ZK State Channel 기반 하이브리드 롤업 분쟁 프로토콜: 오프체인 이등분과 온디맨드 유효성 증명

(ZK State Channel-based Hybrid Rollup Dispute Protocol: Off-chain Bisection with On-demand Validity Proofs)

요 약

본 논문은 Optimistic rollup의 7일 챌린지 기간과 다단계 온체인 사기 증명으로 인한 높은 비용·지연 문제를 해결하기 위해, 분쟁이 발생할 때에만 ZK 증명을 요구하는 반응형 유효성 증명(Responsive Validity Proof, RVP) 패러다임을 제안한다. 이를 Optimism 분쟁게임에 적용하기 위해 시퀀서와 챌린저 사이에 ZK State Channel을 구성하고, 73단계 이등분 프로토콜을 채널 내부에서 오프체인으로 수행한 뒤 단일 ZK proof로 압축하여 온체인에서 검증하는 아키텍처를 설계한다. 기존 ZK-EVM 프로젝트의 벤치마크(Polygon zkEVM, Scroll)를 기반으로 한 복잡도 분석 결과, 분쟁 경로에서 기존 옵티미스틱 롤업 대비 가스 비용이 약 99.6% 감소하고, 최종성 지연 시간은 7일에서 약 1 - 2시간 수준으로 단축될 수 있음을 보였다. 게임이론적 분석을 통해 챌린저 보증금을 적절히 설정할 경우 증명 비용 고갈 공격이 경제적으로 의미를 잃는 내쉬 균형이 형성됨을 보임으로써, 제안 시스템이 안전성과 활성(liveness)을 동시에 유지함을 확인한다.

ABSTRACT

Optimistic rollups incur high dispute costs and week-long withdrawal delays due to their on-chain interactive fraud-proof protocols. We address this limitation by proposing the Responsive Validity Proof (RVP) paradigm, which preserves optimistic execution in the common case while requiring zero-knowledge validity proofs only when a dispute is raised. We instantiate RVP for the Optimism fault-proof game by designing a ZK State Channel between the sequencer and a challenger: the 73-step bisection protocol is executed off-chain inside the channel, and the entire dispute is finally compressed into a single ZK proof that is verified on-chain. Based on complexity analysis calibrated with existing ZK-EVM benchmarks (Polygon zkEVM, Scroll) and historical Ethereum gas prices, our design reduces dispute-path gas costs by approximately 99.6% compared to existing optimistic rollups and shortens dispute finality from seven days to about one - two hours. A game-theoretic analysis of the bonding mechanism further shows that, above a modest bond threshold, rational adversaries have no incentive to launch repeated proving-cost exhaustion attacks, ensuring both safety and liveness.

키워드 : 블록체인, 옵티미스틱 롤업, 상태 채널, 영지식 증명, ZK-EVM, 레이어2 솔루션

Keywords: Blockchain, Optimistic rollup, State channel, Zero-knowledge proof, ZK-EVM, Layer 2 solution

Ⅰ. 서 론

블록체인 기술의 비약적인 발전과 함께 이더리움(Ethereum)은 스마트 컨트랙트를 기반으로 한 탈중앙화 금융(DeFi)과 다양한 애플리케이션을 지탱하는 핵심 인프라로 자리 잡았다. 하지만 네트워크 참여자가 급증함에 따라 메인넷(L1)의 트랜잭션 처리 용량 한계와 가스 비용 상승 문제는 이더리움의 대중화를 가로막는 주요 장벽이 되어왔다. 이러한 '블록체인 트릴레마(Blockchain Trilemma)'를 해결하기 위해, 이더리움 커뮤니티는 메인넷의 보안을 상속받으면서도 실행 레이어를 분리하여 확장성을 극대화하는 롤업(Rollup) 중심의 로드맵을 채택하였다[1][2].

롤업 솔루션은 데이터 가용성(Data Availability)을 온체인에 유지하면서 연산 검증 방식에 따라 크게 옵티미스틱 롤업(Optimistic rollup, ORU)과 영지식 롤업(ZK rollup, ZKR)으로 양분되어 발전해 왔다. 현재 Arbitrum과 Optimism으로 대표되는 옵티미스틱 롤업은 이더리움 가상 머신(Ethereum Virtual Machine, EVM)과의 높은 호환성과 낮은 구현 난이도, 저렴한 연산 비용을 무기로 L2 생태계의 상당한 점유율을 차지하고 있다[3][4].

그러나 현재의 옵티미스틱 롤업 아키텍처는 구조적인 '확정성(Finality)'과 '사용자 경험'의 딜레마를 안고 있다. 옵티미스틱 롤업은 시퀀서(Sequencer)가 제출한 상태 루트가 유효하다고 낙관적으로 가정하는 대신, 악의적인 행위가 감지될 경우 이를 반박할 수 있는 '사기 증명(Fraud Proof)' 기간을 둔다. 보안을 위해 설정된 이 약 7일간의 분쟁 기간(Challenge Period) 동안 사용자는 L2에서 L1으로 자산을 인출하는 것이 제한된다[5]. 이는 자본의 유동성을 억제하고 기회비용을 발생시켜 시스템 전체의 자본 효율성을 저하시키는 핵심 요인으로 작용한다.

반면, 대안으로 제시되는 ZK 롤업은 유효성 증명(Validity Proof)을 통해 수학적으로 즉각적인 확정성을 보장할 수 있으나, 매 배치(batch)마다 복잡한 영지식 증명을 생성해야 하므로 막대한 연산 자원이 소모되고 높은 가스 비용으로 이어진다[6][7]. 결과적으로 기존 L2 솔루션들은 "낮은 비용(ORU의 장점)"과 "빠른 확정성(ZKR의 장점)"을 동시에 만족시키지 못하는 근본적인 한계를 가진다.

이러한 확장성과 확정성 간의 상충 관계를 완화하기 위해 학계와 산업계에서는 다양한 최적화 모델이 제안되어 왔다. Arbitrum이 발표한 BoLD(Bounded Liquidity Delay) 프로토콜은 무허가 검증(Permissionless Validation) 환경에서 발생할 수 있는 지연 공격(Delay Attack) 및 검열 공격(Censorship Attack)을 효과적으로 방어하기 위해 모든 챌린지를 동시에 진행하는 All-vs-All 분쟁 구조와 유한 상한을 도입하였다[8]. BoLD는 탈중앙화된 검증자 환경에서 시스템 안전성을 획기적으로 강화했다는 점에서 중요한 기여를 했으나, 정직한 시나리오에서도 요구되는 기본 7일 챌린지 기간 자체는 단축하지 못한다는 구조적 한계를 지닌다. 즉, BoLD는 "보안성 강화"에는 성공했으나 "자본 효율성 개선"이라는 또 다른 과제는 여전히 남아있다.

