 그 대신, DPoS에서는 선출된 사용자들이 체인 검증작업을 진행한다. 이들을 간단히 블록 생성자(block producer)라고 부르며, 생태계에 따라 각각 대표자(delegates), 공증인(notaries), 검증자(validators), 구축자(forgers), 또는 목격자(witnesses) 등 다양하게 불리운다.

DPoS에서는 토큰 홀더들이 사용자들 중에서 블록 생성자를 직접 선출하기 때문에, 블록생성에 방대한 컴퓨터 집단이 참여하여 블록생성 속도가 낮아지는 것을 사전에 방지할 수 있다. DPoS는 "통제된 준중앙화(controlled semi-centralization)"의 형태로 보일 수도 있다. 이 방식은 효율성과 속도라는 준중앙화의 장점을 취하면서도 일정 수준의 탈중앙화 정도를 유지하는 형태이다. 일정 수준의 탈중앙화라 함은 독립적인 블록 생성자들이 언제든지 토큰 홀더들의 투표를 통해 선출되고 제명될 수 있다는 것을 의미한다.

수십억 달러 가치의 질문을 꼽으라면 "충분한 탈중앙화 정도를 유지하기 위해서는 몇 명의 블록 생성자가 필요한가?"가 될 것이다. 이는 현재 크립토 커뮤니티 내부적으로 뜨겁게 논의되고 있는 주제로 여러 주장이 오가고 있다. 또한, 해당 주제는 주로 DPoS을 비판하기 위한 논리로 사용된다. 즉, DPoS가 충분히 탈중앙화 되어 있지 않다는 것이다.

탈중앙화는 특정 기준점이 존재하지 않는 스펙트럼과 같다고 할 수 있다. 탈중앙화의 정도가 높으면 더 많은 비용이 요구된다. 탈중앙화의 정도를 측정하는데에는 다양한 방법이 있다. Balaji Srinivasan는 탈중앙화의 정도를 정량적으로 측정하고자 시도했지만, 더 많은 후속 연구가 필요하다고 결론내린 바 있다. 그는 네트워크를 여러 하위 시스템(subsystem)으로 구분하였다. 각 하위 시스템은 다른 방식으로 측정되고 시스템 전체적인 탈중앙화에 기여한다. 일부 사람들은 어떤 하위 시스템을 고려하고 각 하위 시스템에 어느 정도의 가중치를 두어야 하는지에 대해 다른 관점을 가지고 있을 수도 있다. 궁극적으로, 해당 방식은 고려되는 변수에 의해 탈중앙화 측정 결과 역시 달라지게 되며 예 혹은 아니오 형식의 이분법적인 결과를 내지 않는다. 즉, **특정 시스템의 탈중앙화 여부**가 아닌 타 시스템에 비해 어느 정도 더 탈중앙화되어 있는가를 파악할 수 있는 것이다. 물론, 이런 측정방식이 좀 더 주관적일 가능성 또한 있다.

탈중앙화를 위한 탈중앙화는 목적이 아니다. **탈중앙화는 다른 목적을 달성하기 위한 하나의 특성이다. 해당 목적에는 검열 저항성, 공개 참여, 특정 공격의 방어, 단일 장애점 제거 등이 포함된다.** 탈중앙화에 기여하는 일부 특징들은 수치적으로 측정될 수 있으나, 전체적인 현상은 정량적으로 나타낼 수 없다. 예를 들어 블록 생성자의 수는 단지 하나의 요소일 뿐, 중요 요소들간의 세부적인 관계를 설명하지 못한다. 블록 생성자의 수는 상기 목적들을 달성하는데 있어서 어느 정도의 탈중앙화가 필요한지, 이론과 실제 탈중앙화의 간극을 어떻게 받아들여야 할지에 대한 기준을 제시하지 못한다.

DPoS는 통제권이 충분히 탈중앙화될 정도의 블록 생성자 수와 악의적인 행동을 용이하게 감시하기 쉬운 블록 생성자 수의 자연스러운 균형을 "찾고자"하지 않는다. 대신, 명시적으로 그 균형을 설정하고, 추후 필요에 따라 수정한다.

이를 단정 지을 수 있는 숫자가 정해져 있는 것은 아니다. 자사는 20명의 블록 생성자가 중국에 집중되어 있는 것이 전세계 각기 다른 관할권 아래 있는 10명의 블록 생성자보다 더 중앙화 되어있다고 판단한다. 코넬 대학교의 IC3 팀은 최근에 비트코인과 이더리움의 탈중앙화 정도를 정량화한 논문을 작성하였다. 해당 논문에서는 블록 생성 측면에서 봤을 때, 비트코인과 이더리움이 우리가 보통 생각하는 것보다 **훨씬 더** 중앙화 되어있다고 기술되어 있다.

IC3 팀은 다음과 같이 말한다:

> "이 결과는 비잔틴 쿼럼 시스템이 PoW 채굴 시스템보다 더 적은 비용으로 더 나은 탈중앙화를 구현할 수 있다는 것을 보여준다. 이는 높은 수준의 중앙화정도를 가지고 있지 않은 상태에서 동시에 무허가성 합의 프로토콜을 만들기 위해서는 추가적인 연구가 필요하다는 것을 의미한다."

DPoS 는 이 문제를 해결할 수 있는 잠재적인 해결책 중 하나이다. 물론 이 부분에 대해서는 추가적인 연구가 필요하다. 탈중앙화의 이점은 정확하게 단일 수치로 정량화할 수 없으며, 반복적, 역동적, 예측 불가능하며 실제 사례들이 관찰되어야 하는 새로운 요인이다. **DPoS 시스템에서 토큰 투표자들은 블록 생성자 수 뿐만 아니라, 어느 관할권에 위치하는지, 누구와 협력하고 있는지 등에 대해서도 고려해야 한다. 만약 투표자들이 블록을 생성하는 21개의 주체들을 각기 다른 관할권에 위치하도록 조치한다면 DPoS 는 여타 블록체인보다 더 탈중앙화될 수 있다.**

왜 DPoS 가 실제로는 PoW 보다 더 탈중앙화 되어 있는가라는 주제는 Ian Grigg가 쓴 포스트에서 잘 다뤄져 있다. 해당 포스트에는 압수, 사업 정지, 인터넷 신호 송수신 방화벽 설치 등의 방법들로 중국 정부가 비트코인 채굴자들을 공격하는 내용이 서술되어있다. 이런 일들이 실제로 일어나면 나중에 복구되더라도 비트코인 네트워크에 큰 지장을 줄 것이며 일정기간 동안 그 피해는 심각할 것이다. 반면 DPoS에서 이 문제는 쉽게 해결될 수 있다. 중국 정부가 위와 같은 행동을 한다면(혹은 하기 전에), 유권자들은 중국을 기반으로한 블록생성자를 투표를 통해 제명시키고 다른 관할권에 있는 블록생성자를 선출하면 되는 것이다.

