

서싱트(Succinct)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록 단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다. 그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다. 두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고, 제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며, 투자 손실은 투자자에게 귀속됩니다.

서싱트 네트워크(Succinct Network) : 전세계 소프트웨어를 증명하다

Uma Roy ; Succinct

John Guibas ; Succinct

Kshitij Kulkarni ; Succinct

Mallesh Pai ; Rice University and SMG

Dan Robinson ; Paradigm

초록

우리는 전 세계의 소프트웨어를 증명(prove)하는 탈중앙화 프로토콜인 서싱트 네트워크(Succinct Network)를 제안한다. 이 네트워크는 프루프 옥션(proof contest)이라 불리는 새로운 인센티브 메커니즘을 통해 영지식 증명을 생성하는 분산된 증명자 집합을 조율함으로써, 세계에서 가장 효율적이고 견고한 증명 클러스터를 만든다.

요청자들은 RISC-V 프로그램 형식으로 입력값과 수수료를 포함한 요청을 제출하며, 이 수수료는 증명의 우선순위를 결정한다. 증명자(prover)는 최소한의 지연과 비용으로 증명

을 생성할 권리를 얻기 위해 프루프 옥션, 즉 모두가 비용을 지불하는 옥션에 참여하여 수수료를 획득한다.

이 옥션은 애플리케이션 전용 블록체인 위에서 정산된다. 프루프 옥션과 블록체인 모두는 SP1과 공동 설계되었으며, SP1은 RISC-V 바이트코드의 실행을 증명하는 영지식 가상 머신(zkVM)이다.

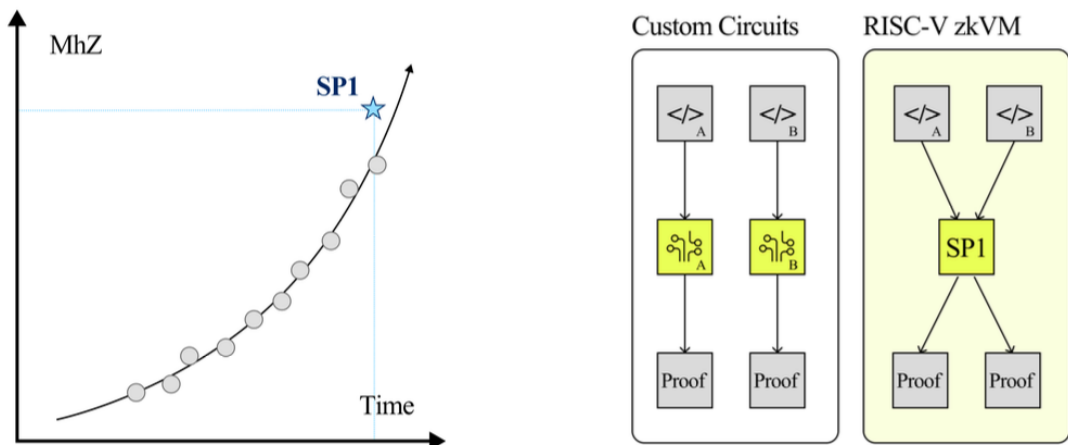
프루프 옥션은 증명 비용을 최소화하는 것과 동시에 탈중앙화된 증명자 풀을 장려하는 것이라는 상충하는 목표를 균형 있게 달성하도록 특별히 설계되었다.

이 네트워크는 요청자, 하드웨어 팀, 인프라 운영자의 생태계를 암호경제적 인센티브로 조율한다. 이 프로토콜에 대한 비허가 참여(permissionless participation)는 전 세계적 인프라 구축을 촉진하며, 모든 이들을 위한 영지식 증명 생성의 비용과 지연을 줄인다.

서론

블록체인과 같은 탈중앙화 시스템은 분산 합의를 기반으로 작동한다: 여러 당사자가 연산을 재실행하고 그 결과에 동의한다. 그 대가로 블록체인은 중앙 중재자 없이 신뢰할 수 없는 애플리케이션을 가능하게 한다. 이 개념은 최초로 비트코인을 통한 탈중앙화 화폐에 적용되었고, 이후 이더리움을 통해 임의의 신뢰할 수 없는 연산으로 확장되었다 [Nak08; But13]. 그러나 이러한 중복 연산은 비용이 많이 들고, 중앙집중형 시스템에 비해 블록체인에 오버헤드를 발생시킨다. 이러한 이유로 블록체인은 여전히 병목현상을 겪고 있다.

서싱트 영지식 증명은 이러한 상황을 개선할 수 있는 가능성을 제시한다. zk 증명은 증명자가 어떤 주장(예: 선택적으로 비공개 입력이 있는 프로그램의 실행)에 대한 지식을 가지고 있음을 검증자(verifier)에게 설득할 수 있게 해준다. 이때 제시되는 증명은 그 주장 자체보다 훨씬 짧다 [BS+13; BS+14]. 이를 통해 블록체인은 연산이 비싼 트랜잭션 실행과 비교적 저렴하게 만들 수 있는 트랜잭션 검증을 분리함으로써 처리량을 확장할 수 있게 된다. 시스템의 일부 참가자만이 고비용 연산을 수행하고, 나머지 많은 노드들은 단지 이를 검증하면 된다. 이더리움의 경우, 실시간 zk 증명을 사용하면 “증명자(attester)는 EVM 트랜잭션을 재실행하는 대신 저렴한 SNARKs를 검증할 수 있게 되어”, 이더리움은 임의적으로 확장할 수 있게 된다 [Dra24].



(a) 증명시스템은 기하급수적으로 성능 향상을 경험 (b) zk가상머신은 애플리케이션 회로를 범용 프로그램으로 변환

[그림 1: zk 증명 기술은 빠른 발전을 이루었다]

zk 증명은 블록체인을 확장 가능하고 상업적으로 실행 가능하게 만드는 것 외에도, 모든 시스템에 대해 검증 가능성을 가능하게 하는 근본적으로 새로운 컴퓨팅 패러다임인 암호화 컴퓨팅을 예고한다. 보편적 검증 가능성의 함의는 광범위하다. 오늘날 인증, 신원 관리, 트랜잭션 검증과 같은 작업은 정부와 글로벌 기업의 자원을 소모한다. 암호화 컴퓨팅을 사용하면, ZK 증명을 소비하고 비공개 요청자 정보에 대한 올바른 프로그램 실행을 자동으로 검증하는 프로토콜을 통해 이러한 기관이 직면한 오버헤드를 대폭 줄일 수 있을지도 모른다. 중요한 점은, zk 증명은 인터넷에서 인증을 가능하게 했던 디지털 서명과 같은 이전 암호학적 원시 구성요소(cryptographic primitives)들과는 달리, 프로그래밍이 가능하다는 점이다. zk 증명은 임의의 공적 또는 비공개 입력에 대해 임의의 연산에 대한 검증 가능한 명제를 허용할 수 있으며, 이는 증명(attestations)이나 신원을 포함하는 탈중앙화 프로토콜과 비즈니스 로직의 설계 공간을 획기적으로 넓힌다.

오늘날, 우리가 중요한 변곡점에 도달했음을 시사하는 zk 기술의 두 가지 중요한 흐름이 존재한다. 첫 번째는 실용적인 zk 증명 시스템에서의 성능의 급격한 향상이다. 효율적인 상호작용 증명 시스템은 1980년대에 도입되었지만 [GMR85], 현대의 증명 시스템이 증명 오버헤드(proving overhead), 비용, 지연 면에서 상당한 진보를 이루기 전까지는 사용하기 어려웠다 [Halo20; Plonky22; Plonky23]. ZK 증명 성능은 소프트웨어와 성능 엔지니어링의 발전으로 인해 지수적 곡선을 따라 증가해왔다 (그림 1(a)).

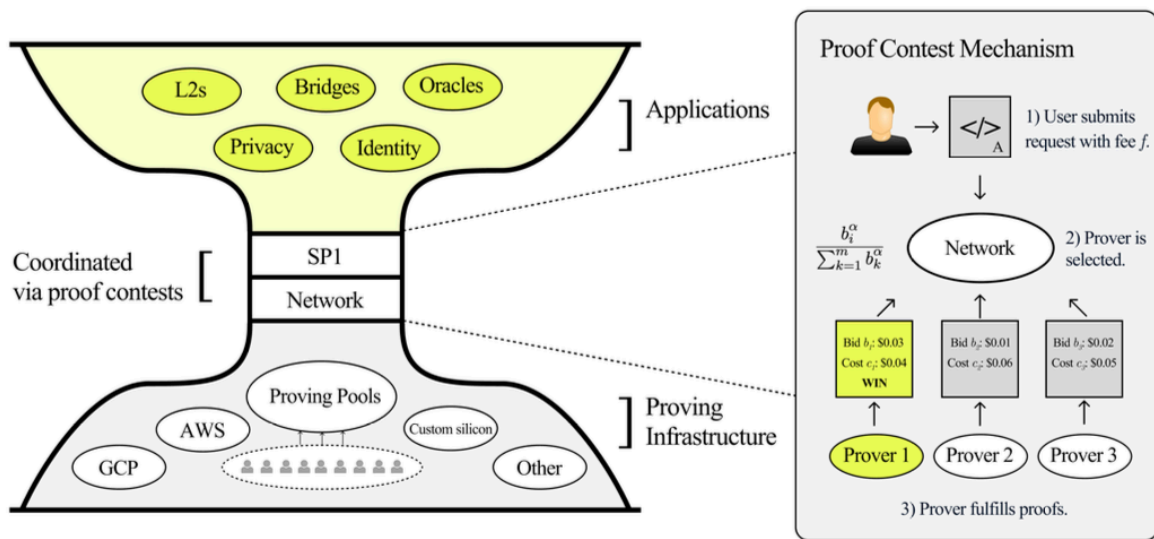
두 번째는 zk 증명 기술이 애플리케이션 특화 회로 — 즉 산술 회로로 프로그램 로직을 인코딩하는 방식 — 에서, 임의의 결정론적 프로그램의 증명을 가능하게 하며 일반적인

코드와 기존 소프트웨어를 활용할 수 있는 범용 zk 가상머신으로 발전해 왔다는 점이다 (그림 1(b)). 일반적인 프로그래밍 언어의 유연성은 기존 코드의 재사용을 가능하게 한다. SP1과 같은 범용 zkVM은 zk를 사용한 애플리케이션을 구축할 수 있는 개발자의 수를 급격하게 늘렸으며, 블록체인이 zk 증명의 초기 수요자가 되는 것을 가능하게 했다 [SP124].

이러한 지수적 성능 향상과 범용 zkVM의 결합은 암호화 컴퓨팅 패러다임의 채택을 가속화하기 위해 필요한 요소들을 재검토할 시점임을 시사한다. ZK 증명은 대규모 AI 시스템이나 비트코인 채굴 수준의 연산 집약적인 작업이다. 예를 들어 블록체인의 상태 전이 함수의 실행을 증명하는 것과 같은 실제 업무는 GPU와 같은 특수 하드웨어를 필요로 하며, 미래에는 맞춤형 ASIC이 필요할 수도 있다. ZK 기술의 채택이 가속화됨에 따라, 증명은 저전력 지역에 데이터센터를 구축하는 것부터 특수 하드웨어의 배치에 이르기까지 인프라 공급자 생태계의 존재를 필연적으로 요구하게 된다. 블록체인 사용 사례에 있어서는, 증명이 탈중앙화되어 있어야 하며, 고장 시 신뢰성과 생존성을 제공할 수 있도록 지리적으로 분산된 증명 운영자와 홈 증명자(home prover)의 존재가 필요하다.

요청자, 증명자, 인프라 공급자로 구성된 이 생태계를 실현하려면, 하드웨어 가속, 증명자의 탈중앙화, zk 증명의 비용 경쟁을 적절히 인센티브화 할 수 있는 글로벌 규모의 조율과 네트워크가 필요하다. 증명 기술의 발전이 최종 요청자에게 전가되도록 보장하려면, 이 네트워크는 단일 zkVM과 공동 설계되어야 한다. 네트워크 공동 설계는 요청자가 지속적인 성능 향상을 경험하는 표준화된 오픈소스 zkVM 위에서 애플리케이션을 작성할 수 있도록 하며, 하드웨어 팀과 인프라 공급자는 통합된 플랫폼 위에서 협업할 수 있도록 한다. 증명자 간의 조율과 경쟁의 결합은 최대 효율 네트워크의 창출을 위한 촉매가 된다.

