목차

I. 초록

Epic Cash는 개인 금융 시스템의 초석인 진정한 P2P 인터넷 캐시를 향한 여정의 최종점입니다. Epic 통화는 세계에서 가장 효율적인 개인 정보 보호 형태의 디지털 통화를 목표로 합니다. 그 목표를 달성하기 위해, 돈의 세 가지 기본 기능을 만족합니다:

1. **가치의 저장** – 저장, 되찾기, 교환이 추후 가능하며, 되찾을 시 가치의 예상이 가능;
2. **교환의 수단** – 가치의 기준이나 상품 및 서비스에 대해 교환 가능한 것으로 받아들여지는 것;
3. **회계의 단위** – 그것이 차지하고 비교되는 가치의 단위.

	$ USD	BTC	EPIC
가치의 저장	✗	✓	✓
교환의 수단	✓	✗	✓
회계의 단위	✓	✗	✓

2009년 비트코인은 다른 암호화폐가 평가되는 것과 대조적인 세 가지 결정적인 특징과 함께 첫 번째 블록체인–기반 디지털 화폐로 부상하였습니다:

- **신뢰할 필요 없음** – 네트워크가 작동하기 위해 중앙형 독립체나 상대 당사자 아무도 신뢰하지 않아도 됩니다.
- **불변성** – 트랜잭션이 취소될 수 없습니다;
  a. 내력을 다시 작성하는 것이 매우 어렵거나 거의 가능하지 않아야 함;
  b. 프라이빗 키의 보유자를 제외하고는 관련 자금을 움직이는 것이 불가능해야 함;
  c. 모든 트랜잭션이 블록체인에 기록됨.
- **분산화** – "블록체인은 정치적으로 분산화 되어있으며 (아무도 제어하지 않음) 구조적으로 분산화 되어있고 (인프라적 실패 지점 없음)..."[1].

비트코인은 통화 정책의 구조에서 오랜 테스트를 거친 기초를 고수하면서 기술적으로 새로운 길을 만들어 냈습니다. 비트코인의 성공은 신뢰할 필요가 없고 불변하며 분산된 블록체인과 결합된 제한된 공급량과 강하게 관련됩니다. Epic Cash는 Epic 통화가 효과적인 가치 창출을 보장할 수 있도록 비트코인의 인플레이션 감소 및 공급 제한 정책을 모방합니다.

비트코인의 성공에도 불구하고 10년 전의 시작 이후 몇 가지 단점이 드러났습니다. 다른 프로젝트는 이러한 단점을 극복하기 위해 노력해왔으며, 저희는 이러한 단점을 최우선적으로 조사하여 시작점으로 삼았습니다. 저희는 어렵게 얻은 목표를 완벽히 하기 위해 Grin 코드베이스와 여러 다른 프로젝트의 탁월한 성과를 활용하기 결정하였으며 Epic Cash 전임자들의 단점을 발견했습니다. Epic Cash는 이상적인 통화가 될 수 있는 주요 특징을 가지고 있습니다:

- **대체 가능** – Epic의 주어진 단위의 가치는 항상 1엔 또는 위안과 같이 항상 다른 엔 또는 위안과 동일하고 교체 가능한 것처럼 Epic의 다른 단위와 동일해야 합니다. 대체로 기능성의 성취는 개인 정보 보호에 달려있습니다.
- **개인 정보 보호** – Epic Cash 블록체인은 거래의 세부 사항을 제3자로부터 보호하여 Epic 보유자 및 사용자의 익명성을 보호하며 추적할 수 없고 감시로부터 보이지 않도록 설계되었습니다.
- **확장성** – Epic Cash는 자원 집약적인 장비 없이 새로운 노드를 쉽게 설치할 수 있는 공간 효율적인 블록체인을 유지합니다. Epic Cash 블록체인은 비트코인 처리량의 최소 두 배 이상을 처리할 수 있습니다.
- **속도** – Epic Cash 트랜잭션은 부드럽고 연속적이며 이전 세대의 블록체인 기술보다 훨씬 빠르게 실행됩니다. 비트코인은 완전한 트랜잭션 확인을 위해 10-분 블록 6개가 필요한 데 반하여 Epic 트랜잭션은 1-분 블록이 채굴되자마자 단일 블록 확인 내에 발생합니다.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. 개인 정보 보호

현대의 돈 사용은 사람들과 기관들 간의 계정 단위의 집단적 이전으로 이해될 수 있습니다. 특정 시점에서 돈의 경관은 다음 질문에 대답하여 매핑 할 수 있습니다:

1. *누가 보유하고 있으며, 그들은 얼마를 보유하고 있는가?*
2. *누가 누구와 거래를 하고 있으며, 얼마에 하고 있는가?*

전통적인 피아트 통화 그리고 실제로 비트코인에 대해서도 저희는 그러한 질문에 답할 수 있습니다. 그렇게 함으로써 소비 패턴, 소유권 및 거래 상대방과 같은 사람들의 삶에 대한 많은 것이 드러날 수 있습니다. 가치 이전을 추적함으로써 개인의 관심과 의도에 대해 상당히 정확한 결론을 도출할 수 있습니다. 개인 정보 보호가 없으면 거래 데이터는 포식적인 제 3자의 손에서의 위험한 정보가 될 수 있습니다.

지난 10년간의 암호화폐 사용은 다양한 블록체인 구현에서 "개인 정보"의 연속성을 보여줍니다. 개인 정보 규모는 공개적이고 악명 높은 것에서부터 익명까지로 간주됩니다. 개인 정보가 침식됨에 따라 암호화폐의 핵심 초석인, "신뢰할 필요 없음"이 저하됩니다. 비트코인 블록체인 분석 서비스의 성공 사례에서 볼 수 있듯이 비트코인은 개인 정보 스펙트럼의 악명 높은 투명한 끝 부분에 더 많이 위치합니다. 사용자는 부패한 비트코인에서 거래를 우연히 처리하지 않도록 조치를 취해야 합니다. Epic Cash 솔루션은 바늘을 익명을 향하여 움직여 개인의 개인 정보 보호와 거래의 개인 정보 보호가 기본 수준에서 시스템으로 설계되도록 보장하여 필수 속성을 복원합니다.

