옵티미스틱 롤업을 활용한 블록체인 기반 분산 클라우드 스토리지 시스템의 성능 개선에 관한 연구

황 재 승◆, 김 영 한°

A Study on Performance Improvement of Blockchain-based Distributed Cloud Storage System using Optimistic Rollup

Jae-seung Hwang◆, YoungHan Kim°

요 약

본 연구는 옵티미스틱 롤업 기술을 활용한 블록체인 기반 분산 클라우드 스토리지 시스템을 제안한다. 기존 블록체인 기반 분산 저장 시스템은 확장성 문제와 높은 가스비로 인해 대규모 데이터 환경에서의 실용성이 제한되어 왔다. 본 연구에서는 이더리움 블록체인과 IPFS를 결합하고, 옵티미스틱 롤업 기술을 적용하여 트랜잭션 처리 속도를 향상 시키고 가스비를 절감하는 방안을 제시한다. Sepolia 테스트넷과 Titan Sepolia 옵티미스틱 롤업 네트워크를 통한 실험 결과, 제안 시스템은 기존 레이어 1 대비 가스비와 트랜잭션 처리 시간을 크게 단축하는 효과를 보였다. 이러한 결과는 블록체인 기반 분산 저장 시스템의 상용화 가능성을 크게 향상하며, 다양한 산업 분야에서의 실질적 응용이 가능할 것으로 기대된다.

Key Words : Blockchain, Distributed storage system, Optimisic rollup, Ethereum, Layer2 solution

ABSTRACT

This paper proposes a blockchain-based distributed cloud storage system utilizing Optimistic Rollup technology. Existing blockchain-based distributed storage systems have faced limitations in practical applications for large-scale data environments due to scalability issues and high gas fees. In this study, we combine Ethereum blockchain with IPFS and apply Optimistic Rollup technology to improve transaction processing speed and reduce gas costs. Experimental results conducted on the Sepolia testnet and Titan Sepolia Optimistic Rollup network demonstrate that the proposed system reduces gas fees and shortens transaction processing time compared to the traditional Layer 1 approach. These results significantly enhance the commercialization potential of blockchain-based distributed storage systems and are expected to enable practical applications across various industries.

◆ First Author : Soongsil University Department of IT Convergence, cd4761@naver.com, 학생(박사과정), 정회원
° Corresponding Author : Soongsil University, younghak@ssu.ac.kr, 정교수, 정회원

Ⅰ. 서 론

블록체인 기술은 데이터 보안성과 투명성을 보장하는 분산 시스템의 핵심 기반 기술로 발전해 왔으며, 다양한 산업 분야에서 응용되고 있다. 특히 데이터 관리 및 저장 영역에서는 블록체인의 합의 메커니즘과 변경 불가능한 특성이 주목받고 있으며, 이를 통해 중앙 집중식 저장 구조의 한계를 극복할 수 있는 분산 스토리지 시스템이 부상하였다.

전통적인 중앙 집중식 클라우드 스토리지 시스템은 단일 장애점(Single Point of Failure), 데이터 소유권 불투명성, 중앙 기관에 대한 의존성 등의 근본적인 한계를 가지고 있다. 이러한 문제를 해결하기 위해 IPFS(Inter Planetary File System)[1], Storj[2], Sia[3] 등과 같은 블록체인 기반 분산 저장 시스템들이 등장하였다. 이들 시스템은 콘텐츠 기반 해시를 활용해 전 세계 노드에 데이터를 분산 저장함으로써 중앙 서버에 의존하지 않는 구조를 구현하였으며, 경제적 인센티브 메커니즘을 결합하여 노드 운영자들이 네트워크에 기여하도록 유도하고, 데이터 무결성과 가용성을 강화하였다[4].

그러나 이러한 블록체인 기반 분산 저장 시스템들은 상용화 과정에서 중대한 기술적 한계에 직면하고 있다. 첫째, 퍼블릭 블록체인 네트워크를 활용할 경우 트랜잭션 처리 속도가 느리고 가스비가 급증하는 확장성(Scalability) 문제가 발생한다[4]. 비트코인의 경우 초당 약 7건의 트랜잭션(TPS)만을 처리할 수 있으며, 이더리움 역시 평균 15 TPS 수준에 불과하다[5]. 이는 수천 TPS를 처리하는 중앙집중식 시스템과 비교했을 때 현저히 낮은 수치이다.

둘째, 높은 가스비 문제로 인해 대규모 데이터 처리 환경에서의 경제성이 크게 저하된다. 블록체인의 합의 구조상 모든 노드가 네트워크 상의 모든 트랜잭션을 검증하고 저장해야 하기 때문에 처리 비용이 증가하며, 결과적으로 시스템 전체의 비용 효율성이 악화된다. 셋째, 네트워크 장애나 데이터 불균형으로 인해 데이터 가용성이 저하될 경우 무결성 손상과 신뢰 저하 위험이 따른다. 이러한 문제들은 기존 클라우드 스토리지의 편리성과 블록체인의 보안성을 동시에 충족하려는 시도에 기술적·경제적 장벽으로 작용하고 있다.

이러한 문제는 흔히 블록체인 삼중 딜레마(Trilemma)로 개념화되는데[5], 확장성, 보안성(Security), 탈중앙화(Decentralization)라는 세 가지 속성을 동시에 충족하기 어렵다는 것이다. 일반적으로 확장성을 높이려면 보안성이나 탈중앙화 중 하나를 희생해야 한다는 관점이 제시되어 왔다. 따라서 블록체인의 확장성 한계를 극복하기 위해 온체인 및 오프체인 확장 기법이 활발히 연구되고 있으며, 이 중 레이어 2(Layer 2) 솔루션이 실질적인 대안으로 주목받고 있다[6]. 특히 옵티미스틱 롤업(Optimistic Rollup)은 메인체인의 보안성을 유지하면서도 트랜잭션 처리 부담을 외부로 분산시켜 확장성을 확보하는 유망한 접근 방식으로 평가되고 있다[7].

이에 본 연구는 옵티미스틱 롤업을 활용하여 이러한 한계를 극복하고, 대규모 데이터 환경에서도 효율적으로 작동하는 블록체인 기반 분산 클라우드 스토리지 시스템을 제안하고자 한다. 블록체인 기반 분산 스토리지 시스템은 데이터 무결성과 보안성을 제공하며, 사용자에게 데이터 소유권을 부여할 수 있는 잠재력을 가진 기술로 주목받고 있다. 하지만 기존 시스템은 확장성 문제와 높은 가스비라는 기술적 한계를 가지고 있어 대규모 데이터 처리와 상용화에 어려움을 겪고 있다. 특히, 대량의 트랜잭션을 처리하거나 실시간 데이터 처리가 요구되는 환경에서는 이러한 한계가 더욱 두드러진다.

본 연구의 주요 목적은 옵티미스틱 롤업(Optimistic Rollup)[7]을 활용하여 블록체인 기반 분산 클라우드 스토리지 시스템의 확장성과 경제성을 개선하는 것이다. 옵티미스틱 롤업은 메인체인의 부하를 줄이고 가스비를 절감하며, 높은 처리 속도를 제공하는 기술로, 기존 분산 스토리지 시스템의 한계를 극복할 수 있는 유망한 솔루션으로 평가된다. 이를 위해 Ethereum 블록체인과 IPFS를 결합하여 데이터를 분산 저장하고, 스마트 계약을 통해 데이터 접근 제어를 자동화하는 효율적인 시스템을 설계한다.

본 연구는 블록체인 기반 분산 스토리지 기술의 상용화를 촉진할 수 있는 새로운 패러다임을 제시하며, 데이터 무결성과 보안을 유지하면서도 확장성과 경제성을 확보하는 실질적인 대안을 제공한다. 확장성 개선 측면에서, 옵티미스틱 롤업의 트랜잭션 처리 메커니즘을 활용하여 기존 블록체인 기반 시스템의 낮은 처리 속도를 개선한다. 이를 통해 대규모 데이터 환경에서도 안정적으로 작동할 수 있는 블록체인 분산 스토리지를 제안한다. 기존 시스템들이 직면한 TPS 한계를 극복함으로써, 실시간 데이터 처리가 요구되는 환경에서도 효과적으로 동작할

수 있는 시스템을 구현한다.

비용 효율성 강화 측면에서는 메인체인에서 발생하는 가스비를 대폭 절감함으로써 블록체인 기술의 경제성을 높인다. 옵티미스틱 롤업의 배치 처리 방식과 낙관적 실행 모델을 통해 트랜잭션 처리 비용을 최소화하며, 이는 상용화 가능성을 확대하는 데 중요한 역할을 한다. 특히 대량의 데이터를 처리해야 하는 기업 환경에서 경제적 부담을 크게 줄일 수 있다.

데이터 무결성과 보안성 강화 측면에서는 IPFS를 활용하여 데이터를 분산 저장하고, 옵티미스틱 롤업의 사기 증명 메커니즘을 통해 데이터 무결성과 보안성을 유지한다. 이러한 이중 보안 구조를 통해 신뢰성과 안정성을 동시에 보장할 수 있으며, 중앙 서버 없이도 높은 수준의 데이터 보호를 실현 한다.
실증적 성능 평가 제공 측면에서는 가스비 절감, 처리 속도, 데이터 저장 비용과 같은 실험적 지표를 설정하고, 이를 통해 제안 시스템의 성능을 정량적으로 평가한다. Sepolia 테스트넷과 Titan Sepolia 옵티미스틱 롤업 네트워크를 통한 실험을 통해 구체적인 성능 개선 수치를 제시하며, 이러한 결과는 블록체인 기반 분산 스토리지 시스템의 상용화 가능성을 검증하는 데 기여 할 것이다.

