미나(MINA)

주요내용설명서(국문백서)

Korean White Paper

2026년 7월 21일

Disclaimer

본 번역본은 2026년 7월 21일 기준의 미나(Mina) 백서, Docs 및 트위터 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총 발행량, 유통량 계획, 사업계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

빗썸

프로젝트 소개

미나(Mina)는 이더리움과 같은 계정 기반 모델을 사용하여 비트코인과 비슷한 기능을 제공하는 결제 중심의 블록체인이지만, 거래 처리 방식이 다릅니다. 이는 비트코인이나 다른 가상자산들이 사용하는 UTXO 모델과는 다릅니다. 각 블록은 전체 상태가 아닌 이 상태에 대한 계약(머클 트리 형태로)만 포함합니다. 따라서 전체 노드는 모든 상태를 저장할 필요가 없으며, 최신 블록 헤더의 계약만으로도 계정 잔액을 효율적으로 확인할 수 있습니다. 하지만 우리 시스템의 증명자(비트코인의 채굴자와 비슷한 역할)는 새 블록의 유효성을 증명할 때 이 정보가 필요하므로 전체 상태를 저장해야 합니다.

미나의 합의 프로토콜로 우리는 간결한 블록체인을 위한 최초의 증명 가능한 안전성을 가진 지분 증명[1] 합의 프로토콜인 우로보로스 사마시카[2]를 제시합니다. 기존의 합의 메커니즘은 간결한 블록체인 구조와 항상 호환되지는 않을 수 있습니다. 여러 경쟁 체인 사이에서 합의를 이룰 때 전체 거래 기록이 필요할 수 있어 노드들이 모든 거래 내역을 저장해야 할 수 있기 때문입니다. 사실 이는 합의 메커니즘의 자연스러운 접근 방식입니다. 정직한 체인과 부정직한 체인을 구별하는 데 필요한 정보는 대개 분기점의 세부 사항과 관련이 있기 때문입니다. 분기가 발생한 후 오랜 시간이 지나서야 그것을 알게 되므로 체인 선택 과정을 돕기 위해 전체 기록을 저장해야 할 수 있습니다. 이는 잘 알려진 지분 증명 합의 메커니즘들에서 실제로 그렇습니다. 또한 다른 지분 증명 합의 메커니즘들은 초기 설정을 위해 신뢰할 수 있는 외부 조언에 의존합니다.

구체적으로 미나의 현재 개발 단계에서 상태 증명 크기는 단 864바이트이며, 이를 검증하는 데 약 200밀리초가 걸립니다. 따라서 이 정도의 계산을 지원할 수 있는 스마트폰을 포함한 모든 기기는 신뢰할 수 있는 외부의 조언 없이도 시스템의 현재 상태를 검증할 수 있습니다.

점진적으로 계산 가능한 비대화형 지식 증명 외에도 우리는 여러 최적화 기법을 사용합니다. 그 중 가장 중요한 것은 병렬 스캔 상태입니다. 이는 순차적으로 계산된 증명의 한계를 넘어 거래 처리량을 향상시킵니다. 이 아이디어는 아직 증명에 반영되지 않은 모든 블록을 대기열에 넣고 여러 증명자들에게 병렬로 분배하여 증명하는 것입니다. 또한 최소 증명 시간으로 인한 제약을 줄이기 위해 최근 거래들의 특별한 대기열을 도입하여 거래 확인 지연 시간을 단축했습니다. 더불어 네트워크에서 검증자들의 참여를 최대화하기 위한 특별한 인센티브 구조도 도입했습니다.

[1] PoS(Proof of Stake)

[2] Ouroboros Samasika

비즈니스 모델

네트워크 역할과 인센티브

대부분의 가상자산 프로토콜은 네트워크 내에 크게 두 가지 역할을 가지고 있습니다. 첫째는 네트워크의 모든 거래를 직접 검증하는 이들로 흔히 풀 노드, 스테이커 또는 마이너[3]라고 합니다. 둘째는 거래 검증을 제3자에게 맡기는 이들로 주로 라이트 클라이언트라고 합니다.