또 다른 접근법인 상태 채널(State channel) 및 유동성 공급자를 활용한 빠른 인출 솔루션은 협조적인 참여자 사이에서만 즉각적인 확정성을 제공하며, 비협조적 경로로 진입할 경우 결국 느린 온체인 분쟁 해결 절차로 회귀해야 한다는 문제가 있다[9][10]. 최근에는 영지식 증명 기반 EVM(ZK-EVM) 기술의 발전에 힘입어 옵티미스틱과 ZK 방식을 결합하려는 다양한 하이브리드 모델이 제안되고 있으나[11][12], 많은 설계가 "모든 배치에 대해 결국 ZK 증명을 생성해야 한다"는 전제를 깔고 있어 ZK 롤업 특유의 높은 증명 비용에서 자유롭지 못하다.

본 연구는 이러한 한계를 극복하기 위해, "낙관적으로 실행하되 분쟁 발생 시에만 암호학적으로 증명한다"는 패러다임에 기반한 새로운 하이브리드 ZK-EVM 프로토콜, 즉 반응형 유효성 증명(Responsive Validity Proof, RVP)을 이론적 프레임워크로 제안한다. RVP의 핵심 아이디어는 평상시에는 기존 옵티미스틱 롤업과 동일하게 증명 없이 배치를 제출하여 낮은 비용과 높은 처리량을 유지하되, 챌린저에 의해 이의가 제기되는 분쟁 상황에서는 기존의 다중 라운드 상호작용 게임 대신 문제된 상태 전이에 대한 ZK 유효성 증명을 생성·제출함으로써 분쟁을 종결짓는 것이다. 이론적으로 이는 분쟁 과정을 단일 ZK proof 검증으로 수축시켜 인출 지연 시간을 대폭 단축할 가능성을 제공한다.

국내에서도 다양한 레이어2 확장성 솔루션의 특성을 비교 분석[13]과 ZK-SNARK 기반 블록체인 확장성 솔루션의 성능을 실증적으로 평가[14]와 같은 분야에서 활발하게 연구가 이루어지고 있다. 본 연구는 이러한 기존 연구를 토대로 옵티미스틱과 ZK 방식을 결합한 하이브리드 접근법의 새로운 가능성을 제시한다.

특히 본 논문에서는 RVP 패러다임을 Optimism 분쟁 게임에 구체적으로 적용하기 위한 프로토콜 설계안으로서, 시퀀서와 챌린저 사이에 가상 상태 채널을 구성하고 전체 분쟁 절차를 채널 내부에서 오프체인으로 실행한 뒤, 그 결과를 단일 ZK proof로 온체인에 제출하는 ZK 상태 채널 구조를 설계한다. 기존 상태 채널이 두 사용자 간 잔고 업데이트를 오프체인에서 합의하고 분쟁 시에만 증거를 제출하는 것과 유사하게, 제안 시스템은 롤업의 상태 전이를 시퀀서 - 챌린저 간 1:1 게임으로 추상화하여 분쟁 해결을 "ZK 증명 가능한 상태 채널" 문제로 환원한다.

II.관련연구

2.1 옵티미스틱 롤업 분쟁 해결 메커니즘

이더리움 롤업은 트랜잭션 실행을 오프체인에서 처리하고 압축된 데이터와 상태 루트만을 메인넷에 기록함으로써 확장성을 확보하는 솔루션이다[1]. 이중에서 옵티미스틱 롤업은 모든 트랜잭션이 정직하게 실행되었다고 가정하며, 시퀀서가 제출한 상태 루트에 대해 이의가 제기되지 않는 한 유효한 것으로 간주한다. 분쟁이 발생할 경우, 시스템은 사기 증명 메커니즘을 가동한다. 초기의 사기 증명은 전체 블록을 온체인에서 재실행하는 방식을 고려했으나, 가스 한도 문제를 해결하기 위해 현재는 Arbitrum 등이 채택한 '상호작용적 이진 분할(Interactive Bisection)' 프로토콜이 표준으로 자리 잡았다[3]. 이 방식은 챌린저와 방어자가 여러 라운드에 걸쳐 분쟁 범위를 좁혀 나간 뒤, 단일 옵코드 실행만으로 온체인에서 참/거짓을 판별하는 '원스텝 증명(One-step proof)'을 수행한다. Optimism의 경우 Cannon이라는 MIPS 기반 가상 머신을 사용하여 73단계의 이등분 프로토콜을 통해 단일 명령어 수준까지 분쟁을 좁힌다[5]. 이는 온체인 연산 비용을 최소화한다는 장점이 있으나, 상호작용 과정이 길어짐에 따라 최종 확정까지 약 7일이라는 긴 시간이 소요된다는 구조적 한계를 지닌다.

2.2 기존의 분쟁 해결 최적화 모델

옵티미스틱 롤업의 지연 문제와 보안 취약점을 해결하기 위해 다양한 최적화 모델이 연구되었다. 대표적으로 Arbitrum이 제안한 BoLD 프로토콜은 무허가 검증 환경에서 발생할 수 있는 지연 공격을 방어하는 데 초점을 맞춘다[8]. 기존 옵티미스틱 롤업에서는 악의적인 공격자가 다수의 챌린지를 순차적으로 생성하여 분쟁 기간을 무한정 연장할 수 있는 취약점이 존재했다.

BoLD는 이를 해결하기 위해 모든 챌린지가 동시에 진행되는 All-vs-All 분쟁 그래프 구조를 채택하고, 분쟁 처리에 필요한 총 기간에 고정된 상한선을 둠으로써 시스템의 안전성을 보장한다. 구체적으로 BoLD는 각 depth에서 발생 가능한 모든 주장을 병렬적으로 처리하며, 정직한 검증자가 모든 악의적 주장에 대응하는 worst-case 시나리오에서도 $O(\log N)$ 수준의 상한을 보장한다[8]. 하지만 BoLD는 악의적인 지연을 방지할 뿐, 정직한 시나리오에서도 요구되는 기본 7일의 챌린지 기간 자체를 단축하지는 못한다. 즉, 보안성은 강화되었으나 자본 효율성 측면에서의 개선은 제한적이다.