신원의 개인 정보 보호

트랜잭션의 개인 정보 보호

신원의 개인 정보 보호

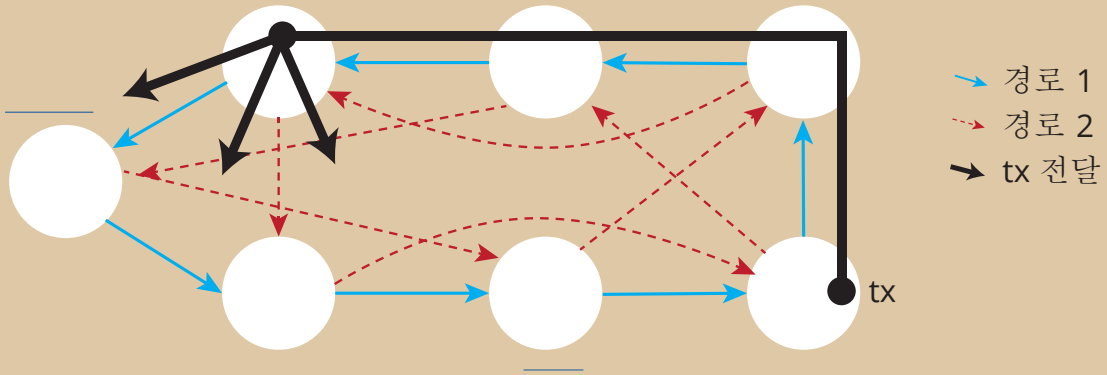
비트코인과 같은 대부분의 암호화폐는 지갑의 프라이빗 키에서 파생된 퍼블릭 키를 나타내는 주소의 지갑에 저장됩니다. 이 주소는 디지털 세계에서 사설 금고의 위치 정보로 간주될 수 있습니다. Epic Cash 블록체인은 주소를 완전히 제거하고 대신 모든 공개 키와 프라이빗 키가 일회용으로 생성되는 하나의 거대한 다중 서명을 적용합니다.

비트코인 지갑 주소는 디지털 세계에서 금고의 위치 탐지기이므로 해당 지갑은 지정된 시점의 고유한 위치에 있는 컴퓨터에 소유자를 고정시키는 소유자의 인터넷 프로토콜 (IP) 주소로 추적될 수 있습니다. 간단히 설명하면: 비트코인 트랜잭션이 발생하면 트랜잭션이 '노드'라는 통신 허브에서 알려지고 '피어'라는 다른 노드로 전달됩니다. 그런 다음 해당 정보는 전체 네트워크에서 연속적으로 각 노드의 피어로 빠르게 퍼집니다. 이 과정은 "가십 프로토콜"이라고 적절하게 명명됩니다. 간단히 말하면, 각 비트코인은 보이는 온라인 위치와 비트코인 또는 그 소유자가 있는 실제 위치를 가집니다. 저널리스트인 Grace Caffyn은 비트코인은 "가정용 인터넷 연결을 통한 구글 검색보다도 비밀이 없다"고 지적했습니다.[2]

Epic Cash 블록체인은 지갑 주소를 제거하는 것 외에도 IP 주소를 추적할 수 없도록 함으로써 신원 정보의 개인 정보 보호를 보장합니다. 이것은 Dandelion++ 프로토콜의 통합을 통해 이를 수행합니다. Dandelion++ 프로토콜은 이전의 민들레 프로토콜 (Dandelion Protocol)을 개선하여 7 명의 연구자가 블록체인에 대한 비명탄 공격을 막을 수있는 지속적인 노력의 결과입니다. Dandelion ++를 통해 트랜잭션은 임의의 얽힌 경로 또는 '케이블'을 통해 전달된 다음 줄기에서 날아갈 때 민들레 꽃의 꼬투리처럼 큰 노드 네트워크로 갑자기 확산됩니다 (수치 1). 따라서 원래의 IP 주소로 트랜잭션을 추적하는 것을 거의 불가능하게 만듭니다.

수치 1: Dandelion++ 프로토콜을 통한 트랜잭션 익명화.

Dandelion++는 4-정규 그래프에서 두 개의 얽힌 경로 중 하나를 통해 메시지를 전달한 다음 확산을 사용하여 알립니다. 그림에서 트랜잭션은 파랑색의 견고한 경로를 통해 전달됩니다[3]. 이 가정은 트랜잭션을 소스로 추적하기 매우 어렵게 만들어 개인 정보를 보호해 줍니다.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

트랜잭션의 개인 정보 보호 ㅇ는ㅇ

Epic Cash 블록체인은 금액과 거래의 발신자-수신자 관계를 모호하게 하여 거래 개인 정보 보호를 보장합니다. 이는 Gregory Maxwell (비트코인 코어 개발자, Blockstream 공동 창립자 및 CTO)이 개발한 ***Confidential Transactions (CT)***[4]와 ***CoinJoin***[5]의 친숙한 아이디어를 적용하여 얻어졌습니다.

Adam Back이 처음에 만들고 나중에 Maxwell에 의해 개선된 CT는 암호화된 정보를 먼저 해독하지 않고 개인 정보를 보호하기 위해 암호화된 정보를 계산하는 방법인 동종 암호화를 통해 트랜잭션을 더 작은 부분으로 나누는 방식으로 작동합니다. 일단 분할되면 관찰자는 임의의 숫자를 트랜잭션 조각의 혼합으로 내는 해당 조각의 값을 숨기는 시스템인 블라인딩 팩터로 인해 트랜잭션의 실제 금액을 볼 수 없습니다. 궁극적으로, 거래 당사자만이 거래의 가치를 알고 있으며, 트랜잭션은 네트워크에 의해 확인되고, 출력 값의 합이 입력 값의 합과 같고, 출력 블라인딩 팩터의 합은 입력 블라인딩 팩터의 합과 동일합니다.

무단으로 보는 작업을 더욱 복잡하게 하기 위해 모든 Epic Cash 거래는 CT로 클로킹되고 거래 당사자 간의 연결을 숨기기 위해 함께 혼합됩니다. 이는 Maxwell의 두 번째 개념인 CoinJoin을 통해 수행됩니다.