DPoS 의 재미있는 특징 중 하나는 블록 생성자 후보자들은 선출되기 전에는 토큰 홀더의 표를 받기 위해서 경쟁하지만, 선출된 이후에는 네트워크 보안을 위해 서로 **협력한다**는 것이다. 블록 생성자들은 블록 보상을 (인플레이션) 동등하게 나누며, 한 라운드에는 하나의 블록만 생성한다. 특정 블록 생성자가 다른 블록 생성자들에 비해서 더 많은 블록을 생성하려고 해도 그에 대한 보상은 받지 못하며 애초에 불가능하다. EOS와 스팀에서 블록 생성자들은 전부 인플레이션으로 보상을 받는다. 이 플랫폼들에는 거래 수수료가 없기 때문에 블록 생성자는 수수료에 따라 거래를 우선순위화 하지 않는다. 그 대신 네트워크 내 지분으로 네트워크 내 대역폭에 대한 소유권을 주장할 수 있기 때문에 예치 금액을 고려한다. 블록 생성자들은 체인 밖에서도 선출되기 위해서 경쟁하지만, 선출되면 생태계를 위해서 협력한다. 또한 그 숫자는 고정되어 있기 때문에 규모의 경제에도 불구하고 블록 생성 권력은 중앙화되지 않는다.

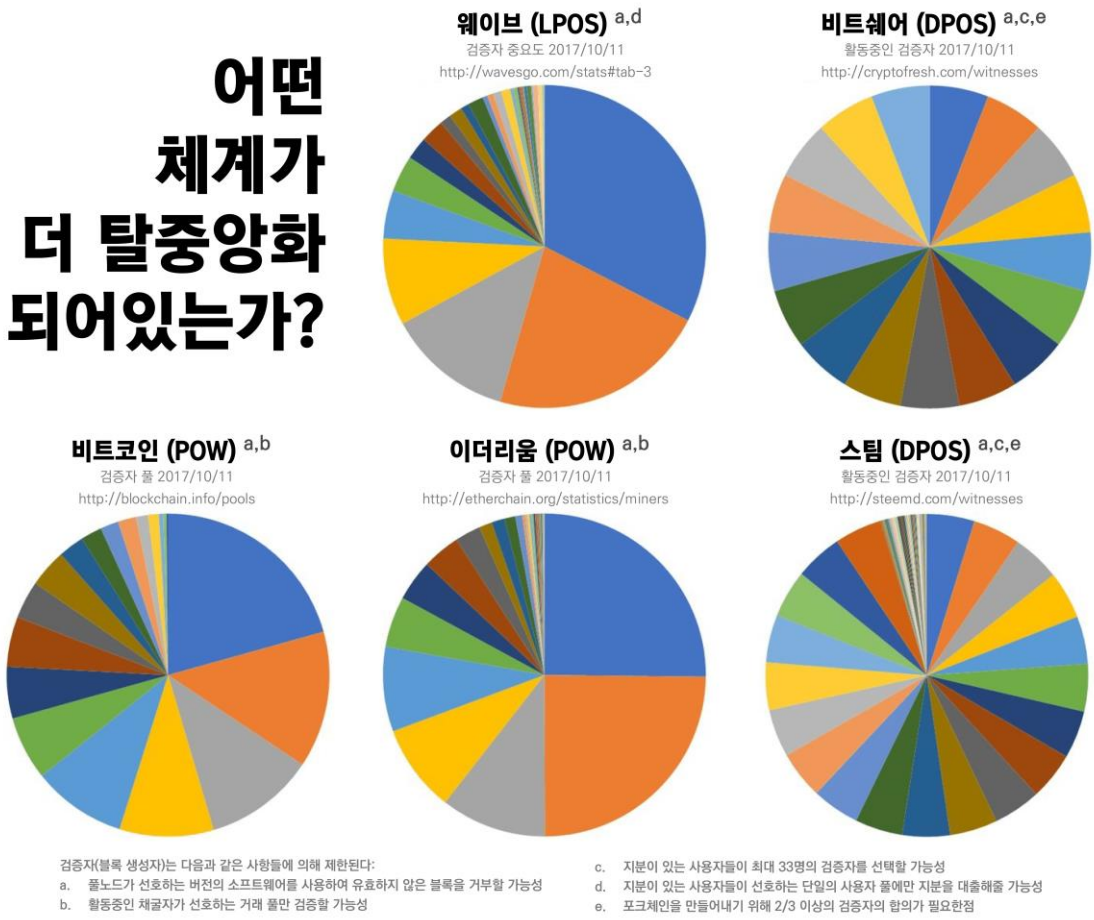
블록 생성의 중앙화

DPoS 기반의 프로토콜들의 공통적인 특징 중 가장 눈에 띄는 것은 블록생성자들의 숫자가 한정되어 있다는 것이다. 블록생성자들의 숫자는 리스크는 101개, EOS 에서는 21개로 각 프로젝트마다 조금씩 다르다. 몇몇 프로젝트에서는 투표를 통해 그 숫자 자체가 변경되기도 한다.

DPoS 검증은 라운드마다 일어나며 각 라운드는 슬롯들로 구성되어 있다. 각 블록 생성자들은 블록을 생성할 수 있는 슬롯을 부여 받는다. 예를 들어, Lisk에서 하나의 라운드는 101개의 블록으로 구성되어 있고 각 round가 시작될 때 모든 블록 생성자들은 슬롯을 하나씩 배정받는다. 1개 슬롯은 1개 블록에 대응하며 배정된 블록

생성자가 블록을 생성할 수 있는 유일한 기간이다. 만약 생성자가 슬롯 안에 블록을 만들지 못하면 그 블록은 생략되고 해당 블록에 속해 있는 거래들은 다음 블록으로 넘어간다. 투표는 매 라운드마다 집계되어 블록생성자들을 새로 선출하거나 제명한다. DPoS 라운드에서는 항상 블록 생성 후보자들의 숫자가 블록 생성자의 숫자보다 많기 때문에 악의적인 블록 생성자가 투표로 제명되더라도 다른 블록 생성자가 투입될 준비가 되어 있다. DPoS의 설정을 조정하여 투표로 제명된 블록 생성자들의 자리를 예비 블록 생성자들이 대체했을 때 인센티브를 제공하여 유인책을 구축하는 것도 가능하다(스팀의 목격자들).