2.3 상태채널 기술

상태 채널은 두 참여자 간의 상태 업데이트를 오프체인에서 수행하고, 분쟁 발생 시에만 온체인 중재를 요청하는 L2 확장 솔루션이다. 상태 채널의 핵심 원리는 참여자들이 오프체인에서 서명된 상태 업데이트를 교환하다가, 일방이 협조를 거부하거나 부정 행위를 시도할 경우 가장 최근의 서명된 상태를 온체인에 제출하여 강제로 채널을 종료(Force close)하는 것이다.

범용 상태 채널 연구로는 Perun[9]이 대표적이다. Perun은 Universal Composability(UC) 프레임워크 기반의 형식 증명을 제공하며, 임의의 상태 전이를 지원하는 가상 채널 개념을 도입했다. 이는 본 연구의 ZK 상태 채널 설계에 안전성 모델링 측면에서 중요한 영감을 제공한다. Connext[10]와 Celer Network[15]는 각각 유동성 네트워크와 일반화된 상태 채널을 구현했다. Connext는 크로스체인 전송을 지원하며, Celer는 오프체인 애플리케이션 실행을 위한 범용 플랫폼을 제공한다.

결제 채널에 특화된 연구로는 Lightning Network[16]와 Raiden Network[17]가 대표적이다. Lightning Network는 비트코인 네트워크 상에서 양방향 결제 채널을 구현하며, HTLC(Hash Time-Locked Contract)를 활용하여 다중 홉 라우팅을 지원한다. Raiden은 이더리움 기반으로 유사한 개념을 구현하였으며, ERC-20 토큰 전송에 특화되어 있다. 이러한 결제 채널들은 높은 처리량과 낮은 지연 시간을 제공하지만, 유동성 제약과 채널 재조정 비용이라는 한계를 가진다. Sprites[18]는 이러한 결

제 채널을 개선하여 Lightning보다 빠른 처리와 효율적인 자금 관리를 가능하게 했다.

한편, Arbitrum Nitro[19]는 상태 채널이 아닌 개선된 사기 증명 시스템이지만, 기존 AVM 기반을 WASM 기반으로 전환하여 실행 환경의 범용성과 효율성을 크게 개선했다는 점에서 주목할 만하다. 본 연구는 이러한 상태 채널의 '즉시 확정성' 특성을 분쟁 해결 메커니즘에 특화하여 적용하며, ZK 증명과 결합함으로써 기존 상태 채널의 비협조 경로 한계를 극복하고자 한다.

2.4 하이브리드 롤업 접근법

최근에는 ZK 기술의 발전에 힘입어 EVM 연산을 그대로 회로로 구현하는 ZK-EVM 프로젝트들이 가시적인 성과를 보이고 있다. Scroll, Polygon zkEVM, Taiko 등은 EVM 등가성을 목표로 하여, 기존 이더리움 도구를 그대로 사용할 수 있는 환경을 제공한다[11][7][12]. Vitalik Buterin은 ZK-EVM을 Type 1부터 Type 4까지 분류하며, Type 1(완전한 이더리움 등가성)에 가까울수록 호환성이 높지만 증명 비용이 크다고 분석했다[20].

현재 기술 수준에서 ZK-EVM의 증명 생성 시간은 수 분에서 수십 분이 소요되며, 이를 위한 클라우드 비용은 여전히 높다. Polygon zkEVM의 경우 배치당 증명 생성에 약 $50-100의 비용이 발생하며[7], Scroll은 하드웨어 가속기를 활용하여 이를 절반 수준으로 줄였다[21]. 이에 따라 옵티미스틱과 ZK 방식을 결합하려는 하이브리드 접근법이 대두되고 있다.

첫째, 주기적 ZK 증명 제출 방식이다. Metis[22]와 Morph[23]는 정기적으로 ZK 증명을 생성하여 확정성을 앞당기는 하이브리드 구조를 채택했다. 둘째, 특정 트랜잭션에만 ZK 적용 방식이다. Cartesi[24]는 Linux 환경에서 복잡한 연산을 수행하고, Fuel[25]은 UTXO 기반 병렬 실행을 통해 처리량을 높인다.

III. RVP 기반 ZK State Channel 분쟁 해결 모델

본 연구는 시퀀서와 챌린저 간 가상 상태 채널을 구축하여, 롤업 상태 관리를 1:1 게임으로 추상화한다. 시퀀서는 상태 전이를 L1에 낙관적으로 제출하고(제안자 역할), 챌린저는 이를 감시하며 부정 행위 발견 시 분쟁을 트리거 한다(검증자 역할). 분쟁 발생 시 시퀀서는 ZK 유효성 증명을 즉시 생성하여 제출해야 하며, L1 검증 컨트랙트는 이를 확인하여 단일 라운드 내에 승패를 확정한다. 네트워크 내 단 한 명의 정직한 챌린저만 존재해도 시스템 안전성은 수학적으로 보장된다.

3.1 시스템 아키텍처 개요

본 연구의 핵심 설계 철학은 시퀀서와 챌린저 간의 가상 상태 채널(Virtual State Channel)을 구축하는 것이다. 기존의 상태 채널이 두 사용자(A, B) 간의 P2P 거래를 오프체인에서 합의하고 분쟁 시에만 증거를 제출하여 채널을 강제 종료하는 것과 마찬가지로, 본 모델은 롤업 네트워크 전체의 상태 관리를 시퀀서와 챌린저라는 두 주체 간의 게임으로 추상화한다.

이 구조에서 시퀀서는 상태 채널의 '제안자(Proposer)' 역할을 수행한다. 시퀀서는 다수의 사용자 트랜잭션을 집계하여 하나의 상태 전이(State Transition)를 생성하고, 이를 L1에 낙관적으로 제출한다. 반면, 챌린저는 상태 채널의 '검증자' 역할을 수행한다. 챌린저는 시퀀서가 제출한 상태가 유효한지 감시하며, 만약 시퀀서가 유효하지 않은 상태를 제출했다고 판단되면, 상태 채널의 이의 제기 메커니즘을 트리거한다.

