비트코인 크립톤

BTC eternity – Bitcoin Krypton

업데이트 없이 미래에도 지속 가능한 **P2P(**개인 대 개인**)** 전자화폐 시스템

사토시**.**케이

satoshi.k@bitcoinkrypton.org

www.bitcoinkrypton.org

초록**.**

“전적으로 P2P 버전인 전자 화폐(Electronic Cash)는 금융기관을 거치지 않고 한쪽에서 다른 쪽으로 직접 전달되는 온라인 결제(payments)를 실현한다. 전자 서명은 솔루션 일부를 제공하지만, 이중 지급(double-spending)을 막기 위해 여전히 신뢰받는 제3자(trusted third party)를 둬야 한다면 그 주된 이점을 잃는다. 우리는 P2P 네트워크를 사용해 이중 지급 문제를 해결하는 솔루션을 제안한다. 이 네트워크가 거래를 암호화한 타임스탬프를 일련의 해시 기반 작업증명(proof-of-work) 체인에 찍고, 이 작업증명을 재수행하지 않고서는 변경할 수 없는 기록을 생성한다. 가장 긴 체인은 목격된 사건의 순서를 증명하는 동시에 그게 가장 큰 CPU 파워 풀에서 비롯했음을 증명하는 역할을 한다. 이 네트워크를 공격하는 데 협력하지 않는 노드가 CPU 파워 대부분을 제어하는 한, 가장 긴 체인을 생성하며 공격자를 압도할 것이다. 이 네트워크 자체는 최소한의 구조만 요구한다. 메시지는 최선의 노력을 기반으로 전파되고, 노드는 네트워크를 마음대로 떠났다가 재합류할 수 있으며, 자신이 빠진 사이에 일어난 일의 증명으로 가장 긴 작업증명 체인을 받아들인다.”

위에 언급한 내용은 사토시 나카모토의 비트코인 백서 초록을 인용한 것이다.

오리지널 비트코인은 초록에서 작업증명을 통하여 신뢰받는 제3자 없는 전자화폐시스템을 구축하는 것을 목표로 하였음을 밝혔다.

오리지널 비트코인이 발표되고 15년이 지난 현재(2024년)를 기준으로 새롭게 업데이트된 비트코인

프로그램과 오리지널 프로그램간 호환이 제대로 되고 있지 않고 있는 사실을 확인하고, 그 문제로 인해 파생된 비트코인의 미래의 지속성의 문제를 제기하며, 해당 문제를 해결하기 위한 대안으로써 비트코인 오리지널의 목표에 부합하는 신뢰받는 제3자가 없이도, 미래의 어떤 시점이라도 업데이트가 없이 지속적으로 운영가능한 새로운 전자화폐 프로그램인 비트코인 크립톤을 발표하고자 한다.

0. 사토시 나카모토의 비트코인과 현재의 비트코인은 다르다**.**

비트코인은 2009년 1월 소스코드 배포와 동시에 시작된 프로그램이며, P2P 금융이다. 비트코인은 초기 의구심에도 불구하고, 세계 금융에서 중요한 자산으로 성장했고, 그 사용자와 전송량은 꾸준하게 늘어났다. 그 태생적인 한계인 블록당 1메가바이트의 제한은 블록당 대략 2,100 트랜잭션이 가능했고, 이런 제한적인 분산장부의 크기 안에서 경쟁시스템을 도입해서 보다 높은 수수료를 제시한 트랜잭션이 먼저 전송되도록 하고, 그렇지 못한 거래에 대해서는 Mempool 메모리공간에 남기도록 되어서, 네트워크의 이용량이 올라가면, 그만큼 수수료는 높아지도록 설계되어 있었다. 비트코인의 전송량 제한을 보다 획기적으로 개선할 수 있는 수많은 제안들 중에, 라이트닝 네트워크를 사용하는 SegWit업데이트는 블록의 트랜잭션을 기록할 때, 서명 부분과 데이터 부분을 분리해서, 서명 부분을 라이트닝 네트워크에 기록하고, 데이터 블록은 비트코인 네트워크에 기록하는 이원화된 방법을 제시하였으나, 초기에는 비트코인 채굴자 네트워크와 사용자 및 지지자 그룹은 세그윗의 도입에 반발이 있었음에도 시간이 지나면서, 효율성과 이익의 관점이 부각되고, 세그윗 업그레이드는 소프트 포킹(Soft forking)에 불과해서, 오리지널 비트코인 소스와 미래의 소스가 서로 호환되고 블록체인 데이터는 노드 간 싱크된다고 주장이 받아들여지면서, 2017년에 드디어 비트코인 오리지널 코드는 세그윗 업그레이드가 적용되게 되었다. 이로 인해, 비트코인 트랜잭션은 2배 정도 향상을 보이게 된다. 다만, 처음에 약속했던 오리지널 프로그램과 현재의 버전 간 호환이 되지 않음에도 불구하고, 누구도 해당 문제에 관심을 갖지 않는다.

