에너지 소비로부터 해방된 합의 알고리즘의 진화: POS 에서 SPOS 로

V SYSTEMS 팀 프로젝트

요약

슈퍼노드 지분증명(Supernode Proof-of-Stake Consensus)은 V SYSTEMS 블록체인 플랫폼을 위해 설계된 성능 지향적 지분증명 합의 알고리즘으로서 고정 인터벌 블록 생성(Minting), 콜드 민팅, 임대를 통한 지분 유동성 확보 기능을 탑재하고 있다. 해당 문서에서는 슈퍼노드 지분증명 방식이 2012 년 Peercoin 에서 발표한 지분증명(PoS)의 개념과 공통되는 점들과 차별화 된 점들에 대해 설명한다.

1. 에너지의 역할

2011 년 비트코인 네트워크는 처음으로 급격한 성장을 경험했고, 당시 탈중앙화 네트워크의 에너지 소비량은 사용자, 지지자들의 관심 밖이었다. 하지만 Peercoin 프로젝트[1]는 탈중앙화 네트워크의 과도한 에너지 소비에 대해 '과연 합의 알고리즘을 위해 이렇게 많은 에너지가 사용되어야 하는가?'라는 질문을 던졌고, 많은 비트코인 지지자들은 '그렇다'라고 답했다. 비트코인은 금과 같다. 금을 캐기 위해 소비되는 에너지는 금이라는 광석에 가치를 부여하고, 비트코인을 채굴하기위해 소비되는 자원은 네트워크 안에서 합의를 도출해내는 동시에 비트코인이라는 자원의 금전적인 가치를 뒷받침한다.

과연 어떤 요소들이 금이라는 자원에 통화적인 가치를 부여하는지에 대한 의견은 분분했다. 오스트리아 학교는 초기 상품가치[2]로부터 발생했다고 주장했고, 다른 이들은 국가의 힘이 금이라는 자원의 화폐적인 가치를 없앨 정도로 강해진다면, 금의 가치는 그들로부터 빼앗길 것이라고 주장했다. 누군가 비트코인의 금전적인 가치를 믿는다고 한다면, 어떤 이는 분명 왜 비트코인이 가치있는지에 대해 질문할 것이다.

한편으로 Peercoin 은 이런 중앙 화폐 미스테리를 풀기 위한 모험을 했다고 할 수 있다. Peercoin 은 금 채굴에서 차용한 에너지의 역할, 즉, 비트코인 생태계 내 채굴 또는 작업증명(PoW)이라는 에너지 소비 개념으로부터 합의 알고리즘을 분리시켜 에너지가 화폐를 발행하는 과정에만 관여하도록 했다. 주식 발행과 같은 모델로 변환하여 화폐의 가치 형성에 있어 '에너지'라는 요소의 개입을 수월히 제거될 수 있도록 했고, 이를 통해 에너지가 화폐 발행과 갖는 연관성을 숨김 없이 보여줬다.

결론적으로 지분증명(PoS) 합의 알고리즘은 통화 가치가 에너지 소비에서 파생되지 않음을 증명했다.

또한 고유적인 내제가치나 다른 일반상품가치 또한 요구되지 않으며 통화적 효용만으로도 가치를 형성할 수 있다는 보여주었다.

2. 지분증명(Proof-of-Stake) 합의 알고리즘 – 에너지 소비로부터 자유로운 합의 알고리즘

Peercoin 의 합의 알고리즘은 출시 당시 선구적이라는 평가를 받았다. Peercoin 은 높은 완성도를 지닌 비트코인의 작업증명(Proof-of-work) 합의 알고리즘을 과감히 버리고, 에너비 소비량에 전혀 의존하지 않는 알고리즘을 개발해냈고, 지분증명 방식이 기존 작업증명 구성요소의 개입 없이 독립적인 합의 알고리즘으로 사용될 수 있으리라 주장했다. 몇몇 학자들을 Peercoin 생태계 내 작업증명 방식이 사용되었다는 오해를 하고 있는데, Peercoin 의 합의 알고리즘은 순수한 지분증명 방식을 사용한다. 작업증명 방식은 공정한 코인의 분배를 위해 사용되었을뿐 합의 알고리즘과는 어떤 연관도 없다.

에너지 소비로부터 자유로운 지분증명 합의 시스템에서는 블록 생성 과정을 에너지 집약적 개념인 '채굴'이라 표현하지 않고 '주조(Minting)'라고 한다.

Peercoin 의 합의 알고리즘은 비트코인의 기능 중 일부를 유지시켰다. Peercoin 역시 무작위 블록 생성 프로세스를 도입했으며, 블록 간 평균 인터벌(블록 간 시간 차)과 목표 블록 인터벌만이 관찰 가능하도록 설계했다. 이 과정에서 적용되는 단위, 개념을 지분증명 난이도라고 칭했고, 난이도 조절을 통해 블록 생성에 소요되는 시간의 한계점을 조정하였다.