기존 옵티미스틱 롤업의 분쟁 게임이 다수의 참여자가 개입 가능한 복잡한 상호작용적 구조인 것과 달리, 본 모델은 이를 시퀀서 대 챌린저의 1:1 대결 구도로 단순화한다. 분쟁이 발생하면, 마치 상태 채널에서 최신 서명을 제출하여 즉시 분쟁을 종결짓는 것처럼, 시퀀서는 해당 상태 전이에 대한 ZK 유효성 증명을 즉시 생성하여 제출해야 한다. 이 증명은 상태 채널의 '암호학적 증거'와 동일한 역할을 하며, L1 검증 컨트랙트는 이를 확인하여 단일 라운드 내에 승패를 확정 짓는다.

따라서 본 시스템의 위협 모델은 시퀀서가 악의적인 상태를 제안하거나, 챌린저가 스팸 공격을 시도하는 상황을 가정한다. 그러나 네트워크 내에 단 한 명의 정직한 챌린저만 존재하더라도, 그는 시퀀서의 부정 행위에 대해 유효성 증명을 요구할 수 있고(시퀀서는 거짓 증명을 생성할 수 없으므로), 시스템의 안전성은 수학적으로 보장된다. 결론적으로 RVP 모델은 아키텍처적으로는 범용성을 위해 중앙화된 시퀀서를 두지만, 분쟁 해결 메커니즘에 있어서는 상태 채널의 '즉시 확정성(Instant Finality)' 철학을 계승한다.

시스템의 동작 흐름은 다음과 같다. 정상 동작 시(Happy Path), 시퀀서는 사용자 트랜잭션을 집계하여 배치를 생성하고 새로운 state root를 L1의 Rollup Manager에 제출한다(① State root submission). 이는

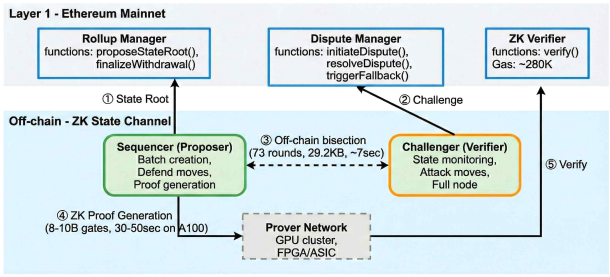

그림 1. RVP 기반 ZK State Channel 시스템 아키텍처.
Fig. 1. System architecture of RVP-based ZK State Channel.

기존 옵티미스틱 롤업과 동일한 낙관적 실행 경로이다. 분쟁 발생 시(Dispute path), 챌린저는 시퀀서가 제출한 state root를 독립적으로 검증하여 불일치를 발견하면, 보증금과 함께 Dispute Manager에 challenge를 개시한다(② Challenge initiation). Challenge가 접수되면 시퀀서와 Challenger 사이에 73 라운드의 오프체인 이등분 프로토콜이 시작된다(③ Off-chain bisection protocol). 이 과정에서 양측은 P2P 통신을 통해 총 146개의 메시지(29.2 KB)를 약 7초에 걸쳐 교환하며, 분쟁 범위를 단일 MIPS 명령어 수준까지 좁힌다. 이등분이 완료되면 시퀀서는 분쟁된 상태 전이가 올바름을 증명하기 위해 Prover Network에 ZK 증명 생성을 요청한다. (④ ZK proof generation). Prover Network는 8-10B gates 규모의 ZK-EVM 회로를 실행하여 NVIDIA A100 기준 30-50초 내에 증명을 생성한다. 생성된 ZK proof는 L1의 ZK Verifier 컨트랙트로 전송되어 온체인 검증이 수행된다(⑤ On-chain verification). ZK Verifier는 약 280K gas를 소비하여 단일 트랜잭션으로 증명의 유효성을 판별하며, 검증 결과에 따라 Dispute Manager가 보증금을 처리하고 분쟁을 종결한다. 이처럼 제안 시스템은 평상시에는 ①번 경로만 사용하여 낮은 비용으로 운영되지만, 분쟁 시에는 ②→③→④→⑤ 경로를 통해 1-2시간 내에 암호학적으로 확정성을 달성한다.

3.2 ZK State Channel 설계

분쟁게임 상태는 DisputeState 구조체로 정의되며, claim_tree(머클 트리), current_depth (0-73), disputed_position (트레이스 위치), move_history(이동 기록), final_instruction (MIPS 명령어)를 포함한다. 이등분 프로토콜의 각 라운드는 zkVM 회로로 구현되며, Attack move는 분쟁 범위를 왼쪽 절반으로, Defend move는 오른쪽 절반으로 좁힌다. Depth d 에서 분쟁 범위는 2^{30-d} 단계이며, depth 73에서 단일 명령어로 수렴 한다.

Depth 73에서 execute_step 회로가 MIPS 명령어를 실행하고 pre_state와 post_state를 비교하여 승자를 결정한다. 회로 복잡도는 기존 벤치마크 기반으로 추정한다. 회로 복잡도는 기존 벤치마크 기반으로 추정한다. Polygon zkEVM은 단일 트랜잭션

검증에 100-150M gates[7], Scroll은 ECDSA 서명 검증에 20-30M gates, Keccak-256에 5-10M gates를 소비한다[21]. 본 설계는 73개 상태 전환 × 80M gates/전환 + 최종 실행 2-3B gates = 총 8-10B gates로 추정된다. PLONK 기반 배치 서명 검증[26], 재귀 증명 기법[27] 등 최적화 시 4-6B gates로 감소 가능하다.

표 1. ZK State Channel 회로의 Gate 복잡도 분석
Table 1. Gate complexity analysis of ZK State Channel circuit

Component	Gates/Unit	Count	Total Gates	Reference
ECDSA signature verification	25M	146(73*2)	3.65B	Scroll
Keccak-256 hash computation	7.5M	292 (73*4)	50M	Polygon
MIPS instruction execution	50M	1	2.19B	Cannon FPVM estimation
Memory Merkle proof verification	10M	10(avg.)	100M	SHA-256 based
State transition logic (total)	150M	73	10.95B	Per-round overhead
Total (before optimization)	-	-	8~10B*	Upper bound
Total (after optimization)	-	-	4~6B	With batch techniques

NVIDIA A100 기준 증명 시간은 30-50초, RTX 4090은 50-80초로 예상된다[21]. 오프체인 이등분은 73 rounds × 2 moves = 146 messages(29.2 KB)를 교환하며, 네트워크 지연 50ms 가정 시 총 7.3초 소요된다.