CoinJoin을 간단하게 설명하기 위해 A, B 및 C가 각각 Epic을 X, Y 및 Z로 EPIC을 전송한다고 가정하십시오. CoinJoin 매체를 통해 보내고 아는 것은 A, B, C가 전송되고 X, Y, Z가 수신되는 것이며 거래 금액은 보이지 않습니다. CoinJoin 시스템은 블록 내부의 모든 트랜잭션을 단일 트랜잭션으로 결합하는 One-Way Aggregate Signatures (OWAS)를 통해 Epic Cash의 기본 요소가 됩니다.

개인 정보 보호: 요약

Epic Cash 블록체인은 개인과 그들의 트랜잭션의 개인 정보를 다음을 통해 보호합니다:

- **지갑 주소 제거 – 블록체인에는 디지털 금고에 대한 위치 식별자가 없습니다. 트랜잭션은 개인-개인, 지갑-지갑으로 구성됩니다;**
- **Dandelion++ 프로토콜 – 거래 발신자의 IP 주소에서 트랜잭션의 디지털 경로를 모호하게 합니다;**
- **기밀 트랜잭션 – 트랜잭션을 여러 조각으로 나누고 그 조각의 수집에 블라인딩 팩터를 도입하여 조각의 값과 다른 트랜잭션 매개변수를 알 수 없습니다.**
- **CoinJoin – 거래를 묶음으로 결합하여 거래 당사자 간의 관계를 숨깁니다.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. 기능성

라이트 코인의 창시자인 Charlie Lee는 비트코인과 라이트 코인에서 누락된 건전화폐의 기능성만이 유일한 재산이라고 말하면서 개인 정보 보호와 기능성이 그 코인의 다음 전장임을 시인했습니다[6]. 세계 최고의 블록체인 전문가 중 한 명인 Andreas Antonopoulos는 "... 부패된 코인은 파괴적이다. 당신이 기능과 개인 정보 보호를 깬다면 당신은 통화를 깨는 것이다."라고 주장합니다.[7]

기능성은 해당 세트의 개별 단위가 동일한 가치를 가지고 상호 교환 가능하도록 보장하는 상품 또는 자산 세트의 재산입니다. 이는 초기 형태의 통화를 이전의 물물 교환 시스템과 차별화하는 것입니다. 돈의 가능성에 대한 확신이 없이, 그 돈은 그 유용성을 빠르게 상실합니다. 아래에 설명되는 것처럼 대부분의 암호화폐의 가능성은 확실하지 않지만 Epic Cash의 개인 정보 보호 아키텍처는 동일한 위협에 대해 불침투성을 보장합니다.

비트코인과 유사한 대부분의 암호화폐는 존재하는 투명한 블록체인의 특성상 보관된 모든 지갑을 통해 확인할 수 있습니다. 개인 제 3자와 정부는 모두 이전 활동에 사용된 코인을 신속하게 식별하는 점점 더 정교한 수단으로 비트코인 블록체인을 모니터링합니다. 이는 자연스럽게 부패된 코인의 트랜잭션이 금지되어 이후의 선의의 소유자가 손실을 입을 수 있다는 우려로 이어집니다.

2018년 3월 19일, 미국 해외 자산 관리국 (OFAC) 은 미국인 또는 사업의 거래가 금지된 단체인 Specially Designated Nationals (SDNs), 목록에 디지털 통화 주소를 포함하는 것을 고려하고 있다고 발표했습니다.

더욱 문제가 되는 것은, OFAC는 부패된 코인을 보유한 주소를 SDN 목록에 포함시키는 것을 배제하지 않았으며 이로 인해 부패된 코인의 무고한 보유자를 보유한 부패된 코인의 제휴로 인해 범죄 블랙리스트에 효과적으로 배치할 수 있다는 것입니다. 이로 인해 뉴욕 대학교 법학교수 Andrew Hinkes는, "기능성에 작별 인사 키스를" 그리고 대중은 "신선하게 발행된 코인 또는 추적된 깨끗한 코인에 대한 프리미엄"을 기대해야 한다고 재담하였습니다[8].

이러한 발전을 염두에 두면, 암호화폐 시장의 급변과 잘 확립된 많은 암호화폐의 고통 그리고 심지어 절멸을 상상하는 것은 어렵지 않습니다. 그러나 Epic은 이전에 이 백서에서 설명한 강력한 개인 정보 보호 기능으로 인해이 문제를 완전히 피할 수 있는 몇 가지 암호화폐 중 하나입니다. 신원과소유권 및 거래 당사자 간의 관계를 제거함으로써 Epic은 절대로 개인이나 활동에 관련될 수 없습니다. 따라서 Epic의 가치는 사용자와 독립적이며 범죄, 금융 또는 정치 분야에서 악의적인 행위자가 쉽게 조작할 수 없는 높은 수준의 개인 정보 보호와 보안을 제공합니다.

> “...부패된 코인은 파괴적입니다. 당신이 기능과 개인 정보 보호를 깬다면 당신은 통화를 깨는 것입니다.”
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. 확장성

Epic Cash는 MimbleWimble 블록체인 구현으로 중복 트랜잭션 데이터를 제거하는 공간 효율적인 디자인의 결과로 확장성이 향상됩니다. 이 기능을 담당하는 컷스루 기능은 비트코인을 비롯한 대부분의 암호화폐와 달리 블록체인이 시간이 지남에 따라 공간 효율성이 향상되고 메모리 및 컴퓨팅 성능에 대한 최소한의 투자로 새로운 노드를 만들 수 있음을 보장합니다. 효율적인 공간을 남겨두면 분산화가 촉진되며 널리 분산된 네트워크를 가능케 합니다. 또한 각 비트코인 노드는 전체 체인을 저장해야 하지만 Epic Cash 노드는 블록의 작은 하위 집합을 기반으로 네트워크 보안에 기여할 수 있습니다.

대부분의 암호화폐는 블록체인에 모든 트랜잭션 데이터를 무기한으로 저장해야 합니다. 비트코인 체인은 현재 매일 0.133 GB의 메모리를 확보하고 있으며, 이더리움의 체인은 하루 0.2719 GB의 빠른 속도로 증가하고 있습니다. 비트코인의 체인이 현재 속도로 계속 성장한다면 2140년에 최종 보상 블록을 채굴할 때 결국 약 6 TB의 크기가 됩니다. 이더리움은 그 날 10 TB를 초과합니다[9]. MimbleWimble이 없는 대부분의 블록체인에서 트랜잭션은 전세계 노드에서 확인되어야 합니다. 데이터가 증가하면 각 노드의 부담도 커집니다. 200 GB (현재 비트코인 체인의 대략적인 크기) 일지라도 데이터를 동기화하려면 안정적인 네트워크와 고속 디스크 읽기 및 쓰기 기능이 필요합니다.