검증자간 공모와 검열은 모든 블록체인 프로토콜이 우려하고 있는 부분이다. 만약, 이더리움 채굴풀들 중 상위 3개가 공모하면 네트워크 안전성에 실질적인 영향을 끼칠 수 있다. DPoS 역시 이 문제를 인지하고 있고 이를 투명성으로 해결하려고 한다. DPoS에서는 검증자 선출권은 토큰 홀더들에게 있다. 이와 같은 권리는 홀더들에게 더 많은 책임을 부여하지만, 네트워크 소유자들이 검증자들의 악의적인 행동에 대한 확고한 대응책이 있음을 의미한다. 이더리움의 관점에서 생각해본다면 채굴풀들이 공모하여 악의적인 행동을 했을 때, 사용자들이 선택할 수 있는 대응책은 채굴풀을 옮기거나, 하드 포크를 실행하는 방법밖에 없다. 두 상황 모두 오프체인 협조를 필요로 한다. 하지만 DPoS에서 블록 생성자들이 공모하여 악의적인 행동을 한다면, 커뮤니티는 한 라운드에서 그들을 투표로 제명시킨 후, 정직한 주체로 대체할 수 있다. 이 역시 사전 프로토콜 차원 합의가(투표권 재배정 방안을 토큰 보유자들이 결정)가 요구되지만 더욱 공식적이고 체계 수립이 쉽다고 할 수 있다. 이 설계는 보안을 유지하는 중앙화의 형태를 가능하도록 하는데 그 시사점과 공격 유형 등은 문서 후반부에 더 자세하게 설명될 예정이다.



이미지 출처

확장성

DPOS에서는 식별된, 제한된 숫자의 블록생성자만이 블록을 생성하기 때문에 블록 전파가 효율적이며 상당한 확장성 향상이 가능하다. 블록은 훨씬 짧은 주기로 일관적으로 생성되며(비트쉐어는 현재 3초마다 블록을 생성) 블록 생성자 중 ⅔이상이 거래를 확인하는 순간 완결성이 확보되고 유효한 체인에 포함됐다는 보장은 그보다도 전에 생긴다.

DPoS는 확실히 PoW 보다 높은 확장성을 가지고 있지만, 구체적인 속도는 여러 요인에 의해 달라진다. EOS는 최고의 거래처리량 최적화를 위해 WASM 가상 머신을 이용하고 상태 기반이 아닌, 메세지 기반 설계를 도입하려고 한다. 완전한 메인넷 조건은 아니지만, 지난 초기 실험에서 EOS 스마트 컨트렉트는 50,000 tps를 기록하였고, 최근에 커뮤니티 주도하에 EOS 테스트 넷을 구동 실험을 하였는데 일반적인 장비와 베타 소프트웨어를 사용하여 600 tps를 기록하였다. Larimer 역시 최근 업데이트에서 병렬 처리를 하지 않고 단일 스레드 구조로도 5000 tps 까지달성했다고 한 것으로 보아 확장성이 지속적으로 개선되고 있음을 알 수 있다.

하루 이용량이 가장 높은 상위 5개의 블록체인 중 3개가 DPoS 기반(출처: Blocktivity.info)이라는 사실은 눈 여겨 볼만하다. 이더리움은 처리량이 비슷한 수준으로 운영이 되는 반면 비트쉐어와 스팀은 대기 중인 거래가 없으며 대역폭에 여유까지 있다. 대규모 dApp을 호스트하는 스마트 컨트렉트 플랫폼의 경우에는 단순 호기심이든 백만 달러 어치 송금이든 매초 수천개의 거래를 처리해야 한다. 이 차트는 비트쉐어의 운영 타입과 수치에 대한 세부 사항들을 나타내고 있으며 이 링크에서는 스팀에 대한 정보를 확인할 수 있다. 비트쉐어가 해당 성능을 어떻게 구현하는지에 대한 더 자세한 정보는 이곳과 이곳에서 확인할 수 있다.

네트워크 인프라 서비스 제공

모든 블록체인 네트워크는 2개 집단으로 구분할 수 있다 – 네트워크 상에서 무언가를 운영하는 집단, 사용자와 그 운영 결과를 검증하는 집단, 검증자이다.

비트코인, 이더리움, 모네로 그리고 다른 PoW 기반의 블록체인에서 검증자(validator)는 채굴자(miner)로 불리운다. 채굴자들은 복잡한 문제를 푸는 경쟁을 하고 가장 먼저 답을 얻는 주체가 블록을 생성하게 된다. (블록 생성에 성공하면 거래 수수료와 블록 보상을 받게 된다) 전통적인 PoS에서는 사용자들은 토큰을 예치하고 예치한 비중에 따라 블록 생성 권한을 부여 받는다.

이때, 검증자들은 거래를 모으고, 나열하며 이중지불을 방지하는 중요한 네트워크 인프라를 제공한다. PoW에서는 최고의 하드웨어와 저렴한 전기세를 갖춘 주체가, PoS에서는 네트워크내에서 최대 지분을 가지고 있는 주체가 검증자가 될 확률이 높다. 반면, DPoS에서의 검증자들은 네트워크의 주인들(토큰 홀더)에게 고용된 직원이라고 할 수 있다. 검증자들은 고용되고(투표로 선출), 업무를 부여 받으며(블록 생성), 그에 따른 보상을 지급받고(인플레이션과 거래 수수료), 열심히 일하지 않으면 해고될 수도(투표에서 제명) 있다.

비트코인과 이더리움에서의 토큰 홀더와는 달리 DPoS에서는 이들이 네트워크의 실소유주들이자 궁극적으로 누가 인프라를 제공할지를 결정하는 자들이다. 만약 채굴자가 특정 동기에 의해서 악의적인 행동을 한다고 해도 비트코인, 이더리움 등의 블록체인 사용자들은 조치할 수 있는 부분이 없다. 반면, DPoS는 유일하게 좋은 서비스를 제공하지 않는 검증자들을 쉽게 *제명할* 수 있다. 제명되는 데에는 다양한 이유가 있지만 다음의 항목들이 대표적일 것이다:

제명되는 행동 유형

- 정직해 보이지 않거나 다른 후보자들에 비해 충분히 투명하지 않을 때
- 욕심/이기적인 행위(다른 생성자들에 비해 더 높은 블록 보상을 요구하는 경우)
- 검열성
- 악의적인 결탁
- 논쟁의 여지가 있거나 네트워크에 해를 끼치는 변화를 지원하는 행위
- 커뮤니티 기반 변화 지원에 실패
- 관할권에서 오는 법적인 문제(예를 들어 중국 기반의 블록 생성자들은 중국 정부가 암호화폐에 대한 강경한 발언을 하면 투표로 제명될 수 있음)

온체인 거버넌스

DPoS는 본질적으로 온체인 거버넌스의 한 종류이다. DPoS에서는 지분 가중치 투표 방식을 사용하여 네트워크 소유자(토큰 홀더)들이 결정권을 가질 수 있게 한다. DPoS에서의 투표는 투표권을 언제든지 다른 주체에게 행사할 수 있고 투표결과가 바뀔 수 있는 리퀴드 대의 민주주의 형태이다. 투표는 블록 생성자들 선출, 제명 의사결정이 가장 주요한 용도이지만, 그 외에도 개발자금 펀딩, 통화 정책 결정, 네트워크 파라미터 결정, 하드포크 등에도 사용될 수 있다.