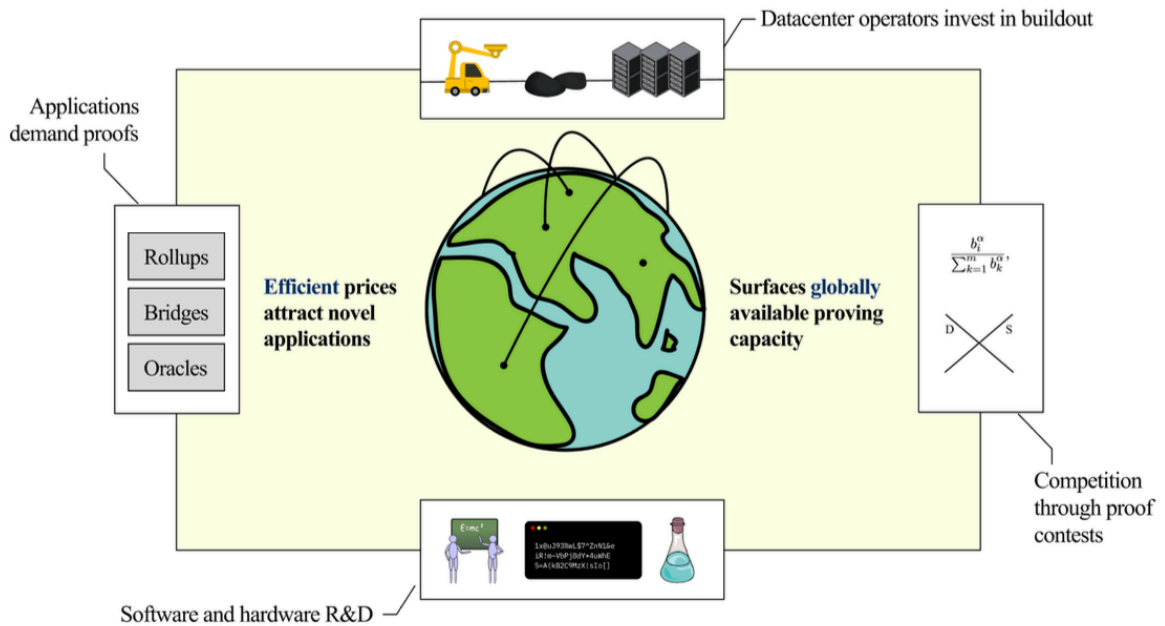
2 서싱트 네트워크



[그림 2: 서싱트 네트워크는 프루프 옥션을 기반으로 요청자에게 통합된 경험을 제공하는 전 세계적 분산 증명 클러스터를 구축한다]

서싱트 네트워크는 SP1과 공동 설계되었고, 프루프 옥션이라 불리는 경쟁 기반 옥션 메커니즘에 의해 구동되는 전 세계적 분산 증명 클러스터의 개념을 도입하여, 세계의 증명 능력을 획기적으로 확장한다 (그림 2).

1. 전 세계적 분산 증명 클러스터: 네트워크는 요청자들이 증명 요청을 제출할 수 있는 통합 플랫폼을 제공하고, 전 세계 누구나 증명 능력을 제공할 수 있도록 한다. 증명자들은 비허가 방식으로 네트워크에 참여할 수 있으며, 노드 소프트웨어를 실행함으로써 요청에 대해 높은 신뢰성을 보장받을 수 있다.
2. 프루프 옥션: 프루프 옥션 메커니즘은 증명 비용과 탈중앙화를 균형 있게 조절하는 새로운 유형의 옥션 방식이다. 이는 담보를 활용한 all-pay auction(모두 비용 지불 옥션)으로 작동하며, 탈중앙화된 증명자 집합을 유지하면서 요청에 대해 효과적인 가격 발견을 가능하게 하고, 스팸 증명, 경합, 악의적 방해 등의 문제를 해결한다. 프루프 옥션은 증명자와 요청을 조율하기 위해 설계된 애플리케이션 전용 블록체인위에서 정산된다.



[그림 3: 네트워크는 수요와 공급을 집계함으로써 증명 인프라와 연구 개발(R&D)을 위한 선순환 구조를 생성한다]

2.1 시장 구조

네트워크에는 두 가지 주요 참여자가 있다: zk 증명을 요구하는 애플리케이션과 증명 능력과 인프라를 제공하는 증명자들이다. 클러스터와 프루프 옥션 메커니즘은 공급과 수요를 집계하여, 선순환 구조를 유도하는 시장 구조를 만들어낸다 (그림 3). 이는 점점 더 효율적인 증명 인프라를 개발하기 위한 전 세계적 경쟁을 장려한다. SP1 개발과 네트워크 간의 긴밀한 통합은 증명에서의 기술적, 알고리즘적 발전이 요청자에게 빠르게 전파되도록 보장한다. 우리는 이 과정과 그것이 시장 참여자에게 어떤 영향을 미치는지 구체적으로 설명한다.

2.1.1 네트워크는 수요와 공급을 집계함으로써 선순환 구조를 작동시킨다

네트워크는 누구나 비허가 방식으로 통합 인터페이스를 통해 요청을 보낼 수 있고, 증명자가 프루프 옥션 메커니즘에 의해 결정되는 가격에 따라 자유롭게 용량을 제공할 수 있도록 명시적으로 설계되었다. 이러한 자유 시장의 존재는 다수의 애플리케이션으로부터의 수요와 다수의 증명자로부터의 공급을 집계한다. 이는 다음과 같은 함의를 가진다:

1. 통합된 요청 경험은 더 높은 효율성을 의미한다. 공급과 수요의 집계가 없다면,

증명 시장은 각 애플리케이션과 증명자가 맞춤형 계약을 맺거나 자체 인프라를 구축하는 방식으로 퇴화할 가능성이 높다. 장기적으로, 애플리케이션 팀이 전문적인 운영 및 기술적 역량이 필요한 증명 인프라를 직접 운영하는 것은 적합하지 않을 수 있다. OTC(Over-the-counter) 거래는 비효율적이며, 시장 내 마찰을 유발한다. 공급망을 집계하고 통합된 가격 책정 프로토콜을 제공하는 투명한 시장은 통합 시간과 개발 비용을 줄이고, 효율적인 가격을 형성한다.

2. 투명한 가격은 인프라 구축을 가속화한다. 투명한 가격 구조와 집계된 수요가 존재하면, 증명자는 보다 예측 가능한 경제 환경에 직면하게 된다. 수익 흐름이 더 예측 가능하므로, 증명자는 인프라를 더 빠르고 확신 있게 구축할 수 있다. 증명을 위한 투명한 시장이 존재한다는 것은, 증명자의 리스크가 효율적으로 가격화되고 자금 조달될 수 있음을 의미한다.
3. 낮은 자본 비용을 가진 홈 증명자는 증명 풀을 형성할 수 있다. 프로토콜은 전 세계 누구든지 여분의 증명 용량이 있다면 참여할 수 있도록 허용한다. 일반적으로, 홈 GPU 및 하드웨어를 보유한 개인은 여분 용량과 저렴한 전기 비용 덕분에 대형 운영자보다 훨씬 낮은 자본 비용을 가진다. 홈 증명자의 참여를 허용함으로써 증명 용량은 급격히 증가할 수 있고, 효율적인 가격도 유지될 수 있다. 섹션 3.4에서는 여러 증명자가 용량을 모아 프루프 옥션 메커니즘에 공동 입찰하는 증명 풀의 개념을 도입한다. 이는 홈 증명자가 경제적 리스크를 완화할 수 있게 해준다.
4. 비허가 참여는 증명자의 탈중앙화를 촉진한다. 시장 진입이 양쪽 모두에서 비허가이므로, 증명 용량을 제공하기 위한 진입 장벽이 최소화된다. 이로 인해, 어디에서든 증명자가 참여할 수 있으며 지리적 탈중앙화가 가능하다. 특정 참여자만 시장에 진입할 수 있는 구조와 달리, 이 구조에서는 하위 요청자 및 애플리케이션도 안정적으로 증명을 받을 수 있고, 특정 지역의 증명자에 의해 병목현상이 발생하지 않는다.

공급과 수요를 집계하는 시장은 역사적으로 항상 더 높은 효율성과 더 나은 가격을 모든 참여자에게 제공해 왔다. 이러한 선순환 구조는 수요 측과 공급 측 모두를 가속화한다.

2.1.2 프루프 옥션은 증명자 탈중앙화를 유지하면서 전세계적 경쟁을 유도한다

프루프 옥션 메커니즘은 증명 비용에 대한 경쟁을 유도하고, 탈중앙화된 증명자 집합을 장려함으로써, 높은 신뢰성과 생존성을 요구하는 애플리케이션이 최소 비용으로 증명을 받을 수 있도록 보장한다. 프루프 옥션은 요청자로부터 제출된 증명 요청이 제시한 수수료를 받기 위해 증명자들이 경쟁하는 전원지불형 옥션(all-pay auction)이다. 이 전원지불

형 옥션의 특성은 증명자의 탈중앙화를 유도한다. 이 메커니즘에 대한 상세 설명은 섹션 3에서 제공된다.

1. 프루프 옥션은 증명자 간 경쟁을 가능하게 한다. 무엇보다도, 프루프 옥션은 전 세계 어디에 있는 증명자든 네트워크에 참여하여 증명 비용에 대해 경쟁할 수 있도록 설계되었다. 이는 증명자가 요청자가 설정한 수수료를 받기 위해 옥션에 입찰하도록 함으로써 달성된다. 프루프 옥션은 수수료를 조정하여 시장 가격을 찾아냄으로써 가격 신호를 드러낸다.
2. 가격 발견은 재투자를 가능하게 한다. 프루프 옥션은 요청자에 의해 설정된 수수료 중 큰 비중을, 요청자가 요구한 기한 내에 저비용 ZK 증명을 효율적으로 생성한 증명자에게 지불한다. 이는 옥션에서의 수익이 보다 나은 증명 인프라, 알고리즘 및 하드웨어 개선에 재투자되도록 만든다. 증명자는 지속적으로 자신의 증명 인프라를 개선할 유인을 갖는다. 프루빙 풀 또한 개별 증명자에게 평준화된 수익을 제공함으로써, 그들이 플러그 앤 플레이(plug-and-play) 방식으로 네트워크에 참여할 수 있게 해준다.
3. 경쟁에서의 이익은 애플리케이션에 귀속된다. 최종 요청자는 증명자 간 경쟁의 주요 수혜자이다. 시간이 지남에 따라, 증명자는 요청자들이 요구하는 가장 중요한 특징—즉, 요청자 정의 기한 내에 전달되는 저비용 증명—을 두고 직접 경쟁하게 된다. 특히, 증명이 저비용으로 제공되지 않으면 확장 가능하지 않은 애플리케이션들이 존재한다. 네트워크는 이러한 애플리케이션을 위해 자유 시장 경쟁을 활용한다.
4. 이 메커니즘은 증명자 탈중앙화를 가능하게 한다. 단순한 역옥션과 같이 가장 저렴하게 증명을 생성할 수 있는 증명자가 옥션에서 100% 승리하는 나이브한 메커니즘과 달리, 프루프 옥션 메커니즘은 그러한 상황에서도 탈중앙화를 유도한다. 이는 톨록 콘테스트(Tullock contest)나 고정된 보상을 갖는 경쟁 대회 구조를 닮은 전원지불(all-pay) 기능을 통해 이루어진다. 이러한 구조는 넓은 범위의 증명자 집합을 유도하고, 증명자 집중화를 방지함으로써 네트워크의 장기적인 견고함을 확보한다. 이 과정은 일부 효율성을 희생해야 하며, 이는 때로는 더 높은 비용의 증명자에게 증명을 배정하게 됨을 의미한다. 그 대가로, 견고하고 탈중앙화된 증명자 집합을 갖게 되어 애플리케이션이 이 네트워크를 신뢰할 수 있게 된다.

2.2 관련 사례

구분	비허가 참여	인센티브	애플리케이션
비트코인	채굴자 설정	작업 증명(Proof-of-work)	탈중앙화된 화폐
파일코인	저장소 설정	복제 증명(Proof-of-replication)	탈중앙화된 저장소
알레오	증명자 설정	간결 작업 증명 (Proof-of-succinct work)	프라이빗 블록체인
서싱트 네트워크	증명자 설정	프루프 옵션	탈중앙화된 증명

[표 1: 인프라 구축을 유도한 네트워크들 간의 비교]

서싱트 네트워크는 비트코인과 파일코인과 같이 암호경제적 인센티브를 사용하여 글로벌 규모의 컴퓨팅 인프라 구축을 조율한 일련의 선행 작업들로부터 영감을 받았다. 현재 비트코인은 어떤 단일 기업이나 국가의 역량을 초과하는 해시레이트를 보유하고 있다. 이는 작업증명 프로토콜에 의해 설정된 인센티브로 인해 촉진되었다. 우리는 인센티브를 활용한 기존 인프라 구축의 주요 특징을 서싱트 네트워크와 비교한다. 표 1은 비허가 참여, 인센티브, 그리고 애플리케이션이라는 세 가지 축에서 이 비교를 요약한다.