현재 비트코인 네트워크는 위기에 봉착하였다. 사토시 나카모토는 사라졌고, 그의 비트코인 오리지널 프로그램은 더 이상 작동하지 않는다.

곰곰이 생각해 보면, 이것은(호환되지 않음) 비트코인의 블록체인의 가장 중대한 모순이며, 위협이다.

비트코인 개발자 집단은 비트코인의 전송속도와 Mempool에 적체된 거래 대기 트랜잭션의 해소를 위한

방법의 일환으로 SegWit방식과 SegWit2X의 두 가지 방식을 제안했다. 물론, 세그위트(SegWit)의 적용이 완료된 2017년 이후에도 메모리풀에 적체된 대기 트랜잭션의 문제는 해결되지 않았다.

전자인 SegWit방식은 소프트포킹(Soft Forking) 방식으로 1MB의 블록용량을 물리적으로 늘리는 것이 아니라, 서명부분과 데이터 부분을 나누어, 실질적으로는 4MB의 블록용량의 증가를 기대할 수 있지만, 과거의 버전(사토시의 비트코인 프로그램)과 완벽하게 호환될 수 있다는 제안이었고, 반면에 SegWit2X 방식은 블록용량을 2MB로 올리고, 많은 부분을 개선해서, 완전히 다른 새로운 블록체인으로 분기되는 하드포킹(Hard Forking)이라는 제안이었다. 당연히 대다수 유저들은 사토시 나카모토의 블록체인의 정체성을 훼손하지 않고, 속도의 개선과 보안성이 개선되고, 여러 버그가 해결되고, 특히나 TPS가 4배나 향상되며, 전송비용이 절감되는 소프트포킹의 과거와 호환이 완벽하게 되는 완벽한 업그레이드에 대해서 기대했을 것이다. 그러나, 실상은 소프트포킹은 실패하였음을 아는 사람은 그리 많지 않다. (해당 담론에 대한 증명은 본 문서 말미 5번 항목에 추가하였다)

숫자 21은 사토시 나카모토가 심어놓은 이스터 애그(Easter Egg)와 같다. 총량은 2,100만 코인이고, 21만 블록마다 반감기에 도달하게 되며, 하나의 블록은 2,100개의 트랜잭션이 가능하도록 하였고, 2021년 이후 추가로 21번의 반감기가 도달하면, 블록체인의 보상은 0에 수렴하도록 설계하였다.
반감기의 보상이 사토시 단위의 보상에 도달하게 되면, 더 이상 비트코인은 반감기로 쪼개지지 않는다.

지금으로부터 80년이 지난 뒤, 비트코인 반감기 보상은 더 이상 실시되지 않는다. 다만, 비트코인은 블록당 전송 수수료 총합을 작업증명의 참여자에게 추가로 보상하도록 설계한바 비트코인은 반감기가 끝나도 유지할 수 있도록 초기버전의 비트코인 프로그램을 고안하였다.

따라서, 시대에 맞는 적당한 수수료의 책정은 비트코인 네트워크의 지속적인 유지를 위 해 매우 중요하고, SegWit의 적용으로 수수료가 낮아지게 되면, 원래의 비트코인 네트워 크의 지속적인 유지를 불가능하게 할 수 있다는 것을 간과해서는 안된다. https://Mempool.space의 데이터를 참고하면, 수수료 보상은 0~0.3 BTC로 매우 가변적 이다. 경우에 따라 수수료 보상이 없는 제로 리워드(Zero Rewards)의 상황이 발생하기도 한다.