블록체인 거버넌스는 여전히 신생 분야이며 최적의 접근 방식에 대해서는 의견이 많이 갈리고 있다. 이더리움 연구원 Vlad Zamfir을 포함한 몇 명은 온체인 거버넌스를 반대해왔다. 여러가지 이유가 있지만, 대표적으로는 블록 생성을 하지 않는 풀노드의 역할이 필요 없어진다는 것이다. 애널리스트 Nic Carter는 다양한 사회적, 기술적 계층들로 구성된 비트코인의 비공식 오프체인 거버넌스가 탈중앙화 네트워크의 가장 이상적인 거버넌스 형태라며 Vlad Zamfir와 비슷한 결론을 내었다. 반면, 코인베이스의 공동 창업자 Fred Ehrsam은 온체인 거버넌스는 복잡한 상황에서 표준 구조를 안착시킬 수 있는 방법이라고 주장한다. 많은 사람들은 비트코인 확장성 논의, 이더리움 DAO 포크 그리고 최근의 패리티사 지갑 버그 문제, 3 가지 사례를 온체인 거버넌스가 더 쉽게 해결할 수 있었을 복잡하고 불확실한 상황으로 제시한다.

DPoS 체인들은 블록체인 네트워크는 본질적으로 정치적인 구조를 갖고 있는 사실을 수용하며 그 과정을 공식화하려고 한다. 온체인 거버넌스, 토큰 투표(추후 분석)에는 문제점들이 분명 있지만 둘 다 DPoS의 가장 주요한 특징들이다. DPoS는 완전히 투명하고 탈중앙화된 방식으로 작동하는 커뮤니티 기반 운영방식이다. 온체인 거버넌스가 다른 형태의 블록체인 거버넌스보다 더 낫다고 할 수는 없지만 크게 뒤떨어지지 않은 것은 확실하다. 멀티코인은 DPoS가 다양한 방면에서 적용되고 검증되어야 한다고 굳게 믿는다.

인플레이션을 통한 자체적 모금

대부분의 블록체인은 인플레이션으로 인프라 구성에 필요한 자금을 모금한다. 비트코인과 이더리움의 경우 채굴자는 검증의 대가로 블록 보상을 받는다. 블록 보상이 다 지급되면, 오직 수수료에 의해서만 인프라가 유지되는데, 이는 곧 앞으로 수수료가 얼마나 높아질 것인가, 채굴 보상에는 어떤 영향을 끼칠 것인가, 보안에는 어떤 영향을 끼칠 것인가 등의 질문으로 자연스럽게 이어지게 된다.

EOS와 스팀에는 거래 수수료가 없기 때문에 다른 모델을 사용한다. 인플레이션은 인프라를 구축하는 블록 생성자들에게 지급되는 보상으로 쓰일 뿐만 아니라 플랫폼 개발 그 자체에도 사용된다. 토큰 홀더들은

인플레이션율 최대치를 결정하기 위한 투표에 참여할 수 있다. 5%로 시작했지만, 그 숫자는 바뀔 수 있으며 실제로 스팀에서는 여러 번 바뀌었다. 또한 홀더들은 블록생성자들에게 직접적으로 어느 정도의 보상을 지급할지에 대해서 투표할 수 있다. 예를 들어 토큰 가격이 상승했을 때 유저는 블록생성자에게 블록당 보상의 크기를 낮춤으로써 일정한 수익이 지급되게 할 지, 아니면 인프라 확대에 사용될 수 있게 추가적인 수익을 지급할지를 결정할 수 있다. 블록 생성자에게 지급되지 않은 부분은 커뮤니티 스마트 컨트렉트로 지급되어 다양한 방법으로 사용되기도 한다. 이 컨트렉트는 개발 펀드로서 커뮤니티 투표에 따라 개발자들을 지원하는 형태를 띌 수도 있고, 개발을 진행하는 회사에 직접 지급될 수도 있다. 해커톤을 개최하는데 사용될 수도 있고 소각될 수도 있으며 기타 다양한 형태로 쓰일 수 있다. DPoS는 개발자, 마케터, 커뮤니티 빌더 등이 **블록체인 자체를 통해** 자금 조달이 가능하게 한다.

많은 사람들은 인플레이션의 개념에 대해 찬성하지 못하고 있으며 인플레이션을 통한 펀딩에 의존하는 것에 반대하고 있다. 멀티코인은 반대하면 안 된다고 판단한다. 인플레이션은 블록체인 상에서 정상적으로 자금을 모집할 수 있는 유일한 방법인 동시에 다양한 문제들을 해결할 수 있다. 모네로 등과 같은 몇몇 블록체인은 커뮤니티의 크라우드 펀딩에 의존한다. 모네로 커뮤니티의 관대함이 인상적이기는 하지만 이것이 지속가능한 개발자금 모금 방법이라고 할 수는 없다. 개발을 통해 플랫폼이 발전하면 모든 이가 이득을 보지만, 오직 소수만이 이를 위한 개발자금을 기여한다. 인플레이션 펀딩을 사용하면 모든 유저들이 **공동으로** 개발 및 보안 자금을 부담하고 공동으로 이익을 취하게 된다. Fred Ehrsam가 짚었듯이, 인플레이션 펀딩은 토큰 홀더들에게 이득이 될 수 있다 :

> "만약 이더 홀더들이 개발 업그레이드로 인하여 (예. 샤딩) 가격이 10% 이상 상승할 것이라고 믿는다면, 그들은 기꺼이 10% 가까이 되는 토큰을 이를 위해 지급할 것이다. 이 말은 즉슨, 이더리움은 30억 달러에 해당하는
>
> 금액을 ETH의 숫자를 10% 늘림으로써 모금할 수 있고 새롭게 생긴 이 토큰을 업그레이드에 기여한 주체들에게 줄 수 있다는 것이다. 이는 세금과도 비슷한 성격을 띈다 : 커뮤니티에 있는 모든 사람은 혼자 짓는 것이 아니라 다수가 함께 만드는 공통 인프라 건설에 자금을 지원한다는 면에서 말이다."

모든 블록체인은 그 네트워크를 유지하기 위해서 거래 수수료, 인플레이션, 혹은 2가지 모두를 동원하여 필요한 비용을 부담해야한다. 하지만, 거래 수수료는 활동적인 사용자만 지불한다. 평생 비트코인 혹은 모네로를 자산으로서만 보유하고 거래 수수료를 통한 기여는 거의 안 하는 유저들도 있다. 이는 무임승차와 같은 문제이다. 추가로 거래 수수료는 가변적이고 예측 불가능하며, 네트워크 보안 유지에 충분하려면 수수료가 천문학적으로 높아져야 할 수도 있다. 반면, 인플레이션은 이에 비해 더 공평하고 사용자 친화적으로 네트워크를 지킬 수 있는 방법이다.