1. 비트코인. 비트코인은 작업증명 메커니즘을 통해 채굴자에게 인센티브를 제공함으로써 탈중앙화된 화폐 시스템을 부트스트랩했다. 비트코인 네트워크의 인센티브는 하드웨어 투자와 특화된 에너지 관리 인프라를 촉진했다. 또한 개인들이 블록 생성을 위해 참여할 수 있는 대규모 채굴 풀의 형성도 이끌어냈다. 하지만 비트코인 요청자들은 채굴자에게 저비용과 저지연의 블록 생성을 명시적으로 요구하지는 않는다.
2. 파일코인(Filecoin). 파일코인은 시공간 증명(proof-of-spacetime)과 복제증명 메커니즘을 통해 탈중앙화된 스토리지 네트워크를 구성했다. 파일코인에서는 스토리지 공급자가 요청자에게 저장 용량을 제공함으로써 보상을 얻을 수 있고, 요청자는 장기적이고 암호화된 저장 서비스를 이용할 수 있다. 이 서비스는 저장이라는 상품이기 때문에, 스토리지 공급자로 참여하기 위한 주요 요건은 하드웨어 구매를 위한 자본이다. 저장 노드를 운영하는 데는 특화된 데이터센터 운영 기술이 요구될 수 있다. 반면, 증명 생성과는 달리 파일코인은 특수한 알고리즘 지식이나 하드웨어 개선에 대한 재투자를 요구하지 않는다.
3. 알레오(Aleo). 알레오는 지분증명과 간결작업증명의 혼합을 통해 프라이버시 우선 블록체인을 가능하게 했다. 알레오에서는 검증자가 트랜잭션 묶음을 네트워크에 제안하고, 증명자는 작업증명 채굴과 유사한 방식의 코인베이스 퍼즐을 해결하고 ZK 증명을 생성함으로써 보상을 얻는다. 이러한 퍼즐은 증명자가 하드웨어 가속

에 투자하도록 유도한다. 하지만 알레오의 증명자는 최종 요청자에게 비용 효율적인 증명을 제공해야 하는 문제에 직면하지 않는다. 이로 인해 증명자는 채굴로 인해 발생하는 중복 작업이나 경합을 감내할 수 있다.

3 프루프 옥션

이제 우리는 프루프 옥션 메커니즘을 소개한다. 이는 네트워크 내에서 요청을 증명자에게 할당하고, 비용 효율성과 탈중앙화라는 두 가지 목표를 균형 있게 조율하면서 수수료를 획득할 수 있도록 하는 옥션 방식이다. 언제든지 요청자들은 $\{r_1, \dots, r_n\}$ 의 제출된 증명 요청 집합을 보냈고, $\{p_1, \dots, p_m\}$ 의 증명자 집합이 이를 증명할 수 있도록 대기하고 있다. 각 요청 r_j 는 요청자로부터 지불되는 수수료 f_j 해당 요청에 대한 증명을 생성하는 데 요구되는 작업량을 나타내는 사이클 수 s_j , 그리고 요청 할당 후 요청자가 기다릴 수 있는 최대 시간인 기한을 포함한다. 증명자들은 자신이 증명할 수 있는 최대 사이클 수에 대한 사적 용량과 사이클당 한계 비용 c_j 를 갖는다. 증명 요청을 증명자에게 할당하는 어떤 메커니즘이든 다음의 기준들을 충족해야 한다.

1. 효율성. 메커니즘은 가장 높은 가치의 요청을 가장 낮은 비용의 증명자에게 매칭시켜 잉여를 극대화해야 하며, 그에 따라 요청자에게 낮은 가격을 제공해야 한다. 증명자들은 요청자에게 우대 가격을 제공하기 위해 경쟁해야 한다.
2. 요청자 경험. 요청자는 투명하고 경쟁력 있는 가격을 경험해야 한다. 요청은 요청자가 지정한 기한 내에 매우 높은 신뢰도로 처리되어야 한다. 증명을 요청하는 행위는 단순해야 한다.
3. 증명자 탈중앙화. 메커니즘은 탈중앙화된 증명자 집합을 장려하고 홈 증명자가 참여할 수 있도록 해야 한다. 규모의 경제로 인해 단일 증명자가 시장을 독점하게 되는 경우, 애플리케이션은 이들에게 의존할 수 없게 된다.
4. 스팸 증명. 증명자나 요청자 모두 수수료를 받기 위해 스팸 증명을 네트워크에 제출하도록 유도되어서는 안 된다. 네트워크는 실제 경제적 가치를 지닌 요청에 증명 용량과 보상을 최대한 할당해야 한다.
5. 처리량. 메커니즘은 요청 간의 경합을 최소화하고, 사용 가능한 증명 용량에 대해 요청을 최대한 할당하여 전체 처리량을 극대화해야 한다.

우리는 먼저 세 가지 후보 메커니즘을 살펴보고 위의 기준에 따라 평가한다. 표 2에서는 곧 설명할 프루프 옥션 메커니즘과 이들을 비교한다.

허수아비 메커니즘: 채굴. 첫 번째 접근 방식은 작업증명 기반 블록체인에서 흔히 볼 수 있는 방식이다. 이 접근에서 여러 증명자가 하나의 증명 요청에 동시에 작업을 수행하고, 결과 증명을 제출하여 보상을 얻는다. 보상을 할당하는 한 가지 방법은 증명자에게 특정 난이도 수준을 만족하는 증명을 제출하게 하는 것이다. 이 방식은 [KB23]과 알레오 [Wu23]에 의해 합의 프로토콜 설계 문맥에서 처음 제안되었다. [KB23]은 작업증명 과정의 여분 에너지를 활용하여 zk 증명을 생성하는 개념을 도입했다. 또 다른 보상 방식은 증명을 제출한 순서에 따라 보상을 부여하는 것이다. 가장 먼저 유효한 증명을 제출한 증명자가 가장 많은 보상을 받고, 그 이후에 제출한 증명자는 더 적은 보상을 받는다. 채굴의 장점은 탈중앙화된 증명자 집합을 가능하게 하며, 홈 증명자나 소규모 하드웨어 팀도 네트워크에 계속 참여할 수 있다는 점이다. 그러나 채굴은 많은 증명자가 동일한 요청을 동시에 작업하게 되어 불필요한 중복 증명이 생성되며, 이로 인해 비용이 크게 증가하고 처리량이 감소한다. 또한 증명자가 난이도 기준으로 인센티브를 받을 경우, 실제 경제적 가치는 없지만 난이도만 높은 요청을 제출해 보상을 얻으려는 인센티브가 생긴다.

구분	채굴	지분 기반 선택	역옥션	프루프 옥션
효율성	X	X	✓	✓
요청자 경험	X	X	✓	✓
증명자 분산화	✓	✓	X	✓
스팸 증명 방지	X	✓	✓	✓
처리량	X	✓	✓	✓

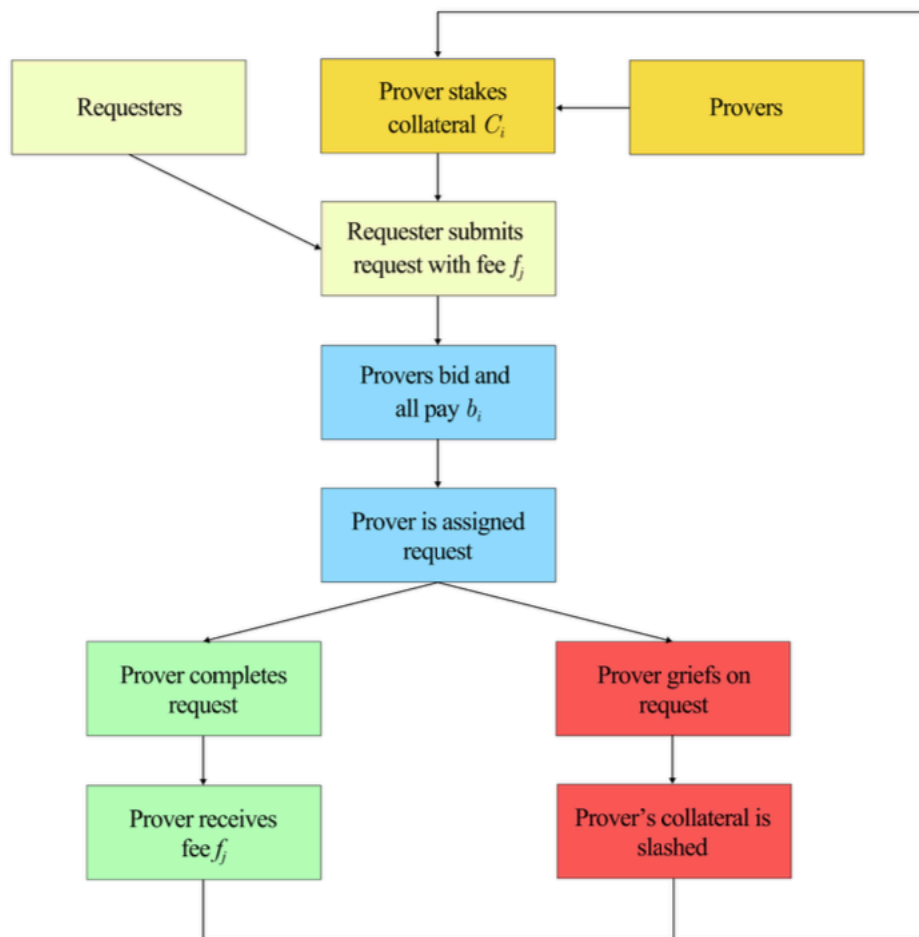
[표 2: 여러 대안 메커니즘과 프루프 옥션 비교 평가]

허수아비 메커니즘: 지분 기반 선택. 두 번째 접근 방식은 지분 기반 선택을 통해 증명자를 요청에 할당하는 것이다. 이는 증명자에게 담보 또는 지분을 예치하게 하고, 보유한 지분에 비례하여 요청을 할당받는 확률을 부여함으로써 구현할 수 있다. 이 방식의 장점은 각 요청을 단일 증명자에게만 할당하여 경합을 방지할 수 있다는 것이다. 그러나 이 방식이 단독으로 구현되고, 시장 균형 가격을 찾는 수수료 메커니즘이 존재하지 않으면, 비용에 대한 경쟁을 직접적으로 유도하지 못한다. 이 메커니즘은 알고리즘과 하드웨어 향상을 목표로 하는 증명자 운영 인센티브와, 자본 운용에 기반한 스테이킹 서비스 운영 인센티브를 분리한다.

허수아비 메커니즘: 역옥션. 세 번째 접근 방식은 증명자에게 가능한 한 낮은 가격으로 증명을 제공하도록 하는 경쟁 옥션에 참여하게 하는 것이다. 이 방식에서 증명자는 역옥션 또는 조달 옥션에 입찰하여 증명 요청을 충족시킬 권리를 획득하려고 한다. 증명자는

각 요청에 대해 입찰가를 제출하며, 이 입찰가는 해당 요청을 수행할 수 있는 최소 가격으로 해석된다. 승자는 최저 입찰가를 제시한 증명자이며, 해당 가격 또는 두 번째로 낮은 가격으로 낙찰될 수 있다. 이 방식은 요청을 효율적으로 할당하고, 단일 증명자에게 요청을 할당함으로써 경합을 최소화한다. 하지만 다른 모든 증명자보다 낮은 비용으로 증명을 생성할 수 있는 단일 증명자가 모든 옵션을 독식할 가능성이 있으므로, 극심한 증명자 집중화를 초래할 수 있다.

3.1 메커니즘 설명



[그림 4: 프루프 옵션은 증명자에게 요청에 입찰하기 위해 담보를 예치하도록 요구한다. 승리한 증명자는 증명을 할당받고, 지정된 기한 내에 이를 완료해야 하며, 그렇지 않을 경우 담보가 슬래시될 수 있다]

프루프 옥션 메커니즘의 주요한 참신함은 이전에 소개된 메커니즘들을 개선하면서, 요구되는 기준을 충족하고 요청자에게 경쟁력 있는 가격을 제공하는 동시에 탈중앙화된 증명자 집합을 장려한다는 점에 있다. 프루프 옥션은 지분기반 선택을 연상시키는 담보와, 단순 역옥션을 연상시키는 전원지불형 옥션을 혼합하여, 증명자들이 증명 생성을 두고 경쟁하도록 유도하면서 시장 균형 가격(market clearing fees)을 형성한다.