본 연구를 통해 블록체인과 분산 저장 기술의 통합을 통해 기존 클라우드 스토리지 시스템의 단점을 보완하고, 블록체인 기술의 실제 응용 가능성을 제시하고자 한다. 특히, 확장성과 비용 문제를 해결함으로써 대규모 데이터를 다루는 현대 데이터 관리 환경에서 블록체인 기술의 실질적 유용성을 입증할 것으로 기대된다. 본 연구는 기존 이더리움 기반 분산 저장 시스템이 직면한 비용 및 확장성 문제를 해결하기 위한 실질적인 해결책을 제시한다. 이를 통해 블록체인 기술의 상용화 가능성을 높이며, 헬스케어, 금융, 공급망 관리 등 다양한 산업에서 실질적인 응용이 가능할 것으로 기대된다. 또한 데이터 주권과 프라이버시 보호가 중요해지는 현대 사회에서 개인과 기업이 자신의 데이터를 안전하고 경제적으로 관리할 수 있는 새로운 방안을 제공한다.

본 논문은 총 5개 장으로 구성되어 있다. 제2장에서는 블록체인 기반 분산 저장 시스템의 현황과 한계점을 체계적으로 분석하고, 기존 분산 저장 시스템들의 특징과 문제점, 블록체인의 확장성 문제, 그리고 이를 해결하기 위한 레이어2 솔루션들에 대해 검토한다. 제3장에서는 본 연구에서 제안하는 옵티미스틱 롤업 기반 분산 스토리지 개선 모델의 전체 아키텍처와 설계 방안을 상세히 설명한다. 제4장에서는 제안된 시스템의 성능을 검증하기 위한 실험 설계와 결과 분석을 제시하며, 가스비 절감 효과와 트랜잭션 처리 속도 개선을 실증적으로 입증한다. 제5장에서는 연구 결과를 종합하고, 옵티미스틱 롤업을 적용한 블록체인 기반 분산 스토리지 시스템의 성능 개선 효과와 상용화 가능성을 평가하며, 향후 연구 방향을 제시한다.

II. 관련 연구

1. 블록체인 기반 분산 저장 시스템

블록체인은 본질적으로 트랜잭션 데이터 위주의 기록을 처리하기 때문에 대규모 파일이나 비정형 데이터를 직접 저장하기에는 한계가 있다.이러한 한계를 보완하기 위해 블록체인과 연동되는 분산 저장 네트워크가 등장하였다. 대표적인 사례가 IPFS(InterPlanetary File System)[1]이다.

IPFS는 콘텐츠 기반 주소 체계를 활용하는 P2P 파일 시스템으로, 데이터를 여러 노드에 분산 저장하여 단일 장애점을 제거한다[1]. 사용자는 파일 해시값을 통해 원하는 데이터를 검색할 수 있으며, 이는 중앙 서버에 의존하지 않는 구조를 가능하게 한다. IPFS의 핵심 특징은 콘텐츠 기반 해시를 통한 데이터 식별과 검증으로, 데이터가 변경되면 해시값도 달라지기 때문에 무결성을 자동으로 보장할 수 있다.

Sia[3]는 피어 간의 저장 계약을 블록체인에 기록하여 신뢰를 보장하는 초기 분산 저장 플랫폼의 하나이다. Sia에서는 데이터 저장을 원하는 사용자가 하드 드라이브 공간을 제공하는 호스트와 스마트 계약을 맺고, 해당 계약(데이터 크기, 기간, 가격 등)이 블록체인에 기록된다. 호스트는 정기적으로 자신이 데이터를 유지하고 있음을 증명하는 스토리지 증명을 블록체인에 제출해야 하며, 이를 지키지 못하면 페널티를 받는다.

이와 유사한 개념의 Storj[2] 등의 플랫폼도 토큰 경제를 통해 신뢰 없는 환경에서 다수의 노드들이 사용자의 파일을 분산 저장하도록 유도하고 있다. Storj는 데이터를 암호화하여 여러 노드에 분산 저장하고, 각 노드는 데이터의 일부분만을 보유하게

되어 프라이버시와 보안을 강화한다. 이러한 시스템들은 중앙 서버 없이도 다중 복제와 암호학적 검증을 통해 데이터의 무결성과 가용성을 확보한다. 특히 국내에서도 데이터 신뢰도 확보를 위한 블록체인 기반 분산 스토리지 연구가 활발히 진행되고 있다[8]. 이처럼 블록체인과 결합된 분산 저장 시스템은 중앙 서버 없이도 데이터 무결성, 가용성, 보안성을 확보할 수 있다는 장점이 있다. 또한 데이터 소유권이 사용자에게 귀속되며, 검열 저항성과 영구 보존 가능성을 제공한다[4].

그러나 높은 트랜잭션 비용과 처리 속도 저하라는 근본적 한계를 여전히 안고 있으며, 이 문제를 해결하기 위한 확장성 기술의 적용이 필요하다.

2. 블록체인 확장성 해결을 위한 기존 접근법

제1장에서 언급한 바와 같이, 블록체인은 확장성(Scalability), 보안성 (Security), 탈중앙화 (Decentralization) 라는 세 가지 속성을 동시에 충족하기 어려운 삼중 딜레마에 직면해 있다[5]. 이러한 한계를 극복하기 위해 온체인(On-chain) 및 오프체인(Off-chain) 확장 기법들이 제안되어 왔다. 온체인 확장 기법은 블록체인 프로토콜 자체를 수정하여 성능을 개선하는 방식이며, 대표적으로 블록 크기 증가, 블록 생성 시간 단축, 합의 알고리즘 개선, 샤딩 등이 있다. 블록 크기를 증가시키는 방법은 한 번에 더 많은 트랜잭션을 처리할 수 있게 하지만, 노드 운영 비용이 증가하고 네트워크 전파 지연이 발생하여 탈중앙화를 저해할 수 있다.

비트코인 캐시(Bitcoin Cash)는 블록 크기를 8MB에서 32MB까지 증가시켜 처리량을 늘렸으나, 이로 인해 네트워크가 분열되고 노드 수가 감소하는 결과를 초래했다. 블록 생성 시간을 단축하는 방법도 처리 속도를 높일 수 있으나, 블록 재편성(Reorganization) 위험이 증가하고 네트워크 안정성이 저하될 수 있다. 라이트코인(Litecoin)은 비트코인 대비 4배 빠른 블록 생성 시간을 채택하여 거래 확정 시간을 단축했으나, 보안성 측면에서는 여전히 논란이 있다. 합의 알고리즘을 개선하는 방법으로는 작업 증명(Proof of Work, PoW)에서 지분 증명(Proof of Stake, PoS)이나 실용적 비잔틴 장애 허용(Practical Byzantine Fault Tolerance, PBFT) 등으로 전환하는 방식이 제안되었다. PoS는 에너지 소비를 줄이고 처리 속도를 높일 수 있지만, 부의 집중화 문제와 Nothing at Stake 공격 가능성이 존재한다. 이더리움은 2022년 The Merge를 통해 PoS로 전환하여 에너지 효율성을 크게 개선했으나[5], 확장성 문제는 여전히 근본적으로 해결되지 않았다. 샤딩(Sharding)[10]은 네트워크를 여러 개의 샤드로 분할하여 각 샤드가 독립적으로 트랜잭션을 처리하도록 하는 기법이다. 이더리움 2.0은 64개의 샤드 체인을 도입하여 이론적으로 처리량을 크게 향상시킬 계획이었으나, 기술적 복잡성과 크로스 샤드 통신 문제로 인해 구현이 지연되고 있으며, 현재는 레이어2 중심의 롤업 중심 로드맵(Rollup-centric Roadmap)으로 전환되었다[5].

오프체인 확장 기법으로는 상태 채널(State Channel)이 대표적이다. 상태 채널은 두 참여자 간의 다수의 트랜잭션을 오프체인에서 처리하고, 최종 상태만을 메인체인에 기록하는 방식이다. 비트코인의 라이트닝 네트워크(Lightning Network)가 대표적인 예로, 소액 결제의 즉시성과 낮은 수수료를 제공한다. 그러나 상태 채널은 참여자 간 채널을 미리 개설해야 하고, 다자간 거래나 복잡한 스마트 계약 실행에는 적합하지 않다는 한계가 있다. 특히 분산 저장 시스템처럼 불특정 다수와의 빈번한 상호작용이 필요한 환경에서는 모든 노드 쌍 간에 채널을 개설하고 관리하는 것이 비현실적이다.

이러한 온체인 확장 기법들은 각각의 장점이 있으나, 보안성과 탈중앙화를 유지하면서 대폭적인 확장성 개선을 달성하기 어렵다는 공통적인 한계를 가지고 있다. 따라서 메인체인의 보안성을 활용하면서도 높은 확장성을 제공할 수 있는 레이어2 솔루션이 차세대 블록체인 확장 기술로 주목받고 있다.

