피피코인(Peercoin): 피어 투 피어(Peer-to-Peer) 암호화된 통화(Crypto-Currency)와 지분증명 (Proof-of-Stake)

Sunny King, Scott Nadal

(sunnyking9999@gmail.com, scott.nadal@gmail.com)

(Translation provided by lutz415@yahoo.com)

August 19th, 2012

개요

피어 투 피어(peer-to-peer) 암호화된 통화는 사토시 나카 모토 (Satoshi Nakamoto)의 비트 코인에서 유래되어 디자인한 것입니다. 이런 혼합설계에서 작업증명(proof-of-work)은 주로 초기 조폐를 제공하고 결국에는 대체로 비본질적인 것입니다. 효율적인 에너지와 더 많은 가격 경쟁력의 피어 투 피어 암호화된 통화의 공급에 따라서 네트워크의 보안수준은 장기적으로 에너지 소비에 의존하지 않습니다.

지분증명 (Proof-of-stake)은 화폐 연령 (coin age)을 기준으로 하고 비트코인(Bitcoins)의 해싱스킴(hashing scheme)의 유사성을 통해하지만 제한된 검색공간을 통해 각 노드 (node)에 의해 생성됩니다. 블럭체인의 역사 (Block chain history)와 거래결제는 중심적으로 알려진 체크포이트 메커니즘(checkpoint mechanism)에 의해 더욱더 보호됩니다.

머리말

비트코인 (나카모토 2008)의 창조이후, 작업증명은 피어 투 피어 암호화된 통화의 주된 디자인이 되었습니다. 작업증명의 개념은 조폐와 나카모토 (Nakamoto)의 디자인의 보안 모델의 근간입니다.

2011년10월, 우리는 화폐 연령의 개념을 비트코인의 작업증명시스템, 지분증명 으로 알려진 대안 디자인을 용이하게 할 수 있음을 인지했습니다. 우리는 그후 9지분증명이 피어 투 피어 암호화된 통화및 그 조폐 프로세스의 일부 보안 모델을 구축한 디자인의 형식을 잘 갖춘 반면, 작업증명은 조폐 프로세스의 초기 부분을 주로 용이하게 하고 점차 그 중요성을 줄일 수 있습니다. 이 디자인은 에너지 소비에 관계없이, 미래에 피어 투 피어 암호화된 통화의 실행 가능성을 보여주기 위해 시도합니다. 우리는 그것을 프로젝트 peercoin이라고 명명했습니다.

화폐 연령

화폐 연령의 개념은 적어도 2010년 초에 나카모토 (Nakamoto) 로 알려졌고

비트코인 보안모델에 중요한 역할의 대부분을 하지 않았더라도, 예를들어 거래의 우선 순위를 돕기위해 비트코인 에 사용되었습니다. 화폐 연령 는 간단히 통화 총액시간처럼 보유 기간으로 정의됩니다. 간단히 이해하기 위해 예를들면, 밥이 엘리스한테 10코인을 받고 90일 동안 갖고있었다면 우리는 밥이 900화폐 시대의 코인 날들을 축척했다고 말합니다. 또한, 밥이 엘리스에게서 받은 10코인을 소비할 때 또한, 우리는 이 10코인으로 밥이 축척한 화폐 연령 를 소비(파괴)했다고 말합니다.

화폐 연령의 계산을 용이하게 하기위해, 우리는 각각의 거래에 타임 스탬프 (timestamp)를 도입했습니다. 블락 타임 스탬프 (Block timestamp) 및 거래 타임 스탬프에 관련괸 프로토콜(protocols)은 화폐 연령의 계산을 확보하기 위해 강화됩니다.