지분증명방식의 도입은 블록체인 기술 발전에 큰 이정표 중 하나이다. 지분증명 합의 알고리즘은 탈중앙화 합의 메커니즘으로부터 요구되는 비용을 감소시켰을 뿐만 아니라 블록체인의 확장성 또한 증진시켜 다양한 응용 분야의 미래를 열었다.

3. 지분증명방식(Proof-of-stake) 합의 알고리즘에 대한 비판

Peercoin 의 발명 이후, 지분증명방식을 향한 몇몇 비판들이 있었다. 이 중 가장 많이 제기된 비판은 지분 연마(Stake grinding)이며, 해당 취약점 2012 년 Peercoin 의 초기 출시[3] 당시 발견됐다. 하지만 그 후 2013 년 2 월 Peercoin 0.3[4] 버전에서 이러한 유형의 취약점에 대처하기 위한 새로운 알고리즘이 도입됐고, 지분 연마에 대한 논란은 사라졌다.

0.3 버전의 알고리즘에서는 커널이라는 새로운 합의 필드가 도입됐다. 커널은 블록체인과 함께 서서히 변화하는 변수인데, 주어진 기간 동안 프로토콜에 의해 선정된 특정 블록이 1 비트의 변화를 커널에 주입하고 이에 따라 커널의 값은 변하게 된다. 커널은 짧은 길이의 블록체인 포크로서 아주

제한적인 영향만 가지고, 이에 따라 느리게 변화하는 블록체인 엔트로피 소스 중 일부라고 간주될 수 있는데, 커널이라는 수의 도입을 통해 Peercoin 블록체인 내 지분 연마 위협은 제거될 수 있었다.

지분 연마 외 거론된 다른 비판은 Nothing-at-stake 이다. 이 문제를 제기한 이들은 블록 주조에 특정량의 작업이나 에너지 소비가 요구되지 않기 때문에 블록 트리에서 포크된 가지들을 모두 주조하더라도 손해가 없다고 했고, 포크로 인해 한 가지가 경쟁력을 잃어 손해보는 경우를 막기 위해 두 가지 모두를 주조하고 체인을 이어가는 행위가 이어지는 것이 지분증명이 취약점이라 주장했다.

이 논리는 지분증명방식의 핵심 원칙을 무시하는 오류를 범했다. 지분증명방식은 한 참여자가 코인의 총 발행량 중 일정 부분을 소유하기 때문에 시스템 공동의 이익을 추구할 인센티브가 부여되고, 시스템을 외부 공격으로부터 막기 위해 노력할 것이라는 전제를 가지고 설계됐다. 포크 후 양쪽 가지 모두의 블록 생성에 참여하는 것은 프로토콜에 대한 공격으로 간주되는데 이 때 두 가지의 주조 과정에 모두 참여하는 것은 참여자의 이익을 반영하는 행동으로 여겨지지 않는다. 이런 관점에서 이성적인 블록 생성자(주조자)라면 생태계 내 통화 단위로 코인의 가치를 측정하기 보다는 외부 안정 통화를 기준으로 자신의 지분 가치를 측정할 것이고, 결국 Nothing-at-stake 가 우려하는 사태는 벌어지지 않을 것이다.

자신의 지분에 부정적인 영향을 미칠 가능성을 고려한다면 이 부분은 공유지의 비극(Tradegy of the commons)[5]과 일맥상통한다. 그러나 공유지의 비극을 염두에 두더라도 주조로 인한 손실은 잠재적인 지분 손실에 비하면 비교할 수 없을 정도로 적기 때문에 실제로 Nothing-at-state 오류를 방지하기 위한 추가적인 프로토콜 도입은 일어나지 않았다.

4. 콜드 주조(Minting)에 대한 논의

지분증명방식 탄생 직후 Peercoin 커뮤니티는 콜드 주조 기능에 대한 논의를 시작했다. 콜드 주조[6][7][8] 기능은 프라이빗 키가 오프라인 지갑에서 관리되는 비트코인의 콜드 스토리지 기능과 유사하다. 지분증명 합의 알고리즘은 주조자가 블록을 서명할 때 프라이빗 키가 온라인 상태로 유지되는 것을 요구하기 때문에 해킹 및 외부 위협으로부터 안전하지 못하고, 이런 이유에서 높은 수준의 보안이 탑재된 유사 콜드 스토리지 기능 도입을 거론하기 시작한 것이다.

이 중 제시된 한 가지 해결책은 블록 주조와 지출 역할이 키를 분리하는 것이다. 지분을 소유하는 키와 주조를 담당하는 키, 이렇게 두 개의 다른 키를 관리함으로써 주조 키는 온라인 상태가 유지되지만 지분 소유권을 담당하는 키는 오프라인에서 보관된다.