3. 레이어2 확장 기술

온체인 확장 기법이 구조적 한계를 가지는 반면, 레이어 2 확장 기술은 블록체인 메인체인의 보안성을 유지하면서 트랜잭션 처리 부담을 외부로 분산시켜 확장성을 확보하는 접근 방식이다. 레이어 2 솔루션은 메인체인 위에서 동작하며, 결과만을 요약해 기록함으로써 성능을 극대화한다. 대표적인 방식으로 플라즈마(Plasma), ZK 롤업, 옵티미스틱 롤업 등이 있다.

플라즈마는 트랜잭션을 별도의 하위 체인에서 처리하고, 요약된 결과만 메인체인에 기록하는 방식이다. 사용자들은 하위 체인에서 빠르고 저렴한 거래

를 할 수 있으며, 주기적으로 상태 변경 사항을 메인체인에 커밋한다[6]. 플라즈마의 구조가 비교적 단순해 구현이 용이하고, 이론적으로는 무제한 확장이 가능하다. 그러나 데이터 가용성(Data Availability) 문제가 내재되어 있어 대규모 데이터 처리에는 한계가 있다. 특히 하위 체인 운영자가 악의적으로 행동하거나 오프라인이 될 경우 사용자가 자신의 자산을 인출하기 어려울 수 있는 문제가 있다.

ZK 롤업은 영 지식 증명(Zero-Knowledge Proof)을 활용하여 트랜잭션을 외부에서 검증하고, 검증된 결과를 메인체인에 기록하는 방식이다. ZKP는 모든 상태 변경이 정확히 검증되었음을 보장하며, 높은 보안성과 데이터 무결성을 제공한다. ZK 롤업의 가장 큰 장점은 수학적 증명을 통해 즉시 최종성(Instant Finality)을 제공한다는 점이다. 사기 증명을 기다릴 필요 없이 트랜잭션이 즉시 확정되므로 사용자 경험이 우수하다. 그러나 ZKP 생성 과정에서의 높은 연산 비용과 구현 복잡성은 대규모 데이터를 처리하는 시스템에서 효율성을 저하시킬 수 있다. 특히 일반적인 스마트 계약 실행에 필요한 ZKP 회로 설계가 복잡하고, 증명 생성에 상당한 시간과 컴퓨팅 자원이 소요된다. 따라서 ZK 롤업은 높은 보안성이 요구되는 응용 프로그램에는 적합하지만, 실시간 데이터 처리가 필요한 환경에서는 비효율적일 수 있다[9].

옵티미스틱 롤업은 트랜잭션을 "대부분 정상일 것"이라는 가정하에 처리하고, 필요할 때만 사기 증명(Fraud proof) 메커니즘을 통해 트랜잭션 오류를 검증한다. 이 방식은 추가 연산이 필요한 경우가 제한적이므로 비용 효율성이 매우 높으며, 처리량이 증가할수록 그 장점이 극대화된다. 특히 이더리움과 높은 호환성을 보유해 구현이 용이하고, 기존 스마트 계약을 거의 수정 없이 이식할 수 있어 실제 산업 현장에서 널리 활용될 가능성이 높다. 대표적인 옵티미스틱 롤업 프로젝트로는 Optimism과 Arbitrum이 있으며, 이들은 이더리움 메인넷 대비 10-100배의 처리량 향상과 가스비 절감을 실현하고 있다[7].

각 레이어2 솔루션은 서로 다른 특징과 장단점을 가지고 있어, 응용 분야에 따라 적합한 기술을 선택하는 것이 중요하다. 분산 저장 시스템의 경우 빈번한 데이터 저장 및 검색 요청을 처리해야 하므로 빠른 처리 속도와 낮은 비용이 핵심 요구사항이 되며, 이러한 관점에서 옵티미스틱 롤업이 가장 적합한 솔루션으로 평가된다.

4. 옵티미스틱 롤업 기술

옵티미스틱 롤업은 블록체인 네트워크의 확장성을 개선하기 위해 설계된 레이어2 솔루션으로, 블록체인의 트랜잭션 처리 부담을 줄이면서 비용 효율성을 높이는 데 중점을 둔 기술이다. 이 기술은 데이터의 일부를 메인체인이 아닌 외부에서 처리하고, 그 결과만 메인체인에 기록함으로써 처리 속도와 가스비 절감 효과를 극대화할 수 있다[7][10].

옵티미스틱 롤업의 핵심은 낙관적 실행(Optimistic Execution) 모델을 기반으로 한다. 기본 가정은 대부분의 트랜잭션이 올바르게 처리된다는 것이며, 트랜잭션 무결성은 사기 증명 메커니즘을 통해 검증된다[10]. 예를 들어, 만약 100개의 트랜잭션이 발생하면, 그 중 오류가 있을 가능성은 극히 낮으므로 100개 모두를 신속하게 처리한 뒤, 나중에 오류 여부를 확인한다. 이를 통해 메인체인에 모든 트랜잭션을 기록하는 대신, 많은 트랜잭션을 빠르게 모아서 처리할 수 있으므로 처리 속도가 획기적으로 증가하고, 가스비 부담이 줄어든다.

사기 증명은 트랜잭션 처리 후 발생할 수 있는 오류나 부정 행위를 검증하는 메커니즘이다. 트랜잭션이 처리된 후, 이의제기 기간(Challenge period) 동안 네트워크 참여자가 트랜잭션의 상태 변경 내역을 감시한다. 만약 부정확한 상태 변경이 발견되면, 참여자는 사기 증명을 제출하여 해당 트랜잭션을 재검증하고, 문제가 확인되면 상태 변경을 무효화 한다. 예를 들어, 사용자가 데이터를 저장하는 트랜잭션을 제출한 후, 다른 참여자가 해당 트랜잭션에 오류가 있다고 판단할 경우, 지정된 이의제기 기간 내에 오류에 대한 증거(예: 잘못된 해시값, 부정확한 상태 업데이트 등)를 제출한다. 증거가 인정되면, 해당 트랜잭션은 취소되고 올바른 상태로 복구되며, 오류를 제출한 참여자에게 인센티브가 제공될 수 있다.

표. 1 Components of optimistic rollup
Table 1. Components of optimistic rollup

Components	Description
Rollup contracts	Smart contracts on Layer 1 managing state updates and proofs
Fraud proof	Verifies and resolves incorrect transactions using challenges
Data availability	Ensures off-chain data remains accessible and secure
Transaction bundling	Aggregates multiple transactions to reduce costs

옵티미스틱 롤업은 메인체인(Ethereum) 상에 스마트 계약 형태로 구현된다. 이 스마트 계약은 롤업 트랜잭션 데이터를 수집하고 이를 통해 상태 변경(State Transition)을 관리한다. 트랜잭션 번들(Bundle)은 메인체인에 기록되지만, 상세 데이터는 외부 저장소(IPFS 등)에 저장되어 메인체인의 데이터 부하를 최소화한다[7]. 롤업 계약은 상태 루트(State Root)를 관리하여 오프체인에서 처리된 모든 상태 변경을 추적하며, 사기 증명이 제기될 경우 해당 상태 변경의 유효성을 검증할 수 있는 메커니즘을 제공한다.

옵티미스틱 롤업은 데이터 가용성을 유지하기 위해 외부 분산 저장 네트워크(IPFS 등)를 활용한다. 이를 통해 트랜잭션 데이터를 효율적으로 저장하고, 블록체인의 데이터 저장 부담을 줄인다. 이러한 접근법은 대규모 데이터를 처리하는 환경에서 특히 유리하다[10]. 데이터 가용성은 사기 증명의 전제 조건이므로, 모든 참여자가 필요시 트랜잭션 데이터에 접근할 수 있어야 한다. 옵티미스틱 롤업의 주요 특징과 장점을 살펴보면, 첫째로 비용 효율성이 뛰어나다. 메인체인의 가스비 부담을 줄이고, 트랜잭션 처리 비용을 획기적으로 절감한다. 사기 증명이 발생하지 않는 경우 추가 연산이 필요하지 않아 가스비 절감 효과가 극대화된다[7]. 둘째로 확장성이 우수하다. 메인체인 외부에서 트랜잭션을 처리하기 때문에 높은 처리량(TPS, Transactions Per Second)을 제공한다. 이는 대규모 데이터를 실시간으로 처리해야 하는 응용 환경에 적합하다[10]. 셋째로 구현이 용이하다. 옵티미스틱 롤업은 기존 이더리움 스마트 계약과의 호환성이 높아 비교적 간단하게 구현할 수 있다. 이는 기존 시스템을 크게 변경하지 않고도 레이어2 솔루션을 도입할 수 있다는 점에서 중요한 이점이다[7].

반면 옵티미스틱 롤업의 한계점도 존재한다. 데이터 가용성 문제와 이의제기 기간 동안의 지연이라는 한계를 가진다. 사기 증명 검증 과정에서 네트워크 참여자의 적극적인 참여가 필요하며, 데이터 가용성이 충분히 보장되지 않을 경우 신뢰성이 저하될 수 있다. 이러한 한계를 극복하기 위해 IPFS와 같은 분산 저장 시스템을 활용하거나, 데이터 샘플링 및 검증 기술을 도입하는 방안이 제안되고 있다[10].