가상자산 프로토콜이 널리 사용될수록 검증 비용이 계속 증가합니다. 그 결과, 점점 더 많은 참여자들이 첫 번째 풀 노드 그룹에서 밀려나 두 번째 라이트 노드 그룹으로 옮겨가게 됩니다. 예를 들어 비트코인은 지금까지 평균적으로 초당 1.5건 미만의 거래를 처리해왔습니다. 그럼에도 불구하고 네트워크에 새로 참여하는 사람이 풀 노드 수준의 보안을 갖추려면 약 5억 건의 거래를 검증해야 합니다. 이 문제는 일부 가상자산에서 더욱 심각해집니다. 이들은 비트코인보다 10배에서 10만 배 더 높은 거래 처리량을 주장하며, 가장 많은 거래가 이루어지는 시기에는 매주 기가바이트 또는 테라바이트 단위의 데이터를 생성합니다. 반면 미나는 일정한 리소스 요구사항을 갖습니다. 네트워크가 처리한 거래 수와 관계없이 사용자들은 작은 크기의 비대화형 지식 증명만으로도 현재 상태를 완전히 검증할 수 있습니다. 이를 지원하기 위해 미나는 네트워크에 세 가지 역할을 두고 있으며 각각 다른 메커니즘을 통해 참여를 유도합니다.

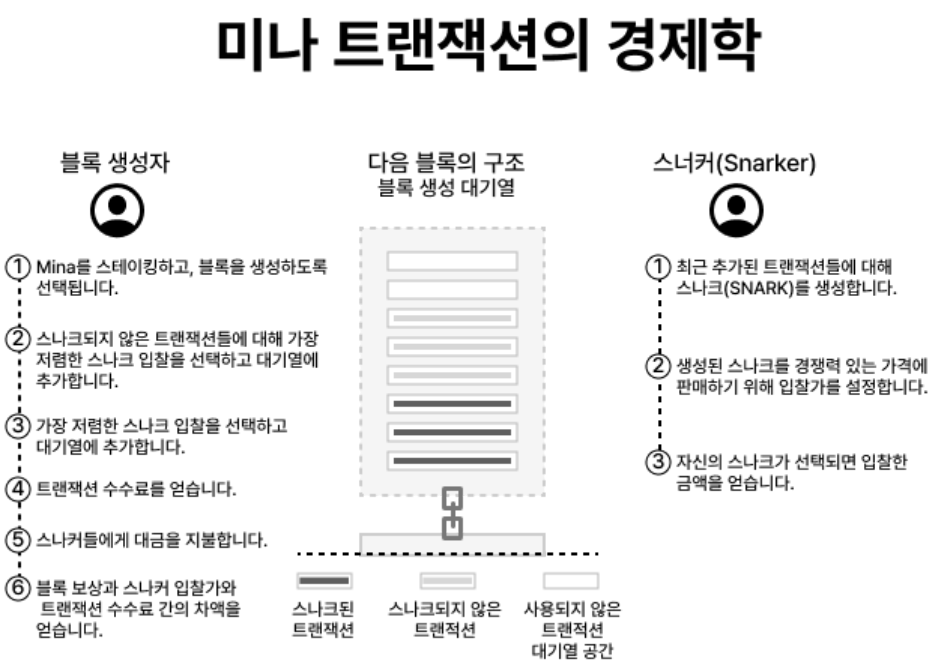
검증자

네트워크 참여자 대부분이 검증 능력을 갖출 것으로 예상됨에 따라 미나는 상태의 유효성을 지속적으로 증명하기 위해 재귀적 비대화형 지식 증명을 사용합니다. 이로 인해 풀 노드 수준의 보안은 단순히 증명 내용을 다운로드하는 것만으로 달성됩니다. 이 내용은 크기가 겨우 몇백 바이트에 불과하며, 검증하는 데에는 몇 밀리초의 시간이 소요됩니다. 비대화형 지식 증명은 합의 정보와 최근 원장 상태에 대한 머클 루트[4]를 인증합니다. 이 시점에서 검증자들은 상태 관련 내용에 대한 머클 루트를 요청할 수 있습니다. 머클 루트를 확인함으로써 검증자들은 자신들이 관심 있는 상태 내용(예: 계정 잔액)이 실제로 비대화형 지식 증명을 통해 인증된 원장에 포함되어 있는지 확인할 수 있습니다.