비슷한 방법을 다른 프로젝트에서도 많이 시도하고있다. Zcash 는 전체 공급량의 10% 를 회사와 그 주주들에게 지급하는 "Founders' Reward"을 만들었고 Dash는 블록 보상의 일부를 마스터노드가 투표하는 개발 펀드에 지급한다. DPoS는 이와 같은 방안들을 공식화하여 프로토콜에 직접 적용하였으며, 최고의 유동성과 공평성을 달성하였다.

DPOS 공격 유형

다음에서는 DPoS에서 일어날 수 있는 공격 유형들을 정리하고 위험성을 평가한다.

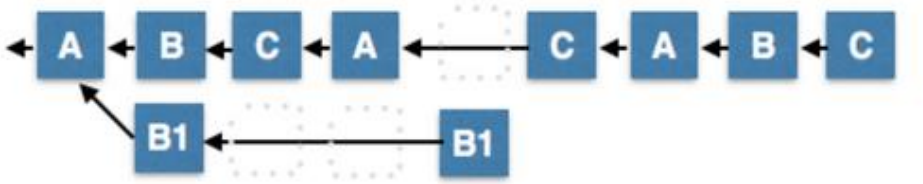
Nothing-At-Stake

"Nothing-At-Stake" 문제는 일부 PoS 체계에서 나타나는 문제이다. 포크가 일어났을 때 양쪽 체인 모두 유효하다고 검증하는 데 발생하는 추가적인 비용이 상당히 적으면 검증자의 최적의 전략은 두 체인 모두 검증하는 것이다.

DPoS에서는 "Nothing-At-Stake" 문제가 발생하지 않는다. DPoS에서 토큰 홀더들은 지분을 활용하여 블록이 아닌 검증자들에게 투표한다. DPoS에서는 최장 체인이 옳은 체인으로 간주된다. 왜냐하면 검증자의 숫자는 정해져 있고 순서는 매 라운드마다 결정되기 때문에 소수의 검증자들이 포크를 하여 메인체인을 능가하는 체인을 만드는 것은 불가능하기 때문이다.

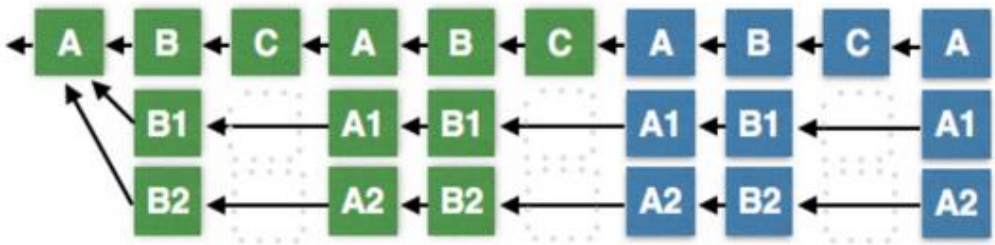
정상 상태에서의 DPoS 블록 생성
이미치 출처

만약 소수의 블록생성자가 아래의 이미지와 같이 다수의 포크에 블록들을 생성했더라도 메인 체인은 정직한 블록생성자들과 함께 지속적으로 성장할 것이다. 최장 체인만이 옳은 체인으로 간주되기에 공격자의 공격은 성공하지 못한다.



이미치 출처

다수의 블록생성자들이 아래의 이미지와 같이 다수의 포크에 블록을 생성하기로 공모했더라도 정직한 일부 검증자들은 최장 체인에 머물 것이다. 이런 경우 블록생성자들이 다수의 충돌하는 체인에 블록들을 형성했다는 암호학적 증거가 명확하게 있을 것이며, 그로 인해 투표로 제명될 가능성이 높다. 또한 악의적 비잔틴 행위에 대한 암호학적인 증거를 토대로한 슬래싱 등과 같은 **프로토콜 차원의** 불이익을 주는 규칙을 적용할 수도 있을 것이다.



이미치 출처

블록생성자들은 약간의 추가 비용만으로도 다수의 포크에 블록을 생성할 수 있다, 그러나 이를 통하여 직업, 명성, 추가 수익 등 잃을 수 있는 것들도 많이 있다. 악의적 비잔틴 행위는 식별될 수 있기 때문에 리스크가 높다. 체인의 무결성을 무너뜨리기 위해서는 압도적인 다수의 블록생성자들의 공모가 필요하다. 이런 공격은 "Nothing-At-Stake" 가 아닌 전통적인 BFT 공격에 조금 더 가까워진다. 더 자세한 내용은 Dan Larimer의 DPoS 백서에 나와있다.

낮은 투표율 악용

DPoS 형 블록체인에서 나타날 수 있는 가장 '당연한' 공격이다. 모든 투표 시스템의 문제인 오직 소수만이 등장하여 투표한다는 점이 이 공격의 핵심이다. 블록체인 토큰 투표 시스템에서 작은 지분을 가지고 있는 사람들은 플랫폼에 실질적인 영향을 미치기 쉽지 않다. 어떻게 투표해야 할지에 대해 고민하는데 소비된 시간이 실질적으로 미칠 영향과 비교했을 때 과도할 가능성이 높다. 이에 따라 적은 지분을 가진 투표자들은 합리적 무관심을 행사할 수 있다. DPoS는 특정 유저가 본인의 투표권을 본인이 생각하기에 더 풍족한 정보에 입각한 결정을 내릴 수 있는 다른 유저에게 위임하는 프록시 투표 방법을 통하여 이 부분을 부분적으로나마 개선하려고 한다. 이 경우에는 누구에게 위임할지 고민하는 비용보다 그를 통해서 얻는 이득이 높을 것이다. 물론, 이런 방법을 도입했음에도 불구하고 시스템 차원의 이유로 투표율이 낮아 고래, 거래소, 지갑 운영사 등이 대부분의 투표권을 행사할 때가 많다. 이 문제는 비탈릭이 블록체인 거버넌스라는 주제로 블로그에 작성하였다.

예를 들어, 전체 토큰 공급량의 10% 만이 투표에 사용되었다고 해보자. 이 상황에서는 공급량의 5% 이상을 가진 고래(혹은 고래 집단)가 거버넌스에 참여하여 결과를 조정할 수 있다. 같은 맥락에서, 비트쉐어에서는 상위 블록 생성자들은 33% 투표권을 가지고 있다. 대부분의 DPoS 시스템은 승인투표 방법을 사용한다. 유저들의 투표권은 모든 후보자들에게 나누어지며 그 중 승인권을 많이 받은 최상위 후보자들이 블록 생성자가 된다. 이로 인해 고래들은 투표 과정을 마음대로 좌지우지 못한다.