지분증명

작업증명 은 나카모토 (Nakamoto) 의 주요 돌파구를 탄생시키는데 도움이 됐지만, 작업증명 의 성질상 암호화된 통화가 에너지 소비에 의존하는 것을 의미하므로, 네트워크의 운영에 상당한 비용의 부담을 사용자가 인플레이션과 거래 수수료의 조합을 통해 감당해야 합니다. 비트코인 네트워크에서 조폐의 비율이 둔화되면서, 결국엔 기본 보안수준을 우지하기 위해 거래 수수료 인상에 압력을 넣을수 있습니다. 분산된 암호화된 통화를 갖기위해 에너지 소비를 유지해야 하는지 여부를 물어볼까요? 따라서, 그것은 피어 투 피어 의 암호화된 통화의 보안이 에너지 소비에 의존하지 않는다는 것을 입증하기 위해, 이론적이고 기술적인 중요한 지표입니다.

지분증명의 개념은 2011년 초에 비트코인 사회에서 논의 되었다고 합니다. 대략, 지분증명 은 통화의 소유권 증명의 형태를 의미합니다. 거래에의한 소모된 화폐 연령은 지분증명 의 유형으로 간주 될수 있습니다. 우리는 2011년 10월에 화폐 연령의 개념및 지분증명의 개념을 독립적으로 발견했고, 지분증명 이 비트코인 의 조폐및 보안 모델의 주의 깊은 재설계와 함께 대부분의 작업 증명의 기능을 대체 할 수있다는 것을 깨달았습니다. 이것은 대부분 작업증명과 유사해서 지분증명 은 쉽게 위조 될수 없습니다. 물론, 이것은 화폐 시스템의 아주 중요한 요건 중위 하나이지요 - 위조의 어려움. 철학적으로 말하자면, 돈은 이전에 작업증명의 형태여서 그 자체로 인해 작업증명을 대체 할수 있어야 합니다.

지분증명에 따른 블럭생성(Block Generation under Proof-of-Stake)

우리의 하이브리드 디자인 (hybrid design)에서, 블럭은 서로 다른 두가지 유형인 작업증명과 지분증명 으로 구분됩니다.

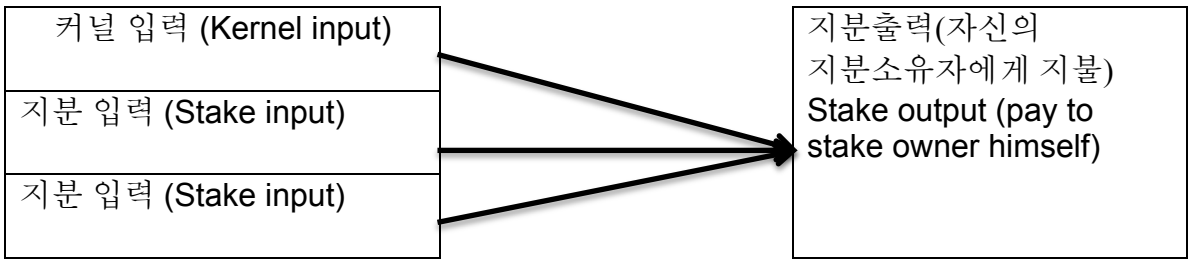

그림: 지분증명(Coinstake) 거래의 구조

새로운 블럭 유형의 지분증명에는 특별한 거래인 코인스테이크 "*coinstake"*이라는 것입니다. (비트코인 의 특별한 거래 코인베이스 "coinbase"의 이름을 따름). 네트워크에대한 블럭생성과 지분증명을위한 조폐의 권한을 확보하면서 코인스테이크 거래에서 블럭 소유자는 화폐 연령 의 소비에따라 그 자신에게 지불합니다. 코인스테이크 의 첫 번째 입력은 커널이라 불리고 작업증명 과 유사한 지분증명 블럭 생성의 확률적인 과정을 만듬에 따라서 특정한 해시 타겟 프로토콜 (hash target protocol) 을 충족시키기 위해 요구됩니다. 그러나 중요한 차이점은 해싱(hashing) 작업이 작업증명 에서 처럼 무제한 검색 공간 대신 제한된 검색공간 (더 구체적으로 하나의 해시는 초당 소비되지 않은 지갑 출력에 대하여)을 거쳐 수행되었다는 것입니다. 따라서, 큰 에너지 소모와 아무런 관계가 없습니다.