비트코인의 가치와 신용이 유지되는 이유는 비트코인의 존재가 내포한 불변한다는 믿음에서 기인하다. 2100만개의 총채굴량이 유지된다는 믿음, 블록체인 기술을 활용해서 분산장부를 통한 위변조가

불가능하다는 믿음, 탈중화되어 외부의 누군가에 의해서 비트코인 네트워크가 사라질 위험이 없다는 확신은 비트코인을 지구상에 존재하는 가장 가치있는 자산이 되게 한다.

만약, 비트코인의 미래의 어떤 개발자가 기존의 믿음을 져버리고, 2100만개의 총발행량을 뛰어넘어 발행하게 되거나, 효율성 혹은 혁신이라는 이름으로 비트코인이 가지고 있는 규칙들을 변경한다면, 경우에 따라 비트코인의 가치는 우리가 생각하지 못하는 방향으로 흘러갈수 있다.

이미, 비트코인은 세그윗업데이트를 통해, 기존의 일원화된 분산장부를 데이터와 싸인부분을 나누는 이원화된 분산장부시스템을 이용하고 있다.

비트코인이 영원한 가치를 지니는 금이나, 다이아몬드의 속성을 디지털에서 구현했다는 대중들의 믿음을 져버리는 중대한 사건임을 인지해야 한다.

1. 업데이트 없이 지속 가능한

비트코인 크립톤은 사토시 나카모토의 비트코인의 설계 목적인 신뢰받는 제3자의 개입 없이 오로지 개인과 개인 간의 전자화폐시스템을 온전하게 계승하는 목적으로 제시된 프로젝트이다.

비트코인 크립톤은 업데이트 없이 미래에도 지속적으로 운영가능한 P2P 전자화폐 프로그램으로 개발되었다. 다만, 비트코인 크립톤의 오리지널 버전은 오픈소스 프로그램을 참고하거나 모방 혹은 변경하여 만들었고, 본 프로그램의 완성 후 충분한 테스트를 실시하였음에도 온전하게 신뢰하여서는 안된다. 이는 알 수 없는 버그나 에러가 발생할 수 있음을 뜻한다. 임의의 개발자들에 의해 성능이 개선되고 오류가 수정되며 효율화 과정을 통한 업그레이드가 가능하지만, 비트코인 크립톤의 오리지널 버전 프로그램과 상위버젼 프로그램은 호환이 가능해야 한다.

2. 비트코인의 반감기와 블록주기

비트코인은 총 2,100만 개의 총통화량을 가지고, 10분당 1블록을 채굴하도록 설계되어 있다. 21만블록마다 반감기에 도달하게 되며, 21만 블록은 시간으로 4년이라는 기간을 가지게 된다. 초기에 블록당 50비트코인의 채굴보상으로 설계되어, 현재 84만 블록이 지나간 후에는 4번의 반감기를 맞이하였고, 그로 인해 현재 블록당 3.125코인 보상된다.

블록 주기는 작업증명에 대한 노드기록의 오류방지를 위해 브로드캐스팅에 필요한 네트워크 간 최소한의

필요시간으로 설정한다면, 여러 가지 변수를 고려해야 한다. 인터넷의 허용 대기 시간 등을 고려하여 볼 때, 시간이 길면 길수록 오류는 적어진다. 다만, 작업 증명의 최소한의 시간은 3초보다 짧아서는 안된다. 비트코인은 충분한 블록당 검증시간을 10분으로 설정하여, 오류의 가능성은 줄이게 되지만, 자산을 전달하는 시간이 인간의 생활패턴에 맞지 않도록 설정되어 있다. 인간이 느끼는 가장 편안한 시간은 블록당 10분 단위보다는 블록 당 1분 이내 시간이 적절할 것이라 생각된다. 경험적으로 미루어 봤을때, 비트코인의 블록주기가 10초이내가 된다면 매우 편리해 질것이 분명하다. 다만, 블록주기가 1초이하로 설정될 필요는 없다. 1초라는 시간은 인간이 물리적으로 체감하는 시간의 최소 단위로 오랜 기간 인간의 몸에 체화 되어 왔고, 초단위보다 작은 단위의 블록체인은 인간을 위한 블록체인이 아니며, 이를 운영하기 위해서는 엄청난 운용비용이 발생하게 되어 블록체인의 익명성과 탈중앙화를 이룰 수 없게 한다. 따라서 비트코인 크립톤은 3초의 블록을 유지하고, 가정용 컴퓨터에서 충분하게 풀노드가 운영될 수 있는 환경을 통해 누구라도 분산장부를 가용할 수 있도록 고안 계획되었음을 밝힌다. 블록주기가 3초정도라면, 인간의 기준에서 느리거나 불편함을 느끼지 않을 것이라 확신한다.