위의 경우 비트코인 마이닝 풀과 비슷한 마이닝 풀의 형성을 자연적으로 도모할 것이고, 비트코인 마이닝 풀의 중앙화 현상을 미뤄 보았을 때 유사한 맥락으로 주조 키와 소유권 키의 분리에 대한 논쟁의 여지가 있다.

결국 중앙화에 대한 우려를 포함한 여러 이유로 인해 콜드 주조방식은 Peercoin 에서 도입되지

않았다. 이 후 주조 키와 소유권 키를 분리하는 형태가 몇몇 타 지분증명방식 시스템에 적용되었는데, 대게 이를 위임 또는 임대라고 정의했다.

5. 슈퍼노드로의 전환

지난 몇 년간 블록체인 산업은 탈중앙화 어플리케이션 개발에 엄청난 성장을 보였다. 비트코인과 이더리움 모두 주기적인 네트워크 체증을 겪었고, 많은 이들이 단일 체인 성능 증진에 노력을 가했다.

이 과정 중 합의 알고리즘 설계에 대한 몇몇 이슈가 제기 되었는데, 첫째는 주조/채굴 노드에게 하드웨어 업그레이드를 위한 인센티브가 충분하지 않다는 주장이었다. 네트워크 총 유지보수 비용 문제로 인해 노드들이 하드웨어 업그레이드를 미룰 것이라는 의견이었다. 사실 비슷한 생각(충분한 인센티브의 부재)을 가지고 있는 노드가 이미 네트워크에 많을 수도 있다.

또 다른 문제는 비트코인의 무작위 블록 생성 프로세스와 연관이 있다. 평균 블록 생성 시간은 10 분이지만 때때로 더 많은 시간이 걸리기도 한다. 이는 성능 지향 시스템으로부터 발생되는 이슈로, 시스템 응답 시간이 일정할 수 있도록 관리가 필요한 부분이다.

이와 같은 문제들은 주조 노드들에게 네트워크 내 타 일반 노드들보다 높은 지위를 부여하여 이들이 일정한 블록 생성 시간을 유지할 수 있도록 하는 방안으로 대처 가능하다.

6. 주조 슬롯과 주조 권한 경합

우리는 일정한 블록 생성 간격을 유지하기 위해 주조 슬롯이라는 개념을 도입할 예정이다. 각 슬롯은 동일한 채굴권을 가지며, 노드가 주조 참가권을 얻기 위해선 슬롯 소유권을 우선적으로 확보해야 한다.

네트워크에는 60 개의 주조 슬롯이 마련되어 있으며, 각 슬롯은 매 분의 특정 초와 일치하도록 설계되어 있다. 주어진 초의 주조 권한을 가지기 위해서는 해당 초에 상응하는 주조 슬롯을 보유해야한다.

각 슈퍼노드의 로컬 시계는 적절한 주조 순서를 위해 위해 네트워크 타임 프로토콜을 통해 동기화 된다. 2009 년, 비트코인은 클럭 동기화에 네트워크 타임 프로토콜을 사용하지 않기로 결정했는데, 이 때 채굴자는 최대 2 시간까지 시간 왜곡이 허락되기도 했다. 네트워크 타임 프로토콜은 일반적으로 도메인 네임 서비스와 같은 주요 인터넷 서비스의 필수 요소로 간주되기 때문에 높은 수준의 보안 체계가 적용된다.

주조 슬롯 경합은 주조자에 대한 도전 의사에 따라 개시되며 도전자는 누구에게나 언제든 자유롭게 경합을 요청할 수 있다. 그러나 경합권의 남용을 막기 위해 높은 경합 비용이 책정되어 있고,

도전자가 경합 트랜잭션을 발행할 경우 주조자, 도전자의 지분은 프로토콜 검사 단계를 거치고 검사가 완료되면 경합의 승자가 결정된다.

7. 주조 경제

주조에 관여하는 지분은 주조자가 타인에게 임대하지 않은 직접 보유 코인과 타인이 해당 주조자에게 임대한 코인으로 구성된다. '임대'라는 용어는 주조자가 마이닝 풀에서 활동하기 위해 사용자로부터 맡겨진 코인을 의미하며, 주조자는 코인의 본래 소유자에게 일정 수준의 이자 지불할 의무를 부여 받는다. 임대 관계에서 코인 자체의 소유권이 전송되는 일은 없기 때문에 주조자가 임대 받은 코인을 사용하거나 임의로 전송하는 것은 불가능하다.

동일한 주조 슬롯의 주조권은 네트워크 내 슈퍼노드 간 동등한 지위와 주조량을 보장한다. 비트코인 블록체인에 내장된 메커니즘이 마이닝 풀 시장 내 독과점을 저지할 수 없어 시스템 탈중앙화에 실질적인 위협을 가하는 구조와는 상반되는 부분이다.