[3] Miner

[4] Merkle root

블록 생산자



[블록 생성자와 스나커 토큰 이코노미]

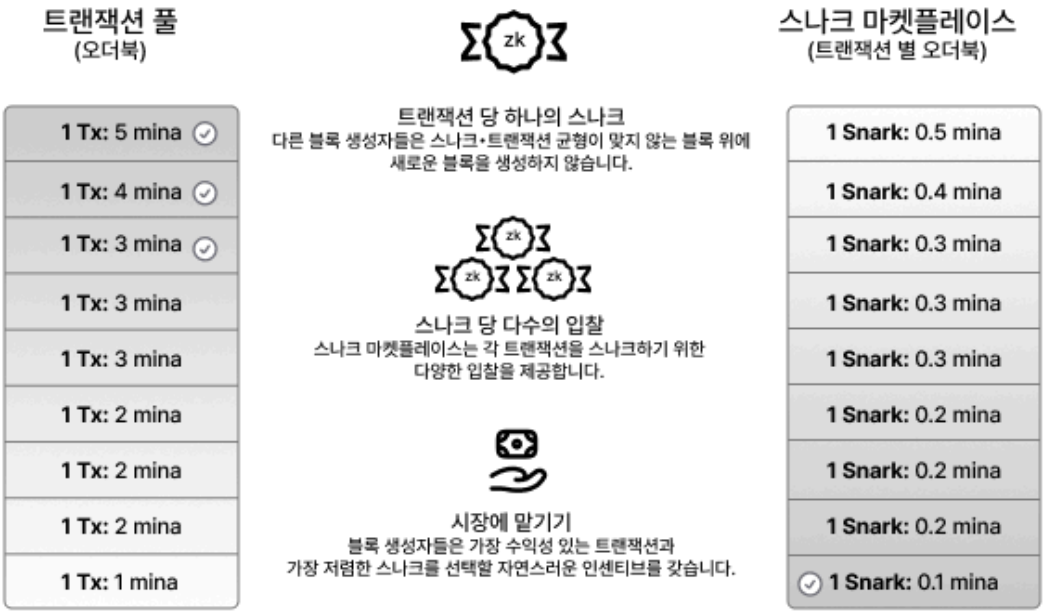
블록 생산자는 다른 프로토콜의 채굴자나 스테이커와 비슷합니다. 이들은 블록 보상이나 코인 기반의 프로토콜 분배 보상, 사용자가 지불하는 네트워크 수수료를 통해 동기부여를 받습니다. 중요한 점은 미나가 우로보로스라는 특별한 시스템을 사용한다는 것입니다. 이 시스템 덕분에 블록 생산자들은 자신의 자산을 잃을 위험 없이 네트워크에 참여할 수 있습니다. 다시 말해, 잘못된 행동을 하면 자산을 빼앗기는 '삭감[5]' 위협 없이도 블록 생산자들이 자발적으로 네트워크에 참여하도록 설계되어 있습니다. 직접 스테이킹하는 것 외에도 개인들은 자신의 지분을 다른 블록 생산자에게 위임할 수 있습니다. 이렇게 위임을 받은 사람은 다른 사람의 코인을 대신 맡아 네트워크에 참여할 수 있습니다. 하지만 중요한 점은 위임받은 사람이 그 코인으로 직접 거래를 할 수는 없다는 것입니다. 다시 말해 코인 주인을 대신해 네트워크를 지원하는 역할만 할 뿐 그 코인을 사용하거나 옮길 권한은 없습니다.

일반적으로 블록 생산자들은 다음 블록에 포함할 거래를 선택합니다. 그들은 수수료가 가장 높은 거래를 포함하도록 동기부여됩니다. 하지만 블록체인을 간결하게 유지하기 위해 블록 생산자들에게는 추가적인 책임이 있습니다: 블록에 새 거래를 추가할 때마다 이전에 추가된 동일한 수의 거래에 대해 비대화형 지식 증명을 생성해야 합니다. 이를 하지 않은 블록은 합의 규칙을 준수하지 않게 되어 다른 노드들에 의해 거부됩니다. 거래 대기열을 상상하면 이해하기 쉬울 수 있습니다. 블록 생산자가 거래 수수료를 받기 위해 대기열 뒤에 10개의 거래를 추가하고 싶다면, 대기열 앞에서 10개의 거래에 대해 비대화형

[5] Slashing

지식 증명을 생성해야 합니다. 그들은 직접 증명 내용들을 생성하거나 다른 전문 네트워크 참여자인 스나커[6]들이 기여하는 마켓플레이스에서 증명 내용을 선택할 수 있습니다.