이 설계에서, 증명자는 증명 요청을 생성할 권리를 부여받기 위한 전원지불형 옥션 또는 톨릭 콘테스트에 참여하기 위해 담보를 예치한다. 톨릭 콘테스트는 고정된 보상에 대해 참가자들이 경쟁하는 형태를 모델링한 것이다 [BTT80]. 이는 블록체인 맥락에서도 연구되어 왔으며, 대표적으로 비트코인 채굴 [LS20], 이더리움 블록 생성 [BGR24], 그리고 블록 생성의 탈중앙화를 장려하기 위한 제안 메커니즘 [NGR24] 등에서 활용되었다. 이 설계에서 옥션에 참여하는 것은 증명자가 증명을 생성할 기회를 두고 경쟁하게 한다.

옥션에서 증명자의 입찰은 증명을 생성할 권리를 얻기 위해 지불할 의사가 있는 금액으로 해석된다. 모든 증명자는 입찰액을 지불하며, 승자는 입찰액의 함수에 따라 확률적으로 무작위로 선택된다.

프루프 옥션의 전원지불형 옥션 기능은 증명에 대한 경쟁을 유도한다. 옥션에서 승리하기 위해 증명자는 경쟁력 있는 입찰을 제출해야 하기 때문이다. 담보는 “무위험(nothing-at-stake)” 문제를 해결하는 역할을 하며, 증명자가 배정된 요청을 방해하지 않도록 유도한다. 우리는 먼저 프루프 옥션에서 사용하는 기본 구성요소들을 소개한다. 메커니즘의 개요는 (그림 4)에 도식적으로 나타나 있다.

검열 저항적인 게시판. 먼저, 우리는 검열에 저항할 수 있는 공개 게시판이 존재한다고 가정한다. 네트워크 구현의 경우, 이는 애플리케이션 전용 블록체인을 사용하며, 네트워크 구현에 대한 더 많은 내용은 섹션 4에서 제공한다. 게시판은 $READ(\cdot)$, $WRITE(\cdot)$, $EXECUTE(\cdot)$ 라는 기능을 제공한다. $READ(\cdot)$ 함수는 호출한 사람이 게시판에 기록된 모든 메시지를 읽을 수 있도록 하며, $WRITE(m)$ 함수는 요청자가 메시지 m 을 게시판에 기록할 수 있게 한다. $EXECUTE(\cdot)$ 함수는 알고리즘의 출력을 계산하고 그것을 게시판에 기록하게 해주며, 이는 스마트 계약기능으로 구현할 수 있다.

진입과 담보. 먼저, 각 증명자 p_i 는 증명 요청에 대해 입찰할 수 있는 권한을 받기 전에 담보금 C_i 를 예치한다. 이 담보는 증명자가 배정된 요청을 방해하는 것을 방지하기 위해 설정되며, 입찰도 이 담보에서 차감된다. 담보는 증명자가 증명에 참여하면서 “무위험” 상태가 되지 않도록 방지한다. 각 증명자가 예치하는 담보의 양은 그들이 참여할 수 있는 옥션 수를 반영한다.

메커니즘. 요청자에 의해 증명요청 r_j 가 $WRITE(r_j)$ 를 통해 게시판에 기록되며, 그 즉시 전체 증명자 집합에게 $READ(\cdot)$ 를 통해 공개된다. 증명자들은 요청을 증명할 권리를 얻기

위해 $b_i, \dots, b_m$ 의 입찰가를 제시하며, 이 입찰가는 증명자의 담보에서 차감된다. 입찰은 증명자가 요청자 r_j 로부터 f_j 를 받고 해당 증명을 완료하기 위해 지불할 의사가 있는 금액으로 해석된다. 옥션은 다음 확률로 증명을 증명자 p_i 에게 할당함으로써 마무리된다:

$$\frac{b_i^\alpha}{\sum_{k=1}^m b_k^\alpha},$$

여기서 $\alpha > 0$ 는 프로토콜이 설정하는 파라미터이다. 모든 증명자는 자신의 입찰액을 지불하며, 이 입찰액은 계약에 의해 수집된 후 요청자에게 리베이트 형태로 환급되거나 입찰자에게 시간이 지나면서 환불될 수 있다.

이 메커니즘의 해석은 다음과 같다: 요청을 수행할 권리에 대해 가장 많은 비용을 지불할 의사가 있는 증명자가 가장 높은 확률로 승리하지만, 적은 금액을 입찰한 다른 증명자들도 일정 확률로 승리할 수 있다. 분산의 정도는 α 에 의해 결정된다. $\alpha = 0$ 일 경우, 요청은 입찰자에게 균등한 확률로 할당된다. $\alpha = 1$ 일 경우, 할당 확률은 각 증명자의 입찰액에 비례한다. α 가 무한대로 증가하면, 증명은 점점 더 최고 입찰자에게 할당된다. 승리한 증명자는 해당 요청을 완료하고, 마감기한 내에 증명이 완료되면 f_j 금액이 요청자로부터 승리한 증명자에게 이전된다. 만약 기한 전에 어떤 증명도 제출되지 않으면 요청은 만료되며, 해당 요청을 증명하기로 배정되었던 증명자의 담보는 슬래시된다. 지불 및 담보 처리 로직은 EXECUTE($\cdot$)를 통해 처리될 수 있다.

반복 요청에 대한 확장. 프루프 옥션 메커니즘은 단일 요청뿐 아니라 롤업이나 반복적인 트랜잭션을 가진 애플리케이션처럼 시간이 지남에 따라 반복되는 요청에도 확장 가능하다. 이 확장된 형태는 금전적인 교환 없이 작동하는 메커니즘이다. 이 경우, 요청자의 수수료 f_j 는 사이클 수 s_j 를 가진 반복 요청 하나당 지불하고자 하는 금액으로 해석된다. 이제 각 증명자는 전원지불형 옥션에서 돈을 입찰하는 대신, 사전에 증명 요청을 처리하기 위한 슬롯 b_i 를 예약한다. 증명자들이 예약한 총 슬롯 수는 가격을 결정한다. 이전의 금전 기반 메커니즘과 달리, 이 경우 증명당 가격은 $f_j - \sum b_i$ 로 감소된다. 증명자 p_i 는 전체 요청 중 $b_i / \sum b_i$ 의 비율만큼 증명할 권리를 할당받고, 증명자 p_i 는 이 비율에 따라 라운드로빈 방식으로 순환한다.

이 메커니즘의 장점은 각 요청마다 옥션에 입찰하지 않고도 탈중앙화된 증명자 집합을 달성할 수 있다는 것이다.

이제 이 반복 모델에서 증명자의 행동이 앞서 설명한 각 요청에 대한 전원지불형 옥션과 어떻게 연관되는지를 설명한다. 각 증명자는 증명당 한계 비용 c_i 를 가진다고 가정한다. 모든 사람이 순환하는 단일 사이클에서 증명자의 총 이익은, 할당받은 슬롯 수 b_i 와 슬

롯당 이익의 곱이다:

$$b_i (f_j - \sum b_i - c_i s_j)$$

이를 $\sum b_i$ 로 나누면, 증명당 이익은 다음과 같다:

$$(b_i / \sum b_i)(f_j - c_i s_j) - b_i$$

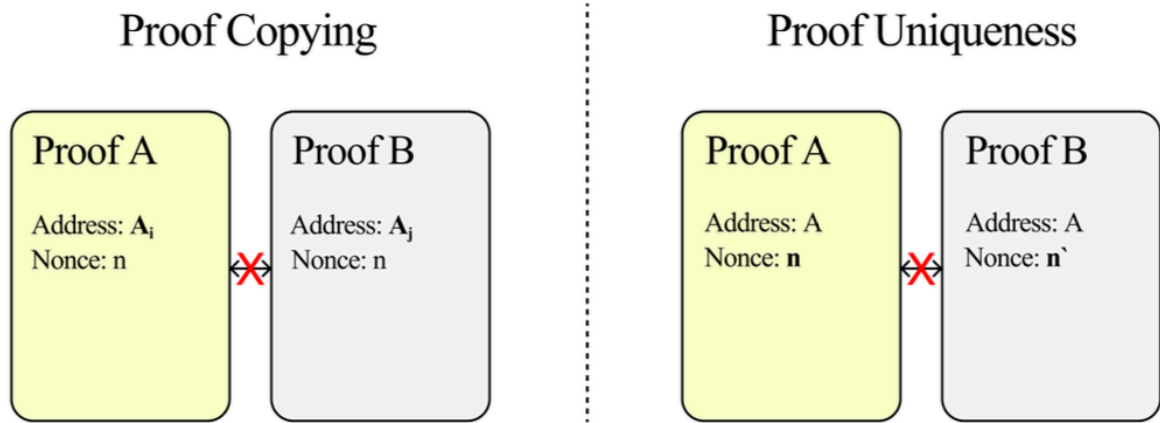
이는 이전의 비반복 메커니즘에서 증명자가 b_i 만큼 입찰하고, 증명당 이익이 $f_j - c_i s_j$ 이며, $\alpha = 1$ 인 경우와 동일하게 해석될 수 있다.

담보 설정. 담보 c_i 는 증명자가 참여할 수 있는 옥션 수를 제한한다. 증명자가 현재 입찰하고 있는 수수료 총합은 언제나 그들이 예치한 담보보다 작아야 한다. 네트워크는 예치된 담보에 따라 증명자가 참여할 수 있는 옥션 수를 자동으로 제한한다.

수수료 설정. 수수료 f_j 를 설정하는 메커니즘은 요청을 모두 처리하면서 옥션 내에서 증명자 다양성을 유지해야 한다. 우리가 고려하는 수수료 메커니즘은 고정된 f 에 따라 모든 요청에 대해 $f_j = f \times s_j$ 인 통일된 사이클당 수수료를 유지한다. 수수료가 높을수록 옥션에 여러 입찰자가 참여할 가능성이 커진다. 제출된 요청이 이전 타임스텝에 남아 있었다면 수수료를 증가시키는 제어 시스템을 통해, 100% 요청 처리율을 달성할 수 있도록 수수료를 조정할 수 있다. 증명자 다양성을 보장할 수 있도록 수수료가 충분히 높게 설정되도록 하기 위해, 전체 요청 중 일부에 대해 단순한 더치 옥션(Dutch auction)을 병행할 수 있다. 이 옥션은 할인된 가격에서 시작하여, 단순 역옥션에서 어떤 수수료 수준에서 정산될지를 파악할 수 있게 해준다. 이를 통해 프루프 옥션 메커니즘은 증명자 다양성을 유도할 수 있도록 보다 높은 수수료를 안전하게 설정할 수 있다. 이러한 수수료 조정 메커니즘을 어떻게 설계해야 조작 없이 다양한 증명자 집합이 유지될 수 있을지는 향후 연구 주제이다. 부록 C에서는 여러 증명자를 지원하기 위해 필요한 최소 거래 수수료를 그들의 비용 함수에 따라 도출한다.

입찰 하한 설정. 경쟁적인 입찰을 유도하기 위해, 프로토콜은 입찰의 하한을 설정하고 이를 시간이 지남에 따라 점진적으로 증가시킬 수 있다. 이는 증명자의 품질과 요청자가 경험하는 비용을 향상시키는 효과가 있다. 증명 풀과 하드웨어 팀은 옥션에 참여하기 위해 하드웨어 및 증명 소프트웨어를 향상시켜야 하며, 이러한 진입 비용은 성능이 향상될수록 요청자가 비용 효율적인 증명을 받을 수 있도록 보장한다.

3.2 메커니즘 구현



[그림 5: SP1과의 네트워크 공동 설계는 증명의 복제 및 작업 재사용을 방지한다]

메커니즘의 실제 구현은 복사된 증명이나 재사용된 작업과 같은 여러 실패 모드를 방지해야 한다 (그림 5). 우리는 네트워크에 제출된 완료된 증명들에 적용되는 변경 사항을 설명한다. 이는 실제로 네트워크가 SP1과 공동 설계됨으로써 실현된다. 예를 들어, 증명 요청 r_j 가 증명자 p_i 에 의해 처리되었다고 가정하자. 네트워크에서 증명은 증명자 p_i 의 온체인 주소 a_i 와 요청 당시 생성된 고유 논스 n 의 함수이다. 우리는 이를 간결하게 증명(r_j, a_i, n)으로 표기한다. 증명은 다음의 속성을 만족하도록 설계된다.

내장된 증명자 주소: 복사 방지. 한 증명자가 생성한 증명이 다른 증명자에 의해 복사되는 것을 방지하기 위해, 증명자의 주소 정보를 증명에 포함시킨다. 우리가 원하는 주요 속성은 $a_k \neq a_i$ 인 어떤 증명자 a_k 에 대해, 증명(r_j, a_i, n)과 증명(r_j, a_k, n')을 구별할 수 있어야 한다는 것이다. 따라서 증명자는 다른 증명자가 게시한 증명을 단순히 재사용하여 보상이나 수수료를 획득할 수 없다. 이는 SP1에서 증명 생성 시 증명자 주소를 내장함으로써 구현할 수 있다.