ZK 롤업과의 비교에서 옵티미스틱 롤업의 특징을 더욱 명확히 할 수 있다. 옵티미스틱 롤업은 낙관적 실행과 사기 증명을 통해 검증하는 반면, ZK 롤업은 영 지식 증명를 사용한다. 데이터 가용성 측면에서는 옵티미스틱 롤업이 외부 데이터 접근을 요구하는 반면, ZK 롤업은 상대적으로 문제가 적다. 처리 속도는 옵티미스틱 롤업이 낙관적 실행으로 인해 빠르지만, ZK 롤업은 ZKP 생성에 시간이 소요된다. 확장성 측면에서는 옵티미스틱 롤업이 이의제기 기간으로 인한 지연이 있을 수 있으나, ZK 롤업은 ZKP를 통한 즉시 검증이 가능하다. 가스비 효율성은 옵티미스틱 롤업이 사기 증명이 없으면 매우 높고, ZK 롤업은 ZKP 생성 비용이 발생하지만 데이터 효율성이 개선된다. 보안성은 옵티미스틱 롤업이 사기 증명을 통해 오류 정정이 가능하고, ZK 롤업은 ZKP를 통한 완전한 검증으로 매우 높다. 구현 복잡성은 옵티미스틱 롤업이 낮고, ZK 롤업은 높다.

본 연구에서는 분산 저장 시스템의 특성상 경제성, 속도, 구현 용이성을 고려하여 옵티미스틱 롤업을 선택하였다. ZK 롤업은 높은 보안성을 제공하지만, ZKP 생성 과정에서의 연산 비용이 커 대규모 데이터를 처리하기에 비효율적일 수 있다. 반면, 옵티미스틱 롤업은 데이터 처리량이 증가할수록 가스비 절감 효과가 더욱 부각된다. 분산 저장 시스템은 빈번한 데이터 저장 및 검색 요청을 처리해야 하므로 빠른 처리 속도가 필요하며, 옵티미스틱 롤업은 사기 증명이 없는 경우 메인체인보다 훨씬 높은 처리 속도를 제공한다. 또한 기존 이더리움 스마트 계약과의 호환성이 높아 구현 및 유지 보수가 용이하다는 장점이 있다.

표 2 Optimistic Rollup vs ZK Rollup
Table 2 Optimistic Rollup vs ZK Rollup

Feature	Optimistic Rollup	ZK-Rollup
Verification	Optimistic execution	Zero-Knowle

Method	+ Fraud proof	dge Proof (ZKP)
Data Availability Issues	Present (requires external data access)	Relatively minimal
Processing Speed	Fast (high TPS due to optimistic execution)	Slow (time required for ZKP generation)
Scalability	Moderate (possible delays due to Challenge Period)	High (instant verification with ZKP)
Gas Fee Efficiency	Very high (minimal gas fee if no fraud proof)	High (ZKP generation incurs cost, but data efficiency is improved)
Security	High (errors can be corrected via fraud proof)	Very high (all states are fully verified via ZKP)
Implementatio n Complexity	Low	High
Applications	Optimism, Arbitrum	StarkNet, zkSync

표 2에서 확인할 수 있는 옵티미스틱 롤업의 장점으로는 첫 번째는 구현이 비교적 간단하며, 기존 이더리움과의 호환성이 높다는 점이다. 두 번째는 높은 처리 속도와 가스비 절감 효과를 제공인데, 특히 데이터 처리량이 증가할수록 효율성이 더욱 부각된다는 점이 있다. ZK 롤업의 경우는 영 지식 증명을 통해 트랜잭션이 즉각적으로 검증되므로 보안성이 탁월하다는 점이 있고, 이로 인해 데이터 가용성 문제가 상대적으로 적으며, 사기 증명에 의존하지 않아도 된다는 장점이 있다. 본 연구에서는 다음과 같은 이유로 시스템에 옵티미스틱 롤업을 선택하였다.

경제성: ZK 롤업은 높은 보안성을 제공하지만, ZKP 생성 과정에서의 연산 비용이 커 대규모 데이터를 처리하기에 비효율적일 수 있다. 반면, 옵티미스틱 롤업은 데이터 처리량이 증가할수록 가스비 절감 효과가 더욱 부각 된다.

속도: 분산 저장 시스템은 빈번한 데이터 저장 및 검색 요청을 처리해야 하므로 빠른 처리 속도가 필요하다. 옵티미스틱 롤업은 사기 증명이 없는 경우 메인체인보다 훨씬 높은 처리 속도를 제공 한다.

구현 용이성: 옵티미스틱 롤업은 기존 이더리움 스마트 계약과의 호환성이 높아 구현 및 유지 보수가 용이하다.

III. 옵티미스틱 롤업 기반 분산 스토리지 개선 모델

본 장에서는 이더리움 기반 분산 저장 시스템에 옵티미스틱 롤업을 적용하여 비용 절감과 성능 개선을 목표로 하는 제안 시스템의 아키텍처를 설명한다. 이 시스템은 블록체인과 분산 저장 시스템의 결합을 최적화하기 위한 솔루션으로, 기존 이더리움 메인체인에서 발생하는 높은 가스비 문제를 해결하고, 동시에 트랜잭션 처리 속도와 확장성을 개선하는 것을 목적으로 한다.

1. 시스템 개요

제안된 시스템은 이더리움 메인체인, 옵티미스틱 롤업 기반 레이어 2 솔루션, IPFS 분산 저장 네트워크 세 가지 요소로 구성된다. 사용자는 데이터를 IPFS에 업로드하고, 그 결과 생성되는 해시값 및 접근 제어 정보를 블록체인에 기록한다. 이때 발생하는 트랜잭션은 레이어2의 옵티미스틱 롤업에서 처리되어, 가스비 절감과 처리 속도 향상이 가능하다. 블록체인 스마트 계약은 데이터 접근 권한과 무결성을 관리하며, 시스템 전체의 신뢰성을 보장한다. 제안하는 시스템은 기존 이더리움 기반 분산 저장 시스템의 한계를 극복하기 위해 다음과 같은 핵심 설계 원칙을 따른다. 첫째, 메인체인의 보안성을 유지하면서도 트랜잭션 처리 비용을 대폭 절감한다. 둘째, 옵티미스틱 롤업의 낙관적 실행 모델을 통해 높은 처리 속도를 달성한다. 셋째, IPFS와의 효율적인 연동을 통해 대용량 데이터 저장과 검색을 지원한다. 넷째, 스마트 계약을 통한 자동화된 접근 제어로 데이터 무결성과 보안성을 보장한다.

이러한 설계 원칙을 바탕으로 제안 시스템은 사용자에게 기존 중앙집중식 클라우드 스토리지와 유사한 사용자 경험을 제공하면서도, 블록체인 기술의 탈중앙화, 투명성, 데이터 소유권 보장 등의 이점을 함께 제공할 수 있다.

2. 주요 구성 요소

제안하는 시스템 아키텍처는 다음과 같은 주요 구성 요소로 이루어진다. IPFS는 데이터의 중앙 집중 저장 문제를 해결하기 위해 설계된 P2P 기반의 분산 저장 네트워크이다[1]. 사용자가 업로드한 데이터는 여러 노드에 분산 저장되며, 각 파일은 고유한 해시값으로 식별된다[11]. 이를 통해 데이터의 무결성과 보안성이 보장되며, 사용자는 특정 해시값을 통해 원본 데이터를 확인하고 접근할 수 있다.

이더리움 메인체인은 데이터 무결성을 보장하고, 스마트 계약을 통해 데이터 접근 제어를 수행하는 역할을 한다[5]. 사용자가 데이터를 저장하면, 해당 데이터의 메타데이터(예: 해시값, 접근 권한, 저장 위치)는 스마트 계약을 통해 기록된다. 이를 통해 사용자는 데이터에 대한 소유권을 가지며, 특정 권한을 가진 사용자만이 데이터에 접근할 수 있도록 설정할 수 있다. 이더리움의 스마트 계약 기능을 활용하면 복잡한 접근 제어 로직을 구현할 수 있다. 예를 들어, 시간 기반 접근 제어, 역할 기반 접근 제어, 조건부 접근 제어 등을 프로그래밍적으로 정의할 수 있다. 또한. 모든 접근 기록이 블록체인에 불변의 형태로 저장되므로 감사 추적(Audit Trail)이 가능하며, 이는 규제가 엄격한 산업 분야에서 중요한 요구사항을 충족할 수 있다. 메인체인은 또한 경제적 인센티브 메커니즘을 제공하여 네트워크 참여자들의 올바른 행동을 유도한다. 스마트 계약을 통해 저장 제공자에게 보상을 지급하거나, 부정행위에 대한 페널티를 부과하는 등의 자동화된 경제 시스템을 구축할 수 있다.