블록 보상에 대한 4년주기의 반감기는 비트 코인 블록체인을 유지하기 위한 동기를 제공하는 분명한 요소이지만, 한편으로는 작업 증명에 참여자들에게는 모험이다. 작업증명에 참여하기 위해서는 먼저 그 행위에 대한 채산성을 따져서 참여하여야 하기 때문에 그 행위의 참여자들은 최소한 참가에 대한 수익성이 보장되지 않는다면, 작업증명에 선뜻 참여를 하지 않게 될 것이다. 그것은 비트코인의 미래의 지속성에 대한 의심을 가지게 할 것이다. 비트코인의 미래에 대한 지속성을 담보하기 위해서는 비트코인의 높은 수수료는 필수 요소이다. 사토시 나카모토의 비트코인 오리지널 소스코드에 의해 제시된 비트코인의 전송 수수료의 블록당 총합 만큼 소각되고, 소각된 만큼 작업증명의 참여자에게 보상하는 시스템의 가장 중요한 요소이다.

따라서, SegWit의 목표인 블록당 더 많은 트랜젝션과 더 낮은 전송 수수료는 먼저 비트코인의 단일 블록체인의 신뢰성을 무너뜨릴 수 있고, 그들이 제시하는 낮은 수수료는 미래의 비트코인 블록체인의 지속적인 유지가 가능한가에 대한 의구심을 가지게 한다.

비트코인 크립톤은 이런 의구심을 해소하고 미래에도 지속가능하며, 지속적인 작업증명 참여 동기를 부여하기 위해서, 블록주기, 반감기, 총보상의 합계 등의 여러 요소를 고려하여 프로그램에 적용하였다.

이를 위해서, 11 데시말(소수점 11자리)까지 표현 가능하도록 설계하였고, 전송 수수료는 보상의 범위와 비교하여 낮아지게 하여 3번의 반감기마다 10분의 1만큼 수수료가 줄어들도록 하였다.

이는 비트코인의 소수점 8자리까지 계산 가능한 것에 비해 1000배 작은 단위까지 계산할 수 있지만, 비트코인의 자료형 unit64를 사용하여 블록당 데이터의 효율성을 높였다.

(참고로 1Satoshi는 1,000 Krypton으로 하나의 단위를 추가로 생성했다.)

비트코인 크립톤은 1번블록부터 1백만 블록까지 3초의 블록주기로 빠른 테스트하게 된다. 1,000,001블록 이후에는 소스코드와 프로그램을 공개하게 되며, 블록주기는 63초로 , 210만블록까지 유지된다. 1번블록부터 210만 블록까지 1블록당 5코인의 보상이 주어지게 되며, 이후 210만 블록마다 3초씩 블록주기가 줄어들게 되며, 21번째 반감기에는 블록주기가 3초로 줄어들게 된다.

비트코인 크립톤의 총통화량은 2,100만 개인 비트코인과 동일하지만, 이더리움 주소규칙으로 변경하여 이더리움의 디앱들(Dapp)과 호환되도록 설계하였다.

비트코인 크립톤은 기존의 비트코인 방식인 Mempool을 이용하여 높은 수수료에 따른 경쟁방식을 도입하지 않으며, 각 트랜잭션이 사용하는 실질 사용량에 따른 데이터의 무게만큼 수수료로 사용하도록 계획하였고, 210만 블록의 3 배수인 630만 블록마다 1/10만큼 수수료율이 줄도록 설계하였고, 21번의 반감기 이후 더 이상의 반감기는 없도록 설계하였고, 3초당 수수료의 단위 무게당 비용은 고정되도록 설계하였으며, 초기 블록당 100kb를 사용하도록 제한되어 있으나, 2,100만 블록마다 블록당 100kb씩 증가하도록 설계하였다.

3. 블록체인 노드의 데이터 증가량 전송속도 그리고 탈중앙화

비트코인노드는 3년마다 대략 100GB의 풀노드(Full node) 저장공간을 사용하며, 2024년 6월 5일 기준 577GB 노드저장 공간이 필요하다.