스나커



[스나크 마켓플레이스 오더북]

기술 백서에서 설명하는 스나커는 거래를 검증하는 비대화형 지식 증명 내용을 만드는 네트워크 참여자입니다. 이들은 이 작업에 대한 수수료를 제시하는데 이를 '입찰'이라고 합니다. 만약 스나커가 만든 증명 내용이 블록에 사용되면 블록 생산자는 전체 거래 수수료에서 비용을 지불합니다. 여러 스나커가 하나의 거래에 대해 수수료를 제시할 수 있고, 블록 생산자들은 증명 내용 생산 작업에 지불하는 수수료를 최소화하려고 합니다. 이로 인해 자연스럽게 참여자들이 가장 비용 효율적인 증명 내용을 만들기 위해 경쟁하는 시장이 형성됩니다. 편의상 이를 '스나켓플레이스[7]'라고 부를 수 있습니다.

이제 이 시스템의 경제적 특성을 몇 가지 살펴보겠습니다. 첫 번째로, 네트워크에 어느 정도의 잠재적 여유 컴퓨팅 능력이 있는 한 블록 생산자들의 네트워크로 거의 확실히 보장됩니다. 스나켓플레이스는 프로토콜이 계속 원활하게 작동하는 것과 검열 저항성에 영향을 미치지 않을 것입니다. 왜냐하면 항상 어떤 비용으로든 증명 내용을 생산하려는 입찰이 있을 것이기 때문입니다. 이를 이해하기 위해 여유 컴퓨팅 능력이 있는 네트워크 참여자의 동기를 생각해 봅시다. 이 참여자가 증명 내용

[6] SNARKer

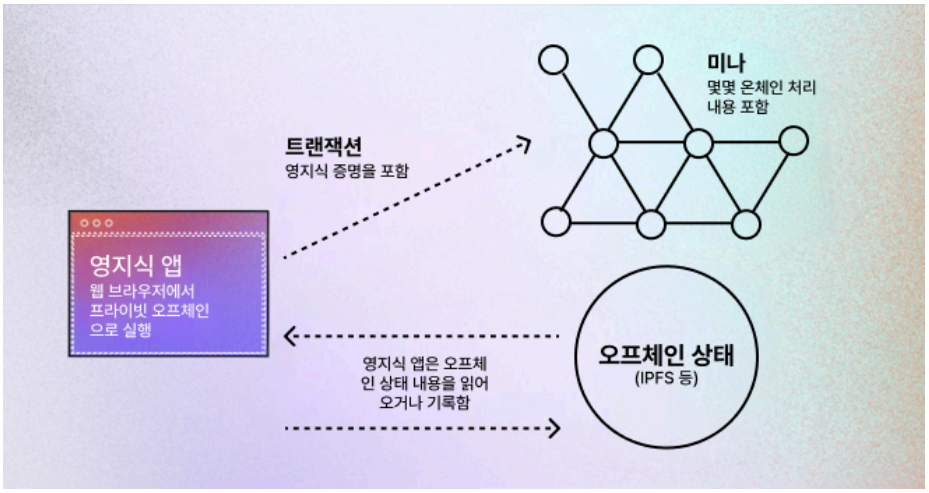
[7] Snarketplace

생산 부족으로 네트워크에서 수수료가 오르는 것을 관찰한다고 가정해 보면, 증명 내용을 만드는 비용보다 수수료가 더 높아지는 경우 합리적인 참여자들은 자신이 증명 내용을 만드는 데 드는 비용보다는 조금 더 높고, 현재 시장에서 거래되는 가격보다는 조금 더 낮은 가격에 증명 내용을 팔겠다고 입찰할 것입니다. 이는 이익을 얻기 위함이며 결과적으로 수수료를 안정화시킬 것입니다. 블록 생산자들은 이 수수료를 단순히 거래하는 사람들에게 전가하여 거래를 하는 사람이 추가 비용을 지불하게 됩니다. 실제로 증명 내용을 생성하는 계산 비용은 매우 낮을 것으로 예상됩니다. 현재의 클라우드 컴퓨팅 가격으로 볼 때 거래당 1센트 미만의 범위일 것입니다.