옵티미스틱 롤업은 메인체인의 확장성을 향상 시키는 핵심 기술로, 다수의 트랜잭션을 모아 하나의 블록으로 압축하여 메인체인에 기록하는 방식을 채택한다[7][12]. 이 방식은 트랜잭션을 "낙관적으로" 처리하며, 추가적인 검증이 필요한 경우에만 사기 증명을 활용해 트랜잭션의 무결성을 검증한다. 이를 통해 블록체인 네트워크의 부담을 줄이고, 가스비 절감과 트랜잭션 처리 속도 향상을 가능하게 한다. 옵티미스틱 롤업의 핵심 구성 요소는 다음과 같다. 롤업 계약(Rollup Contracts)은 레이어1에서 상태 업데이트와 증명을 관리하는 스마트 계약이다. 사기 증명(Fraud Proof)은 잘못된 트랜잭션을 검증하고 해결하는 이의제기 메커니즘이다. 데이터 가용성(Data Availability)은 오프체인 데이터가 접근 가능하고 안전하게 유지되도록 보장한다. 트랜잭션 번들링(Transaction Bundling)은 다수의 트랜잭션을 집계하여 비용을 절감한다. 상태 전이(State Transition)는 오프체인에서 상태 전이를 처리하고 업데이트한다. 옵티미스틱 롤업은 메인체인과 높은 호환성을 가지므로 기존 이더리움 애플리케이션을 쉽게 이식할 수 있으며, EVM(Ethereum Virtual Machine) 호환성을 통해 개발자들이 익숙한 도구와 언어를 사용할 수 있다. 이는 기존 분산 저장 시스템을 크게 수정하지 않고도 성능 향상을 달성할 수 있다는 중요한 장점이다.

스마트 계약은 데이터 접근 제어 및 저장 로직을 자동화한다[13]. 사용자의 데이터 저장·검색 요청은 모두 스마트 계약을 거쳐 처리되며, 이 과정에서 롤업을 통한 비용 절감이 실현된다. 본 시스템에서 스마트 계약은 여러 계층의 기능을 수행한다. 첫째, 데이터 메타데이터 관리 기능으로 파일 해시, 크기, 타임스탬프, 접근 권한 등의 정보를 저장하고 관리한다. 둘째, 접근 제어 기능으로 사용자 권한을 검증하고 데이터 접근을 허용하거나 거부한다. 셋째, 경제적 인센티브 관리 기능으로 저장 비용 지불, 제공자 보상, 페널티 부과 등을 자동으로 처리한다. 넷째, 무결성 검증 기능으로 저장된 데이터의 무결성을 주기적으로 확인하고 문제 발생 시 복구 프로세스를 시작한다. 스마트 계약의 자동화된 실행은 중앙 관리자 없이도 시스템이 안정적으로 동작할 수 있게 하며, 모든 거래와 접근 기록이 투명하게 기록되어 신뢰성을 보장한다. 또한, 업그레이드 가능한 프록시 패턴을 사용하여 시스템의 지속적인 개선과 버그 수정을 가능하게 한다.

3. 시스템 동작 흐름

제안하는 시스템의 전체 동작 흐름은 다음과 같다. 사용자가 데이터를 업로드 하는 과정은 여러 단계로 구성된다. 먼저 사용자가 클라이언트 애플리케이션을 통해 저장하고자 하는 파일을 선택한다. 시스템은 파일을 암호화하고 청크 단위로 분할 한 후 IPFS 네트워크에 업로드 한다. IPFS는 각 청크에 대해 고유한 해시값을 생성하고, 전체 파일에 대한 메타 해시를 반환한다. 이후 사용자는 스마트 계약을 통해 해당 해시값과 데이터 접근 권한 정보를 블록체인에 기록한다. 이때 접근 권한은 소유자 정보, 읽기/쓰기 권한, 공유 설정, 만료 시간 등의 세부 정보를 포함한다. 옵티미스틱 롤업을 통해 해당 트랜잭션이 배치 처리되어 메인체인에 기록된다. 롤업 시스템은 다수의 저장 요청을 하나의 배치로 묶

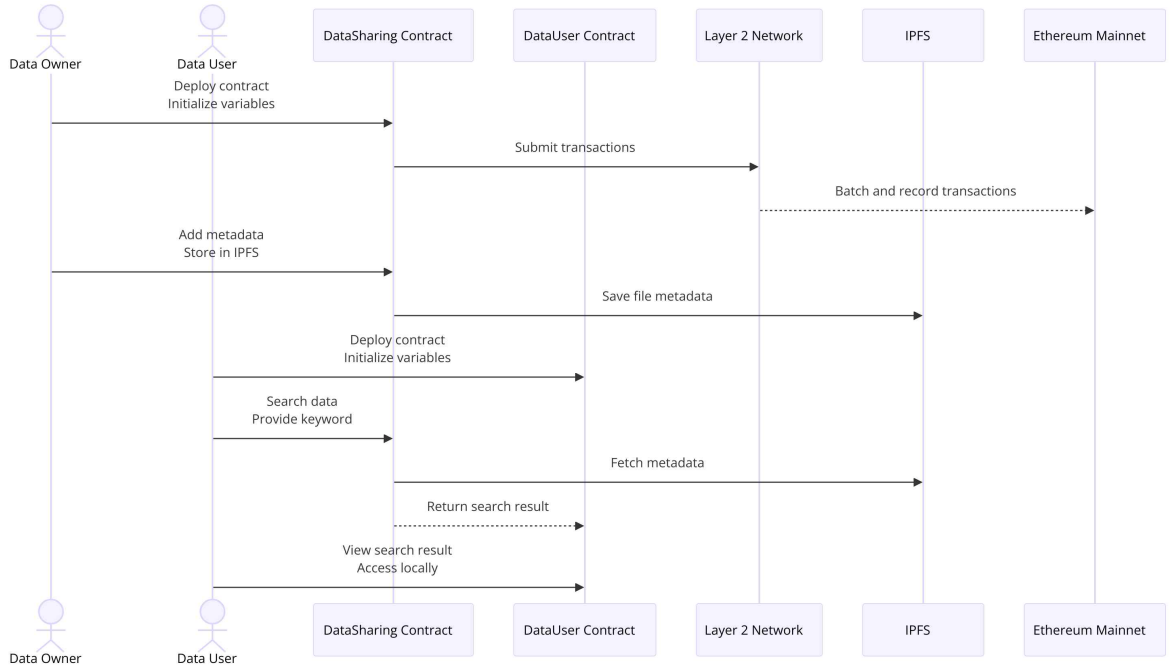

그림 1. 컨트랙트 흐름도
Fig 1. Contract flow diagram

어 처리함으로써 개별 트랜잭션 비용을 대폭 절감한다. 사용자는 트랜잭션 확인 후 파일 접근을 위한 고유 식별자와 접근 토큰을 받게 된다.

데이터 검색 과정은 효율성과 보안성을 모두 고려하여 설계되었다. 사용자는 특정 데이터에 접근하기 위해 먼저 스마트 계약을 조회한다. 스마트 계약은 사용자의 접근 권한을 확인한 후, 해당 데이터의 해시값과 접근 허용 토큰을 반환한다. 권한 검증 과정에서는 사용자 신원, 요청 시간, 접근 목적 등이 종합적으로 검토된다. 권한이 확인되면 사용자는 반환된 해시값을 사용하여 IPFS 네트워크에서 데이터를 검색한다. IPFS의 DHT 시스템을 통해 해당 데이터를 보유한 노드를 찾고, 가장 빠른 경로를 통해 데이터를 다운로드 한다. 다운로드 과정에서 데이터 무결성이 자동으로 검증되며, 손상된 청크가 발견될 경우 다른 노드로부터 재다운로드한다. 옵티미스틱 롤업을 통해 데이터 조회 요청이 메인체인에 기록되어 감사 추적을 가능하게 한다. 이는 규제 요구사항을 충족하고 시스템의 투명성을 보장한다.

롤업 시스템의 트랜잭션 처리 과정은 높은 효율성과 보안성을 동시에 달성하도록 설계되었다. 사용자가 발생시키는 다수의 트랜잭션은 롤업 노드에서 실시간으로 수집되고 배치 단위로 처리된다. 롤업 노드는 트랜잭션의 유효성을 사전 검증하고, 상태 변경을 계산하여 새로운 상태 루트를 생성한다. 일정 기간 동안 (일반적으로 7일) 트랜잭션의 무결성이 검증되며, 네트워크 참여자들은 이의를 제기할 수 있다. 이의가 없는 경우 해당 배치는 최종적으로 메인체인에 기록되어 확정된다. 만약 사기 증명 메커니즘을 통해 비정상적인 트랜잭션이 감지되면 해당 배치는 롤백되고 올바른 상태로 복구된다[14]. 사기 증명 과정에서는 챌린저가 구체적인 증거와 함께 이의를 제기하며, 온체인 검증을 통해 분쟁이 해결된다. 올바른 이의를 제기한 참여자는 보상을 받고, 잘못된 배치를 제출한 운영자는 예치금을 잃게 되어 시스템의 경제적 보안성이 유지된다. 이러한 메커니즘을 통해 시스템은 높은 처리량과 낮은 비용을 달성하면서도 메인체인 수준의 보안성을 보장할 수 있다. 또한, 이의제기 기간에 사용자는 언제든지 자신의 자산을 메인체인으로 인출 할 수 있어 자금의 안전성이 보장된다. 본 시스템은 기존 이더리움 기반 분산 저장 시스템이 직면한 비용 및 확장성 문제를 해결하기 위한 실질적인 해결책을 제시하고자 한다.