결과적으로, 비용이 많이 드는 컴퓨팅 리소스를 활용하는 대규모 풀 간의 채굴이 점차 중앙화되었습니다. **비트코인의 전체 블록체인 기록이 대신 Epic Cash 블록체인에 저장되면 공간이 거의 90% 줄어듭니다.** 각 트랜잭션은 전송 및 보안 시간이 덜 걸리므로 작을수록 빠릅니다.

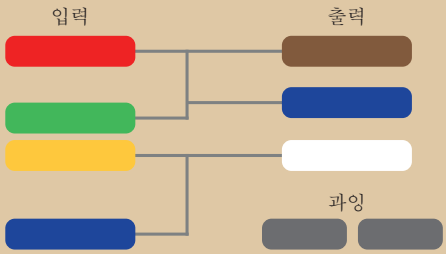
MimbleWimble은 '컷스루'라고 하는 블록 가지 치기의 혁신적인 방법으로 이 저장소 딜레마를 해결합니다. 컷스루의 작동 방식을 이해하려면 MimbleWimble 블록체인에서 트랜잭션과 블록이 어떻게 구성되는지 먼저 살펴보는 것이 가장 좋습니다.

입력:
이전 출력에 대한 참조;

출력:
기밀 트랜잭션 출력 및 범위증명;

과잉:
출력과 입력의 차이점, + 서명 (인증 및 비-인플레이션 증명)

수치 2:
MimbleWimble 트랜잭션 부분.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

모든 Epic Cash 블록은 다음을 포함합니다:

트랜잭션 입력의 머클 트리; **트랜잭션 출력과 범위증명의 머클 트리;** **과잉 가치 및 서명 목록.**

수치 2와 3에서 Andrew Poelstra의 프리젠테이션에서부터[10] 새로 채굴된 Epic이 흰색 입력 셀로 표시되는 것을 볼 수 있습니다. 동일한 색상의 셀은 상응하는 소비 입력이 있는 출력을 나타냅니다. 컷스루 프로세스를 사용하면 입력 및 일치하는 사용된 출력이 제거되어 블록 내의 공간을 확보할 수 있으므로 블록체인에 저장해야 하는 데이터의 양이 줄어듭니다. 트랜잭션이 원장에서 생략되지만 나머지 과잉 커널 (100 바이트)은 트랜잭션이 발생했음을 영구적으로 문서화 합니다.

블록이 계속 만들어지면 MimbleWimble은 블록 전체에 컷스루를 적용하므로 블록 헤더 (약 250 바이트), 사용하지 않는 트랜잭션 및 트랜잭션 커널 (약 100 바이트) 만 남게 됩니다. 출시될 두 번째 MimbleWimble 구현인 Grin은 비트코인 체인과 비슷한 수의 트랜잭션을 사용하는 MimbleWimble 체인이 비트코인 체인의 크기의 거의 10%를 차지하는 것으로 나타났습니다[11]. 또한 노드의 크기는 "비트코인 크기의 체인의 경우 대략 몇 GB 정도이며 잠재적으로 몇 백 메가바이트까지 최적화 할 수 있습니다."[12]

이는 전체 블록체인이 각 노드에 의해 저장되어야 하는 비트코인과 현저한 대조를 이룹니다. 시간이 지남에 따라 Epic Cash 블록체인의 공간 효율성이 비트코인 블록체인에 비해 증가함에 따라 Epic Cash 네트워크에 노드의 참여와 관련된 비용 효율성도 증가합니다. 낮은 참여 장벽은 네트워크 설계의 노드 계층에서 중요한 복원력을 보장합니다.

Epic Cash 블록체인은 MimbleWimble을 구현하고 컷스루 프로세스로 체인 가지 치기를 적용함으로써 암호화폐 커뮤니티에서 종종 간과하는 방식으로 확장성을 제공합니다. 비트코인과 비슷한 생각을 가진 프로젝트의 본질인 분산화를 포착한 것입니다. 코인이 처리할 수 있는 초당 거래 수에 관계 없이 광범위하고 다양한 네트워크에서 코인을 유지할 수 없다면 어떤 이점이 있을까요? 검증이 궁극적으로 강력한 채굴 대기업에 끌리는 등의 메모리 요구 사항이 있는 것이라면 분산된 생태계를 만들기 위한 모든 암호화폐 공동체의 노력이 배제됩니다. 추가 처리량을 제공하기 위해 Epic Cash 개발 로드맵에서 단기 목표로 라이트닝 스타일의 레이어 2 구현을 계획되어 있습니다.

수치 3: 컷스루 전후의 MimbleWimble 트랜잭션.

[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. 통화 정책

Epic Cash와 비트코인의 통화 정책은 매우 유사합니다. Epic Cash 순환 수량은 먼저 빠르게 확장된 다음 2028년 비트코인의 순환 수량과 동기화 됩니다. 이후 2140년에 최대 수량인 2,100만 Epic에 도달할 때까지 감퇴 비율로 증가합니다. Epic Cash는 순환 수량이 배출 수명주기와 함께 어느 시기에서나 알려져 있고 고정된 최대 수량으로 최고치를 도달하기 때문에 장기적인 가치의 안전한 저장 장치가 되는 자질을 갖추고 있습니다. Epic Cash 통화 정책은 다음과 같은 네 가지 특징이 있습니다:

- 수명의 처음 9년 동안 빠른 배출, 그 동안 20,343,750 Epic (총 수량의 96.875%)을 채굴해야 합니다. 정확한 배출 속도는 이 백서의 배출 일정 섹션에 요약되어 있습니다;
- Epic 순환 수량 및 배출 속도는 2028년 5월 24일 경 Epic 특이점에서 비트코인의 것과 동기화 됩니다. 특이점에 이어 배출 속도는 증가하는 속도로 감소하는 반면 순환 공급은 감소하는 속도로 증가합니다;
- 비트코인이 최대 1,200만 단위에 도달할 때와 거의 동시인 210년에 최대 2,100만 Epic가 공급될 것입니다;
- Epic은 8의 십진수로 나눌 수 있는 구조를 가지고 있습니다: 1 Epic은 100,000,000 freeman과 같습니다 (비트코인은 100,000,000 사토시와 같음).