주조 슬롯의 동등한 주조 권리는 주조 경제에서 핵심 역할을 맡는다. 슈퍼노드들은 주조 풀 시장을 만들 것이고 임대 이자가 이 시장의 주요 상품이 될 것이다. 풀 시장에 접속한 지분 소유자는 높은 이자율을 보장하는 슈퍼노드를 선호할 것이고, 주조 수익이 동일하다는 전제가 적용되어 있는 상황 속에서 늘어난 수요로 인해 추가 임대를 진행하는 슈퍼노드는 결국 손해를 막기 위해 이자율을 낮출 것이다. Peercoin 의 수수료 파괴 모델 또한 주조자 간의 상충을 없애고 인플레이션을 낮추기 위한 목적으로 도입되었다.

네트워크 내 슈퍼노드의 하드웨어 수준은 합의 프로토콜 밖에서 커뮤니티를 통해 표준화되고 전파될 것이다.

8. 지분 유동성과 혼잡 경합 공격

기존 지분증명 합의 시스템은 주조 활동에 참여하는 이들의 지분 이동에 많은 제약을 두었다. 기술적으로 이런 제약들이 적용된 타당한 이유가 있을 수 있지만, 경제적인 관점에서 이는 주조에 참여하고 싶어하는 이들에게 진입장벽으로 작용한다.

지분증명 합의 시스템에서 주조에 관여하는 지분량은 합의의 보안과 직결된다. 이러한 의미에서 지분 이동에 제약이 없는 환경은 네트워크 보안 확보에 긍정적인 영향을 끼칠 것이다. 우리는 이것을 '지분 유동성'이라고 부르며 지분 유동성이 확보된다면 주조자들은 언제든 소유 지분을 소비하거나 양도할 수 있다. 임대 지분의 소유자 또한 언제든 임대 관계를 파기할 수 있고, 지분을 사용하거나 전송할 수 있다.

반면 지분 유동성을 도입하는 것은 특정 공격의 위협에 네트워크를 노출시킨다. 이러한 가능성을 염두에 둔다면 한 사용자가 같은 지분을 사용해 여러 주조 슬롯의 주조권을 차지할 수 없도록 저지해야한다. 지분 자체가 유동성을 지니고 있기 때문에 한 사용자가 지분을 여러 슬롯으로 빠르게 움직여 허용된 양보다 많은 슬롯들을 차지할 수 있는데, 우리는 이러한 형태의 공격을 혼잡 경합 공격(Busy Contention Attack)이라고 부른다.

혼잡 경합 공격으로부터 네트워크를 방어하는 방법은 주조 슬롯에 경제학의 '누적 평균치'와 유사한 측정치를 도입하고 사용자 계정 잔고를 계산하는 것이다. 이 방법은 총 계좌 잔액 측정을 위해 지분 이동 전, 해당 자산이 일정 기간 동안 계좌 내에 머물러야 한다는 조건을 적용하고 이를 통해 혼잡 경합 공격의 여지를 제거한다.

9. 회계 모델 및 잔액 계산법

전통적인 회계 시스템은 즉각적으로 변화하는 잔고를 통해 거래 내역을 정확히 추적하여 계좌에 반영하는 모델을 사용한다.

비트코인은 내부적으로 코인백(Coin Bag)이라는 모델을 사용한다. 비트코인 네트워크 내 계좌의 잔고 정보를 얻기 위해선 계좌 혹은 주소와 연관된 코인백의 정보를 수집해 각 가방(Bag)의 금액들을 합산해야 한다.

지난 몇 년간, 많은 암호화폐 시스템은 전자로 언급된 전통적인 회계 모델로 회귀했다. V SYSTEMS 에서도 유사한 회계 모델을 사용하고 있고 네트워크 내에서 효율적으로 잔고를 추적할 수 있다.

임대 관계가 정의된 경우, 각 계정의 기본 잔액은 소유 잔액인 일반 잔액과 주조 잔액이라고 하는 소유 잔액과 임대된 잔액을 더하고 임대 맡긴 잔액을 뺀 두 부분으로 나누어 설명할 수 있는데, 이 두 가지 유형 모두 트랜잭션이 확인될 경우 관련 내역이 즉시 반영되고 그에 따라 값이 변경된다.

10. 제안된 잔액 체계

10.1.코인 연령

코인 연령은 화폐 보유기간으로 정의된다. 그리고 코인 연령을 판별하는 코인 데이(Coin-day)는 코인의 개수와 코인을 보유일을 곱하여 계산된다.

Peercoin 의 백서의 예시를 참고하면, Bob 이라는 사람이 앨리스로부터 10 개의 코인을 받고, 90 일 동안 보유했을 경우, Bob 이 900 의 코인데이를 축적했다고 계산한다. 만약 Bob 이 Alice 로부터 받은 10 개의 코인을 사용한다면 Bob 이 축적한 900 의 코인데이가 10 개의 코인과 함께 소비되었다고 (혹은 파기되었다고) 한다.