IV. 실험 및 성능분석

본 장에서는 이더리움 기반 분산 저장 시스템에 옵티미스틱 롤업을 적용하여 가스비 절감 및 성능 향상 효과를 분석하기 위한 실험 설계와 성능 분석

방법을 설명한다. 실험은 제안 시스템이 기존 이더리움 메인체인에서의 분산 저장 시스템과 비교하여 가스비 절감 효과를 얼마나 달성할 수 있는지, 그리고 트랜잭션 처리 속도와 확장성을 얼마나 개선할 수 있는지를 확인하는 것을 목표로 한다..

1. 실험 환경 설정

실험은 이더리움 Sepolia 테스트넷과 Titan Sepolia 옵티미스틱 롤업 네트워크에서 수행된다. Sepolia는 이더리움 메인넷과 유사한 환경을 제공하여, 실제 메인넷 대비 낮은 비용으로 트랜잭션을 실험할 수 있는 표준 테스트 환경이다. Titan Sepolia는 옵티미스틱 롤업을 지원하는 레이어2 솔루션으로, 동일한 조건에서 가스비 절감 효과와 트랜잭션 처리 속도 향상을 비교하기에 적합하다. 본 실험의 핵심 목적은 레이어1과 레이어2 환경 간의 블록체인 트랜잭션 비용 및 처리 성능 차이를 정량적으로 비교하는 것이다. 이를 위해 실험은 데이터 저장 자체(IPFS 업로드)를 포함하지 않고, 데이터 접근 권한 및 메타데이터 기록 과정만을 대상으로 진행하였다. 이러한 실험 설계의 근거는 다음과 같다. 실험 환경은 다음과 같은 주요 요소로 구성된다.

첫째, IPFS를 통한 데이터 업로드 성능은 네트워크 대역폭, 노드 분포, 파일 크기 등 다양한 환경 변수에 따라 크게 변동하며, 블록체인 레이어의 성능과는 독립적으로 작동한다. IPFS는 P2P 네트워크 기반의 분산 저장 시스템으로, 데이터 업로드 속도는 참여 노드의 수와 네트워크 상태에 크게 의존하지만, 블록체인 상의 메타데이터 기록과는 별도로 병렬 처리된다.

둘째, 실제 시스템 구현에서 사용자는 먼저 IPFS에 데이터를 업로드하여 해시값을 획득한 후, 이 해시값과 접근 권한 정보를 블록체인에 기록하는 두 단계 프로세스를 거친다. 이 과정에서 전체 응답 시간의 병목 구간은 블록체인 트랜잭션 처리 시간이며, IPFS 업로드는 비동기적으로 처리되거나 선행될 수 있다. 따라서 블록체인 트랜잭션 성능이 시스템의 전체적인 사용자 경험을 결정하는 핵심 요소가 된다.

셋째, 본 연구의 주요 기여는 옵티미스틱 롤업을 통한 블록체인 트랜잭션 비용 및 속도 개선에 있으며, 이는 메타데이터 관리 트랜잭션의 성능을 직접 측정함으로써 가장 명확하게 검증할 수 있다. 레이어1과 레이어2 간의 비교 실험에서 IPFS 업로드를 포함할 경우, 블록체인 레이어의 순수한 성능 차이를 정확히 측정하기 어렵다.

넷째, 블록체인 기반 분산 저장 시스템의 핵심 가치는 데이터 소유권 증명, 접근 제어, 무결성 검증 등 메타데이터 관리의 신뢰성과 투명성에 있다. 이러한 메타데이터 관리 작업은 모두 블록체인 트랜잭션을 통해 수행되므로, 본 실험은 시스템의 가장 중요한 성능 지표를 직접 측정한다고 할 수 있다.

실험 환경은 다음과 같은 주요 요소로 구성된다. Sepolia 테스트넷은 이더리움 메인체인 역할을 수행하며, 트랜잭션을 실험적으로 처리하고 가스비와 처리 속도를 측정하기 위한 블록체인 환경이다. Titan Sepolia 옵티미스틱 롤업 네트워크는 레이어2 솔루션으로서 옵티미스틱 롤업을 설정하여, 메인체인과 롤업 간의 트랜잭션 비용 및 성능 차이를 비교 분석한다. 스마트 계약은 데이터의 접근 권한과 메타데이터를 관리하며, 트랜잭션이 발생할 때마다 메타데이터를 이더리움에 기록한다. 본 실험에서 측정하는 주요 함수는 addIndex, search, deleteFile, deleteKeyword이며, 각 함수는 블록체인 상에서 실제로 발생하는 메타데이터 관리 작업을 대표한다. 이와 같은 환경 구성을 통해, 본 연구는 동일한 트랜잭션이 L1과 L2에서 각각 어떻게 처리되는지를 정량적으로 비교할 수 있었다.

2. 실험 설계

본 연구의 실험은 제안된 옵티미스틱 롤업 기반 분산 저장 시스템이 기존 레이어 1 환경 대비 가스비 절감 효과와 트랜잭션 처리 성능 향상을 어느 정도 달성할 수 있는지를 검증하는 데 목적이 있다. 이를 위해 다음과 같은 네 가지 단계로 실험을 설계하였다.

첫 번째 실험에서는 옵티미스틱 롤업을 사용하지 않고, Sepolia 테스트넷에서 데이터를 저장하고 관리하는 시스템을 구현한다. 데이터를 업로드하고, 메타데이터를 Sepolia 메인체인에 기록하는 과정에서 발생하는 가스비와 처리 시간을 측정한다. 이를 통해 레이어1 환경에서의 기준 성능(Baseline Performance)을 확보하였다.

두 번째 실험에서는 Titan Sepolia 옵티미스틱 롤업을 적용하여 동일한 데이터를 업로드하고 메타데

이터를 기록하는 시스템을 구현한다. 옵티미스틱 롤업을 통해 데이터를 메인체인 외부에서 처리하고, 다수의 트랜잭션을 묶어 메인체인에 기록함으로써 발생하는 가스비 절감 효과와 처리 속도 개선을 측정한다. 이 실험은 옵티미스틱 롤업이 Sepolia 메인체인과 비교하여 어느 정도의 비용 절감과 성능 개선을 제공하는지 확인하는 데 중점을 둔다.

성능 분석을 하기 위한 절차는 다음과 같다. 우선, 각 시스템에서 트랜잭션 처리량이 증가할 때의 성능 변화를 분석한다. 트랜잭션을 5건, 10건, 20건 등으로 점진적으로 늘려가며 가스비와 처리 시간을 측정하여, 시스템의 확장성을 평가한다. 이를 통해, 트랜잭션 증가에 따라 Titan Sepolia 옵티미스틱 롤업이 Sepolia 메인체인에 비해 얼마나 더 많은 트랜잭션을 효율적으로 처리할 수 있는지를 확인한다.

마지막으로 각 실험에서 수집한 가스비 데이터를 기반으로 Titan Sepolia 옵티미스틱 롤업이 적용된 시스템의 가스비 절감율을 계산한다. 가스비 절감율은 Sepolia 메인체인에서 발생한 가스비와 Titan Sepolia 옵티미스틱 롤업 적용 후 발생한 가스비를 비교하여 산출한다. 이를 통해 옵티미스틱 롤업이 실제로 비용 절감에 어느 정도 기여하는지 명확하게 확인할 수 있다.

3. 성능 측정 지표 및 실험 결과

본 실험에서 측정할 주요 성능 지표는 다음과 같다. 가스비(Gas Fee)는 각 실험에서 발생한 트랜잭션 처리 비용을 측정하여, Titan Sepolia 옵티미스틱 롤업이 실제로 가스비를 얼마나 절감할 수 있는지 평가한다. 트랜잭션 처리 속도(Transaction Processing Time)는 각 트랜잭션이 처리되는 데 걸린 시간을 측정하여, Titan Sepolia 옵티미스틱 롤업이 Sepolia 메인체인 대비 처리 속도를 얼마나 개선할 수 있는지를 분석한다. 트랜잭션 처리량(Transaction Throughput)은 트랜잭션 처리량이 증가함에 따라 시스템의 성능이 어떻게 변화하는지 평가하여, 제안된 시스템의 확장성을 분석한다. 가스비 절감율은 Sepolia 메인체인 대비 Titan Sepolia 옵티미스틱 롤업 적용 후의 가스비 절감 비율을 계산하여, 옵티미스틱 롤업의 비용 효율성을 평가하며 실험 결과는 표 3과 표 4에 정리되어 있다.

각 실험 항목의 결과를 분석하면 다음과 같다. 먼저 Gas used는 각 트랜잭션별로 사용한 가스량을 나타낸다. 파일을 1개만 사용할 때는 한 번의 트랜잭션을 사용한 결과이고, 파일을 20개를 사용할 때는 20번의 트랜잭션을 전송한 후 함수 별 가스 사용량의 총합을 구한 결과이다. Tx Fee는 Gas used에 Gas price를 곱한 값으로 트랜잭션 전송을 위해 사용한 ETH의 양을 나타낸다. Sepolia에서는 계속해서 Gas price가 변하기 때문에 실험을 진행하는 동안의 평균 Gas price인 4 Gwei를 기준으로 하여 계산하였다. Titan Sepolia에서의 Gas price는 0.000000001 Gwei로 고정되어 있다. USD 값은 2024년 11월 15일의 이더리움 가격인 3171.84 달러를 기준으로 하여 Tx Fee와 곱하여 계산하였다. 마지막으로 Duration은 트랜잭션을 전송한 시점부터 트랜잭션이 처리된 시점까지의 시간을 누적시켜서 구하였다.