반면, 이더리움 메인넷은 2024년 6월 5일 기준으로 풀노드 저장공간은 18.195TB이며, 매년 5TB 이상이 노드에 추가되어야 한다.

이더리움 2의 업데이트는 2022년 9월에 더 머지(The Merge) 업데이트로 명명되어 기존의 작업증명 방식(POW)에서 지분증명 방식(POS)으로 전환됨을 의미하고, 이로 인해 급격하게 이더리움 네트워크의

사용량이 늘어나게 되었다.

이더리움의 덴쿤 업그레이드(EIP-4844 ,2024년 3월 13일)의 적용으로 이더리움 수수료율은 최대 1/60 정도 줄어들었고, 평균적으로 75% 이상 줄었다. 이로써 보다 많은 이용자들이 이더리움 네트워크를 통한 스마트컨트랙트 및 DAPP의 개발 및 이용에 따른 자금부담이 줄게 된다. 이에 따라 이더리움의 최대 문제는 사용량에 따른 노드의 물리적 하드디스크의 증가문제이고, 이것을 조금이나마 경감시키고자 실시하는 버클트리(Verkle Tree) 업그레이드는 스테이킹 데이터를 저장하는 디스크 공간을 효율적으로 관리해서, 그 용량을 줄이고자 하는 노력임에도 불구하고, 데이터에 사용되는 절대적인 디스크 공간은 지속적으로 증가하게 될것으로 예상된다.

이더리움 관련 개발자들이 날이 갈수록 풀노드를 직접 운영하기 어렵게 될 것이고, 노드의 숫자는 지금보다 줄어들 수밖에 없을 것으로 예상된다. 이는 시간이 흐름에 따라, 블록체인은 분산장부가 아닌 중앙화로 분산장부에서 중앙장부로 변할 수밖에 없는 구조적 문제를 가지고 있음을 증거 한다.

비트코인 크립톤은 블록당 사이즈는 100kb에서 시작하며, 풀노드가 사용하는 저장공간은 점진적으로 늘어난다. 1년 동안 예상가능한 사용되는 디스크 용량은 30GB~ 50GB로 예상되며, 평균적으로 년간 5% 정도 블록의 데이터 늘어나도 문제가 없도록 설계가 되었다. 이는 현재의 기술의 기준으로 저장장치의 가격이 GB당 10% 이상 감소하는 것에 비교하여, 미래에도 지속가능 하도록 유지 비용을 고려하였다.

4. 비트코인 크립톤의 목적

비트코인 크립톤의 목적은 제3자의 개입 없는 온전한 익명성을 추구하는 개인간 P2P 금융 프로그램으로써 미래의 작업증명 참여자들에 대한 유효한 보상체계를 유지하고, 이미 공개된 오리지널 프로그램과 미래의 개선 버젼이 호환되도록 하는 것이다.

비록 2024년 비트코인 크립톤이 특정 집단과 개발자에 의해서 개발되었음에도 불구하고, 발표 후에 특정기간이 지나면, 초기개발자 및 초기에 지정된 사토시케이의 임무는 종료되며, 익명의 대체자인 새로운 사토시케이에게 모든 권한(도메인의 관리, 오픈소스의 관리, 이메일의 관리 및 초기 채굴자산의 관리)이 위임되고, 초기 개발자 집단은 2024년을 12월 31일 이전에 해산한다.

비트코인 크립톤은 어떤 자산의 가치로 보장하지 않을 뿐만 아니라, 미래의 존속여부, 상장, 비전, 계획 커뮤니티의 운영 등에 대한 계획도 존재 하지 않는다.

비트코인 크립톤 네트워크는 공식적으로 어느 개인이나 집단에 존속되거나 귀속되지 않는다. 누구나 원하면, 비트코인 크립톤을 상장하는 것도 가능하고, 누구나 마음대로 그 이름을 사용할 수 있다. 다만, 사용 시 어떤 권리를 주장해서도 안되며, 공식적인 직함이나 이름을 사용하여도 안된다. 상장조건을 만족시기키 위해서, 일반적인 거래소에서 요구하는 기본 문서에 요구사항인 공식적인 주체, 멤버, 기관, 커뮤니티에 내용을 임의로 기재하여서는 안된다.

