블록체인 트랜잭션 데이터 분산 저장 기술 동향

Research Trends on Distributed Storage Technology for Blockchain Transaction Data

최병준 (B.J. Choi, bjchoi92@etri.re.kr) 스마트데이터연구실 연구원
김창수 (C.S. Kim, cskim7@etri.re.kr) 스마트데이터연구실 책임연구원
이명철 (M.C. Lee, mclee@etri.re.kr) 스마트데이터연구실 책임연구원

ABSTRACT

Recently, the blockchain technology, which can decentralize business ecosystems using secure transactions without trusted intermediaries, has been spotlighted. Full nodes play an important role in maintaining decentralization in that they independently verify transactions using their full historical transaction data. However, the storage requirement of a full node for storing historical data is continuously increasing, and thus, has become harder for users to run a full node due to the heavy price for storage costs. In this paper, we investigate research trends on reducing the costs of storing blockchain transaction data so that nodes with low storage requirements can be used in the blockchain network.

KEYWORDS 라이트 노드, 부호 이론, 분산 해시 테이블, 블록체인, 샤딩 기술, 이레이저 코드, 트랜잭션 데이터

Ⅰ. 서론

블록체인 기술은 P2P 기반의 분산 원장 기술로, 중앙 관리자 없이 사용자 간의 신뢰 있는 거래를 가능하게 한다. 이것이 가능한 이유는 블록체인 참여자들이 동일한 원장을 공유하고, 원장의 갱신 내역이 생길 때마다 참여자들이 합의 과정을 통해 원장을 최신 상태로 유지하기 때문이다. 모든 사용자가 최신 원장의 복제본을 보유하고 있으므로, 악의적인 사용자가 거래 내역을 임의로 수정하거나 누락시킬 수 없게 된다. 이러한 블록체인의 신뢰성과 투명성 덕분에 물류, 유통, 금융 등 다양한 산업에서 활용되고 있다.

하지만, 블록체인 시스템에서 모든 참여자가 원장의 복제본을 보유하고 있어야 하므로 각 참여자의 저장 부담이 크다는 문제가 있다. 2022년 1월 기준으로 비트코인 풀 노드의 크기가 380GB, 이더리움 풀 노드의 크기가 1TB를 넘는 등 일반적인 사용자가 블록체인 네트워크에 참여하기에는 저장 공간이 매우 많이 요구된다[1]. 더욱이, 시간이 지남에

* DOI: https://doi.org/10.22648/ETRI.2022.J.370309
* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임[No. 2021-0-00136, 다양한 산업 분야 활용성 증대를 위한 대규모/대용량 블록체인 데이터 고확장성 분산 저장 기술 개발].

따라 블록체인에 저장해야 할 트랜잭션 내역이 추가되면서 사용자의 저장 부담은 더욱 심해지고 있다. 더 높은 TPS(Transactions Per Second)를 지원하는 확장성이 높은 블록체인일수록 그에 비례하게 저장 부담 문제가 커진다.

원장 저장 부담으로 인해 거대 마이닝 풀(Mining Pool)이 블록체인 데이터의 저장 관리를 독점하여 오히려 탈중앙화를 훼손할 우려가 커지고 있어서, 완전한 탈중앙화를 위해서는 일반 사용자들도 블록체인 네트워크에 쉽게 참여할 수 있어야 한다. 이를 위해서는 사용자가 더 적은 저장 용량을 사용하며 블록체인 네트워크에 참여하기 위한 기술이 필수적이다. 이에 탈중앙성을 만족하며 트랜잭션 데이터의 저장 부담을 줄이는 분산 저장 기술이 요구되고 있는 상황으로, 본고에서는 트랜잭션 분산 저장 기술에 대한 동향을 조사하고 분석하여 앞으로의 발전 방향에 대하여 고찰해 보고자 한다.

본고의 구성은 다음과 같다. 먼저 Ⅱ장에서 저장 용량 문제를 해결하고자 하나 탈중앙성이 떨어지는 한계를 갖는 초기 단계의 트랜잭션 저장 경량화 기술에 대하여 간단히 살펴본다. Ⅲ장에서 저장 공간 효율성뿐만 아니라 탈중앙성 문제를 해결하고자 하는 다양한 트랜잭션 데이터 분산 저장 기술들의 동향을 알아본 후, Ⅳ장에서 결론을 맺는다.

Ⅱ. 트랜잭션 저장 경량화 기술

먼저, 블록체인 시스템에서 블록의 구조에 대해 살펴본다. 블록체인 종류에 따라 조금씩의 차이는 있으나 전체적으로 유사한 구조를 갖고 있으며, 그림 1과 같이 블록의 중요 정보를 담고 있는 블록 헤더(Block Header) 부분과 데이터가 저장된 블록 바디(Block Body) 부분으로 나뉜다.