Epic Cash 통화 정책은 다음과 같은 이유로 비트코인을 모델로 합니다:

- 비트코인의 경제적 기본 원칙과의 합의, 즉 순환 수량의 희소성과 예측 가능성은 강력한 가치 속성 저장소에 있습니다;
- 대중은 이미 비트코인의 모델과 처음 10년 동안 입증된 실적을 잘 알고 있습니다. Epic은 비트코인의 순환 수량과 대략 동기화하고 비트코인의 최대 수량과 분산 구조를 미러링함으로써 대량 채택에 대한 저항이 가장 적은 경로를 취합니다.

VI. 배출 일정

Epic Cash는 총 33회의 채굴 시대를 가지고 있으며, 각각 이전의 시기에 비해 블록 보상이 감소한 것으로 정의됩니다. Epic 블록 #1이 채굴된 날짜인 Epic 제네시스는 2019년 8월 1일에 열립니다. 블록은 분당 1개씩 채굴됩니다. 처음 5개 시대는 Epic 최대 공급량의 거의 97%를 생산하며 약 9년 내에 20년 간의 비트코인 배출량에 부합합니다. 이는 비트코인의 화려한 상승을 놓친 사람들을 위해 '시계를 되돌릴' 기회라고 생각할 수 있습니다.

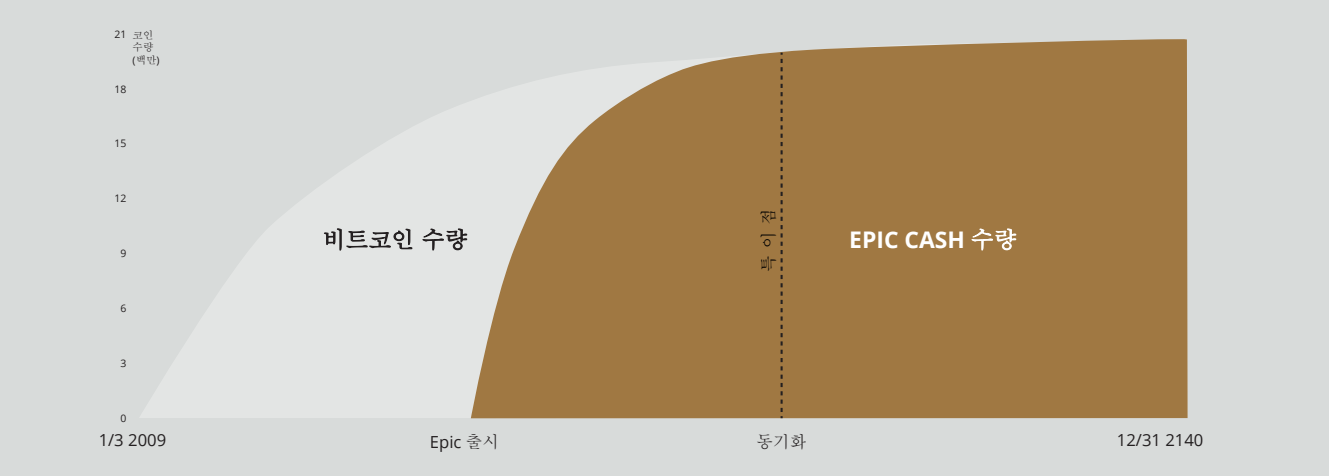
표 1의 배출 일정은 처음 7개의 채굴 시대의 시작 및 종료 날짜, 해당 블록 보상 및 각 시대에 대한 다음 순환 수량을 요약합니다. 8부터 33까지의 기간은 간략하게 하기 위해 표에 포함되어 있지 않습니다. 그 시대에, 차후의 각 시대는 비트코인에서와 마찬가지로 이전 시대의 보상 금액의 절반에 해당하는 블록 보상을 가질 것임을 이해하는 것으로 충분합니다. 각 시대에 배출된 Epic의 양은 4-년 시대 (약 1460일) 내에 블록 보상의 합이 됩니다.

Epic 특이점 (2028) 때, Epic 순환 수량은 비트코인의 순환 수량과 교차하여 Epic Cash는 비트코인 블록 보상과 반감 패턴을 채택하여 4년마다 블록 보상이 절반으로 감소합니다. 유일한 예외는 비트코인이 10분마다 1블록이 채굴되는 것에 반해 Epic 블록이 1분마다 1블록의 비율로 계속 채굴되는 것입니다. 이를 통해 Epic 순환 수량은 비트코인의 순환 수량과 나머지 수명 동안 대략적인 동등성을 유지합니다.

표 1: 첫 7개 채굴 시대의 배출 일정. 날짜는 근사치입니다.

시대	1	2	3	4	5	특이점	6	7
블록 보상	16	8	4	2	1		0.15625	0.078125
시작일	8/1 2019	6/29 2020	10/11 2021	6/3 2023	8/10 2025		5/24 2028	5/22 2032
종료일	6/29 2020	10/11 2021	6/3 2023	8/10 2025	5/24 2028		5/22 2032	5/20 2036
시간 (일)	334	470	601	800	1019		1460	1460
시작 수량	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
종료 수량	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
최대 수량에 대한 %	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

수치 4: Epic과 비트코인의 배출 일정.



VII. 채굴

Epic Cash 블록체인은 광범위한 계산 하드웨어를 환영함으로써 분산화를 추구합니다. Epic 채굴은 처음에 세 가지 해싱 알고리즘: RandomX, ProgPow, 및 CuckATOO31+을 사용하여 CPUs, GPUs, 및 ~~ASICs~~에서 사용할 수 있습니다. 알고리즘은 체인의 무결성을 손상시키지 않으면서 평범하게 핫-스왑될 수 있습니다.

1 RandomX 및 CPUs

RandomX는 범용 CPU에 최적화된 작업증명 (PoW) 알고리즘입니다. 다음과 같은 목표를 달성하기 위해 몇 가지 메모리-하드 기술과 함께 무작위로 프로그램 실행을 사용합니다:

- 단일-칩 ASIC 개발 방지;
- 범용 CPU에 비해 특수 하드웨어의 효율성 우위를 최소화.