고유 논스: 재사용 방지. 증명자가 동일한 작업을 반복 재사용하는 것을 막기 위해, 요청 시 생성된 고유 논스를 증명에 포함시킨다. 이 논스는 하위 증명 시스템의 챌린저(challenger)에 포함될 수 있으며, 온체인 베리파이어는 해당 논스가 사용되었는지 검증할 수 있다. 우리가 원하는 주요 속성은, 모든 a_i 에 대해 $n \neq n'$ 이면 증명(r_j, a_i, n)과 증명(r_j, a_i, n')을 구별할 수 있어야 한다는 것이다. 논스는 요청 시마다 고유하게 생성되기 때문에, 증명자는 자신의 이전 작업을 재사용할 수 없다.

3.3 분석 및 인센티브

이제 프루프 옥션가 설정한 인센티브의 주요 특징들과 그것이 다른 메커니즘들이 직면한 문제를 어떻게 해결하는지를 설명한다. 우리는 전원 지불 기능이 비용 경쟁과 탈중앙화 사이에서 어떤 균형을 이루는지, 시빌(Sybil) 공격에 대한 저항력, 그리고 채굴에서 발생하는 경합을 해소하여 어떻게 처리량을 증가시키는지 고려한다.

증명자 경쟁. 프루프 옥션 메커니즘은 요청을 처리할 권리를 두고 증명자가 입찰하도록 요구함으로써 증명에 대한 경쟁을 유도한다. 증명자가 요청에 대해 입찰하도록 요구함으로써, 이 메커니즘은 증명자의 인센티브를 요청자 요구와 일치시킨다. 즉, 경쟁력 있는 증명을 생성할 수 있는 증명자를 찾는 것이다. 우리는 m 개의 증명자가 있고, 각각이 증명당 한계 비용 $c_1 < c_2 < \dots < c_m$ 을 가질 때, 수수료 f 와 사이클 수 s , 그리고 $\alpha = 1$ 인 증명 요청에 대해 프루프 옥션에 참여하는 상황을 고려한다. 이 경우, 증명자가 입찰 b_i 를 하고, 나머지 증명자들이 b_{-i} 를 입찰했을 때 해당 증명자의 효용은 다음과 같다:

$$u_i(b_i, b_{-i}) = \frac{b_i}{\sum_{j=1}^m b_j} (f - c_i s) - b_i.$$

$f - c_i s > 0$ 일 때, 우리는 일차 조건 $\partial u_i / \partial b_i (b_i, b_{-i}) = 0$ 을 사용하여 각 증명자의 균형 입찰 b_i^* 를 계산할 수 있다. 이 조건은 다음과 같다:

$$\frac{\partial u_i}{\partial b_i} (b_i^*, b_{-i}^*) = (f - c_i s) \frac{\sum_{k \neq i} b_k^*}{(\sum_{k=1}^m b_k^*)^2} - 1 = 0.$$

이 조건을 재정렬하면 다음과 같다:

$$\frac{\sum_{k \neq i} b_k^*}{(\sum_{k=1}^m b_k^*)^2} = \frac{1}{(f - c_i s)},$$

모든 증명자에 대해 이를 합하면:

$$\sum_{i=1}^m \frac{\sum_{k \neq i} b_k^*}{(\sum_{k=1}^m b_k^*)^2} = \sum_{i=1}^m \frac{1}{(f - c_i s)}.$$

이제 $\sum_{i=1}^m \sum_{k \neq i} b_k^* = (m-1) \sum_{k=1}^m b_k^*$ 임을 주목하면,

$$\sum_{k=1}^m b_k^* = \frac{m-1}{\sum_{i=1}^m \frac{1}{f - c_i s}} \quad (1)$$

$$= \frac{m-1}{m} H(f - c_1 s, \dots, f - c_m s), \quad (2)$$

여기서 H 는 조화 평균을 의미한다.

입찰이 시간이 지남에 따라 요청자에게 리베이트로 환급되는 설정에서, 우리는 이것을 다음과 같이 해석할 수 있다: 증명자들의 비용이 가장 효율적인 증명자의 비용과 매우 근접해 있다면, 요청자에게 제시되는 유효 가격은 거의 최고의 증명자 비용에 가까워진다. 반면, 증명자 간 비용 차이가 클 경우 유효 가격은 더 높아질 수 있다. 부록 B에서는 리베이트 구조와 탈중앙화 선호가 단순 역옥션과 어떻게 비교되는지를 모델링한 내용을 제공한다.

증명자 탈중앙화. 프루프 옥션가 유도하는 할당 메커니즘(및 일반적인 톨릭 콘테스트)은 본질적으로 다양한 증명자 집합의 참여를 인센티브화하며, 이는 비트코인의 채굴자, 이더리움의 검증자, [NGR24]에서 설명된 "실행 티켓(execution ticket)" 기반 블록 빌더 등 블록체인에서 탈중앙화된 서비스 제공자 집합을 달성하려는 시도들의 기반이 되었다.

단순한 역옥션는 항상 가장 낮은 가격으로 입찰한 증명자에게 증명을 할당한다. 이는 증명을 효율적으로 할당할 수는 있으나, 증명을 지속적으로 가장 효율적으로 생성할 수 있는 단일 증명자가 있을 경우, 다른 증명자가 입찰할 유인이 사라지게 되어 견고한 증명자 마켓플레이스를 형성하지 못할 수 있다.

반면, $\alpha = 1$ 일 때 프루프 옥션에서의 비례 할당 규칙은 각 증명자의 입찰액에 비례하여 증명을 할당한다. 이로 인해 이미 높은 금액을 입찰한 증명자는 입찰을 더 늘릴수록 수익의 한계 효용이 감소하는 구조가 된다 (전체 입찰 합계가 증가하면, 자신이 입찰한 금액의 당첨 확률이 줄어든다). 이 메커니즘은 단일 증명자가 수수료의 100%를 독식하는 것을 어렵게 만들며, 소규모 입찰자도 일부 확률로 당첨될 수 있기 때문에 0보다 큰 입찰을 하는 것이 이득이 되는 구조다.

톨릭 콘테스트는 탈중앙화를 장려하지만, 트레이드오프도 존재한다. 때때로 덜 효율적인 증명자에게 증명을 할당하기 때문에, 단순 역옥션에 비해 요청자 입장에서는 증명 비용이 더 높아질 수 있다. 이 메커니즘은 증명자 다양성이 주는 장기적 견고함과 증명자 효율성이 주는 단기적 이점을 균형 있게 맞출 수 있도록 적절히 파라미터화되어야 한다.

시빌 저항성. 프루프 옥션 메커니즘은 전원 지불형 구조와 입찰을 위한 담보 요구를 통해, 증명자가 자신의 신원을 쪼개어(Sybil 공격) 입찰하는 것을 억제한다. 우리는 증명자가 b_i 라는 입찰을 M 개의 크기 b_i/M 의 입찰로 쪼개어 제출하는 경우를 고려한다. 이때 수수료 f , 사이클 수 s , 임의의 α 를 갖는 프루프 옥션에 대해, 변경된 입찰 프로파일 $\tilde{b}_i$ 에서 해당 증명자의 효용은 다음과 같다:

$$u_i(\tilde{b}_i, b_{-i}) = M \left(\frac{\left(\frac{b_i}{M}\right)^\alpha}{M \left(\frac{b_i}{M}\right)^\alpha + S} (f - c_i s) - \frac{b_i}{M} \right),$$

여기서 $S = \sum_{k \neq i} b_k^\alpha$ 로서, 나머지 증명자들의 입찰 고정 값이다.

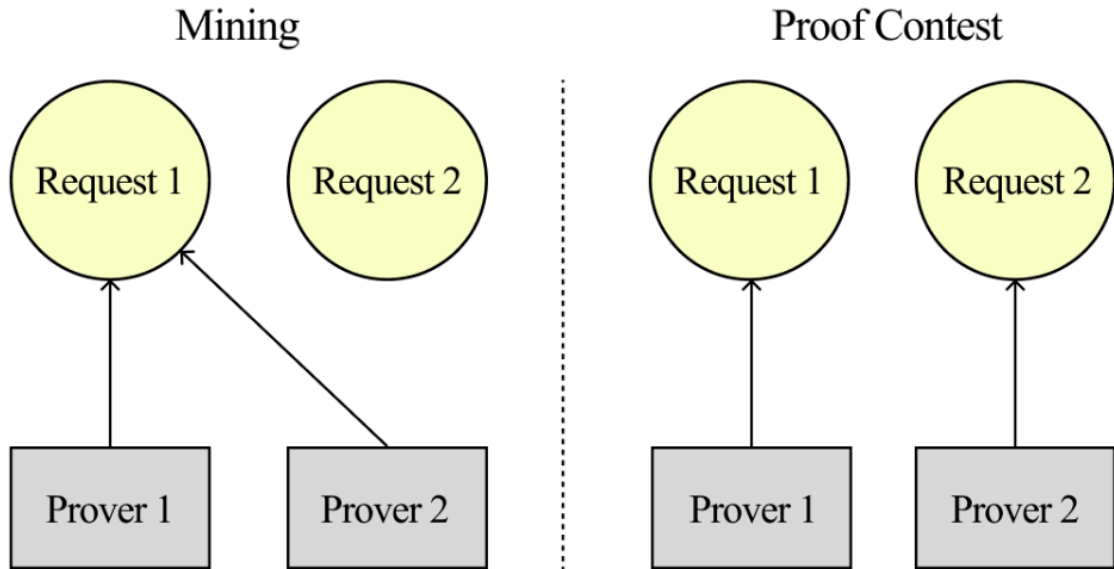
부록 D에서는 $\alpha \geq 1$ 인 경우에 증명자가 자신의 입찰을 여러 개로 쪼개는 것이 이득이 되지 않음을 증명한다. 즉, $u_i(b_i, b_{-i}) \geq u_i(\tilde{b}_i, \tilde{b}_{-i})$.

처리량. 프루프 옥션 메커니즘은 증명 요청을 입찰을 통해 단일 증명자에게 할당함으로써, 채굴 방식에서 발생하는 경합을 해소하고 처리량 저하를 방지한다. 우리는 매 시간마다 n 개의 요청이 도착하고 m 개의 증명자가 이를 증명할 수 있는 모델을 고려한다. 각 증명자는 정확히 하나의 요청을 처리할 수 있는 용량을 가진다.

채굴과 같은 메커니즘에서는 증명자가 작업할 요청을 자유롭게 선택할 수 있기 때문에, 여러 증명자가 하나의 요청을 선택해 일부 요청은 처리되지 않을 수 있다. 반면, 프루프 옥션에서는 입찰 단계를 통해 경합을 줄이고, 사용 가능한 증명 용량에 요청을 정확히 매칭시킨다.

우리는 채굴 방식에서 각 증명자가 무작위로 요청 하나를 선택한다고 가정한다. 부록 E에서는 채굴과 프루프 옥션 간의 처리량 차이를 다음 식으로 나타낸다:

$$\text{처리량 감소율} = 1 - \frac{n}{m} \left[1 - \left(\frac{n-1}{n} \right)^m \right]$$



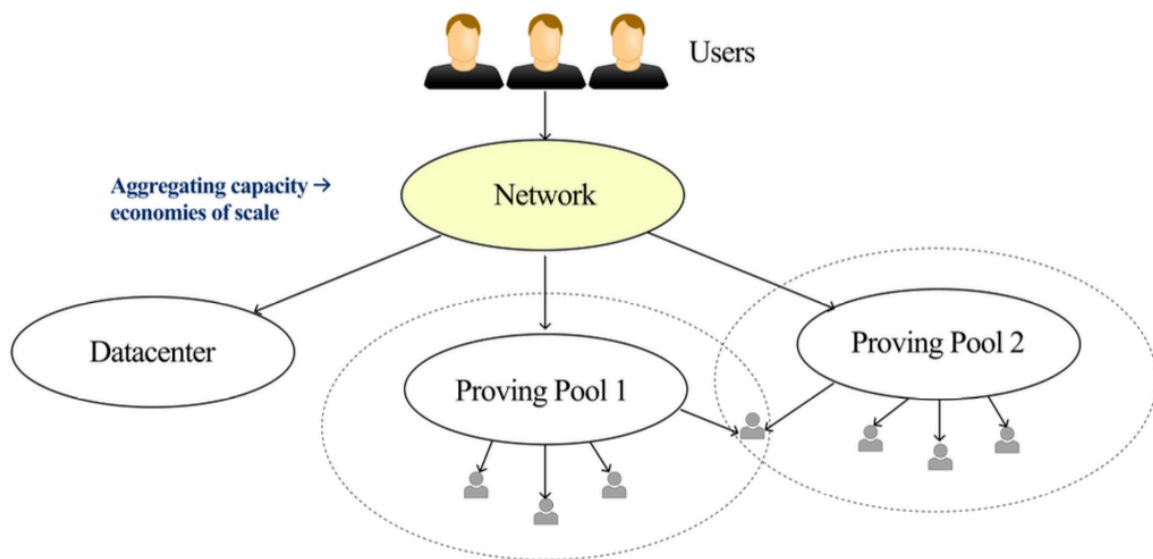
[그림 6: 프루프 옥션은 각 요청을 단일 증명자에게 할당함으로써 채굴에서 발생하는 경합을 해소하고, 그에 따라 처리량을 증가시킨다]

간단한 예로, 요청이 2개($n = 2$)이고 증명자도 2명($m = 2$)인 경우를 (그림 6)에서 보여준다. 이 경우 처리량 감소율은 25%이다. 이는 프루프 옥션에서 시간 단위당 최대 처리량

이 2이지만, 채굴에서는 완료된 요청의 기대값이 $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 2 = 1.5$ 가 되므로, 처리량 감소율은 $100 \left(1 - \frac{1.5}{2}\right) = 25\%$ 가 된다.