일반적으로 블록 헤더가 차지하는 저장 용량은

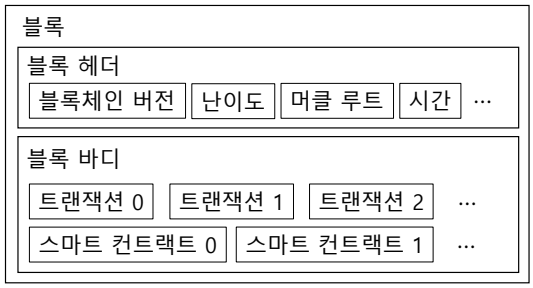

그림 1 블록체인의 블록 구조

전체 블록의 크기에 비하여 매우 적다. 예를 들어 비트코인의 블록 헤더에는 이전 블록의 해시값, 비트코인 버전, 머클 루트 해시(Merkle Root Hash), 채굴 난이도, 논스(Nonce) 등이 포함되어 있으며, 블록 헤더의 크기는 총 80바이트에 불과하다[2]. 반면 블록 바디는 개별 사용자들의 트랜잭션 내역을 담고 있고, 블록당 약 1MB의 크기를 갖고 있다.

1. 라이트 노드 기술

비트코인, 이더리움 등 많은 블록체인 플랫폼은 블록체인의 모든 블록 정보를 저장하는 풀 노드(Full Node) 이외에 블록 헤더의 정보만 저장하는 라이트 노드(Light Node)로 블록체인에 참여하는 방법을 제공한다[2,3]. 이 방식을 통해 스마트폰 등 저장 용량이 작은 모바일 기기에서도 블록체인에 참여할 수 있다. 비트코인 네트워크에서 각 노드가 블록 헤더만을 저장한다면 모든 트랜잭션을 저장하는 풀 노드 대비 저장 용량을 최소 10,000배 이상 절약할 수 있다.

라이트 노드는 노드가 보유하고 있지 않은 트랜잭션 내역을 다음과 같이 검증할 수 있다. 먼저, 풀 노드에게 해당 트랜잭션이 속한 블록과 경로 정보를 요청한다. 그 후, 풀 노드에게 받은 정보를 통해 블록의 머클 루트 해시값을 계산하여, 라이트 노드

의 블록 헤더에 저장된 머클 루트 해시값과 동일한지 여부로 트랜잭션의 타당성 여부를 검증한다. 이 검증 방식을 단순 지불 검증(SPV: Simplified Payment Verification)이라 한다[2]. 하지만 SPV 방식은 풀 노드의 정보에 의존하기 때문에 블록체인의 탈중앙성과는 거리가 먼 방식이다.

2. 트랜잭션 프루닝 기술

블록체인 노드의 저장 용량을 줄이기 위하여 오래된 트랜잭션을 삭제하고 최신 트랜잭션 내역만 저장하는 프루닝(Pruning) 방식을 이용할 수 있다[2]. 자주 사용되지 않는 트랜잭션들을 제거함으로써 상당한 수준의 저장 용량 절감 효과가 있다. 라이트 노드 기술과 마찬가지로, 삭제된 트랜잭션의 정보가 요구되는 상황에서 풀 노드의 정보에 의존한다는 단점이 있다.

스웨덴의 룰레오 대학 연구팀은 서로 상쇄되는 트랜잭션 등 추후 발생할 트랜잭션 검증에 필요하지 않은 트랜잭션을 선별하여 제거하는 선택적 트랜잭션 프루닝(Selective Transaction Pruning) 기술을 발명하였다[4]. 이 기술을 활용한 하이퍼레저 패브릭 블록체인 노드는 풀 노드 대비 약 15%의 저장 공간을 사용한다.

CoinPrune은 비트코인에 최적화된 트랜잭션 프루닝 기술로, 비트코인의 UTXOs(Unspent Transaction Outputs) set을 기반으로 쓸모없는 트랜잭션을 선별하여 프루닝한다[5]. 비트코인 네트워크에서 해당 기술을 적용한 노드는 풀 노드 대비 약 2%의 저장 공간을 사용한다.

로커스체인은 사용자가 일정 기간 이전의 트랜잭션 데이터를 프루닝할 때 데이터 위변조를 증명할 수 있는 데이터를 별도로 보관하여 사용자가 데이터 검증에 지장을 주지 않는 베리파이어블 프루닝(Verifiable Pruning) 기술을 개발하였다[5].