블록 주조 확률을 관리하는 증거 값으로서 코인 연령은 그 안정성과 이점을 증명한다. 그러나 이것은 트랜잭션에 기반한 값이기 때문에 이 값의 계산 복잡성은 해당 기간 동안 트랜잭션을 실행한 횟수와 연관되어 있다. 또한 코인 연령은 주조자의 커뮤티니 기여도를 측정하기 위한 정확한 값으로 쓰일 수 없다.

10.2 확정 잔고

확정 잔고는 N 블록만큼이 확정된 이후의 주조 잔고이다.

$$C_n = \min\{B_n, B_{n-1}, \cdots, B_{n-N}\}, \quad (1)$$

B_i 는 블록/높이 i 의 주조 잔고를 나타내고, N 은 유효 간격을 추정하기 위한 상수이다.

확정 잔고의 이점은 아래와 같다.

• 잔고는 큰 수량의 입금을 즉시 반영하지 않지만, 대량 출금은 즉각적으로 반영한다.

• 높은 수준의 확정 잔고에 다다르기 위해 채굴자/주조자는 오랜 기간 코인을 보유해야한다.

하지만 아래와 같은 단점도 있다.

• 연속/누적된 입금은 해당 기간 동안의 계산값에 반영되지 않는다.

• 계산 복잡성은 $O(N)$ 이다. 높은 주조 속도라는 조건 속에서 더 나은 성능과 안정성을 확보하기 위해서는 큰 N *값을* 선택해야 한다. 이 경우 $O(N)$ 알고리즘이 시스템 성능에 영향을 줄 수 있다.

3. 제안된 잔액 계산 방식

10.3.1 가중 평균 잔액

확정 잔고 사용 단점들을 피하고 계산 복잡성을 줄이기 위해 더 많은 변수를 포함하지만 간단한 계산 방식으로 구상된 잔고 계산법이 높은 채굴/주조 속도의 블록체인 시스템에서 요구된다.

이를 위해 운영체제의 부하평균과, 확률적 프로세스 공식을 차용해 아래의 가중 평균 잔액 계산식을 고안했다.

$$W_{hn} = aB_{h\,n-1} + (1-a)W_{h\,n-1} \tag{2}$$

$$a = \begin{cases} \frac{h_n - h_{n-1}}{N}, & if\ h_n - h_{n-1} < N, \\ 1 & otherwise \end{cases}$$

h_n은 현재 블록의 높이고, h_{n-1}은 계정 작성 시 잔액이 변경되는 바로 이전 블록의 높이다.

새롭게 고안된 식에서 계산 복잡성은 0 *(1)* 로 감소되며, 모든 주조 잔액이 변경된 이후에는 가중 평균 잔액이 기록되고, 최대 증가 속도는 선형을 띈다. (예제 11.1 참고) 그러나 예제 11.1.1 과 11.1.2 에서 잔액이 자주 변경되는 경우에는 가중 평균 잔액 계산이 느려진다는 것을 확인할 수 있다. 가중 평균 잔액이 예상 범위 내에 머무는 경우는 긍정적인 요소로 간주될 수 있는데, 잔고가 근거 없는 소스로 만들어지지 않는 것을 의미한다. (물리학의 에너지 보존 법칙과 유사) 11.2.1 과 11.2.2 의 예시에서 가중 잔액 공식이 보존 법칙을 따르지 않는다는 결론을 유추할 수 있다.

10.3.2 주조 평균 잔액

가중 평균 잔액의 장점을 유지하고, 단점을 극복하기 위해 주조 평균 잔액 (Minting Average Balance)이라는 새로운 계산식을 아래와 같이 고안했다.

$$S_{h\,n} = \min\{B_{h\,n}, aB_{h\,n-1} + (1-a)S_{h\,n-1}\}, \quad (3)$$

여기서 $B_{h\,n}$은 h_n에서의 잔액을 나타낸다.

주조 평균 잔액은 현재 잔액 및 가중 평균 잔액의 최소값을 통해 계산된다. 계산 복잡성은 여전히 $O(1)$이며 이 공식에서 MAB 는 사용자의 자산을 모두 옮기는 경우 바로 0 으로 감소한다. 이 계산식을 사용할 경우 전체 주조 평균 잔액은 전체 잔액에 의해 보수적으로 통제될 것이다.

11. 예시

이 부분에서는 주조 평균 잔액이 계산되는 과정을 보여주는 수치적인 예를 제시할 것이다. 주조 속도가 초당 1 블록이라고 가정할 경우, 하루 기준 $24 * 60 * 60 = 86400$ 개의 블록이 생성될 것이다. 모든 예제의 $N = 86400$ 으로 설정하고 모든 거래 수수료를 이상적인 수치인 0 으로 설정한다.

11.1.속도 증가 및 감소

첫번째 예시는 속도의 증가 및 감소에 대한 예시이다.