알아두어야 할 점은 투표 시스템에 대한 공격은 네트워크 전체에 악영향을 미치고, 성공하더라도 토큰 가격은 하락한다는 것이다. 네트워크에 상당한 양의 지분을 가진 사람들은 토큰의 가치를 지키기 위한 투표하도록 인센티브 체계가 확립되어야 한다. 투표권을 행사하는 토큰 홀더가 소수일 수 있으나, 투표를 하는 사람은 최대 지분을 가진 사람들일 것이다. 하지만, 이 역시 공격자가 거버넌스에 공격을 감행하기 위해서는 많은 양의 지분을 가져야만 한다는 것을 의미한다. 다른 PoS 시스템처럼 DPoS 역시 소수의 큰 이해관계자들이 의사결정의 대부분을 결정하는 파레토 원칙을 따를 가능성이 높다. 그러나 이게 나쁜 것만은 아니다. 앞서 언급한 것처럼, 큰 지분을 가진 이해관계자들이 네트워크를 위해서 일할 요인이 있기 때문이다.

사실, 참여율 문제는 이더리움의 캐스퍼 PoS 를 포함하여 모든 PoS 시스템에서도 나타나는 문제이다. ETH는 스테이킹 이외에 유틸리티 기능도 가지고 있기에 전체 유통량 중 일부만이 스테이킹된다. 전체 유통량 중 극소량만이 스테이킹 되면, 고래가 언제든지 들어와서 검증 과정을 조작할 수 있게 된다. 이 위험성은 Cosmos 블로그 포스트에 잘 설명되어있다. DPoS의 장점은 대부분의 DPoS 설계에서 해당 토큰들은 투표권을 위임하더라도(블록 생성자에게 직접 투표 혹은 프록시 투표자에게 위임) 유틸리티로서의 가치는 유지한다는 점이다. 따라서 투표 시스템에 참여하는 데 드는 비용은 투표권을 어떻게 사용할지 고민하는 시간 밖에 없다. 이더리움에서 지분 비중이 낮은 이용자들은 스테이킹 풀을 활용하여 수동적인 수익을 얻을 수 있기는 하지만 스테이킹 풀에 가입하는 절차가 간단하지 않으며 그 과정에서 자금이 일정기간동안 묶이기도 한다. DPoS 에서 토큰 홀더들은 그들의 투표권을 적절하게 임무를 수행할 것으로 보이는 다른 주체에게 쉽게 위임할 수 있으면서 토큰을 자유롭게 사용할 수 있다.

특정 DPoS 모델은 "리스크를 감수한(skin in the game)" 투표에 대한 인센티브를 주기 위해서 토큰을 일정 시간동안 묶어 둔다. 이는 유권자들로 하여금 플랫폼의 장기적인 이익을 고려하여 더 신중하게 투표하도록 유도하지만, 투표에 참여하고자 하는 유권자 수를 줄이기도 한다. 이는 현재 EOS 커뮤니티에서 논란이 되고 있는 주제이다.

투표 참여율은 사회적 계약의 일환으로서의 투표, 커뮤니티의 투표 장려 노력 성공 여부, 유저의 투표 및 위임권 행사 용이성 등 몇가지 요소에 의해 정해질 것이다.. 이런 맥락에서 사전 교육 및 사용자 친화적인 투표 인터페이스가 특히 중요할 것이다.

투표 매수 공격

실사용 사례가 있는 다음 공격 방안은 투표 매수이다. 실제로 최근 리스크와 스팀에서 매수행위가 생태계에 영향을 미쳤다. 물론 관점에 따라서, 또한 선출된 블록 생성자가 매수한 투표권으로 어떤 행위를 했느냐에 따라서 공격인지 아닌지에 대한 판단이 달라질 수는 있다. 어찌되었던 해당 행위가 바람직하지는 않기에 본 리포트에서는 악의적인 행동으로 규정하고 분석하였다.

리스크에서는 투표권을 위임한 사용자들에게 블록 보상의 일부를 나눠주겠다고 약속한 2개의 풀이 있다(LiskElite 과 LiskGDT). 심지어 가장 많은 보상을 줄 수 있는 대표자를 보여주며 보상을 주지 않는 대표자들의 제명을 부추기는 웹사이트도 있다.

투표 매수 공격의 지속가능성과 효과는 프로토콜의 다른 요인들에 따라 달라진다. 이 공격은 DPoS 기반 시스템과 모든 온체인 투표 체계에서 발생할 가능성이 있지만 다른 조치들로 그 가능성을 낮출 수 있다. 블록 생성자의 역할이 단순히 검증 작업을 하는 클라우드 인스턴스를 구동하는 것이라면 수익 분배를 약속하는 것이 쉬운 선택일 것이다. 리스크 같이 초기 단계이고 사용처가 많지 않은 블록체인에서는 블록 생성자에게 많은 역할을 요구하지도 않는다.

EOS에서 블록 생성자의 역할은 단순히 소프트웨어를 돌리는 것 이외에도 많은 것들이 있다. EOS 블록 생성자는 저장 공간을 제공하고, 거버넌스에 참여하며, 수익을 하드웨어 성능 향상에 투자하여 점진적으로 네트워크 전체 기능 향상에 기여한다. Larimer는 EOS가 결국 상호간 직접적으로 기가비트 수준의 통신을 할 수 있는 21개 이상의 데이터 센터를 갖출 것이라고 주장했다. 블록 생성자가 들여야 하는 운영 비용은 다른 시스템들에 비해서 훨씬 높을 것이며 투표 매수는 기대 수익을 낮추는 행위일 것이다. 투표 매수에 투자한 블록 생성자들은 시스템 성능 향상에 사용할 수 있는 자본이 적어질 것이고, 이는 네트워크 전반적인 손해이다. 네트워크의 장기적인 건전성과 토큰 가격을 중요시하는 투표자들은 단기적인 수익을 가져다 주는 블록 생성자보다는 네트워크 성능을 전체적으로 향상시키는 블록 생성자를 선호할 것이다. 대규모 토큰 홀더일 가능성이 높은 EOS 기반 비즈니스들도 투표자들을 매수하는 블록 생성자들이 아닌 자들에게 투표하는 것이 합리적인 선택일 것이다.

블록 보상 분배만 제공하려고 하는 블록 생성자들은 네트워크의 비효율적인 비용을 부과하지 않고는 지속 가능하지 않을 것이다. 예를 들어 스팀 검증자들은 네트워크 향상 방안을 공략으로 내세우며 선거운동을 한다. 비슷한 일들이 EOS에서도 일어나고 있다(EOS New York, EOS SoCal, EOSYS, 기타 등등). 투표 매수에 집중하는 블록 생성자들은 그들이 야기하는 비효율성으로 네트워크를 침체시키는 요인이라는 점과 결국 투표로 제명해야

하는 주체라는 점을 토큰 홀더들이 깨닫아야 한다. 추가로 EOS는 시간이 지날수록 특정 투표의 중요도가 감소하는 투표 가중치 감소 시스템을 적용하였다. 매달 투표권을 재행사하는 유권자들은 가중치를 최대로 유지할 수 있는 반면 오래된 투표들은 가중치가 서서히 감소하여 2년 후에는 최소화된다. 이는 참여를 독려하는 동시에 일회성 투표에 대한 영향력을 감소시킨다. 블록 생성자가 수익 분배를 제안했고 그 안건에 투표를 한번만 하고 수동적인 이익을 취하려고 했던 사람들의 영향력은 지속적으로 감소할 것이다. 투표를 하려면 토큰을 일정 기간동안 락업해야 하는 요구조건 등의 방법으로 투표 매수를 억제할 수도 있다.