비트코인 크립톤의 오리지널 개발자 및 그 개발에 역할을 담당했던 이들은 향후 비트코인 크립톤으로 발생할 모든 결과에 대한 어떠한 법률적 경제적 책임도 지지 않는다.

다만, satoshi.k@bitcoinkrypton.org의 메일을 통해 새로운 아이디어, 제안, 신규 개발에 대한 논의, 새로운 소스 코드 등에 대한 검증 및 인증 등을 논의할 수 있다. 회신을 보장할 수 없지만, 욕설이나 스팸 혹은 사기 메일이 아닌 우호적이고, 예의를 갖춘 글이라면, 긍정적으로 검토하여 회신을 할 수도 있다.

5. 사토시 나카모토 비트코인 소스코드에 대한 실험

비트코인 오리지널 소스코드 Bitcoin-V0.1은 2008년 11월 1일 토요일 사토시 나카모토에 의해 작성된 비트코인백서(bitcoin.pdf (md5sum d56d71ecadf2137be09d8b1d35c6c042))를 근거로 하여, 2009년 1월 8일 14:27:40(EST)에 정식 공개버전이 공개되었으며, 그전인 2008년 11월 16일에 비공개버전이 출시되었다.

해당 버전은 비트코인의 현재 소스코드 공개주소(https://github.com/bitcoin/bitcoin)가 아닌, 다른 공개주소(https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html)에 공개되었다.

SegWit에 대해서, 현재의 개발자 집단들이 주장하는 소프트포킹에 대한 거짓 주장에 대해 반박하고자 직접 실험을 실시하였다.

먼저, metzdowd.com에서 구한 소스코드를 컴파일하여, 실행한 결과 브로드캐스팅을 위한 최신의 노드들을 찾을 수 없고, 노드들과 싱크가 되는 것이 불가능했기 때문에 이에 대한 실험은 무의미했다. 실행 후 결과에서 “Not Connected” 에러만 호출되었다. 여러 테스트를 통해 알게 된 것은 여러 노드를 연결하기 위한 브로드캐스팅 주소가 현재는 작동하지 않고, 이것에 대한 IRC주소가 더 이상 존재하지

않기 때문인 것으로 추정된다.

비트코인의 기트허브(github) 공식계정은 어떤 이유에서인지 24.x 가 가장 오래된 버전이었고,

최신버전은 27.x버전이었다.

다음으로 테스트를 실시한 소스코드는 bitcoinv0.3이다.

124,276블록에서 더 이상 노드 싱크가 되지 않으며, 출력된 메시지는 아래와 같다.

```
ERROR: ConnectInputs() : fb0a1d8d34 VerifySignature failed
InvalidChainFound: invalid block=0000000000004939267f
height=124276  work=6613870563198902508
```

V0.4와 v0.5에서는 258,354블록에서 싱크를 할 수 없으며, 아래의 메시지를 출력한다.

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessage()

ProcessMessage(block, 901212 bytes) FAILED
received block 000000000000023e872
REORGANIZE
```

V0.6 버전은 364,670블록에서 더 이상 싱크를 할 수 없으며, 아래의 메시지를 출력한다.

```
EXCEPTION: 11DbException
Db::put: Cannot allocate memory
bitcoin in ProcessMessages()

ProcessMessage(block, 999787 bytes) FAILED
received block 00000000000000001d3
```

V0.7 버전은 364,671블록부터 더 이상 싱크를 할 수 없으며, 아래의 메시지를 출력한다.