CPU를 사용한 Epic 채굴은 채굴 스레드 당 2GB의 물리적 램, 16KB의 L1 캐시, 256KB의 L2 캐시 및 2MB의 L3 캐시를 연속적으로 할당해야 합니다[13]. Windows 10 장치에는 8GB 이상의 램이 필요합니다. 그리 멀지 않은 장래의 휴대폰에서 언젠가는 실행 가능한 채굴 노드가 될 수 있다는 것을 상상할 수 있습니다. Epic Cash 채굴 네트워크의 조기 CPU 통합은 Epic Cash 네트워크의 보안을 유지함으로써 블록 보상을 얻을 수 있는 보통의 컴퓨팅 수단으로 많은 사람들에게 훌륭한 기회입니다.

2 ProgPow 및 GPUs

프로그램적 작업증명 (ProgPow)은메모리 대역폭 및 GPU 컴퓨팅 기능의 많은 부분을 활용하여 하드웨어의 전체 에너지 비용을 효율적으로 포착하는 무작위 수학적 순서의 핵심 계산에 의존하는 알고리즘입니다. ProgPow는 범용 GPU를 최대한 활용하도록 특별히 설계되었으므로 특수 하드웨어를 통해 효율성을 크게 높이는 것은 어렵고 비용이 많이 듭니다. 그와 같이 ProgPow 알고리즘은 비트코인의 SHA-256과 같은 다른 많은 PoW알고리즘에서 흔히 볼 수 있듯이 대규모 ASIC 풀의 GPU를 능가하는 인센티브를 완화합니다. GPU는 CPU만큼 널리 사용되지는 않지만 여전히 일반적으로 사용 가능합니다. 유력 집단, Nvidia 및 AMD가 주도하는 기술 개발을 통해 GPU는 단위 단위로 CPU보다 많은 여러 채굴 솔루션을 병렬처리 할 수 있습니다. 이러한 편재와 높은 처리 성능의 조합으로 인해 GPU는 표 2에 표시된 것처럼 초기 시대 동안 많은 채굴 활동에 근간을 제공할 것입니다.

3 CuckATOO+31 및 ASICs

CuckATOO31+는 네덜란드 컴퓨터 과학자 John Tromp가 개발한 Cuckoo Cycle 알고리즘의 ASIC 친화적 순열입니다. ASIC 저항성 CuckAROO29의 비교 대상인 CuckATOO31+는 임의의 이분 그래프를 생성하고 해당 그래프의 꼭짓점을 통과하는 주어진 길이 'N'의 루프를 찾는 작업을 채굴자에게 제공합니다.

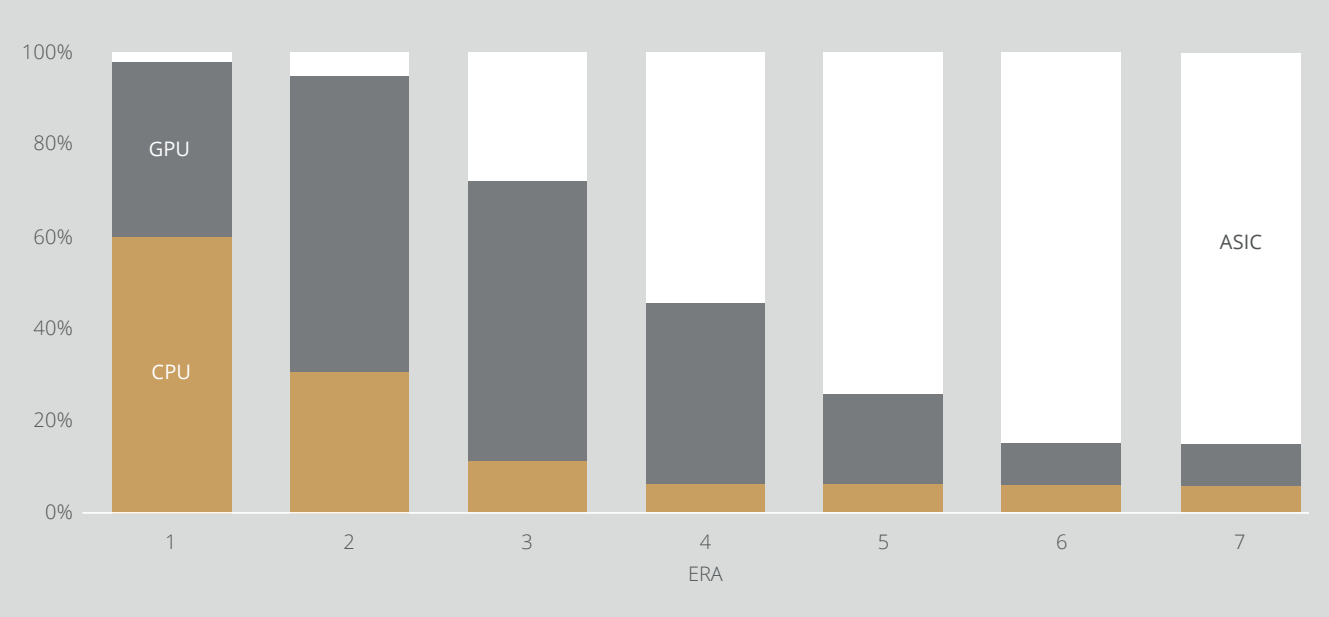
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

이는 메모리에 얽힌 작업이므로 해결 시간이 원시 프로세서 또는 GPU 속도가 아닌 메모리 대역폭에 의해 제한됩니다. 결과적으로 Cuckoo Cycle 알고리즘은 기존의 PoW 알고리즘에 비해 적은 열을 발생시키고 에너지 소비를 획기적으로 줄입니다. ASIC 친화적인 CuckATOO31+는 수백 MB의 SRAM을 사용하여 메모리 I/O[14]에 의해 병목 현상을 겪으면서 GPU를 능률적으로 개선합니다. 궁극적으로 ASIC은 세 가지 채굴 옵션 중 가장 큰 잠재 규모의 경제를 제공합니다. 그러나 포괄성의 측면에서 초기에 CPU 및 GPU와 관련하여 채굴 보상의 작은 부분이 할당되었지만 결국 ASIC은 CuckATOO31+ 장치 제조업체의 경쟁력 있는 생태계가 있을 것이라는 가정하에 채굴 블록 보상의 다수 지분을 맡습니다.