두 번째로, 규모의 경제로 인해 일부 비대화형 지식 증명 운영자들은 시간이 지남에 따라 더 큰 영향력을 가질 수 있습니다. 비트코인에서 일부 채굴 작업장이 규모의 경제를 달성해 지배적인 위치에 서게 된 예시를 생각하면 됩니다. 하지만 증명 내용 생산이 일부 운영자에게 집중되더라도 프로토콜의 검열 저항성이나 시스템 활성에 영향을 미치지 않을 것입니다. 누구나 어떤 가격으로든 증명 내용을 생산할 수 있기 때문입니다. 따라서 더 저렴한 증명 내용을 제공할 수 있는 생산자가 있더라도 만약 그들이 특정 거래 처리를 거부한다면 네트워크의 다른 누구라도 조금 더 높은 수수료로 증명 내용을 제공할 수 있습니다. 그리고 블록 생산자들은 여전히 이를 원장에 포함시키려는 동기를 가질 것입니다.

세 번째로, 중복 증명을 방지하는 명시적이고 자발적인 조정 메커니즘이 있다면 증명 내용 수수료와 네트워크의 컴퓨팅 낭비를 줄일 수 있을 것입니다. 다만 이런 메커니즘이 보안이나 생동성[8]을 위해 꼭 필요한 것은 아닙니다.

영지식 앱[9]



[영지식 앱의 구동 방식]

[8] Liveness

[9] zkApp

영지식 앱은 비대화형 지식 증명을 사용하여 구동되는 미나 프로토콜 스마트 컨트랙트입니다. 영지식 앱은 약간의 오프체인 실행 모델과 오프체인 상태 모델을 사용합니다. 이 아키텍처는 공개되거나 공개되지 않을 수 있는 비공개 연산과 그 상태를 허용합니다. 영지식 앱은 체인 밖에서 임의로 복잡한 계산을 수행할 수 있으며, 이 계산의 검증을 위해 결과적인 영지식 증명을 체인으로 보내는 데 일정 수수료만 부과됩니다. 이러한 비용 절감의 이점은 체인에서 계산을 실행하고 가변 가스 수수료 모델을 사용하는 다른 블록체인과 대조적입니다.

비대화형 지식 증명

zk-SNARK는 Zero Knowledge Succinct Non-Interactive Argument of Knowledge의 약자로 개인 정보 보호 혜택과 함께 간결하다는 점에서 장점을 가집니다. 복잡하고 높은 스펙의 컴퓨터를 가진 사람만이 현재 대부분의 기존 블록체인이 요구하는 어려운 계산을 처리할 수 있는 것과 달리 누구나 쉽게 확인하고 참여할 수 있습니다. S- 간결함(Succinct)은 증명하려는 개념이 복잡하더라도 증명이 간단하고 검증하기 쉽다는 것을 의미합니다.

- N- 비대화형(Non-interactive)은 증명자와 검증자 사이에 양방향 통신이 필요 없다는 것을 의미합니다.
- AR- 논증(Argument)은 이러한 증명에 관해 논하는 형식주의를 말합니다. 왜냐하면 비대화형 지식 증명 처리 과정 내에 이러한 "형식적 증명"이 이루어지기 어렵게 만드는 복잡한 암호화 과정과 불확정성이 있기 때문입니다.
- K – 지식(Knowledge)은 증명자가 실제로 증거를 가지고 있다는 사실을 말합니다.

모든 비대화형 지식 증명은 이러한 속성을 가지고 있습니다. 정보를 유출하지 않고, 증명하려는 개념이 복잡하더라도 작고 검증하기 쉬우며, 상호간 통신이 필요하지 않은 지식의 증명 방식인 것입니다. 즉, 주장하는 것이 사실이라는 것과 그 내용을 증명자만이 실제로 알고 있어야 합니다.