11.1.1.간단한 속도 증가 및 감소

Alice 와 Bob 은 모두 0 의 초기 잔고를 가지고 있다. Alice 는 블록 당 1 코인을 받고, Bob 은 블록높이가 43200 에 다다르면 86400 코인을 받게 된다. Alice 의 증가분은 등비 수열 공식으로 계산될 수 있는데, Figure 1(a)는 하루 기준 Alice 와 Bob 의 가중 평균 잔액과 주조 평균 잔액을 나타낸다.

마찬가지로 Charlie 와 Dave 의 초기 WAB/MAB 잔액은 동일 값인 86400 으로 설정되어있다. Charlie 의 잔액은 하루 1 코인 씩 줄어들 것이며, Dave 는 블록 높이 43200 에서 86400 만큼의 코인을 잃을 것이다. Figure 1(b)는 Charlie 와 Dave 의 하루 기준 평균 잔액과 주조 평균 잔액을 나타낸다.

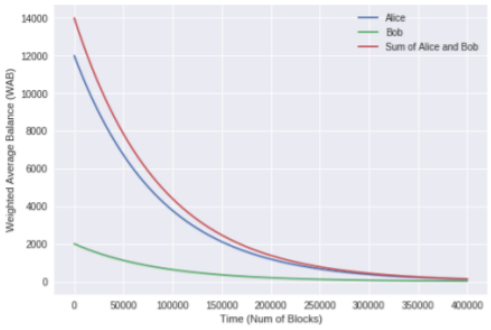
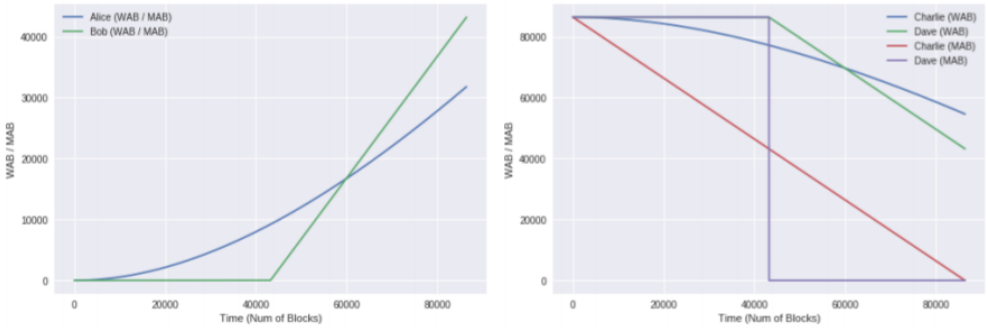


Figure 2: Decreasing speed case



(a) Increasing speed (b) Decreasing speed

Figure 1: Increasing and decreasing speed

11.1.2.느린 감소 속도

Alice 와 Bob 의 초기 가중 평균 잔액은 각각 12000 과 2000 이다. Bob 은 초기 잔고 1 을 가지고 있고, 블록 높이가 홀수인 경우 Bob 은 모든 잔고를 Alice 에게 전송한다. 반대로 블록 높이가 짝수인 경우 Alice 는 모든 잔고를 Rob 에게 전송한다. Figure 2 는 400000 개의 블록 생성되는 동안 Alice 와 Bob 의 가중 평균 잔액을 나타낸다. WAB 의 합계값이 더 느리게 줄어드는 것을 확인 할 수 있으며 아무 조치를 취하지 않는다는 가정하에 Alice 와 Bob 의 잔액은 86400 의 블록 높이에서 1 로 수렴한다.

11.2 균형 보존법

주조 평균 잔액(MAB)을 설명하는 몇 가지 예시가 하단에 제시되어있다.

11.2.1 보수적인 경우

이 예제에서 Alice 와 Charlie 의 WAB 와 잔고는 100 으로 설정되어 있고, Bob 과 Dave 의 초기 잔고는 0 으로 설정되어 있다. h=0 일 경우, Charlie 는 100 코인을 Dave 에게 전송하고, 다른 그룹에서 Alice 와 Bob 은 10800 번째 블록마다 서로의 잔고를 교환한다. Figure 3 은 각 그룹의 전체 잔고가 보수적이라는 나타낸다.