표 2: 채굴 보상 할당. 변경 대상. 할당은 최대 분산화를 달성하고 네트워크의 장기적인 이해와 일치하도록 지시됩니다.

시대	1	2	3	4	5	6	7
일	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

수치 5: 표 2에 따른 각 시대별 채굴 보상 할당. 변경 대상.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 채굴 기여

Epic 제네시스 (2019)에서 시작하여 Epic 특이점 (2028) 때 끝나는 채굴 과정에서 EPIC 블록체인 재단에 채굴 기여로 리디렉션되는 Epic 할당이 있습니다.

EPIC 블록체인 재단은 창업 시작 초기에 금융 기술 산업 내에서 마케팅 활동을 만들고 파트너십을 개발함으로써 Epic Cash 프로젝트의 기술 개발 및 인식 및 활용에 전념하고 있습니다.

특이점 이후, EPIC 재단의 역할은 EPIC Distributed Autonomous Corporation (EDAC에 의해 맡아질 것이며, 양도 이전에 재단에 의해 개발될 것입니다.

EPIC 블록체인 재단은 다음 연간 요금에 따라 블록 보상에서 공제된 일정 비율의 채굴 보상으로 자금을 조달합니다:

표 3: 채굴 보상의 백분율로서의 재단 채굴 기여에 대한 연간 비율.

년	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
채굴 보상 %	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. 결론

Epic은 비트코인이 분산화된 디지털 금으로 인정한 위치의 교환 매체인 '분산화된 디지털 실버'로 인정 받기를 목표로 합니다. Epic Cash는 훨씬 에너지 효율적이고 환경 친화적인 하드웨어 근간에서 손실된 기능을 다시 도입함으로써 최근 중앙 집중화 추세와는 대조적으로 개별 사용자에게 유리한 전력 균형을 기울입니다. 비트코인 경제학, 게임 이론 및 입증된 작업증명 공식과 최신 블록체인 기술을 결합하여 확장 가능하고 대체할 수 있으며 사용자의 개인 정보를 보호하는 신뢰할 필요가 없고 불변하며 분산된 통화 (Epic)가 생성됩니다. Epic Cash 블록체인은 개방형, 공개형, 국경 없음 및 검열-저항성입니다. 이는 사용자의 개인 정보와 자산을 보존하고 채굴을 통해 네트워크를 지원하기 위해 하드웨어를 배치하는 사람들에게 보상합니다. 모든 Epic은 작업증명을 통해 존재로 채굴됩니다. 공급량은 0에서 시작하고 네트워크는 기능 테스트넷이 현재 실행중이며 공정한 출시로 간주됩니다.

Epic Cash 핵심 사실:

- **채굴은 2019년 8월 1일에 시작됩니다.**
- **Epic Cash 블록체인은 MimbleWimble을 기반으로 합니다.**

  프로토콜의 정의 기능은 다음과 같습니다:

  1. **컷스루** – 공간 효율성을 높이기 위해 블록체인에서 중복된 정보를 제거하고 네트워크 유효성 확인에 광범위한 참여를 장려하며 분산화를 담당;
  2. ***CoinJoin*** – Epic 암호화폐의 기능성을 보장하기 위한 블록 내의 거래 묶음;
  3. ***Dandelion++ 프로토콜*** – 서로 얽힌 채널을 통해 통신하고 광범위한 노드 네트워크에 분산시켜 트랜잭션을 전파함으로써 트랜잭션과 그 원점 간의 연결을 끊음;
  4. **지갑 주소 없음** – 당사자와 거래하기 위한 일회용 프라이빗 키를 생성하기 위해 대–다중 서명을 사용하여 지갑주소가 전혀 필요하지 않음.

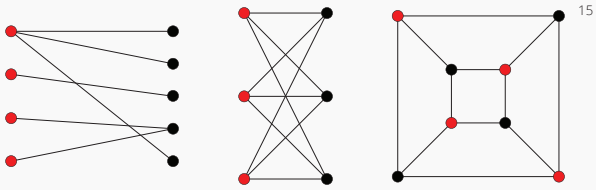
- **Epic Cash 통화 정책은** 약 9년 동안 Epic 순환 수량을 비트코인의 순환 수량과 동기화하고 2140년에 비트코인과 동시에 최대 1,200만 단위의 수량에 도달하도록 설계되었습니다. 이러한 인플레이션 억제 정책은 투명성, 공급량의 예측 가능성 및 희소성을 보장함으로써 장기적인 가치 창출의 안전을 도모합니다.

- 해당 RandomX, ProgPow 및 CuckATOO31 알고리즘을 통해 CPU, GPU 및 ASIC을 통합하는 **채굴**은 대량 채택 및 네트워크 효율성을 촉진합니다.

X. 어휘

ASIC 응용 분야별 집적 회로; 단일 목적으로 설계된 칩

2분할 그래프 동일한 세트 내의 2개의 그래프 정점이 인접하지 않도록 2개의 분리된 세트로 분해된 그래프 정점 세트.



블라인딩 팩터 암호화를 용이하게 하기 위해 디지털 메시지에 도입된 랜덤 요소; 거래 당사자의 퍼블릭 및 프라이빗 키뿐만 아니라 특정 거래에서 입력 및 출력을 암호화하는 두 당사자 간의 공유된 비밀[16].

블록 보상 새로운 블록 내에서 거래를 검증하기 위해 수행된 계산에 대한 보상으로 네트워크에 의해 분배된 새로운 Epic.

캐시 데이터를 저장하는 하드웨어 또는 소프트웨어 구성 요소로, 해당 데이터에 대한 향후 요청이 더 빨리 제공될 수 있습니다.

순환 수량 특정 시점에 존재하는 Epic의 양.

CPU 중앙 처리 장치: 컴퓨터의 다른 하드웨어 및 소프트웨어에서 대부분의 명령을 해석하고 실행하는 컴퓨터 구성 요소입니다.

컷스루 입력 및 일치된 소비 출력을 제거하여 블록 내의 공간을 확보하여 블록체인에 저장해야하는 데이터 양을 줄이는 MimbleWimble 블록체인 프로세스.

분산화 네트워크 운영 및 관리의 분산 상태.