미나는 재귀적 비대화형 지식 증명 기술을 통해 많은 트랜잭션 혹은 블록이 추가되더라도 빠르고 안전하게 처리할 수 있습니다. 또한 개인 정보 보호 및 보안성이 뛰어나 주요 데이터를 로컬 장치에 보관하고 온라인에서는 결과값만을 공유할 수 있습니다.

스나켓플레이스

비대화형 지식 증명 작업을 이해하는 데 있어 중요한 원리 및 과정은 다음과 같습니다. 블록 생산자는 블록 보상을 사용하여 증명 작업자로부터 작업 내용을 구매합니다. 증명 내용의 가격 책정에는 프로토콜이 관여하지 않으며, 작업자가 증명 내용을

생산할 수 있는 프로토콜 수준의 보상도 없습니다. 인센티브는 오직 작업자 사이에서 생성되며, 공개된 마켓플레이스인 스나켓플레이스에서 동적으로 설정됩니다.

블록 생산자가 증명 내용을 구매해야 하는 이유는 미나 블록체인의 헤드에 있는 상태값이 유효한지 확인하기 위해서는 트랜잭션이 비대화형 지식 증명 과정을 거쳐야 하기 때문입니다. 하지만 이 과정을 거치지 않고 같은 속도로 트랜잭션을 계속 추가하면 시간이 지남에 따라 완료되지 않는 작업이 누적됩니다. 안정된 상태에 도달하려면 작업이 추가되는 속도와 거의 같은 속도로 처리되어야 합니다. 블록 생산자는 블록에 거래를 포함시켜 수익을 창출하기 때문에 완료된 증명 작업을 같은 수만큼 구매하여 거래를 상쇄하고 증명 작업에 대한 수요를 창출해야 합니다. 그러나 그들의 의무는 스나켓플레이스에서 가장 낮은 가격으로 증명 내용을 구매하는 것입니다. 반대로 증명 작업자는 내용을 판매할 수 있는 동시에 수익을 극대화하고자 합니다. 이 두 가지 역할은 시장의 양면 역할을 하며 시간이 지남에 따라 증명 작업에 대한 시장 가격으로 균형을 이룹니다.

증명 내용 가격 결정 방식에서 우리는 스나켓플레이스가 수요-공급 법칙과 같은 방식으로 계속 재조정되기를 기대합니다. 각 증명 작업은 다른 거래에 적용되지만, 더 큰 관점에서 볼 때 증명 작업은 하나의 상품입니다. 아래의 가격 책정 전략에 대한 몇 가지 발견법[10]이 도움이 될 수 있습니다.

- 시장 가격이 X라면, 운영 비용을 뺀 후 수익성이 있는 한, 증명 작업을 X보다 낮은 가격(예: X - 1)에 판매하는 것이 효과적일 가능성이 높습니다.

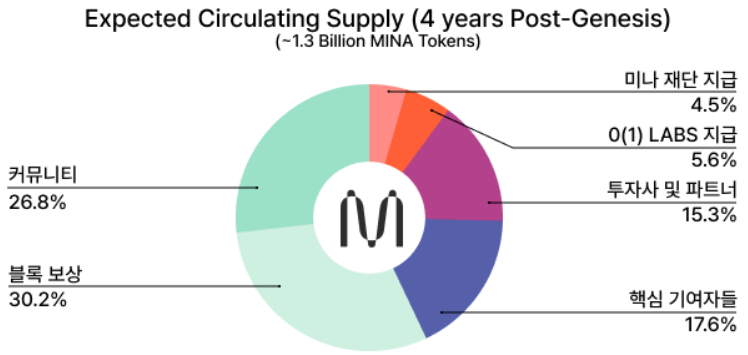
- 블록 생산자는 동일한 증명 작업자로부터 더 많은 증명 작업 단위를 구매할 인센티브를 받는데, 그 이유는 블록에 포함해야 하는 수수료 전송 거래가 하나뿐이기 때문입니다.
    - 기본적으로 블록 생산자가 증명 작업자에게 비용을 지불하는 방식은 수수료 전송라는 특별한 유형의 거래를 통해서입니다. 블록 생산자가 수익을 극대화하기 위해서는 수수료 전송의 수를 최소화해야 합니다. 각각은 블록에 추가되어야 하는 개별 거래이기 때문입니다(결과적으로 더 많은 증명 작업으로 상쇄됩니다). 따라서 가장 좋은 시나리오는 동일한 증명 작업자에게서 작업 묶음을 구매하는 것입니다.