지분커널이 반드시 충독해야하는 해시타겟(hash target)은 커널에서 단위 당 소모된 화페연령, 화페 일 (coin-day)입니다. 비트코인 의 작업증명과는 대조적으로 모든 노드에 적용되는 목표값이 변하지 않습니다. 따라서, 커널 (kernel) 에서 더 많은 화페 연령의 소모는, 더 쉽게 해시 타겟프로토콜을 충족시킵니다. 예를들어, 밥이 100동전 년이 축적된 지갑 출력을 가지고 있다면, 이틀에 커널을 생성시킬 예상이되고 앨리스는 대략 그녀의 200동전 년 지갑 출력이 하루에 커널 (kernel) 을 생성될것으로 기대할수 있습니다.

우리의 디자인은 작업증명 해시타겟 및 지분증명 해시타겟 모두에서 네트워크 생성율의 급격한 급등을 방지하기 위해 비트코인의 2주간 조정 간격 보다는 지속적으로 조정됩니다.

지분증명에 근거한 조폐(Minting based on Proof-of-Stake)

새로운 조폐공정은 비트코인의 작업증명 조폐에 추가해서 지분증명 블럭(proof-of stake blocks)에 도입됩니다. 지분증명 블럭은 코인스테이크 거래에서 사용된 화페 연령에 따라 코인 으로 주조합니다. 소비된 화폐 년 당 1센트의 조폐율은 낮은 미래 인플레이션의 상승을 제공하기 위해 선택됩니다.

우리가 작업증명을 조폐과정의 일부로 유지하더라도 그것은 순수한 초기 조폐한 지분증명 시스템에 주식시장의 공개 공모와 유사한 과정을 통해 창세블럭 (genesis block)에 완전히 씨앗이 뿌려질수 있었다고 생각할수 있습니다.

주된 체인 프로토콜 (Main Chain Protocol)

주 사슬로하는 경쟁 블럭 체인(chain) 승리를 결정하는 프로토콜 은 소모된 화폐 연령을 사용하여 전환되었습니다. 여기 모든 블럭에 거래는 블록의 점수를 소비된 화폐의 연령에 기여하고있습니다. 가장 높은 총 소비 화폐 연령이 블록 체인 (block chain)의 주된 사슬로 선택됩니다.

이것이 비트코인 의 주요 체인 프로토콜 (main chain protocol)에 작업증명을 사용하는 반변 블럭체인 의 전체 작업은 주된 체인을 결정 하는 데 사용 됩니다.

이 디자인은 양호한 노드가 네트워크 채굴 전력 (mining power)이 적어도 51 %를 제어 할 때 시스템은 안전한 것으로 간주된곳에만 비트 코인의 51 % 가정의 문제 중 일부를 완화합니다. 우선 상당한 지분을 제어하는 비용은 강력한 실체에 대한 공격의 비용을 높이는데 따라서 중요한 채굴 전력을 획득하는 비용보다 높을수 있습니다. 또한 공격자의 화폐 연령이 공격시 소비되는 것은 공격자를 더욱 어렵게 주요체인에 들어가는 거래를 방지하기에 끊임없이 만들수 있습니다.

체크포인트 (Checkpoint): 역사의 보호

주된 체인(main chain)을 결정하기 위해 전체 소비된 화폐 연령을 사용의 단점 중 하나는 역사의 전체 블록 사슬에 공격의 비용을 절감한다는 것이다. 비록 비트코인이 역사상 상대적으로 강력한 보호책이 있어도 나카 모토는 여전히체크 포인트 이전 블록 체인 의 일부에 대한 가능한 모든 변화를 방지하고 블럭 체인의 역사를 공고히 하는 기구로 2010 년에 체크 포인트 를 도입하였습니다.