실험 결과, Titan Sepolia 옵티미스틱 롤업 네트워크는 Sepolia 테스트넷에 비해 가스비 절감과 처리 속도 개선이 통계적으로 유의미하게 확인되었다. 특히, 호출 횟수가 증가할수록 Titan Sepolia에서의 가스비 절감 효과는 더욱 뚜렷하게 나타났다. Sepolia 테스트 넷에서는 네트워크 상황에 따라 가스비와 처리 시간에 편차가 크지만, Titan Sepolia에서는 가스비와 처리 시간이 일정하기 때문에 시스템을 더 안정적으로 운영할 수 있을것으로 판단된다.

실험 결과를 종합하면, Titan Sepolia 롤업 환경에서 평균 80% 이상의 가스비 절감과 99% 이상의 트랜잭션 처리 속도 개선을 달성하였다. 또한 L2는 트랜잭션 수가 증가하더라도 성능을 안정적으로 유지하여, 대규모 데이터 처리 환경에 적합한 확장성을 보여주었다.

본 연구는 동일한 블록체인 기반 분산 저장 시스템을 레이어 1과 레이어 2 환경에서 구현했을 때의 성능 차이를 정량적으로 비교하는 것을 목적으로 한다. 실험 결과 레이어1 환경에서 20개 파일의 메타데이터를 기록하는 데 $30.06와 277.7초가 소요된 반면, 레이어2 환경에서는 $0.002와 1.7초만 소요되어 각각 99.99%와 99.4%의 성능 개선을 달성하였다. 이는 기존 블록체인 기반 분산 저장 시스템의 가장 큰 장벽이었던 비용과 속도 문제를 실질적으로 해결할 수 있음을 보여준다.

표 3. Sepolia에서 테스트 결과
Table 3. Test result on Sepolia

The number of files	Function	Gas used	Tx Fee(ether)	USD	Duration(sec)
1	addIndex	116,372	0.0004772778593	1.513849005	14.405
	search	66,361	0.0002721671538	0.8632706652	14.697
	deleteFile	38,586	0.000158253218	0.5019538869	10.672
	deleteKeyword	27,117	0.0001112152727	0.3527570505	10.833
5	addIndex	564,760	0.002316256865	7.346796173	73.798
	search	341,231	0.001399494734	4.438973378	70.616
	deleteFile	199,784	0.000819376481	2.598931098	58.670
	deleteKeyword	27,117	0.0001112152727	0.3527570505	26.860
10	addIndex	1,146,620	0.004702646161	14.9160412	132.271
	search	673,036	0.002760330503	8.755326704	124.618
	deleteFile	392,714	0.001610642571	5.108700532	139.806
	deleteKeyword	27,117	0.0001112152727	0.3527570505	10.957
20	addIndex	2,310,700	0.009476901227	30.05921439	277.655
	search	1,336,766	0.005482494199	17.3895944	309.137
	deleteFile	778,764	0.003193954	10.13071105	312.082
	deleteKeyword	27,117	0.0001112152727	0.3527570505	11.022

표 4. Sepolia Titan 에서 테스트 결과
Table 4. Test result on Sepolia Titan

The number of files	Function	Gas used	Tx Fee(ether)	USD	Duration(sec)
1	addIndex	22,696	0.000000000000031813	0.000000000100905746	0.081
	search	21,664	0.000000000000029317	0.000000000092988833	0.081
	deleteFile	22,120	0.000000000000030325	0.000000000096186048	0.078
	deleteKeyword	21,664	0.000000000000029185	0.000000000092570150	0.079
5	addIndex	113,480	0.000000000000159065	0.000000000504528730	0.531
	search	108,320	0.000000000000146585	0.000000000464944166	0.501
	deleteFile	110,600	0.000000000000151625	0.000000000480930240	0.448
	deleteKeyword	21,664	0.000000000000145925	0.000000000462850752	0.078
10	addIndex	226,960	0.000000000000318130	0.000000001009057459	0.887
	search	216,640	0.000000000000293170	0.000000000929888333	0.879
	deleteFile	221,200	0.000000000000303250	0.000000000961860480	0.868
	deleteKeyword	21,664	0.000000000000291850	0.000000000925701504	0.085
20	addIndex	454,280	0.000000000000636260	0.000000002018114918	1.689
	search	433,400	0.000000000000586340	0.000000001859776666	1.728
	deleteFile	442,640	0.000000000000606500	0.000000001923720960	1.685
	deleteKeyword	21,664	0.000000000000583700	0.000000001851403008	0.094

Storj, Sia 등 다른 아키텍처를 가진 분산 저장 시스템들과의 직접적인 성능 비교는 실험 환경과 측정 방법론이 상이하여 본 연구의 범위를 벗어난다. 다만 기존 연구[2][3]에서 보고된 바와 같이 이들 시스템은 저장 비용 측면에서는 우수하지만, 스마트 계약 기반의 복잡한 접근 제어나 자동화된 데이터 관리 기능이 제한적이라는 차이가 있다. 본 연구에서 제안하는 시스템은 이더리움의 완전한 스마트 계약 기능과 블록체인의 탈중앙화 특성을 유지하면서도, 옵티미스틱 롤업을 통해 경쟁력 있는 비용 효율성과 처리 속도를 달성했다는 점에서 차별화 된다.

실제 메인넷 환경에서는 다른 결과가 나올 수 있겠지만, 이 결과는 옵티미스틱 롤업이 블록체인 기반 분산 저장 시스템의 상용화를 위해 가스비와 처리 속도 문제를 효과적으로 해결할 수 있음을 시사한다.

표 5. Layer 1 vs Layer 2 간 성능 비교
Table 5. Performance comparison between Layer 1 vs Layer2

	Sepolia (Layer 1)	Titan Sepolia (Layer 2)	Improvement Rate
Transaction Processing Time (1 file)	14.405 sec	0.081 sec	99.4%
Transaction Processing Time (20 files)	277.655 sec	1.689 sec	99.3%
Gas Used (1 file)	116,372 gas	22,696 gas	80.5%
Gas Used (20 files)	2,310,700 gas	454,280 gas	80.3%
Actual Cost (1 file)	$30.059	$0.0021	99.9%
Actual Cost (20 files)	$0.863	$0.0001	99.9%

4 성능 개선 효과 분석

본 실험 결과를 바탕으로 제안 시스템의 성능 개선 효과를 분석하면 다음과 같다. 옵티미스틱 롤업을 적용함으로써 메인체인의 가스비 부담을 줄이고, 트랜잭션 처리 속도를 획기적으로 향상시킬 수 있음을 실증적으로 확인하였다. 롤업을 활용하면 다수의 트랜잭션을 하나로 묶어 메인체인에 기록할 수 있기 때문에 전체적인 비용이 대폭 절감되며[15], 롤업의 배치 처리 방식 덕분에 데이터 접근 및 저장 속도가 향상되어 블록체인 기반 분산 저장 시스템의 상용화 가능성이 실질적으로 제고되었다.

제안 시스템의 비용 구조는 기존 메인체인 기반 시스템과 근본적으로 다르다. 메인체인에서 각 개별 트랜잭션마다 발생하던 기본 가스비(Base Fee)와 우선 수수료(Priority Fee)가 롤업을 통해 다수의 트랜잭션에 분산되어 개별 사용자가 부담하는 비용이 크게 줄어든다. 실험 결과에서 확인된 바와 같이, n개의 트랜잭션을 하나의 배치로 처리할 경우 메인체인 기록 비용은 1/n로 감소하며, 네트워크 혼잡도가 높을수록 이러한 절감 효과는 더욱 뚜렷해진다. 또한 롤업 시스템은 데이터 압축 기술을 활용하여 메인체인에 저장되는 데이터양을 최소화함으로써 추가적인 비용 절감을 달성한다.

운영 비용 측면에서도 롤업 노드의 운영비는 기존 메인체인 노드 대비 훨씬 낮으며, 이는 전체 시스템의 경제성을 높이는 요소로 작용한다. 사용자는 메인체인과 유사한 보안성을 유지하면서도 훨씬 저렴한 비용으로 서비스를 이용할 수 있다는 점이 실험을 통해 입증되었다.

처리 속도 측면에서 옵티미스틱 롤업은 메인체인의 블록 생성 시간에 구애받지 않고 즉시 트랜잭션을 처리할 수 있다. 실험 결과에서 보듯이 메인체인에서 수백 초에 걸쳐 처리되던 트랜잭션이 롤업에서는 수 초 내에 처리되어 사용자 경험이 크게 향상된다. 확장성 측면에서는 메인체인의 TPS 한계를 뛰어넘어 수천 건의 트랜잭션을 병렬로 처리할 수 있음을 확인하였다. 이는 대규모 사용자가 동시에 데이터를 업로드 하거나 검색하는 상황에서도 시스템이 안정적으로 동작할 수 있음을 의미한다.

V. 결론

본 연구에서는 Optimistic Rollup 기술을 블록체인 기반 분산 저장 시스템에 도입함으로써, 데이터 저장 과정의 확장성과 경제성을 크게 개선하고자 하였다. 이러한 L2 롤업 기반 설계를 통해 온체인 저장소의 한계였던 낮은 처리량과 높은 가스비 문제를 완화하여, 대용량 데이터도 비교적 저렴한 비용으로 빠르게 저장·처리할 수 있는 가능성을 제시하였다[15].