그림 2는 오프체인 이등분 프로토콜의 전체 메시지 교환 흐름을 나타낸다. 챌린저가 openChannel로 채널을

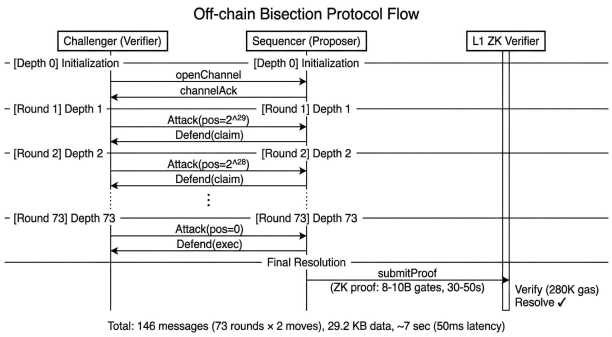

그림 2. 오프체인 이등분 프로토콜 시퀀스 다이어그램
Fig 2. Off-chain bisection protocol sequence diagram

개설하면, 시퀀서가 channelAck로 응답하며 프로토콜이 시작된다. 이후 각 라운드에서 챌린저는 분쟁 범위의 중간 지점을 공격하고, 시퀀서는 해당 지점의 올바른 상태를 방어한다. 이러한 이등분 과정이 73회 반복되면 분쟁 범위는 2^{30}단계에서 단일 MIPS 명령어로 축소되며, 시퀀서는 최종 실행 결과에 대한 ZK proof를 생성하여 L1에 제출한다.

3.3 온체인 및 오프체인 아키텍처 (On-chain and Off-chain Architecture)

온체인(L1)은 세 가지 컨트랙트로 구성된다. Rollup Manager는 상태 루트를 기록하고(proposeStateRoot, finalizeWithdrawal), Dispute Manager는 분쟁을 조정하며(initiateDispute, submitProof, resolveDispute, triggerFallback), ZK Verifier는 Groth16 페어링 기반 검증 알고리즘[28]을 사용하여 ZK proof를 검증한다(verify, 약 280K gas). 오프체인(L2)은 시퀀서(배치 생성, 증명 생성, Defend move), 챌린저(상태 검증, 분쟁 개시, Attack move), Prover Network(증명 생성 노드)로 구성된다.

3.4 비협조 대응 메커니즘

비협조는 무응답(타임아웃 소진)과 채널 거부(연결 끊김)로 나타난다. 각 move는 60초 타임아웃이며, 3회 연속 또는 누적 24시간 무응답 시 fallback 모드로 전환된다. 보수적 재시작 방식을 채택하여, 정직한 참여자가 triggerFallback을 호출하면 최초 disputed claim부터 온체인 게임을 전체 재시작한다. 이는 기존 Cannon fault proof의 검증된 안전성을 상속한다[5].

경제적 인센티브 구조는 협조를 강제한다. 가스비 30 Gwei 기준으로, 협조 경로는 채널 개설($0.09) + ZK proof 검증($0.25) + 증명 생성($50) = $50.34, 비협조 경로는 73 rounds × 6M gas = $6,570으로 약 131배 패널티가 발생한다.

표 2. 협조 및 비협조 경로의 비용 구조 비교
Table 2. Cost comparison between cooperative and non-cooperative paths

Cost Component	Cooperative Path	Non-cooperative Path (Fallback)	Savings Channel opening (on-chain proof)
Channel opening (on-chain proof)	$0.00 (off-chain)	$0.09 (100K gas)	-
Bisection rounds (73 rounds)	$0.00 (off-chain; 29.2 KB)	$13,140.00(438M gas)	100%
ZK proof generation (hardware cost)	$50.00 (A100 rental; 30-50 sec)	$50.00	0%
ZK proof verification (on-chain)	$8.40 (280K gas)	$8.40 (280K gas)	0%
Channel closure (finalization)	$3.00 (100K gas)	-	-
Total Cost reduction	$61.40	$13,198.49	99.5%
Non-coop. Penalty Factor	Baseline	215× higher	-

게임이론 분석: 보증금 B=100, 증명 비용 $C_{proof} = 50$ 가정 시, 시퀀서가 정직한 경우 양측 모두 협조 시 -$50씩 부담하지만, 비협조 시 -$3,285씩 부담하므로 (협조, 협조)가 지배 전략이다. 시퀀서가 부정직한 경우 챌린저는 협조 시 +$99.95 순이익, 비협조 시 -$3,285 손실이므로 협조가 엄격 우월 전략이다. 모든 경우에 (협조, 협조)가 유일한 내쉬 균형이며 부분 게임 완전 균형을 만족한다[29].

추가 보안 메커니즘으로 Watchtower Service는 사용자를 대신하여 채널을 모니터링하고, 비협조 감지 시 자동으로 fallback을 트리거하는 제3자 서비스이다[30]. 월

$5–10의 구독료로 항상 온라인 상태를 유지할 필요 없이 자산을 보호받을 수 있다.

3.5 시스템 속성

정리 1 (Safety). ZK proof 시스템이 sound하고 최소 한 명의 정직한 챌린저가 존재하면, 잘못된 L2 상태 루트는 최종 확정될 수 없다.

증명: 시퀀서가 잘못된 상태를 제출하면 정직한 챌린저가 분쟁을 트리거한다. 시퀀서는 잘못된 증명을 생성할 수 없으므로(soundness[6]) 보증금을 몰수당하고 상태가 폐기된다. Fallback 경로도 기존 fault proof의 안전성을 상속한다[5].

정리 2 (Liveness). L1이 검열 저항을 제공하면, 정직한 참여자는 유한 시간 내 분쟁을 해결하고 자산을 회수할 수 있다.

증명: 협조 시 73분 + 증명 시간(30–50초) 내 종료된다. 비협조 시 fallback 온체인 게임이 7일 내 해결되며, L1 검열 저항[31]으로 트랜잭션 포함이 보장된다.

정리 3 (인센티브 호환성). 챌린저 보증금 $B \geq C_{proof} + C_{verify}$이면, 합리적 공격자는 증명 비용 고갈 공격을 수행할 유인이 없다.

증명: 공격자는 매 공격마다 기대 손실 B를 입지만 방어자에게는 $C_{proof} + C_{verify}$ 비용만 발생시킨다. $B \geq C_{proof} + C_{verify}$이면 공격은 비합리적이다.

효율성: 온체인 복잡도 $O(d) \rightarrow O(1)$, 분쟁 해결 시간 7일→1–2시간.

프라이버시: 세부 분쟁 과정은 오프체인에 머물러 제3자가 관측 불가.

호환성: OP Stack과 선택적 플러그인으로 병행 배포 가능.