DPoS 는 커뮤니티가 주도하는 합의 알고리즘이기 때문에 블록 생성자의 매수 행위에 대한 결단은 결국 커뮤니티의 선택에 의존한다. 커뮤니티가 참고할 수 있는 한 가지 사례는 뇌물성 수익 분배 금지를 EOS 헌법에 직접 추가한 것이다. 헌법은 "p2p 서비스 약관이자 계약에 서명한 당사자간 구속력이 있는 계약" 이라고 정의되어있다. 사용자는 거래마다 헌법 해시값을 포함함으로써 해당 계약 내용에 대한 동의를 표현한다(디지털 헌법에 대한 내용은 추후에 나올 EOS 분석 및 가치에 대한 보고서에서 설명될 것). 리스크는 블록생성 보상을 분배하는 블록 생성자들로 하여금 그 의도를 공개하게 하였고 행위의 주체를 쉽게 식별할 수 있도록 하는 조치를 취했다.

멀티코인은 블록 생성자가 투표권을 매수하는 행위는 옳지 않은 것이라고 판단한다. 왜냐하면 네트워크를 위한 최선의 선택이 아닌 가장 많은 보상을 위한 선택을 하도록 유도될 것이기 때문이다. 장기적으로 보면 이는 네트워크 및 토큰 홀더 모두에게 바람직한 선택은 아닐 것이다. 멀티코인은 DPoS 기반 체인 중심으로 형성된 커뮤니티들이 투표 매수 행위를 지양하는 규범을 만들기를 바라며 스스로도 그러한 규칙들을 장려할 것이다. 또한 투표 락업, 가중치 감소 등과 같은 인-프로토콜 메커니즘에 대한 추가적인 리서치도 장려할 계획이다.

대규모 공격

아직 실제로는 관찰되지 않은 공격 유형 중 하나인 "대규모 공격"은 엔터프라이즈 수준의 블록체인을 전제로 한다. Larimer는 EOS 거대 데이터 센터들이 블록 생성자 역할을 하며 네트워크가 필요로 하는 일정량의 대역폭과 속도를 제공할 수 있도록 성장할 것이라고 주장했다. 이러한 양상이 되려면 시일이 걸리겠지만 고려할 만한 분석이다.

만약 블록 생성자가 전용 데이터 센터에 속한다면 잠재적 블록 생성자의 수와 제명된 블록 생성자들의 자리를 대체할 수 있는 후보군들의 수가 제한적일 것이다. 따라서 검증자 교체율이 매우 낮을 것이다. 제명된 블록 생성자를 대체할 수 있는 예비 블록 생성자의 수가 충분치 않다면 네트워크 전체적으로 문제가 생길 것이다. 유권자들은 잘못된 행위를 한 블록 생성자들을 제명시킬 때 네트워크 전반적인 성능 하락을 감수해야 될 것이다.

중요한 것은 DPoS 네트워크는 새로운 주체가 블록 생성자로 참여할 준비가 될 때까지 적은 수의 검증자로도 운영 가능하다는 점이다. 이상적이지는 않지만 전환기에도 평소 같이 네트워크 운영을 할 수 있다는 것이다. 새로운 블록 생성자들은 기존 블록 생성자와 같은 자원을 가지고 있지는 않겠지만, 블록 보상으로 빠르게 확장하겠다는 공약을 내세워 선거운동을 진행할 수는 있을 것이다.

블록생성자간 담합

모든 블록체인 시스템에서 블록 생성자 간 담합 가능성은 내재되어 있다. DPoS는 검증자 수가 적어 이론상으로 담합하기가 더 쉽기 때문에 특히 더 위험하다. 바람직하지 않다는 점은 당연하지만, 블록 생성자 간 담합이 끼칠 수 있는 피해의 종류와 공격 행위에 대한 동기에 대해서는 분석해봐야 한다.

DPoS 시스템에서 블록 생성자들이(전체의 ⅔ 이상) 공모하여 시행할 수 있는 공격은 다음과 같이 3가지이다:

1. 검열
2. 시스템 파라미터 변경
3. 이중지불

DPoS 맥락에서 검열(Censorship)이란 블록 생성자가 유효한 거래의 처리를 거부하는 것이다. 만약 한 개의 블록 생성자가 개인 혹은 주체를 검열한다면 노력이 수포로 돌아갈 것이다. 해당 거래는 다음 순서의 블록 생성자에 의해 바로 블록에 포함되어 채굴될 것이며, 검열 행위가 체인 상에서 명확하게 식별되어 반복적으로 시도된다면 투표로 제명될 것이기 때문이다. 개별 블록 생성자, 혹은 소수의 블록 생성자가 가할 수 있는 최대의 피해는 특정 거래를 블록에 누락시켜 거래 처리를 지연시키는 것 뿐이다. 결국 이 거래들은 정직한 다수의 블록 생성자들에 의해 검증될 것이기 때문에 공격자의 규모가 충분히 크지 않다면 검열을 하더라도 그 영향이 미미하기 때문에(거래의 몇 초 지연) 시도도 하지 않을 가능성이 높다. 물론 거래를 지연시켜 피해를 입힐 수는 있겠지만, 블록 생성자는 명성, 미래 수입원을 총체적으로 잃을 수 있으며 중재 대상이 될 수도 있다(해당 백서의 6페이지 참조). 제대로 기능하는 DPoS 상에서는 블록 생성자가 검열을 시도하면 빠르게 투표로 제명될 것이다.

블록 생성자 간 담합으로 실행할 수 있는 또 다른 공격은 프로토콜 파라미터 변경이다. 파라미터 변경은 헌법 변경, 블록 보상 증가, 포크를 통한 특정 이해당사자 방출 등 여러가지를 의미할 수 있다. 운이 좋게도, DPoS에서는 투표자들의 내포된 동의 없이는 해당 공격들이 불가능하게 설계되어 있다. EOS를 예로 들자면 시스템 파라미터 변경이 실제로 적용되기까지 일정 시간 소요된다. 헌법을 바꾸려면 21개 중 17개의 블록 생성자의 동의를 받아야 하며, 그 결정이 30일 연속 유지되어야 한다. 만약 사용자들이 변경에 동의하지 않는다면, 해당 기간 동안 찬성한 블록 생성자를 투표로 제명한 후 변경에 반대하는 블록 생성자로 교체할 수 있다. EOS 프로토콜 업데이트에 대한 추가적인 정보는 여기서 확인할 수 있다. 궁극적으로 시스템 차원의 변화는 최소한 토큰 보유자들의 수동적 승인을 받아야 한다는 것이다. 파라미터 변경이 적용되려면 시간이 소요되며, 그 기간 동안 해당 변경사항은 무효화될 수 있다. 이러한 장치들 덕분에 악의적인 블록 생성자가 끼칠 수 있는 손실은 굉장히 제한적이다.