스팸 증명. 이 모델에서는 증명자가 받는 모든 보상은 요청자가 지불한 것이므로, 증명자가 실제 경제적 수요가 없는 "스팸 증명"을 제출할 인센티브가 없다. 또한 증명자는 스팸 요청을 제출해도 다른 증명자로부터 입찰을 받을 수 없다. 이는 입찰금이 계약에 의해 수집되어 리베이트로 균등 분배되기 때문이다. 향후 작업에서는, 네트워크 보상이 증명 비용을 보조하되, 경제적 가치가 없는 증명 요청을 유도하지 않도록 설계하는 방법을 다룰 것이다.

3.4 증명 풀



[그림 7: 증명 풀은 네트워크의 용량을 획기적으로 확장할 수 있으며, 흠 증명자들이 입찰 없이 참여할 수 있도록 해준다]

입찰에 직접 참여할 만큼 숙련도나 담보가 충분하지 않은 개별 증명자는 비트코인의 채굴 풀과 유사하게 요청 슬롯을 공동으로 입찰할 수 있는 증명 풀을 형성할 수 있다. 우리는 여러 증명자가 자신들의 용량을 모아 프루프 옥션 메커니즘에 공동 입찰하는 증명 풀 개념을 도입한다. 이 풀은 흠 환경의 증명자가 옥션 입찰을 배우지 않고도 증명을 생

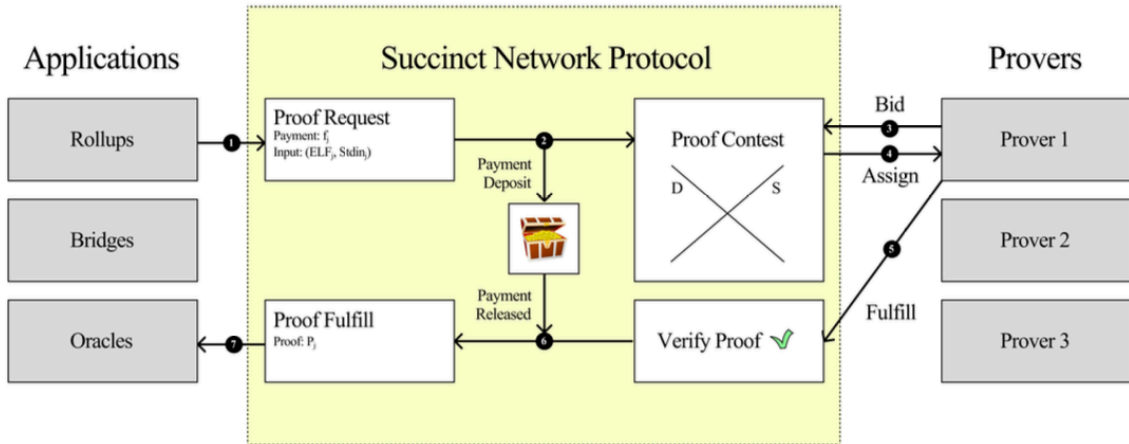
성할 수 있게 하며, 비허가 방식으로 입찰 없이도 조율될 수 있게 한다. 이는 누구나 참여할 수 있는 글로벌 분산 증명 클러스터의 기초를 형성한다. 증명 풀은 특수 하드웨어나 규모의 경제가 가져오는 중앙집중화 효과에 대한 견제 역할을 할 수 있다. 네트워크 내 증명 풀 구조는 (그림 7)에 나타나 있다.

비허가 증명 풀. 증명 풀 구성원은 반드시 입찰에 참여하지 않아도 되기 때문에, 풀 자체도 비허가하게 구성될 수 있고, 홈 증명자가 진입하기 위한 기술 장벽도 매우 낮다. 풀 운영자는 전 세계적으로 증명 용량을 자유 시장을 통해 집계하고 수수료를 벌 기회를 갖는다. 풀 수수료는 비트코인 채굴 풀처럼, 구성원에게 용량을 질의한 후 그 비율에 따라 수수료를 분배하는 방식으로 지급될 수 있다. 증명 풀의 분산되고 글로벌한 특성은 이 네트워크의 핵심적인 특징이다.

풀의 경쟁력. 증명 풀은 초기 하드웨어 팀이 요구하는 대규모 선행 자본 비용을 필요로 하지 않는다는 추가 이점을 가진다. 풀은 증명 수요가 높은 시간에 용량을 온라인 상태로 유도하고, 수요가 적을 때는 오프라인으로 유도하는 인센티브 구조를 설정할 수 있다. 만약 풀이 주로 홈 증명자로 구성되어 있다면, 전기세나 임대료와 같은 지속적인 운영 비용도 부담하지 않는다. 풀은 전기 비용이 낮은 지역의 용량을 탐색할 수도 있다. 따라서 잘 운영되는 증명 풀은 하드웨어 팀과 경쟁력을 유지할 수 있으며, 수수료 획득이라는 인센티브 아래 최적화를 지속할 수 있다. 이는 작업증명 기반 암호화폐의 채굴 풀이 경쟁력을 유지하는 방식과 유사하다.

증명의 위임(Proof delegation). 풀링은 증명 용량을 여러 개의 풀에 위임하는 것도 가능하게 한다. 이는 홈 셋업을 가진 증명자들이 메커니즘에서 보다 공격적이거나 덜 공격적으로 입찰하는 풀에 참여함으로써 자신의 리스크 선호를 표현할 수 있다는 것을 의미한다. 풀은 그들의 필요에 따라 증명 용량을 조율할 수 있다. 이 모델은 지분증명 기반 통화, 특히 탈중앙화 스테이킹 풀에서 발견되는 위임 방식과 유사하다. 글로벌 증명 풀의 등장과 함께 증명 리스크를 집단적으로 풀링할 수 있는 금융 도구들이 나타날 것으로 예상된다.

4 네트워크 구조



프루프 옥션 메커니즘을 소개한 이후, 우리는 이제 네트워크를 실제로 애플리케이션 전용 블록체인을 통해 어떻게 구현할 수 있을지를 다룬다. 먼저, 네트워크가 가져야 할 바람직한 속성과 프루프 옥션이 어떻게 실현될 수 있는지를 설명하고, 구현이 왜 애플리케이션 전용 블록체인을 필요로 하는지를 보여준다. 이어서, 아키텍처와 요청자 및 증명자가 어떻게 참여할 수 있는지를 설명하며, 이 아키텍처는 (그림 8)에 나타나 있다.

[그림 8 : Succinct 네트워크 구조]

4.1 Implementation Requirements

증명자에게 요청을 할당하는 네트워크를 위한 프루프 옥션 메커니즘의 어떤 구현도 다음 조건을 만족해야 한다.

1. 낮은 지연 시간. 구현은 결제, 입찰, 증명 수행을 조율해야 한다. 따라서 시스템은 낮은 지연 시간과 높은 처리량을 갖추어야 한다.
2. 검열 저항성. 구현은 하위 애플리케이션들에게 그들의 요청에 대해 검열 저항성 보장을 제공해야 한다.
3. 생존성. 일부 애플리케이션의 경우 증명의 지연은 의미 있는 경제적 피해를 야기할 수 있다. 구현은 높은 신뢰성과 생존성을 바탕으로 요청 및 이행을 안정적으로 조율해야 한다.

이러한 이유로 우리는 신뢰된 중개자 시스템이 아닌 애플리케이션 전용 블록체인을 통해 요청자와 증명자를 조율하기로 선택했다. 이 블록체인은 하위 애플리케이션에 필요한 검열 저항성과 탈중앙화를 제공한다. 요청자는 요청을 블록체인에 제출하고, 증명자는 그

위에서 입찰하고 증명을 이행한다. 블록체인은 SP1과 공동 설계되어 증명 생성 및 검증 과정을 매끄럽게 하고, 스팸 제출 및 방해 벡터를 방지한다. 이 블록체인은 현대적 레이더 1이나 롤업으로 구현될 수 있으며 점진적인 탈중앙화를 목표로 설계된다. 구체적인 구현 내용은 본 백서의 범위를 벗어난다. 비허가 참여와 결제는 누구나 자금을 블록체인으로 브리지하고 즉시 요청을 시작할 수 있게 하며, 이는 요청자 경험 측면에서 바람직하다.

4.1.1 성능. 이 블록체인은 성능을 극대화하고 이행의 불필요한 지연을 최소화하도록 설계되었다. 짧은 블록 시간 덕분에 각 요청에 대해 빠르게 프루프 옵션을 수행할 수 있다. 입찰은 짧고 사전 지정된 시간 내에 이루어진다. 블록체인은 또한 요청과 관련된 데이터를 임시로 저장할 수 있는 데이터 저장소의 이점을 누린다.

4.1.2 합의. 블록체인은 점진적 탈중앙화를 목표로 설계되었으며, 요청, 입찰, 증명 이행에 대해 합의를 형성하는 노드들을 통해 견고한 검열 저항성과 생존성 보장을 제공한다. 만약 모던 레이어 1으로 구현된다면, 이는 블록체인을 위한 탈중앙화된 검증자 집합을 가지게 된다. 롤업으로 구현된다면, 이는 요청의 순서에 대해 합의를 형성할 수 있는 탈중앙화된 시퀀서(sequencer) 계층을 가진다는 것을 의미한다.

4.2 참여

네트워크에는 두 가지 주요 참여자가 있다. 요청을 제출하는 요청자와 증명을 수행하는 증명자들이다. 또한 릴레이어(relayer)라 불리는 제삼자가 있는데, 이들은 프로그램 실행을 시뮬레이션하는 등의 서비스를 제공하여 요청자 경험을 향상시킨다. 요청자와 증명자가 어떻게 참여하는지 설명하며, 릴레이어의 역할은 부록 A에서 다룬다.

4.2.1 요청을 제출하는 요청자. 요청자는 프로그램, 입력값(stdin), max_cycles 파라미터, 최대 수수료 f_j , 기한(deadline), vkey를 입력하여 네트워크에 증명 요청을 제출한다. 프로그램과 입력은 증명자가 증명을 생성하는 데 필요한 데이터이다. 프로그램과 입력의 저장 방법에 대한 추가 설명은 부록 A에 제공되어 있다. max_cycles는 요청자가 해당 증명이 소모할 것으로 예상하는 최대 RISC-V 사이클 수이며, f_j 는 요청자가 이 요청에 대해 지불하고자 하는 최대 금액이다. 이 수수료는 요청자가 독립적으로 설정할 수도 있고, 이더리움의 가스 추정 기능과 유사한 시스템의 제안에 따라 설정할 수도 있다. 요청을 제출하면 요청자의 수수료는 에스스로에 보관되어 방해로 방지한다. 마지막으로 vkey는 증명

검증자가 증명의 정확성을 확인할 수 있도록 사용하는 키이며, 초기 설정 단계에서 생성된다. 제출된 모든 요청은 고유한 증명_id를 가진다. 증명 요청은 표준화된 알피씨(RPC) 엔드포인트를 통해 네트워크에 전송될 수 있다. 요청자 입장에서 이 네트워크는 높은 생존성과 경쟁력을 갖춘 증명 요청 인터페이스 역할을 한다. 증명자가 증명을 제출하면 요청자는 이를 네트워크에서 목적 체인(destination chains)으로 직접 전송할 수 있다.