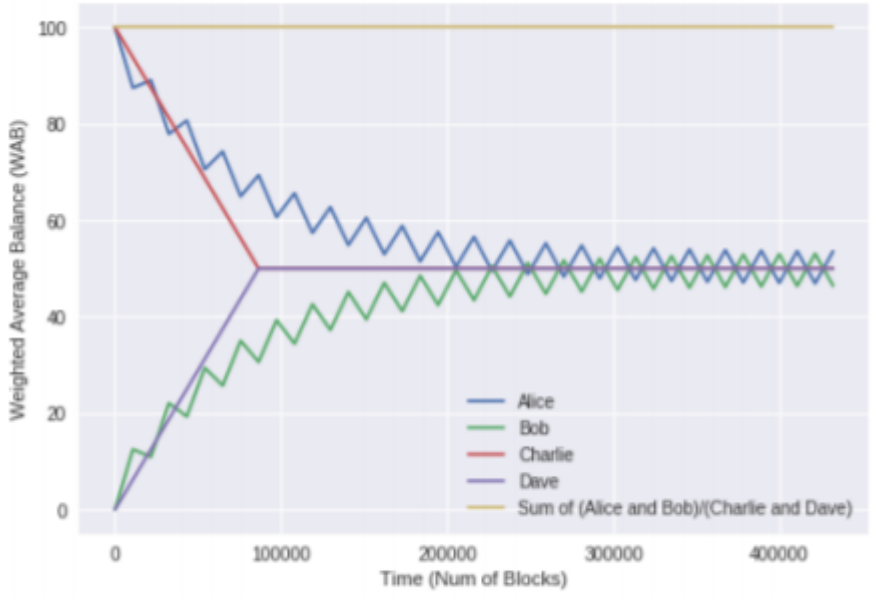
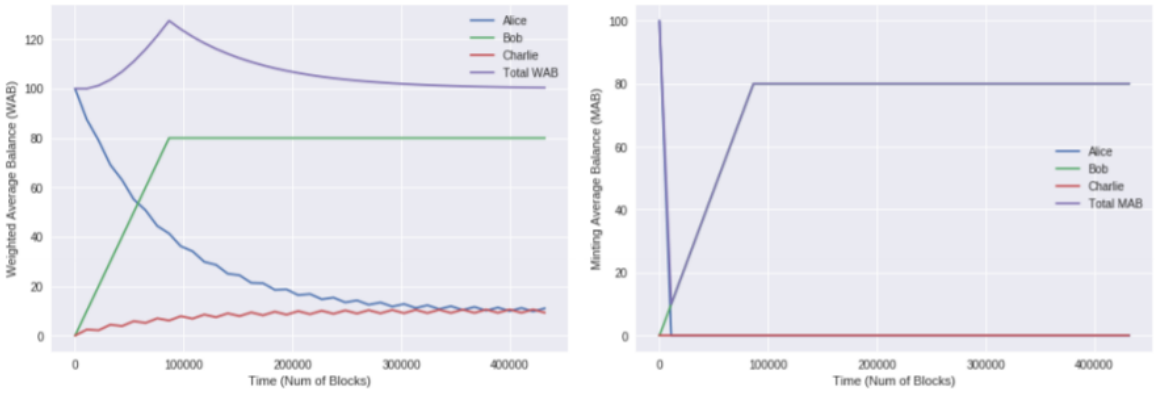


Figure 3: Case with conservative balance

11.2.2 보수적이지 않은 경우

이 예시에서는 Alice 가 특정 WAB/MAB 값과 100 의 잔고를 가지며, Bob 과 Charlie 도 모두 특정 WAB/MAB 값이 있으며 잔고가 0 이라고 가정한다. 주조 h=0 일 때, Alice 는 80 코인을 Charlie 에게 전송하고, 그 기간 동안 Alice 와 Bob 은 서로의 잔고를 10800 번째 블록마다 교환한다. Figure 4a 와 4b 는 두 잔고의 계산 공식의 차를 나타낸다.



(a) Weighted average balance

(b) Minting average balance

Figure 4: Nonconservative case

Figure 4a 에서는 특정 인터벌에서 총 WAB 가 100 을 초과하는 것을 확인할 수 있는데, 이는 "좋은" 전략을 통해 WAB 를 생성할 수 있다는 것을 의미한다. Figure 4b 에서는 MAB 의 값이 항상 100 미만인데, 이는 실제 응용프로그램에서 좋은 자산으로 쓰일 수 있다는 것을 나타낸다.

11.2. 주조자 주조 평균 잔고

이 예시에서는 주조자의 주조 평균 잔고를 다룰 것이다. 첫번째 주조자는 초기 잔고를 가지며 WAB/MAB 는 100 과 0 이고, 주조 보상은 분당 1 이다.
Figure 5 는 하루 동안 WAB 와 MAB 그리고 주조자 잔고의 변화를 나타낸다.