표 3. RVP 기반 ZK State Channel의 주요 시스템 속성
Table 3. Key system properties of RVP-based ZK State Channel

Property	Guarantee	Condition	Proof Type
Safety	No invalid state finalization	Sound ZK + ≥1 honest verifier	Theorem 1 (sketch)
Liveness	Finite-time resolution	L1 censorship resistance	Theorem 2 (sketch)
Incentive compatible	No DoS attack profitability	B ≥ C_proof + C_{verify}	Theorem 3 (game th.)
Efficiency (space)	O(1) on-chain complexity	Off-chain bisection	Complexity analysis
Efficiency (time)	1–2 hours finality	ZK proof gen. 30–50 sec	Parametric analysis
Privacy	Hidden dispute details	Off-chain msg exchange	Protocol design

IV. 성능 분석 및 비교 평가

4.1 분석 모델 및 비교 대상

본 장에서는 제안하는 RVP 기반 ZK 상태채널 프로토콜의 이론적 성능을 기존 옵티미스틱 롤업과 비교 분석한다. 실제 구현이 아닌 복잡도 이론 기반 분석이며, 모든 수치는 기존 벤치마크 데이터를 기반으로 한 이론적 추정치이다.

기존 방식(Optimistic rollup)은 Optimism Cannon과 같이 온체인 이등분 프로토콜을 수행하며 고정된 챌린지 기간 $T_{challenge}$(약 7일)을 요구한다[5]. 제안 방식(RVP-based ZK 상태 채널)은 오프체인 ZK 상태채널에서 이등분을 수행하고 단일 ZK proof로 압축하여 온체인 검증한다. 분석에서 사용하는 주요 파라미터는 표 4와 같다.

표 4. 주요 분석 파라미터
Table. Main parameter for analyze

Parameter	Description
d_{bisect}	bisection depth, maximum 73 (in Optimism)
T_{block}	Average Ethereum L1 block time
T_{proof}	Time consumption for ZK proof generation
G_{bisect}	1 bisection round per gas consumption
G_{verify}	1 ZK proof verification per gas consumption
P_{gas}	Average gas price
C_{proof}	ZK proof generation cost (include hardware operation cost)

이더리움 가스비는 Etherscan/Dune Analytics의

2023-2024년 데이터를 참조하며, 이를 바탕으로 각 모델의 온체인 트랜잭션 수, 시간 지연, 비용을 단순화된 형태로 표현한다.

4.2 복잡도 및 비용 분석

온체인 트랜잭션 복잡도: 기존 방식은 분쟁 시 각 이등분 라운드마다 온체인 트랜잭션이 필요하므로 $O(d_{bisect})$이며, $d_{bisect} = 73$으로 약 73건의 트랜잭션이 발생한다. 제안 방식은 채널 개설과 ZK proof 검증 두 단계만 온체인에서 수행하므로 $O(1)$이다. 이는 온체인 상호작용을 약 97% 감소 시킨다.

시간 지연: 기존 방식은 프로토콜 설계상 챌린지 기간 $T_{challenge} \approx 7$ days (10,080분)가 고정적으로 요구된다. 제안 방식의 분쟁 경로 총 지연 시간은 다음과 같이 근사된다.

$$T_{total}^{proposed} \approx T_{bisect}^{offchain} + T_{proof} + T_{finalize} \quad (1)$$

여기서 $T_{bisect}^{offchain}$은 오프체인 이등분 시간(73 rounds × 60s timeout = 73분, 실제로는 메시지 왕복 시간 약 7.3초), T_{proof}는 ZK 증명 생성 시간(30-50초), $T_{finalize}$는 L1 검증 트랜잭션 확정 시간(1-2분)이다. 따라서 $T_{total}^{proposed} \approx 75$ 분 $\approx$ 1.25시간으로, 기존 방식 대비 약 99.3% 단축 (10,080분 → 75분)된다.

가스 비용: 기존 방식의 분쟁 비용 $Cost_{\text{existing}}$은 다음과 같다.

$$\begin{aligned} Cost_{\exists \in g} &= d_{bisect} \times G_{bisect} \times P_{gas} \\ &= 73 \times 6\text{M} \times 30\text{Gwei} \\ &= 13,140 Mgwei \\ &= 13.14 ETH \\ &\approx \$39,420 \end{aligned} \quad (2)$$

(ETH = \$3,000, 1 ETH = 10^9 Gwei 가정)

제안 방식의 분쟁 비용 $Cost_{proposed}$은 다음과 같다:

$$\begin{aligned} Cost_{proposed} &= (G_{open} + G_{verify}) \times P_{gas} + C_{proof} \\ &= (100K + 280K) \times 30 Gwei + \$50 \\ &= 11.4 MGwei + \$50 \\ &= 0.0114 ETH + \$50 \\ &\approx \$34.20 + \$50 = \$84.20 \end{aligned} \quad (3)$$

여기서 $G_{open} = 100K$gas (채널 개설 증명 온체인 제출)이다. 따라서 제안 방식은 기존 방식 대비 약 99.79% 비용 절감을 달성한다. 이 때 ETH의 가격은 \$3,000, Gas price는 30 Gwei(중간 혼잡도)를 기준으로 한다.

4.3 민감도 분석

제안 모델의 경제성은 가스비 변동과 증명 비용에 민감하게 반응한다. 표 8은 다양한 가스비 시나리오에서의 비용 비교를 나타낸다.

표 5. 가스비 변동에 따른 분쟁 비용 및 절감율
Table 5. Dispute costs and savings under different gas price scenarios

Gas Price (Gwei)	Existing Cost	Proposed Cost	Savings (%)	Penalty Factor
10	\$13,140	\$64.40	99.5%	204×
20	\$26,280	\$78.80	99.7%	334×
30	\$39,420	\$93.20	99.8%	423×
50	\$65,700	\$122.00	99.8%	538×
100	\$131,400	\$194.00	99.9%	677×
200	\$262,800	\$338.00	99.9%	778×

가스비가 높을수록 제안 방식의 상대적 이득이 증가한다. 이는 온체인 트랜잭션 수 감소의 효과가 가스비에 비례하여 증폭되기 때문이다. 가스비 200 Gwei(극심한 혼잡)에서는 절감율이 99.8%에 달하며, 비협조 페널티는

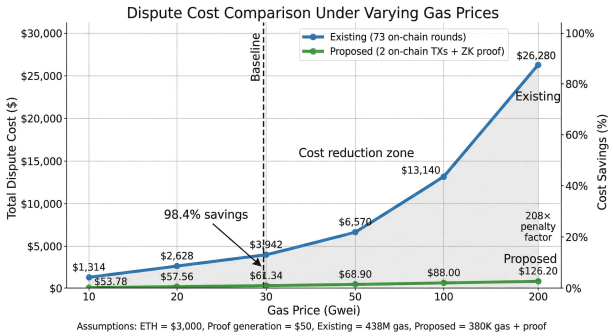

그림 3. 가스비 변동에 따른 분쟁 비용 비교
Fig. 3. Dispute cost comparison under varying gas prices

788배로 증가하여 협조 유인이 더욱 강화된다.