마지막으로 절대 다수의 공모가 일어나면 이중 지불이 가능할 수 있지만, 그런 일이 실제로 발생할 가능성은 매우 낮다. DPoS는 같은 체인 상에 있는 블록 생성자 중 2/3 이상이 찬성했을 때 완결성을 제공하는 "불가역적인 최종 블록" 개념을 사용한다. 거래 완결성에 대한 명확한 보증이 필요한 사용자들은 해당 블록 확인(Confirmation)을 기다리면 된다.

디도스(DDOS) 공격

DPoS를 적용한 대다수의 시스템에서는 활동중인 블록 생성자의 신원이 네트워크에 알려져 있다. 일부 경우에는 해당 블록 생성자들이 대중들에게 친숙한 공인 혹은 조직이기도 하며, 물리적인 위치 혹은 IP 주소마저 알려져 있을 수도 있다. 또한, 각 라운드마다 블록 생성 순서는 사실상 결정되어 있다. 따라서 공격자는 특정 시간에 누가 블록을 생성할지 식별할 수 있고, 이를 통해 해당 블록 생성자에게 DDoS 공격을 감행할 수 있는 것이다.

다만, 이러한 공격은 실제로 실행에 옮기기 어려울 것이다. 공격자가 단일 블록 생성자를 목표로 삼아 공격하는 것은 가능할 수 있어도, 다수의 블록 생성자들을 동시에 공격할 가능성은 상당히 낮다. 공격자가 동시에 타게팅하는 블록생성자의 수에 따라 네트워크가 일시적으로 장애를 겪을 수 있지만, 대다수의 노드에게 동시에 DDoS 공격을 하는 것은 사실상 불가능에 가깝다. 또한, 블록 생성자들은 다른 곳에 위치한 백업 서버 등 다양한 방법을 이용하여 DDoS 공격을 방지할 수 있는 능력을 내세워 득표하기 위한 캠페인을 벌이기도 한다. 마지막으로, 만약 단일(혹은 일부) 블록 생성자가 DDoS 공격으로 인해 블록 생성에 계속 실패하면, 그들은 한 라운드만에 투표로 제명되고 다른 생성자로 교체될 수도 있다.

결론

DPoS는 세련되고 견고한 합의 방식이다. 그 중에서도 가장 중요한 것은, DPoS가 확장성 문제를 해결하는 가장 **실용적이고 검증된** 방법이라는 것이다. 뿐만 아니라, 블록체인 거버넌스, 자금 조달, Nothing-at-stake 문제 등에 대한 해결책을 제시한다.

DPoS 기반의 블록체인은 높은 확장성을 가질 수 있질 수 있는 반면, 확장성 트릴레마에 따라 "블록 생성의 탈중앙화"를 대가로 치뤄야만 한다.

트릴레마에 포함된 3개 요소 중 2가지, 즉, 확장성과 안정성은 블록체인에서 굉장히 중요하며 필수적으로 고려되어야 있다. 다만, 탈중앙화는 목적을 달성하기 위한 하나의 수단이다. 원하는 목적을 달성할 수만 있다면 탈중앙화에 대해서는 어느정도 타협해도 무방하다. 탈중앙화의 목적은 검열저항성, 공개성, 단일지점 실패 방지를 달성하는 것이다. 자사는 DPoS가 해당 목적을 모두 달성한다고 판단한다.

탈중앙화는 오직 부분적으로만 수치화 될 수 있다. 검증자의 수는 하나의 요인일 뿐, 이 외에도 수많은 요인들을 고려해야 한다. 그중 하나는 DPoS의 투표자들이 시스템이 탈중앙화의 이점을 모두 누릴 수 있는 방향으로 투표하는 것이다.

물론, DPoS에 대한 일부 비판적인 시각 또한 존재한다. 이는 네트워크의 건전성 자체가 토큰 홀더에 의해 관리되어진다는 것이다. 토큰홀더들은 지속적으로 악의적인 행동을 감시하고 충분한 탈중앙화를 이루기 위한 결정을 내려야하는 책임이 있다. 하지만, DPoS는 블록체인의 성능을 크게 향상시키며 큰 혜택을 가져올 수 있다. 자사는 DPoS가 다양한 종류의 dApp을 수용할 수 있도록 다양한 기능과 장점을 제공한다는 점에서 경쟁력을 가진다고 판단한다.

DPoS는 탈중앙화를 이루기 위해서는 필연적으로 경제적·성능적 비용이 소요된다는 것을 인지하고 확장성을 개선하기 위해 준중앙화를 선택한다. 만약 DPoS를 적용한 시스템이 일정 수준의 검열 저항성, 무허가성, 무신뢰성을 달성할 수 있다면, DPoS는 더 넓은 범주의 탈중앙화 어플리케이션을 수용할 수 있을 것이다. 디지털 금, P2P 디지털 화폐 등과 같이 검열저항성이 절대적으로 필수적인 특정 사례는 경제적 비용과 성능을 희생해서라도 탈중앙화를 취하는 것이 적합하다. 하지만, 그 외의 대부분의 어플리케이션에서는 확장성을 취하는 것이 더 실용적일 것이다.

물론, DPoS만이 확장성 문제를 해결하는 유일한 해결책은 아니다. 모든 어플리케이션들이 DPoS를 사용하기에는 적합하지 않을 수는 있으나, DPoS를 사용하는 것이 명확한 해결책이 되며 유용하게 쓰일 수 있는 분야는 분명히 존재한다. 만약 최악의 상황을 가정한다면, 21명의 알려진 주체들이 데이터베이스를 주도적으로 통제하거나 국제적인 정부의 노력으로 검열이 될 가능성 또한 존재한다. 그렇다 하더라도 DPoS는 여전히 특정 사례에는 매우 필수적인 기능을 제공한다. 사업체들은 확장성이 높고 지연시간이 짧은 중립적인 데이터베이스를 원할 것이며 더 나아가서는 정부기관의 보증을 요망할 수도 있다. 해당 시장의 크기는 수조 달러로 평가된다.

자사는 **실제로는** DPoS가 위에서 설명한 것보다 더 탄력적일 것으로 추정한다. 또한, DPoS라는 놀라운 사회적 실험으로부터 많은 교훈이 도출되길 기대한다.

본 보고서를 작성함에 있어 많은 도움을 주시고 의견을 개진해주신 Jesse Walden, Denis Nazarov, Trent McConaghy, Sam Kazemian, Malcolm Mason Rodriguez, Thomas Cox, Ian Grigg 그리고 모두에게 감사의 말씀을 전합니다.