실험은 Sepolia(L1)와 Titan Sepolia(L2) 환경에

서 진행되었으며, 그 결과 L2는 L1 대비 평균 80% 이상의 가스비 절감과 99% 이상의 트랜잭션 처리 속도 개선을 달성하였다. 또한, L2는 트랜잭션 수가 증가하더라도 성능을 안정적으로 유지하여, 대규모 데이터 처리 환경에 적합한 확장성을 보여주었다. 이러한 결과는 옵티미스틱 롤업이 블록체인 기반 분산 스토리지 시스템의 상용화 가능성을 크게 높인다는 점을 실증적으로 입증한다. 특히, 비용 절감과 실시간 응답성이 중요한 산업 환경에서 블록체인 기술이 실제로 적용될 수 있는 토대를 마련하였다.

향후 개선 방안으로, 몇 가지 개선해야할 사항이 있다. 첫 번째로는 사기증명 메커니즘의 고도화이다. 사기증명은 옵티미스틱 롤업에서 무효한 상태 전이를 감지하고 이에 대한 벌칙을 부과함으로써 오프체인 트랜잭션의 올바른 상태 전이를 보장한다. 본 연구에서는 기본적인 사기 증명 프레임워크를 구현하였으며, 롤업 노드가 상태 루트를 제출하고 이의 제기 기간 동안 검증자가 이를 확인하는 구조를 채택하였다. 구체적으로 롤업 노드는 트랜잭션 배치를 처리한 후 새로운 상태 루트를 메인체인에 제출하며, 검증자는 7일의 이의 제기 기간 동안 해당 상태 전이의 정확성을 검증할 수 있다. 만약 검증자가 오류를 발견하면 구체적인 증거와 함께 이의를 제기하고, 메인체인 상에서 해당 트랜잭션을 재실행하여 올바른 상태를 복구한다. 향후 연구에서는 Arbitrum의 멀티라운드 인터랙티브 증명 방식[14]과 같은 더욱 효율적인 사기 증명 알고리즘을 도입하여 검증 비용을 최소화하고 보안성을 강화할 예정이다.

아울러 본 시스템의 효율성과 실용성을 더욱 높이기 위해 추가적으로 다음과 같은 개선 방향을 고려할 수 있다. 데이터 검색 최적화 측면에서는 저장된 데이터를 검색하고 불러오는 과정을 더욱 효율적으로 만드는 최적화 기법을 적용할 필요가 있다. 현재는 단순한 해시 기반 검색만을 지원하지만, 메타데이터 인덱싱, 콘텐츠 기반 검색, 캐싱 메커니즘 등을 도입하여 시스템 규모가 커져도 사용자들이 데이터에 신속하게 접근할 수 있도록 개선할 수 있다. 특히 대용량 파일이나 멀티미디어 콘텐츠의 경우 부분 다운로드 및 스트리밍 기능을 지원함으로써 사용자 경험을 크게 향상시킬 수 있을 것이다.

네트워크 효과 분석도 중요한 연구 과제이다. 네트워크 참여자(사용자와 노드)가 증가함에 따라 시스템 성능과 비용 구조가 어떻게 변하는지 분석해야 한다. 이를 통해 이용자가 많아지는 상황에서도 시스템의 확장성과 경제성이 유지되는지를 평가할 필요가 있다. 네트워크 효과는 특히 IPFS와 같은 P2P 네트워크에서 중요한 요소이므로, 참여자 증가에 따른 데이터 가용성, 다운로드 속도, 네트워크 안정성 등의 변화를 체계적으로 모니터링하고 최적화 방안을 모색해야 한다.

멀티유저 환경에서의 스마트 컨트랙트 적용 가능성도 검증이 필요하다. 여러 사용자가 동시에 데이터를 저장하고 조회하는 멀티유저 시나리오에서 본 시스템을 적용해야 한다. 동시다발적 트랜잭션 환경에서도 스마트 컨트랙트가 안정적으로 동작하고 시스템 성능이 저하되지 않는지를 검증해야 한다. 이를 위해서는 동시성 제어, 트랜잭션 순서 보장, 충돌 해결 메커니즘 등을 고려한 더욱 견고한 시스템 설계가 필요하다. 또한. 사용자 간 데이터 공유, 협업 기능, 권한 위임 등의 고급 기능을 지원하기 위한 스마트 계약 확장도 고려해볼 수 있다.
보안 측면에서는 현재 시스템이 기본적인 암호화와 접근 제어만을 제공하고 있으나, 더욱 강화된 보안 기능이 필요하다. 예를 들어, 영지식 증명을 활용한 프라이버시 보호, 동형암호를 이용한 연산 가능한 암호화, 키 관리 시스템의 개선 등을 통해 사용자 데이터의 기밀성과 무결성을 한층 더 강화할 수 있을 것이다.

상호운용성 측면에서도 개선의 여지가 있다. 현재는 이더리움과 IPFS만을 지원하지만, 다양한 블록체인 네트워크와 분산 저장 프로토콜과의 호환성을 확보함으로써 사용자의 선택권을 넓히고 시스템의 활용도를 높일 수 있다. 크로스체인 기술을 활용하여 서로 다른 블록체인 간 데이터 이동과 상호작용을 지원하는 것도 미래의 중요한 연구 방향이 될 것이다.

결론적으로, 본 연구를 통해 Optimistic Rollup 기반 솔루션이 블록체인 분산 저장 시스템의 확장성 한계를 극복하고 비용 효율성을 높일 수 있음을 확인하였다. 이러한 연구 결과는 향후 더욱 확장 가능하고 경제적인 분산 저장 플랫폼을 개발하는 데에 중요한 토대를 제공할 것으로 기대된다. 특히 블록체인 기술이 실제 산업 현장에서 활용되기 위한 핵심적인 기술적 장벽을 해결함으로써, Web3 생태계의 발전과 탈중앙화된 데이터 경제의 실현에 기여할 수 있을 것이다. 앞으로의 연구를 통해 위에서 제시한 개선 방안들이 구현된다면, 블록체인 기반 분산 저장 시스템은 기존 중앙집중식 클라우드 서

비스의 실질적인 대안으로 자리잡을 수 있을 것으로 전망된다.

References

[1] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," Protocol Labs, 2014. (https://doi.org/10.48550/arXiv.1407.3561)

[2] S. Wilkinson, T. Boshevski, J. Brandoff, and P. Butcher, "Storj: A Peer-to-Peer Cloud Storage Network," Storj Labs Inc., 2014.

[3] D. Vorick and L. Champine, "Sia: Simple Decentralized Storage," Nebulous Inc., 2014.

[4] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Y. Wang, "Blockchain-Based Data Storage Framework in the Cloud," Information Systems Frontiers, vol. 20, no. 6, pp. 1257-1265, Dec. 2018. (https://doi.org/10.1007/s10796-018-9833-z)

[5] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Foundation, 2018.

[6] J. Poon and V. Buterin, "Plasma: Scalable Autonomous Smart Contracts," Plasma Whitepaper, 2017.

[7] Optimism Team, "Optimistic Rollup: Scaling Ethereum's Layer 2," Optimism PBC, 2020.

[8] H. Jang and J. Kim, "Design of Blockchain-based Distributed Storage and Metadata for Ensuring Data Reliability," in Proc. Korea Information and Communications Society (KICS) Conference, pp. 24, Seoul, Korea, June 2022

[9] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in Proc. IEEE Symposium on Security and Privacy, pp. 459-474, San Jose, USA, May 2014. (https://doi.org/10.1109/SP.2014.36)

[10] M. Al-Bassam, A. Sonnino, and S. Bano, "Chainspace: A Sharded Smart Contracts Platform," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, USA, Feb. 2021.

[11] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Foundation, 2014. (https://doi.org/10.48550/arXiv.2202.01905)

[12] Z. Ye, U. Misra, J. Cheng, W. Zhou, and D. Song, "Specular: Towards secure, trust-minimized optimistic blockchain execution," in Proc. IEEE Symposium on Security and Privacy, San Francisco, USA, May 2024.

[13] C. Yu, N. Mei, C. Du, and H. Luo, "Blockchain Data Scalability and Retrieval Scheme Based on On-Chain Storage Medium for Internet of Things Data," Electronics, vol. 12, no. 6, pp. 1454, Mar. 2023. (https://doi.org/10.3390/electronics12061454)

[14] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in Proc. 27th USENIX Security Symposium, pp. 1353-1370, Baltimore, USA, Aug. 2018.

[15] J. Hao, Y. Sun, and H. Luo, "A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking," Journal of Computer, vol. 29, no. 6, pp. 158-167, 2018.

황 재 승 (JaeSeung Hwang)

2014년 2월 : 숭실대학교 산업정보시스템공학과 졸업
2017년 2월 : 숭실대학교 소프트웨어공학 석사
2021년 3월~현재 : 숭실대학교 IT 융합학과 박사과정

<관심분야> 블록체인, 클라우드 컴퓨팅
[ORCID: 0009-0000-7993-5914]

김 영 한 (YoungHan Kim)

한국통신학회 논문지 49권 8호, pp. 1183-1195, 8월 2024 참조

<관심분야>
[ORCID:]