```
received block 0000000000000000221
ERROR: ConnectBlock() : UpdateTxIndex failed
InvalidChainFound: invalid block=0000000000000000221  height=364671
ERROR: SetBestChain() : SetBestChainInner failed
ERROR: AcceptBlock() : AddToBlockIndex failed
ERROR: ProcessBlock() : AcceptBlock FAILED
```

모든 에러의 원인은 동일하다고 판단된다. 블록을 데이터와 서명 부분으로 나누면서, SegWit을 적용한 최신노드들과 과거의 노드들의 알 수 없는 여러 원인에 의한 충돌로 의심해 볼 수 있다. 즉, 소프트 포킹으로 과거의 프로그램과 현재의 프로그램이 서로 호환될 수 있다는 명제가 실질적으로 깨졌다는 것을 명확하게 알 수 있었다.

6. 크립톤**(Krypton)**

크립톤은 화학 원소로 기호는 Kr이고 원자 번호는 36이다. 무색, 무취, 무미의 비활성 기체로 대기 중에 미량이 존재하며, 액체 공기를 분별 증류하여 얻는다. 1898년 영국의 윌리엄 램지에 의해 처음 발견되었다.

헬륨과 아르곤을 발견한 램지는 그 두 개의 원자량 4와 40 사이에 위치하는 비활성기체를 찾기 시작했다. 1898년. 그들은 소량의 액체공기를 붉게 달군 구리와 마그네슘에 흘려서 증류했고, 녹색의 새로운 원소를 발견했다. 이 녹색의 원소는 다른 비활성기체에 비해 발견이 곤란했기 때문에 그리스어로 '숨겨진 것'이라는 뜻의 '크립톤'이란 이름을 붙였다.

비활성기체인 헬륨과는 반대로 고에너지 물질의 분자를 느린 이동속도로 변경시켜 주는 특성으로, 크립톤 가스를 들여 마시게 되면, 헬륨가스를 들여마신 것과는 반대로 낮은 저음의 음파를 가진 목소리를 만들어 낸다.

영화 슈퍼맨을 보게 되면 가상의 물질인 크립토나이트를 슈퍼맨의 약점으로 사용하게 되는데 이는 크립톤을 따서 만든 상상 속의 물질이다.

비트코인 크립톤은 채굴(작업증명)에 있어서, ASIC칩등의 비정상적인 접근을 약화시키는 의미로써 CPU기반의 채굴을 옹호하며, 웹기반 원클릭채굴 방식을 도입하여 누구나 쉽게 작업증명에 참여할 수

있도록 하였다.

뿐만 아니라, 오리지널 비트코인 프로그램의 최소단위인 사토시(소수점 8자리) 자리를 보다 세분하여, 크립톤(소수점 11자리)자리로 확장하였다. 다시 말해서, 1kr(Krypton)은 0.00000000001BTCK이고, 1,000kr은 1satoshi이다. 즉, 1BTCK는 1억 사토시 혹은 1,000억 크립톤으로 표현할 수 있다.

비트코인 크립톤은 21번의 반감기와 7번의 수수료 인하를 거치면서, 사토시이하의 수수료가 필요해지게 되며, 이를 원활하게 실행하기 위해 크립톤이라는 단위를 비트코인 네트워크에 도입하였다.

비트코인 크립톤의 실행 프로그램의 자료형을 unit64로 정하게 되면, 최대 2,100만 개의 총 통화량과 소수점 최대 11자리까지 연산이 가능하게 된다. 이에 블록의 사이즈는 unit128의 자료형을 사용하는 것보다 효과적으로 줄일 수 있게 된다.

7. 사라져야 한다**.**

비트코인 크립톤이 목표하는 바는 완전한 탈중앙화이며, 그 탈중앙화의 마지막은 비트코인 크립톤을 관리하는 주체가 사라짐을 의미한다.

해당 주제는 비트코인 크립톤이 가진 숙명이고, 비트코인 크립톤이 다름을 증명하는 과정이다.비트코인 크립톤의 노드는 소스코드내의 Seed node의 연결 및 탐색에서 부터 시작한다.

Seed node의 연결은 비트코인 크립톤 세계관을 거미망 처럼 연결하는 과정이고, Seed node는 지속적으로 추가되고, 업데이트 되어야하며, 이것은 비트코인 크립톤의 생명력에 영향을 미친다.

이것에 생명력을 부여하기 위해, 바이러스처럼 대중적으로 퍼져나가게 하기 위한 절차로써, 비트코인 크립톤에 특별한 절차를 고안하였다. Seed Node는 어떤 노드라도 가능하기때문에 해당 노드의 정보를 제공하는 정보제공자에게 특별한 보상을 제공하는 것으로 초기 Seed Node는 퍼져나가도록 설계하였다.

보상의 제공방법은 정보로 제공된 Seed Node의 상태 즉, 서버의 유지능력을 수치화하여, 점수화하고, 그 점수에 따라 매달 차별적으로 보상을 제공하게 된다.

이후 비트코인 크립톤의 Seed node가 충분하게 공급되면, 이후에는 충분한 Seed에 의해 안정적인 탈중앙화된 네트워크가 유지될 것이라 확신한다.

BITCOIN KRYPTON