또 다른 관심사는 공격 이중 지출의 비용이 인하될수 있었다는것 뿐만 아니라 공격자가 그냥 화폐 연령의 일정 금액을 축적하고 블록체인의 개편을 할수도 있다는 것입니다. 이러한 시스템에서 상거래가 실용적으로 하기 위해, 우리는 블록 체인을 동결하고 거래를 마무리하는 역할을하는, 그런 일을 몇 번 정도 더 짧은 간격으로, 중심적으로 방송이되는 체크 포인트 의 추가 양식을 도입하기로 결정했습니다. 체크 포인트 의 새로운 유형은 비트 코인 의 경보 시스템과 유사 방송됩니다.

로리 (Laurie) (2011) 는 비트 코인은 체킹포인팅 (checkingpointing)로 분산되지 않는 메커니즘이 분포된 컨센서스 문제가 완전히 해결되지 않았음을 주장했다. 우리는 실용적인 분포된 체킹포인트 프로토콜을 설계하려고 시도했지만 네트워크 분할 공격에 대비한 안전한 보안이 어렵다는것을 발견했습니다. 방송된 체킹포인팅 메커니즘이 중앙 집중화의 한 형태이지만, 분산된 솔루션이 제공되기 전에 우리는 수용 할 수있는 것을 고려해야합니다.

또 다른 기술적인 이유는 중앙 방송 체킹포인팅의 사용을 수반한다는 것입니다. 지분증명 블록 이 각 노드의 로컬 데이터베이스 (블록 트리 (block tree)에 받아들여지기 전에 서비스 거부 공격 코인스테이크 커널 (coinstake kernel)의 유형에 맞서 방어하기 위해서 반드시 확인 해야 합니다. 비트 코인 노드의 데이타 모델 때문에 (특히 거래 지표) 체킹포인팅 의 마감은 블럭 트리로 블럭을 수락하기 전에 각 코이스테이크 커널의 연결을 확인하는 모든 노드의 기능을 보장하기 위해 필요합니다. 위의 실제적인 고려 사항으로 인해 우리는 노드의 데이터 모델을 수정 안하지만 대신에 중앙체킹포인팅을 사용하기로 결정했습니다. 우리의 해결책은 최소연령을 필요로하는 화폐의나이의 계산을 0 이하로 계산되는 화폐 연령은 1 개월로 계산하는 것처럼 수정하는 것입니다. 그러면 중앙 체킹포인팅은 모든 노드를 한 달 이전의 과거 거래에 동의 할 수 있도록하는 데 사용되므로, 1 개월 이상 전의 출력을 반드시 사용해야 합니다. 따라서 0 아닌 화폐나이가 요구되므로 코인스테이크 커널의 연결확인을 허용합니다.

블럭서명및 중복지분 프로토콜 (Block Signatures and Duplicate Stake Protocol)

각 블록은 복사 공격자에 의해 사용되는 동일한 증거의 지분을 방지하기 위해 소유자가 반드시 서명해야합니다.

중복 - 지분 프로토콜 은 서비스 거부 (DoS) 공격과 같은 블록의 다수를 생성하는 하나의 증거의 지분을 사용하는 공격자에 대한 방어하도록 설계되었습니다. 각 노드는 본 코인스테이크 거래 의 모든 쌍 (커널, 타임스탬프 을 수집합니다. 수신 된 블록이 다른 이전에 수신 블록 (block) 으로 중복 쌍을 포함하는 경우 후속 블록이 고아 블록 (orphan block) 으로 수신 될 때까지, 우리는 중복 - 지분 블록을 무시합니다.