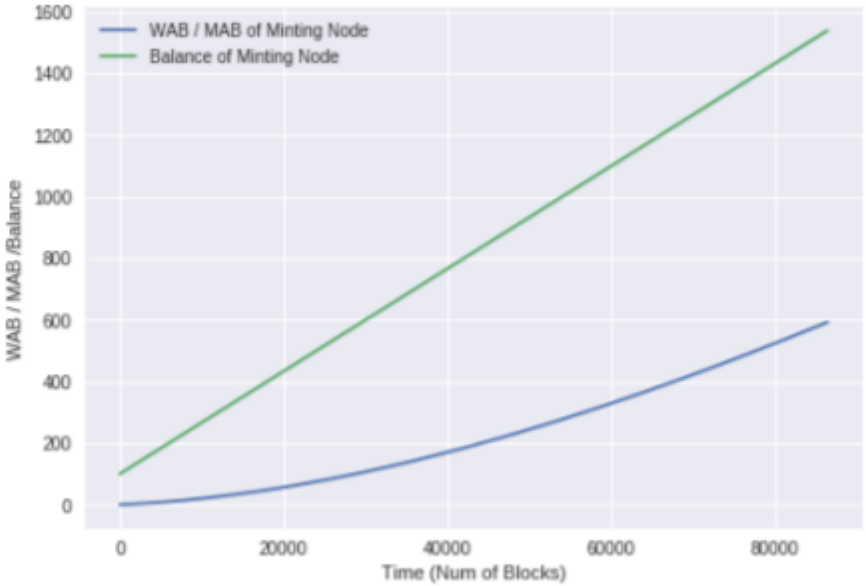
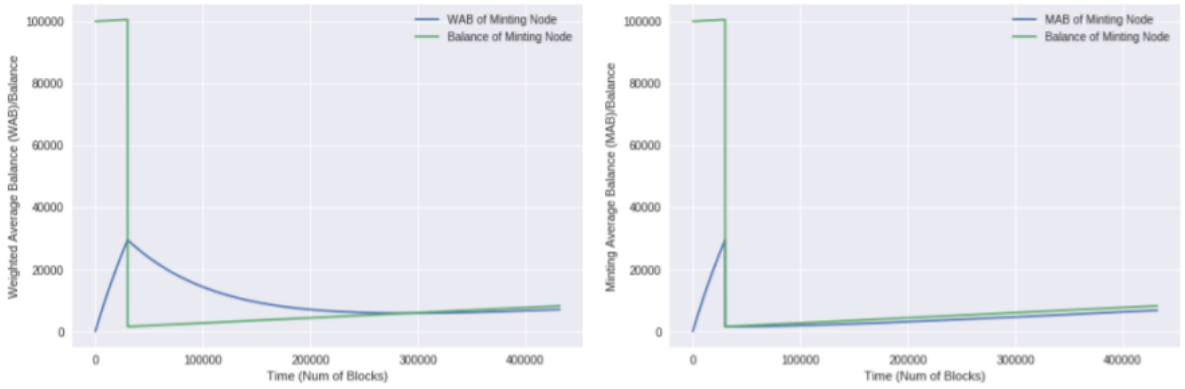


Figure 5: Weighted/Minting average balance/Balance of minter 1

두번째, 주조자는 특정 초기 잔고를 가지며 WAB/MAB 는 각각 10000 과 0 이다. 주조 보상 역시 분당 1 이며, 500 의 블록 높이에서 주조자는 99000 만큼을 잔고에서 인출한다. Figure 6a 와 6b 는 5 일 간 주조자의 WAB 와 MAB 변화를 나타낸다.



(a) Weighted average balance/Balance (b) Minting average balance/Balance

Figure 6: Case of minter 2

12. 요약

슈퍼노드 지분증명방식 합의(Supernode Proof-of-Stake consensus)는 고성능 블록체인 시스템 구축을 향한 진화이다. 생태계 내 자원은 하드웨어 업그레이드를 통해 더 효과적으로 분배될 수 있으며 시스템 응답 수준은 즉각적일 뿐만 아니라 예측 가능한 범위이고 안정적이다. V SYSTEMS 팀은 지분 유동성을 확보하기 위해 주조 평균 잔고 계산식 또한 설계하였다.

참고문헌

[1] Sunny King, Scott Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012, https: //peercoin.net/assets/paper/peercoin-paper.pdf 11

[2] Murray N. Rothbard, The Case for a Genuine Gold Dollar, 1992, https://mises.org/library/ case-genuine-gold-dollar

[3] Sunny King, Disclosure of Stake Generation Vulnerability, 2013, https://bitcointalk.org/index. php?topic=131940.0

[4] Sunny King, Peercoin 0.3 Release Announcement, 2013, https://bitcointalk.org/index.php? topic=144964.0

[5] Elinor Ostrom et al., Revisiting the Commons: Local Lessons, Global Challenges, 1999, http:// dusk2.geo.orst.edu/prosem/Ostrom_etal1999.pdf

[6] Jutarul, Peercoin Offline Coinstake Creation, 2012, https://bitcointalk.org/index.php?topic= 115608.0

[7] Sunny King, Proposal for Peercoin Online Stake Safety, 2013, https://bitcointalk.org/index. php?topic=194054.0 [8] Sigmike, Cold Storage Minting Proposal, 2014, https://talk.peercoin.net/t/ cold-storage-minting-proposal/2336

[8]Sigmike, Cold Storage Minting Proposal, 2014, https://talk.peercoin.net/t/ cold-storage-minting-proposal/2336