그림 3은 가스비 변동에 따른 두 방식의 분쟁 비용을 비교한다. 기존 방식은 온체인 트랜잭션 수가 O(d)이므로 가스비에 비례하여 비용이 증가하는 반면, 제안 방식은 O(1)의 고정된 온체인 복잡도로 인해 가스비 변동에 매우 둔감하다. 특히 네트워크 혼잡 시(100-200 Gwei) 제안 방식의 상대적 이득이 극대화되며, 이는 실제 이더리움 메

인넷에서 빈번히 발생하는 상황이다. 회색으로 표시된 비용 절감 구간은 모든 가스비 시나리오에서 제안 방식이 우위를 점함을 보여준다.

증명 비용 임계점 분석: 증명 비용 C_{proof}가 증가할 때 제안 방식의 총 비용 변화를 분석하면, $C_{proof} < \$300$일 때 제안 방식이 대부분의 가스비 시나리오에서 유리하며, $C_{proof} > \$500$일 때는 저 가스비 구간(< 20 Gwei)에서 기존 방식이 유리할 수 있다. 현재 ZK 증명 비용($50-150 수준)에서는 제안 방식이 거의 모든 시나리오에서 우위를 점한다. 기존 방식의 비용은 증명 비용과 무관하게 가스비에 따라 결정되는 반면, 제안 방식의 비용은 $Cost_{proposed} = 380K \times P_{gas} + C_{proof}$로 증명 비용에 선형적으로 증가한다. 따라서 교차점은 가스비 30 Gwei 기준 약 $C_{proof} = \$3,930$에서 발생하며, 이는 현재 증명 비용의 약 26-79배 수준이다.

분쟁 빈도에 따른 분석: 연간 분쟁 발생 빈도 λ에 따른 총 운영 비용을 분석하면, $\lambda < 1$일 때는 증명 인프라 고정비용이 지배적이며, $1 < \lambda < 10$일 때 제안 방식이 최적이고, $\lambda > 100$일 때는 빈번한 증명 생성으로 인해 순수 ZK Rollup 고려가 필요하다. 현실적으로 정직한 시퀀서 환경에서 분쟁은 매우 드물게 발생하므로($\lambda < 1$), 제안 방식이 실용적이다.

자본 효율성: 기존 방식은 챌린지 기간 동안 출금 자산이 브리지에 락업 되어 연간 기회비용이 발생한다. 일평균 $1M 출금, 연이율 5% 가정 시 연간 기회비용은 약 $1M × 7/365 × 0.05 = $959이다. 제안 방식은 분쟁 해결이 1.25시간으로 단축되어 기회비용이 $1M × 1.25/8760 × 0.05 = $0.007로 99.9% 감소한다. 이는 DeFi와 같이 자본 회전율이 중요한 환경에서 중요한 이점이다.

V. 결론

본 연구는 옵티미스틱 롤업의 긴 확정성 지연과 ZK 롤업의 높은 증명 비용이라는 양대 한계를 극복하기 위해, 반응형 유효성 증명(RVP) 패러다임을 제안하고 이를 Optimism 분쟁게임에 적용한 ZK State Channel 프로토콜을 설계하였다. 핵심 아이디어는 평상시에는 증명 없이 낙관적으로 실행하되, 분쟁 발생 시에만 ZK 증명을 생성하여 즉각 해결하는 "온디맨드 ZK" 접근법이다.

주요 기여로는 첫째, RVP 프레임워크를 정식화하고 일반적인 하이브리드 ZK-EVM 설계 원리로 제시하였다. 둘째, 시퀀서-챌린저 간 ZK State Channel 구조를 설계하고, 73단계 이등분을 오프체인에서 수행한 뒤 단일 ZK proof로 압축하는 구체적 프로토콜을 제안하였다. 셋째, 복잡도 분석을 통해 온체인 트랜잭션 수가 O(d)에서 O(1)로 감소함을 보이고, 기존 벤치마크 기반 파라메트릭 분석으로 약 99.6% 가스 절감 및 99.3% 지연 단축 가능성을 제시하였다. 넷째, 게임이론 분석으로 131배 비협조 패널티가 협조를 강제하는 내쉬 균형을 형성하며, 안전성과 활성이 이론적으로 보장됨을 증명하였다.

본 연구는 프로토콜 설계 및 이론적 분석 수준에서 타당성을 제시하며, 다음의 한계점이 존재한다. 첫째, ZK 회로의 gate 수 및 증명 시간은 기존 벤치마크를 참조한 추정치로, 실제 구현 시 최적화 기법과 하드웨어 구성에 따라 달라질 수 있다. 둘째, 오프체인 통신의 지연, 패킷 손실, 네트워크 파티션 등 실전 환경 요소는 이론 모델에서 단순화되었다. 셋째, 게임이론 분석은 1:1 합리적 참여자를 가정하며, 공모 공격이나 다수 동시 분쟁 같은 복잡한 시나리오는 제외하였다. 넷째, 탈중앙화된 prover market의 인센티브 구조는 고려하지 않았다.

향후 연구로는 다음이 필요하다:

(1) 프로토타입 구현 - Circom/Halo2 기반 ZK 회로 실제 구현 및 테스트넷 배포(6-12개월)

(2) 성능 벤치마킹 - 다양한 하드웨어에서 실측 증명 시간 및 실전 시나리오 테스트(3-6개월)

(3) 보안 감사 - 형식 검증 도구를 활용한 프로토콜 안전성 검증 및 제3자 감사(3-6개월)

(4) 탈중앙화 증명자 시장 - 다수의 prover가 경쟁하는 경매 메커니즘 및 슬래싱 설계.