배출 블록 보상으로 채굴자가 획득한 새로운 Epic의 생성. Epic은 트랜잭션이 블록체인으로 확인되면 매 60초마다 생성됩니다.

Epic 특이점 Epic의 순환 수량이 비트코인의 순환 수량과 동기화되는 지점 (2028년 5월).

과잉 (MimbleWimble) 출력과 입력의 차이, + 서명 (인증 및 비-인플레이션 증명).

기능성 개별 단위가 본질적으로 상호 교환 가능하고 각 부분이 다른 부분과 구분될 수 없는 재화 또는 상품의 재산.

제네시스 (사건) 첫 번째 Epic 블록의 채굴 및 블록체인의 공식적인 시작.

GPU 그래픽 처리 장치: 디스플레이 기능에 특화된 프로그램이 작동 가능한 로직 칩 (프로세서)을 포함하는 장치. 소비자 GPU는 암호화폐 채굴에 적합합니다.

Halving (비트코인) 4년마다 발생. 반감 이벤트가 발생할 때마다 수량이 50% 감소합니다.

해시 해싱 함수를 사용하여 기본 입력 번호에서 계산된 값.

해싱 알고리즘 (기능) 임의의 크기의 데이터를 디지털 서명, 메시지 인증 코드 (MAC) 및 기타 인증 형식을 생성하고 확인하는 데 사용되는 고정 크기의 해시로 매핑하는 수학 알고리즘.

동형 암호 암호화된 정보를 먼저 해독하지 않고 계산을 수행하는 방법.

불변성 (프로그래밍에서) 객체가 생성된 후에는 수정할 수 없는 상태.

입력 (MimbleWimble) 거래의 전송 당사자를 나타내는 MimbleWimble 거래의 구성 요소; 이전 트랜잭션의 출력으로 생성됩니다.

I/O 입출력; 컴퓨터와 같은 정보 처리 시스템과 외부 세계, 가능하게는 인간 또는 다른 정보 처리 시스템 간의 통신

.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

최대 수량 이후 순환 수량이 증가하지 않을 시점에 도달할 수있는 Epic의 양 (21,000,000 Epic).

메모리-하드 시도를 병렬로 실행하는 동시 연결을 배제하기 위한 많은 RAM의 사용. 메모리 하드 함수는 데이터를 보유하기 위해 사용 가능한 메모리에 의해 주로 결정된 계산 시간을 갖는 알고리즘입니다. 메모리-바운드 기능이라고도 합니다.

머클 트리 컴퓨터 과학 응용 프로그램에 사용되는 데이터 구조. 블록체인에서는 머클 트리를 사용하여 대용량 데이터 구조의 내용을 효율적이고 안전하게 확인할 수 있습니다.

MimbleWimble 비트코인 개발자 대화방에서 Tom Elvis Jedusor가 진행하는 가상의 기여자가 작성한 프로토콜.

다중 서명 사용자 그룹이 단일 문서에 서명할 수 있는 디지털 서명 체계. 일반적으로 다중 서명 알고리즘은 모든 사용자의 고유한 서명 모음보다 더 작은 공동 서명을 생성합니다[17].

노드 블록체인 네트워크에 연결하고 네트워크 내 다른 노드로 분기하여 P2P 방식으로 트랜잭션 및 블록에 대한 정보를 배포하는 컴퓨터.

단방향 합계 서명 (OWAS) 합계의 일부인 개별 서명을 계산하는 것이 매우 어려운 방식으로 암호화 된 많은 서명으로 구성된 트랜잭션 서명.

출력 (MimbleWimble) 트랜잭션의 수신을 나타내는 MimbleWimble 트랜잭션의 구성 요소; 다음 거래의 입력으로 사용됩니다.

페데르센 약속 체계 증명자가 값에 대한 커밋을 철회할 수 없이 값에 대한 정보를 공개하지 않고 선택된 값에 커밋할 수 있도록 하는 암호화 프리미티브.

프라이빗 키 프라이빗 키는 텍스트 암호화 및 해독을 위한 알고리즘을 설정하기 위해 퍼블릭 키와 쌍을 이루는 아주 작은 코드입니다. 비대칭-키 암호화 동안 퍼블릭 키 암호화의 일부로 생성되며 메시지를 읽기 쉬운 형식으로 해독하고 변환하는 데 사용됩니다.

작업증명 (PoW) 생산하기 어렵지만 (비용과 시간이 많이 소요) 다른 사람이 쉽게 검증할 수 있고 특정 요구 사항을 충족시키는 데이터. 작업증명은 암호화폐 블록 생성에 종종 사용됩니다.

퍼블릭 키 퍼블릭 키는 비대칭-키 암호화 알고리즘을 사용하는 퍼블릭 키 암호화 작성술로 작성됩니다. 퍼블릭 키는 메시지를 읽을 수 없는 형식으로 변환하는 데 사용됩니다.

RAM (랜덤 액세스 메모리) 운영 체제 (OS), 응용 프로그램 및 현재 사용중인 데이터가 저장된 컴퓨팅 장치의 빠른 액세스 데이터 저장 칩을 통한 장치의 프로세서에서의 빠른 액세스.

범위증명 트랜잭션 입력의 합이 트랜잭션 출력의 합보다 크고 모든 트랜잭션 값이 양수인지 확인하는 확약 검증. 범위증명은 화폐 수량이 변경되지 않았음을 보증합니다.

(디지털) 서명 블록체인 프로토콜의 표준 부분으로 주로 트랜잭션 및 블록 트랜잭션, 정보 이전, 계약 관리 및 외부 변조 감지 및 방지가 중요한 모든 경우에 사용됩니다. 이들은 블록체인에 정보를 저장하고 전송하는 데 있어서의 3가지 이점을 제공합니다:

- 전송되는 데이터가 변조되었는지 여부를 드러냅니다.
- 거래에 특정 당사자의 참여를 확인합니다.
- 법적 구속력이 있을 수 있습니다.

SRAM (스태틱 랜덤 액세스 메모리) 전원이 공급되는 동안 메모리에 데이터 비트를 유지하는 램 (랜덤 액세스 메모리).

처리량 주어진 암호화폐 프로토콜로 수행할 수 있는 초당 트랜잭션 측정.

신뢰할 필요 없음 중앙 파티에 의한 집행 없이 프로토콜의 규칙을 준수하기 위한 암호화폐 네트워크의 품질

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10