4.2.2 증명자: 입찰 및 증명 제출. 증명자는 하드웨어를 연결하고 노드 소프트웨어를 실행함으로써 비허가로 네트워크에 참여할 수 있다. 증명자는 증명을 생성하기 위한 용량과 운영 비용을 가지지만, 이 정보는 네트워크에 반드시 노출되지 않아도 된다. 입찰 과정은 이 정보를 간접적으로 도출하는 데 도움을 준다. 입찰과 증명 이행은 애플리케이션 전용 블록체인 위에서 수행된다. 증명자는 먼저 제출된 증명 요청을 확인하고 프로그램 및 입력 데이터를 가져온다.

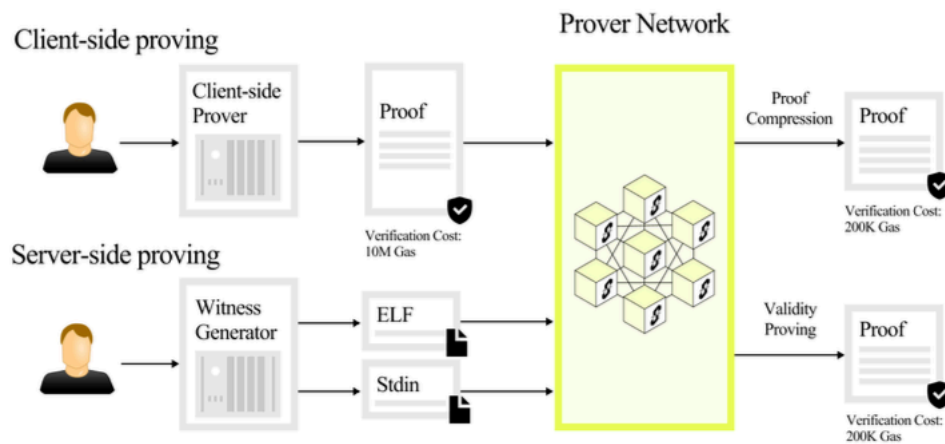
입찰. 그런 다음 증명자는 프루프 옥션에 입찰하여 요청을 완료할 권리를 얻는다. 프루프 옥션은 요청이 공개된 후 온체인에서 수행된다. 입찰 창은 사전에 고정되어 있어 투명성을 확보한다. 블록체인은 증명 생성 시간보다 훨씬 짧은 시간 단위로 입찰이 이루어질 수 있도록 짧은 블록 시간으로 설계되어 있다.

증명 제출. 배정된 증명자가 증명 생성을 완료하면, 그들은 이를 애플리케이션 전용 블록체인에서 제출할 수 있다. 증명자는 proof_id, 프로그램, stdin, 그리고 증명 정보를 입력한다. 증명 요청 시 함께 제출된 vkey는 verifier가 해당 증명이 올바르게 생성되었는지를 검증할 수 있게 해준다. SP1은 세 가지 유형의 증명 생성을 지원한다: CORE, COMPRESSED, 그리고 GROTH16/PLONK. CORE 증명은 프로그램 실행량에 비례하여 크기가 커지고, COMPRESSED 증명은 고정된 크기를 가지지만 생성 비용이 더 높다. GROTH16과 PLONK 증명은 생성 비용이 가장 높지만, 매우 압축된 상태이며 온체인 검증이 가능하다. CORE 증명의 가변적이고 큰 크기 때문에, 네트워크는 요청자가 COMPRESSED 또는 GROTH16/PLONK 증명을 요청할 수 있도록 허용한다.

5 전세계 소프트웨어를 증명하다

이 네트워크는 인터넷 상에서의 증명 가능성을 가속화하는 데 있어 중요한 함의를 가진다. 증명 가능성은 애플리케이션이 고비용 연산과 비즈니스 로직을 신뢰할 수 있는 중개자 없이 외부에 위임할 수 있게 하며, 요청자에게는 민감한 정보가 비공개로 유지되고 연산 실행이 정확하다는 보장을 제공한다. 하나의 비허가 및 글로벌한 네트워크 아래에서 증명 용량이 집약됨으로써, 탈중앙화 시스템은 공통된 표준을 기반으로 최소한의 오

버헤드로 확장할 수 있게 된다. 이는 가격을 낮추고 요청자 경험을 향상시켜, zk를 사용하는 애플리케이션에 순풍을 불어넣는다.



[그림 9 : 서버 측 증명을 통해 탈중앙화 애플리케이션의 확장을 가능하게 하며, 클라이언트 측 증명을 통해 보편적인 프라이버시를 실현]

요청자는 이 네트워크와 두 가지 방식으로 상호작용할 수 있다: 독립적인 서버 측 증명자로서 또는 클라이언트 측 증명과 결합된 방식이다 (그림 9). 서버 측 증명은 공용 블록체인이거나 롤업처럼 계산을 위임해야 하는 애플리케이션에 유용하다. 클라이언트 측 증명은 요청자 정보를 비공개로 유지하면서 큰 증명을 생성하고, 이를 네트워크를 통해 압축하는 방식이 필요한 프라이버시 애플리케이션에 적합하다. 이제 이 네트워크를 사용하거나 활용할 수 있는 여러 애플리케이션들을 설명한다.

1. 롤업. 이더리움의 롤업 중심 로드맵은 과거의 거짓 증명 기술 사용에서 벗어나 점점 더 트랜잭션 검증을 위해 zk 기술을 사용하는 방향으로 전환되고 있다. zk 롤업의 낮은 비용과 사용 편의성으로 인해 트랜잭션 수요가 증가함에 따라, 요구되는 증명의 수도 빠르게 증가하게 될 것이다. 롤업은 경쟁력 있는 가격과 높은 신뢰성으로 제공되는 증명을 위해 네트워크를 활용할 수 있으며, 이로써 모든 탈중앙화 시스템은 검증 가능성을 희생하지 않고도 처리량을 확장할 수 있게 된다.
2. 오라클 및 브릿지. 탈중앙화 시스템의 다른 구성 요소들 역시 이 네트워크를 사용할 수 있는데, 대표적으로 오라클과 브릿지가 있다. zk 오라클은 외부 데이터 피드로부터 블록체인으로의 입력을 신뢰 없이 제공할 수 있으며, zk 브릿지는 모든 블록체인 간의 상호운용성을 가능하게 한다. 이러한 애플리케이션은 단일 장애 지점에 의존할 수 없기 때문에, 탈중앙화된 증명자 집합이 필수적이다.

3. 신원 및 인증. 영지식 속성은 요청자의 비공개 입력이 누구에게도 공개되지 않은 채 증명에 포함될 수 있음을 보장한다. 이는 개인정보를 필요로 하는 신원 및 인증 애플리케이션에 필수적인 특성이다. 증명 과정에서도 이러한 입력이 비공개로 유지되도록 하기 위해, 네트워크와 함께 클라이언트 측 증명을 병행 사용할 수 있다.
4. 신용평가 및 감사. 현재 신용평가, 공증, 감사 기능을 수행하는 기업들은 높은 운영 비용과 복잡한 레거시 데이터베이스를 관리해야 한다. 이 네트워크를 사용하는 애플리케이션은 zk 증명을 감사 형식으로 활용함으로써 이러한 작업의 비용을 대폭 줄일 수 있다.
5. 검증가능한 추론. AI 애플리케이션은 주어진 질의에 대한 AI 모델의 출력을 요청자에게 증명하는 데 네트워크를 활용할 수 있다. 이 네트워크는 높은 처리량의 추론 애플리케이션에서 필요한 대량의 증명을 제공할 수 있게 한다.
6. 코프로세서(coprocessor). 블록체인은 네트워크를 활용해 오프체인 연산을 수행하는 코프로세서를 사용할 수 있다. 이로써 블록체인은 과거 데이터를 접근하고, 정교한 경제 모델을 바탕으로 수수료를 계산하며, 제3자가 블록체인을 신뢰 없이 질의할 수 있도록 할 수 있다.
7. 외부 클라우드 컴퓨팅(Outsourced cloud computing). 이 네트워크는 범용 외부 위임 컴퓨팅 레이어로 사용될 수 있다. 요청자는 클라우드 서버에서 실행할 법한 프로그램을 증명자에게 전송할 수 있으며, 이때 기존 서버가 제공하지 못하는 신뢰성과 검증 가능성을 네트워크를 통해 확보할 수 있다.

6 결론

우리는 서싱트 네트워크를 제안한다. 이는 zk 증명 생성을 위한 요청자 요청을 분산된 증명자 집합이 경쟁 옥션인 프루프 옥션을 통해 처리하도록 조율하는 프로토콜이며, 전 세계적 분산 증명 클러스터를 구축하기 위한 것이다. 이 네트워크는 임의의 결정론적 러스트(Rust) 프로그램을 증명할 수 있는 zkVM인 SP1과 공동 설계되어 통합되었다. 프루프 옥션은 요청을 증명자에게 할당할 때 비용 경쟁과 증명자 탈중앙화의 균형을 유지하며, 요청자와 증명자를 조율하기 위해 특별히 설계된 애플리케이션 전용 블록체인에서 정산된다. 이 네트워크는 증명자로서의 비허가 참여를 허용하고 자유 시장 경쟁을 유도한다. 이는 다른 암호경제 시스템과 마찬가지로 증명 생성을 위한 광범위한 인프라 구축을 가능하게 하며, 블록체인 확장성부터 프라이버시까지 다양한 애플리케이션이 견고하고 경쟁력 있는 증명에 접근할 수 있도록 보장한다. 인센티브를 활용해 전 세계의 증명 능력

을 획기적으로 확장함으로써, 이 네트워크는 모든 이들에게 저비용, 저지연의 zk 증명 생성을 제공한다.

7 Acknowledgments

우리는 이 백서에 귀중한 피드백을 제공한 Tarun Chitra, Ciamac Moallemi, Dave White, 그리고 Max Resnick에게 감사를 전합니다.

참고문헌

[Nak08] [But13] [BS+13] [BS+14] [Dra24] [GMR85] [Halo20] [Plonky22] Satoshi Nakamoto. 비트코인: A peer-to-peer electronic cash system. 2008. url: <https://비트코인.org/비트코인.pdf>.

Vitalik Buterin. Ethereum whitepaper. 2013. url: <https://ethereum.org/en/whitepaper/>.

Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. "SNARKs for C: Verifying program executions succinctly and in zero knowledge". In: Annual Cryptology Conference. Springer. 2013, pp. 90–108.

Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. "Succinct {Non-Interactive} zero knowledge for a von neumann architecture". In: 23rd USENIX Security Symposium (USENIX Security 14). 2014, pp. 781–796.

Justin Drake. [AMA] We are EF Research (Pt. 12: 05 September, 2024). 2024. url: https://www.reddit.com/r/ethereum/comments/1f81ntr/comment/llmfi28/?utm_source=share&utm_medium=web3x&utm_name=web3xcss&utm_term=1&utm_content=share_button.

Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The knowledge complexity of interactive proof-systems". In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing. 1985, pp. 291–304.

The Zcash Team. Halo2. <https://github.com/zcash/halo2>. 2020. PolygonZero. Plonky2. 2022. url: <https://github.com/0xPolygonZero/plonky2>.

[Plonky23] Polygon. Plonky3. 2023. url: <https://github.com/Plonky3/Plonky3>.

[SP124] Succinct Labs. Introducing SP1: A performant, open-source, contributor-friendly zkVM. Feb. 2024. url: <https://blog.succinct.xyz/introducing-sp1/>.

[Ben17] Juan Benet. Filecoin: A Decentralized Storage Network. Protocol Labs. 2017. url: <https://filecoin.io/filecoin.pdf>.

[Wu23] Howard Wu. The Aleo Whitepaper. <https://hackmd.io/@aleo/HJRwnnhM6>. Oct. 2023.

[KB23] Assimakis Kattis and Joseph Bonneau. "Proof of necessary work:succinct state verification with fairness guarantees". In: International Conference on Financial Cryptography and Data Security.Springer. 2023, pp. 18–35.

[BTT80] James Buchanan, Robert Tollison, and Gordon Tullock. "Toward a theory of the rent-seeking society". In: Texas A&M University economics series (1980).

[LS20] Jacob D Leshno and Philipp Strack. "비트코인: An axiomatic approach and an impossibility theorem". In: American Economic Review: Insights 2.3 (2020), pp. 269–286.

[BGR24] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. "Centralization in block building and proposer-builder separation". In:arXiv preprint arXiv:2401.12120 (2024).

[NGR24] Michael Neuder, Pranav Garimidi, and Tim Roughgarden. On blockspace distribution mechanisms. <https://ethresear.ch/t/on-block-space-distribution-mechanisms/19764/1>. June 2024.