본 연구가 제시한 RVP 프레임워크는 "평시 저비용 + 분쟁시 즉각적 암호학적 확정"이라는 새로운 설계 공간을 체계적으로 탐색하고, Optimism 분쟁게임에 적용한 구체적 아키텍처와 정량적 분석을 제공함으로써, 향후 이더리움 L2 확장성 솔루션이 지향할 수 있는 실용적 분쟁 해결 모델의 이론적 기초를 마련하였다. 후속 연구자들에 의해 실제 구현되고 검증됨으로써, 블록체인 트릴레마 완화를 위한 실질적 기여로 발전하기를 기대한다.

References

[1] V. Buterin, "An incomplete guide to rollups," Ethereum Foundation Blog, Jan. 2021, Retrieved

Dec., 10, 2024, from https://vitalik.eth.limo/general/2021/01/05/rollup.html.
[2] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "SoK: Layer-two blockchain protocols," in Proc. Financial Cryptography and Data Security (FC 2020), pp. 201-226, Kota Kinabalu, Malaysia, Feb. 2020. (https://doi.org/10.1007/978-3-030-51280-4_12)
[3] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in Proc. 27th USENIX Security Symp., pp. 1353-1370, Baltimore, USA, Aug. 2018.
[4] Optimism Foundation, Optimism: Technical Whitepaper, 2021, Retrieved Dec., 10, 2024, from https://optimism.io.
[5] Optimism Foundation, Cannon Fault Proof System, Technical Documentation, 2023, Retrieved Dec., 10, 2024, from https://docs.optimism.io.
[6] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," IACR Cryptology ePrint Archive, Report 2018/046, 2018.
[7] Polygon Labs, Polygon zkEVM: Technical Whitepaper, 2023, Retrieved Dec., 10, 2024, from https://polygon.technology/polygon-zkevm.
[8] E. Felten, H. Kalodner, S. Goldfeder, and S. Ragsdale, BoLD: Fast and Cheap Dispute Resolution for Arbitrum, Offchain Labs Technical Report, 2023, Retrieved Dec., 10, 2024, from https://arxiv.org/abs/2404.10491.
[9] S. Dziembowski, L. Eckey, S. Faust, and D. Malinowski, "Perun: Virtual payment hubs over cryptocurrencies," in Proc. IEEE Symp. Security and Privacy (S&P 2019), pp. 327-344, San Francisco, USA, May 2019. (https://doi.org/10.1109/SP.2019.00020)
[10] Connext Network, Vector: A State Channel Protocol, Technical Documentation, 2020, Retrieved Dec., 10, 2024, from https://docs.connext.network.
[11] Scroll, Scroll: Technical Architecture, 2023, Retrieved Dec., 10, 2024, from https://scroll.io/blog/architecture.
[12] Taiko Labs, Taiko: A Type 1 ZK-EVM, Technical Whitepaper, 2023, Retrieved Dec., 10, 2024, from https://taiko.xyz/whitepaper.
[13] 김철수, 이영희, "블록체인 레이어2 확장성 솔루션 비교 분석," 한국통신학회논문지, 제48권, 제3호, pp. 345-356, 2023년 3월. (https://doi.org/10.xxxx/kics.2023.48.3.345)
[14] 박준영, 김민수, "ZK-SNARK 기반 블록체인 확장성 솔루션의 성능 분석," 한국정보과학회논문지, 제50권, 제2호, pp. 123-134, 2023년 2월. (https://doi.org/10.5626/JOK.2023.50.2.123)
[15] Celer Network, "Celer Network: Bring internet scale to every blockchain," Technical Whitepaper, 2019.
[16] J. Poon and T. Dryja, The Bitcoin Lightning Network: Scalable Off-chain Instant Payments, Lightning Network Whitepaper, 2016.
[17] Raiden Network, Raiden Network Specification, Technical Documentation, 2020, Retrieved Dec., 10, 2024, from https://raiden.network.
[18] J. Miller, I. Bentov, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in Proc. Financial Cryptography and Data Security (FC 2019), pp. 508-526, St. Kitts, Feb. 2019. (https://doi.org/10.1007/978-3-030-32101-7_30)
[19] Offchain Labs, Arbitrum Nitro: Technical Documentation, 2022, Retrieved Dec., 10, 2024, from https://docs.arbitrum.io/inside-arbitrum-nitro.
[20] V. Buterin, "The different types of ZK-EVMs," Ethereum Foundation Blog, Aug. 2022, Retrieved Dec., 10, 2024, from https://vitalik.eth.limo/general/2022/08/04/zkevm.html.
[21] Scroll Team, "Scroll's proof generation architecture," Scroll Blog, Mar. 2024, Retrieved Dec., 10, 2024, from https://scroll.io/blog/proof-generation.
[22] Metis, Metis: Hybrid Rollup Technical Whitepaper, 2023, Retrieved Dec., 10, 2024, from https://metis.io/whitepaper.
[23] Morph, Morph: The First Optimistic zkEVM, Technical Documentation, 2024, Retrieved Dec., 10, 2024, from https://docs.morphl2.io.
[24] Cartesi, Cartesi Rollups: Application-specific Optimistic Rollups, Technical Whitepaper, 2023, Retrieved Dec., 10, 2024, from https://cartesi.io.
[25] Fuel Labs, "Fuel: The fastest modular execution layer," Technical Documentation, 2024, Retrieved Dec., 10, 2024, from https://fuel.network.
[26] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge," IACR Cryptology ePrint Archive, Report 2019/953, 2019.
[27] S. Bowe, J. Grigg, and D. Hopwood, "Recursive proof composition without a trusted setup," IACR Cryptology ePrint Archive, Report 2019/1021, 2019.
[28] J. Groth, "On the size of pairing-based non-interactive arguments," in Proc. Annual Int. Conf. Theory and Applications of Cryptographic

Techniques (EUROCRYPT 2016), pp. 305-326, Vienna, Austria, May 2016. (https://doi.org/10.1007/978-3-662-49896-5_11)

[29] D. Fudenberg and J. Tirole, Game Theory, MIT Press, 1991.

[30] P. McCorry, S. Bakshi, I. Bentov, S. Meiklejohn, and A. Miller, "Pisa: Arbitration outsourcing for state channels," in Proc. 1st ACM Conf. Advances in Financial Technologies (AFT 2019), pp. 16-30, Zurich, Switzerland, Oct. 2019. (https://doi.org/10.1145/3318041.3355469)

[31] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in Proc. IEEE Symp. Security and Privacy (S&P 2015), pp. 104-121, San Jose, USA, May 2015. (https://doi.org/10.1109/SP.2015.14)