에너지 효율

작업증명의 조폐율이 0에 근접하면 작업증명 블럭을 조폐하는데 점점적은 인센티브가 있습니다. 이 장기적인 시나리오에서 사심이없는 채굴자가 작업증명 블럭 의 채굴의 중지로 네트워크에 에너지 소비는 매우 낮은 수준으로 급감할지도 모릅니다. 비트코인 네트워크는 거래량/요금을 충분히 높은 수준으로 상승하지 않은한 너무나 큰 위험에 직면해 있습니다. 우리의 설계에서는 에너지 소비가 제로로 접근하는 경우에도 네트워크는 여전이 지분증명 에 의해 보호됩니다. 암호화 통화 만약에 작업증명에 있는 에너지 소비가 0에 접근이 허용된다면, 우리는 장기적인 에너지 효율의 암호화 통화 을 소집한다.

다른 고려사항

우리는 블록의 높이 (시간)에의해 결정하는 대신 어려움으로 인한 결정되지 않을 수있는 작업 증명 조폐율을 수정했습니다. 채굴의 어려움이 증가하면, 작업 증명

조폐율이 저하됩니다. 인위적으로 판매 충격을 피하기 위해 비트 코인 의 스텝 함수와 달리 비교적 매끄러운 곡선이 선택됩니다. 더 구체적으로, 연속적인 곡선이 채굴의 난이도가 각각 16x 오른 블럭 조폐양을 절반이 되도록 선택됩니다.

장기적으로 작업 증명 조폐 곡선은 무어의 법칙을 지속 제공으로, 인플레이션 행동의 측면에서 비트 코인의 그것과 너무 다르지 않을 것입니다. 우리는 의견의 이념적인 이유로 일부 주류 경제학자에게 비트코인의 상당한 비판에도 불구하고, 높은 인플레이션의 통화를 넘어 낮은 인플레이션 통화를 선호하는 시장의 전통적인 관찰에 따라 현명하게 고려합니다.

바바이오프 등 (Babaioff et al.) (2011) 은 거래수수료의 효과를 연구하고 거래수수료는 채굴자들사이서 협력하지않는 인센티브라고 주장했습니다. 우리의 시스템에서 이 공격은 악화되서, 우리는 더 이상 소유자를 차단하기 위해 거래 수수료를 제공하지 않습니다. 우리는 대신 거래 수수료를 없애기로 결정했습니다. 이것은 다른 채굴자의 블럭을 인정하지 않도록 인센티브를 제거합니다. 또한 지분증명 조폐 에서 인플레이션 힘에 대응하기 위해 통화수축의 힘 역할을 합니다.

우리는 또한 블록 팽창 의 공격에 대항해서 방어하기 위해 프로토콜 수준에서 거래 수수료를 적용하기로 선택합니다.

우리의 연구 동안 우리는 또한 작업 증명 및 지분증명 외 에 세 번째 가능성으로 우리가 지칭한 증거의 우수성 을 발견했습니다. 이 시스템에서 일반적으로 대회는 실제 대회의 상금을 흉내 낸, 대회 참가자의 실적을 기반으로 화폐주조 를 주기적으로 개최됩니다. 이 시스템은 인공 지능이 포함 된 게임을 능가 할 때뿐만 아니라 에너지를 소비하는 경향이 있지만, 그것은 에너지 소비의 다소 지능적인 양식을 제공하기 때문에 우리는 아직 이런상황에서도 흥미로운 개념을 발견했습니다.

결론

시장에서 우리의 디자인의 인증하에 우리는 지분증명 디자인이 에너지 소비의 의존도의 배제때문에,네트워크 보안 수준에서 낮은 인플레이션/낮은 거래 수수료를 달성함으로써 작업증명 디자인에 피어 투 피어 암호화 통화의 형태에 잠재적으로 더 경쟁적이라고 기대합니다.

감사의 글

테스트 및 다양한 네트워크 / 포크 관련 업무로 돕는 리처드 스미스 (Richard Smith) 에게 많은 감사를 드립니다.

우리는 그의 훌륭한 선구적인 작업이 우리의 마음을 열고 이렇게 가능한 프로젝트를 만든 나카 모토 사토시 (Nakamoto Satoshi) 와 비트 코인 개발자에게 감사의 말씀을

전합니다.

참조

Babaioff M. et al. (2011): On Bitcoin and red balloons. Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least

make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)