- 일부 증명 작업은 다른 작업보다 먼저 완료하는 것이 더 중요할 것입니다. 전체 트리의 메모리를 확보할 수 있기 때문입니다. 이는 다양한 작업 선택 방법을 통해 가능합니다. 현재 기본적으로 순차적 방법과 무작위적 방법, 두 가지 방법이 지원됩니다. 그러나 이 두 가지 방법 모두 동적 시장을 활용하지 못하며, 이는 미나 커뮤니티가 솔루션을 개발할 수 있는 영역입니다.

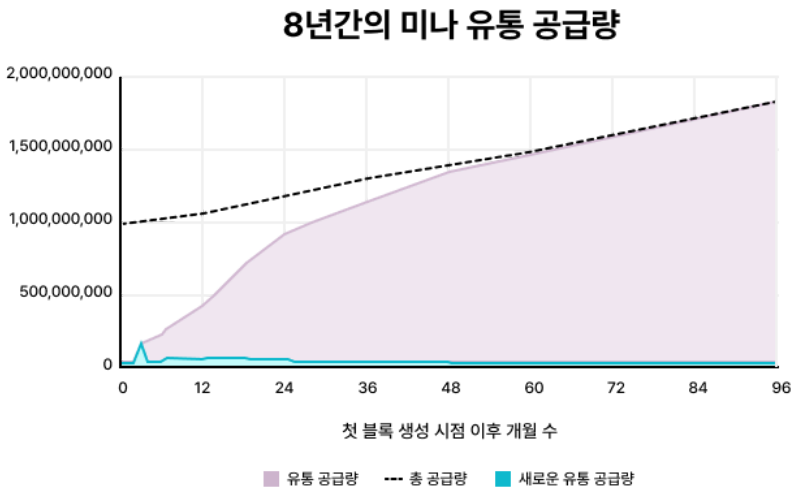
[10] Heuristics

증명 내용과 가격 등의 모든 데이터가 공개되어 있기 때문에 스나켓플레이스를 검사하는 방법은 여러 가지가 있습니다. 한 가지 예로 GraphQL API를 사용하는 방법이 있고 , 다른 옵션으로는 CLI를 사용하거나 비대화형 지식 증명 멤풀[11]에서 증명 작업을 추적하는 사용자 지정 솔루션을 롤링[12]하는 방법이 있습니다.

토크노믹스



[8년간의 미나 유통 공급량]



[11] Mempool

[12] Rolling

[8년간의 미나 유통 공급량]

- MINA는 정해진 공급량이 없는 인플레이션 통화입니다. 모든 토큰 보유자는 락업[13]이나 본딩[14]할 필요 없이 인플레이션에 비례하는 보상을 받기 위해 지분을 스테이킹하거나 위임할 수 있습니다.
- 미나 메인넷 출시 당시 초기 배포량은 805,385,694 MINA였으며, 토큰 락업 일정에 따라 배포되었습니다.
- MINA는 고정 공급량 모델이 아닌 연간 인플레이션 발생하며, 초기 연간 인플레이션율은 약 12%에서 7년 매년 점진적으로 감소하고, 최종적으로 7% 인플레이션율로 수렴합니다.
- 메인넷 출시 첫 15개월 동안 락업 해제된 계정(o1Labs 및 미나 재단 제외)은 락업 계정이 받은 블록 보상의 두 배를 받았습니다. 이는 새로운 네트워크 참여자와 락업이 해제된 토큰 보유자가 생태계를 벗어나지 않도록 하는 인센티브입니다.

로드맵

미나는 별도 로드맵을 공지하고 있지 않으나, 공식 홈페이지 및 블로그를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 홈페이지 https://minaprotocol.com/
- 블로그 https://minaprotocol.com/blog?cat=68
- X(구 트위터) https://x.com/MinaProtocol

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.

[13] Lockup

[14] Bonding