A 네트워크 구조

A.1 데이터 저장소

실제로 프로그램과 입력 데이터는 매우 클 수 있으며, 블록체인에 저장하기 어려울 수 있다. 이를 위해 네트워크는 외부의 임시 저장소를 사용하여 요청 데이터를 저장한다. 임시 저장소에 있는 관련 데이터의 artifact ID는 데이터의 가용성 증명과 증명에 필요한 프로그램 및 stdin 질의에 사용될 수 있다. 대규모 온체인 데이터 저장 기술이 발전함에 따라, 시간이 지나면서 증명에 필요한 모든 데이터가 요청자로부터 증명자에게 신뢰 없이 전달될 수 있게 될 것이다.

A.2 릴레이어

릴레이어는 요청자 경험을 향상시키고 증명자가 증명을 수행하기 위해 필요할 수 있는 추가 정보를 제공하는 제3자이다.

프로그램 시뮬레이션. 릴레이어는 요청에 연관된 공개된 입력값(public input)인

public_values를 계산하기 위해 프로그램을 시뮬레이션한다. 이 시뮬레이션 단계는 증명자가 잘못된 혹은 구성 오류가 있는 요청에 자원을 낭비하지 않도록 방지한다. 또한 요청자가 입력한 사이클 상한값 max_cycles는 지나치게 보수적일 수 있다. 릴레이어는 증명자보다 먼저 프로그램을 실행하여 정확한 사이클 수 s_j 를 계산함으로써, 실제 증명이 요구하는 작업량이 최대 사이클 수를 초과하지 않도록 보장한다. 릴레이어의 존재는 증명 과정에서 지연과 비효율을 초래하는 여러 공격 벡터를 방지해 준다. 예를 들어 증명자가 증명 도중 해당 요청을 이행할 수 없거나, 실제 사이클 수가 기대보다 높다는 사실을 뒤늦게 알게 되는 경우 등을 막는다.

릴레이어 보상(Relay payment). 릴레이어는 네트워크로 들어오는 모든 요청에 대해 표준화된 서비스를 제공하기 때문에, 시뮬레이션 결과와 사이클 수를 네트워크에 게시하는 작업에 대해 고정 수수료를 받는다. 실제로 프로그램 시뮬레이션은 증명 생성 비용 중 매우 적은 비율을 차지한다. 따라서 비허가 진입이 가능한 릴레이어 역할과 고정 수수료 모델의 조합은 증명자가 필요한 정보를 안정적으로 획득하게 하고 네트워크가 증명 이행을 지속할 수 있도록 한다. 릴레이어가 시뮬레이션 결과나 사이클 수를 진실되게 보고하도록 유도하기 위해 담보를 예치하게 한다. 증명자 역시 증명과정에서 시뮬레이션 단계를 거치므로, 릴레이어가 잘못된 출력을 보고했는지 쉽게 검증할 수 있다.

B. 증명자 옥션

프루프 옥션 메커니즘은 증명자가 옥션에 제출하는 입찰을 통해 경쟁하도록 인센티브를 부여한다. 시간이 지남에 따라 이 입찰액이 요청자에게 리베이트로 환급되는 설정에서는, 요청자가 실제로 받게 되는 유효 가격은 $f - \sum_{k=1}^m b_k^*$ 로 계산할 수 있다. 이 가격이 단순히 탈중앙화를 고려하지 않는 경쟁 옥션 모델에서의 결과와 어떻게 다른지 설명하기 위해, 프루프 옥션을 2등 가격 역옥션과 비교한다. 이 역옥션에서는 증명자들이 가능한 한 요청자의 거래 가격을 낮추는 방향으로 경쟁하며, 최저 입찰자가 두 번째로 낮은 가격에 승리한다. 2등가 옥션의 인센티브 정합성 때문에 균형 상태에서 요청자는 유효 가격으로 c_2s (두 번째로 효율적인 증명자의 비용)를 경험하게 된다. 따라서 탈중앙화된 증명자 집합을 지원하는 데 따른 초과 비용은 다음과 같이 계산된다:

$$E(c_1, \dots, c_m) = f - \frac{m-1}{m} H(f - c_1s, \dots, f - c_ms) - c_2s$$

여기서 H 는 조화 평균이다. 증명자의 한계 비용이 매우 유사한 경우 이 값은 거의 0에 가까우며, 몇몇 증명자가 비효율적일 경우 상당히 커질 수 있다.

C. Setting Fees

우리는 두 명의 증명자 (Alice와 Bob)가 $\alpha = 1$ 조건 하에 사이클 수 s 를 가진 요청에 대해 프루프 옥션에 입찰하는 모델을 고려한다. 이때 증명자가 b_i 를 입찰했을 때의 효용 함수는 다음과 같다:

$$\frac{b_i}{b_1 + b_2}(f - c_i s) - b_i$$

[NGR24]의 계산에 따르면, 수수료 f 에 대한 균형 입찰은 다음과 같다:

$$b_1^*(f) = \frac{(f - c_1 s)^2 (f - c_2 s)}{(2f - c_1 s - c_2 s)^2}, \quad b_2^*(f) = \frac{(f - c_2 s)^2 (f - c_1 s)}{(2f - c_1 s - c_2 s)^2}$$

따라서 유효 증명 가격은

$$f - b_1^*(f) - b_2^*(f) = f - \frac{(f - c_1 s)^2 (f - c_2 s)}{(2f - c_1 s - c_2 s)^2} - \frac{(f - c_2 s)^2 (f - c_1 s)}{(2f - c_1 s - c_2 s)^2}$$

요청자가 두 증명자 모두가 옥션에 남아 있도록 하면서 가장 낮은 가격을 지불하려면, 위 수식의 도함수를 f 에 대해 0으로 놓고 푼다:

$$\frac{2(f^2 - f c_1 s - f c_2 s + c_1 c_2 s^2)}{4f^2 - 4f c_1 s - 4f c_2 s + c_1^2 s^2 + 2c_1 c_2 s^2 + c_2^2 s^2} = 0$$

즉, $f^2 - f c_1 s - f c_2 s + c_1 c_2 s^2 = 0$ 이 되며, 이는 $(f - c_1 s)(f - c_2 s) = 0$ 을 의미하므로 $f = c_1 s$ 또는 $f = c_2 s$ 가 된다. 따라서 두 증명자 모두 옥션에 남아있게 하면서 요청자가 경험하는 가격을 최소화하는 수수료는 두 번째로 효율적인 증명자의 비용인 $c_2 s$ 이다. 직관적으로, 요청자는 최고의 증명자와 경쟁할 수 있도록 두 번째 최고의 증명자에게 인센티브를 제공함으로써 최소 유효 가격을 확보할 수 있다.

D. Sybil 저항성

증명자가 자신의 입찰 b_i 를 여러 개로 쪼개는 것이 이득이 될 수 있을까? 우리는 $\alpha \geq 1$ 인 모든 프루프 옥션 상황에서, 증명자가 이와 같은 전략으로 이익을 얻을 수 없음을 보인다.

증명자가 입찰한 금액 b_i 와, 나머지 증명자들의 가중치 합 $S = \sum_{k \neq i} b_k^\alpha$ 가 주어졌다고 하자. 수수료 f , 사이클 수 s 를 가진 프루프 옥션에서 증명자의 기대 효용은 다음과 같다:

$$u_i(b_i, b_{-i}) = \frac{b_i^\alpha}{\sum_{k=1}^m b_k^\alpha} (f - c_i s) - b_i \quad (4)$$

$$= \frac{b_i^\alpha}{b_i^\alpha + S} (f - c_i s) - b_i. \quad (5)$$

이제 증명자가 자신의 입찰 b_i 를 M 개의 동일한 입찰 b_i/M 으로 나누는 경우를 가정하자. 이때 수정된 입찰 프로파일 $\tilde{b}_i$ 에 대한 기대 효용은 다음과 같다

$$u_i(\tilde{b}_i, b_{-i}) = M \left(\frac{\left(\frac{b_i}{M}\right)^\alpha}{M \left(\frac{b_i}{M}\right)^\alpha + S} (f - c_i s) - \frac{b_i}{M} \right) \quad (6)$$

$$= \frac{\frac{b_i^\alpha}{M^{\alpha-1}}}{\frac{b_i^\alpha}{M^{\alpha-1}} + S} (f - c_i s) - b_i \quad (7)$$

$$= \frac{b_i^\alpha}{b_i^\alpha + SM^{\alpha-1}} (f - c_i s) - b_i, \quad (8)$$

마지막 등식은 분자와 분모에 $M^{\alpha-1}$ 을 곱함으로써 도출된다. 식 (5)와 식 (8)을 비교해보면, $\alpha \geq 1$ 인 모든 경우에 대해 다음이 성립함을 알 수 있다.

$$u_i(b_i, b_{-i}) - u_i(\tilde{b}_i, b_{-i}) = \frac{b_i^\alpha}{b_i^\alpha + S} (f - c_i s) - \frac{b_i^\alpha}{b_i^\alpha + SM^{\alpha-1}} (f - c_i s) \geq 0.$$

증명자는 자신의 입찰을 여러 개로 쪼개는 전략으로는 이득을 얻을 수 없다. 따라서 프루프 옥션에서는 입찰 분할에 대한 인센티브가 존재하지 않는다.

E. 처리량

요청 수 n 개와 증명자 수 m 개가 주어진 모델을 고려하자 (단, $m \leq n$). 각 증명자는 단 하나의 요청만 처리할 수 있다. 채굴 모델에서는 각 증명자가 무작위로 하나의 요청을 선택한다. 여러 증명자가 동일한 요청을 선택하는 경우, 경합이 발생하고 단 하나의 증명자만 요청을 완료하며 나머지는 대기 상태로 남는다. 반면, 프루프 옥션은 각 요청을 하나의 증명자에게만 할당하므로 경합을 해소하고 처리량을 보존한다. 이 경우 최대 처리량은 시간당 m 개의 증명이다.

우리는 n 개의 요청에 대해, 각 증명자가 무작위로 요청 하나를 선택하는 경우를 가정하고 경합으로 인한 순수 처리량 손실을 계산한다.

요청 r_j 를 정확히 k 명의 증명자가 선택할 확률은 다음과 같은 이항 분포를 따른다:

$$\mathbb{P}(\text{Exactly } k \text{ provers select } r_j) = \binom{m}{k} \left(\frac{1}{n}\right)^k \left(1 - \frac{1}{n}\right)^{m-k}$$

요청에 경합이 발생할 확률 ($k \geq 2$) 은

$$\begin{aligned} \mathbb{P}(\text{Contention on } r_j) &= 1 - \mathbb{P}(0 \text{ provers select } r_j) - \mathbb{P}(1 \text{ prover selects } r_j) \\ &= 1 - \left(1 - \frac{1}{n}\right)^m - m \left(\frac{1}{n}\right) \left(1 - \frac{1}{n}\right)^{m-1}. \end{aligned}$$

정확히 1명의 증명자가 선택한 요청 수의 기댓값은

$$\begin{aligned} \mathbb{E}[\text{Fulfilled without contention}] &= n \times \mathbb{P}(1 \text{ prover selects } r_j) \\ &= n \times \left[m \left(\frac{1}{n}\right) \left(1 - \frac{1}{n}\right)^{m-1} \right] \\ &= m \left(1 - \frac{1}{n}\right)^{m-1}. \end{aligned}$$

경합이 발생한 요청 중 실제로 처리된 요청 수의 기대값은

$$\begin{aligned} \mathbb{E}[\text{Fulfilled with contention}] &= n \times \mathbb{P}(\text{Contention on } r_j) \\ &= n \left[1 - \left(1 - \frac{1}{n}\right)^m - m \left(\frac{1}{n}\right) \left(1 - \frac{1}{n}\right)^{m-1} \right]. \end{aligned}$$

따라서 총 mining 기반 처리량은

$$\begin{aligned} \mathbb{E}[\text{Fulfilled (mining)}] &= m \left(1 - \frac{1}{n}\right)^{m-1} + n \left[1 - \left(1 - \frac{1}{n}\right)^m - m \left(\frac{1}{n}\right) \left(1 - \frac{1}{n}\right)^{m-1} \right] \\ &= n \left[1 - \left(1 - \frac{1}{n}\right)^m \right]. \end{aligned}$$

프루프 옵션이 달성할 수 있는 최대 처리량은 m 이므로, 처리량 손실은 다음과 같다:

$$\begin{aligned} \text{Throughput reduction} &= 1 - \frac{\mathbb{E}[\text{Fulfilled (mining)}]}{m} \\ &= 1 - \frac{n}{m} \left[1 - \left(1 - \frac{1}{n}\right)^m \right]. \end{aligned}$$