Ⅲ. 분산 트랜잭션 저장 기술

Ⅱ장에서 살펴본 트랜잭션 저장 경량화 기술은 일부 노드의 저장 요구량을 줄일 수는 있지만, 블록체인의 전체 트랜잭션 내역을 보유하는 풀 노드를 별도로 구성해야 한다는 단점이 존재한다. 필연적으로 블록체인 시스템은 더 많은 정보를 가지고 있는 풀 노드에 의존하기 때문에 저장 경량화 기술 방식은 블록체인의 핵심 특징 중 하나인 탈중앙성이 떨어진다. 따라서, 탈중앙성을 만족하며 저장 요구량을 줄이는 방식으로 트랜잭션 내역을 분산 저장하는 샤딩 기술, DHT 및 이레이저 코드 기반 기술이 연구되고 있다.

1. 샤딩 기술

샤딩 기술은 하나의 큰 네트워크를 샤드라 불리는 여러 개의 작은 네트워크로 나누어 병렬적으로 동작하게 함으로써, 분산 원장의 확장성을 높이는 솔루션으로 분산 데이터베이스 기술에서 널리 사용되는 역사가 깊은 기술이다. 블록체인 시스템도 다수의 노드가 참여하는 데이터베이스임에 착안하여, 블록체인 네트워크에서 샤딩 기술을 적용하여 확장성을 높이려는 연구가 진행되었다[6-12].

샤딩 방식을 적용하면 여러 노드가 블록체인 트랜잭션 데이터를 나누어 저장함으로써 각 노드의 필요 저장 공간을 줄일 수 있고, 각 샤드에 속한 노드들이 주로 정보를 주고받기 때문에 노드 간 통신 부담이 적어지며, 병렬적으로 거래 내역을 검증할 수 있어 초당 트랜잭션 처리 속도가 높아진다는 장점이 있다(그림 2 참조).

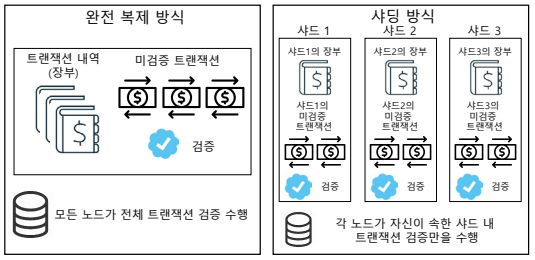

그림 2 완전 복제 방식과 샤딩 방식

가. 샤딩 기술 적용 블록체인 연구 동향

샤딩 기술을 활용하여 블록체인의 확장성을 높인 다양한 연구의 특징을 표 1과 같이 요약하였다. 샤딩 방식은 완전 복제 방식에 비하여 더 적은 노드가 합의에 참여하므로, 보안성을 위해 샤드 내 합의 알고리즘을 견고하게 설계하는 것이 요구된다. 또한, 여러 개의 샤드에 영향을 끼치는 크로스 샤드(Cross-Shard) 트랜잭션을 효율적으로 처리할 수 있어야 한다.

대부분의 선행 연구들은 샤드 내 합의 알고리즘으로 Byzantine Fault Tolerance(BFT) 기반의 프로토콜을 사용한다[6,8-12]. 악의적인 노드가 하나의 샤드를 망가뜨리기 위해 필요한 컴퓨팅 자원이 적어 전통적인 PoW(Proof of Work) 방식을 적용하기 어렵기 때문이다. Monoxide는 모든 샤드의 블록 내역을 저장하는 Merkle Patricia Trie(MPT) 구조를 도입하여 하나의 샤드를 특정하여 공격하기 어려운 PoW 기반 합의 알고리즘을 사용하였다[7]. RapidChain은 알고리즘을 최적화하여 결함 내성을 1/3에서 50%까지 상승시켰고[10], Ethereum 2.0은 BFT 프로토콜과 PoS(Proof of Stake)를 동시에 적용하여 더 높은 TPS를 달성하였다[11]. 또한 TEEChain은 신뢰 실행 환경(TEE: Trusted Execution Environment) 개념을 도입해 샤드 내 PBFT(Practical BFT) 합의 과정의 안정성을 높이는 방법을 제시하였다[12].

현재 샤딩 기술을 사용하는 많은 연구가 전체 장부의 잠금/해제(Lock/Unlock) 방식을 사용하여 크로스 샤드 트랜잭션을 처리한다[6-7,9-12]. 여기서, 잠금 방식은 샤드 리더가 크로스 샤드 트랜잭션에 대응하는 UTXOs의 모든 서명을 검증한 뒤, 정상 트랜잭션으로 인식하면 모든 샤드에서 해당 UTXOs의 사용을 중지하는 방식을 의미한다. 또한 해제 방식은 크로스 샤드 트랜잭션이 영향을 미치는 모든 샤드 내의 노드들이 해당 트랜잭션을 승인하였을

표 1 샤드 기반 트랜잭션 데이터 분산 저장 기술

사례	특징	샤드 내 기반 합의 알고리즘	크로스 샤드 트랜잭션
Locus Chain[6]	샤드를 주기적으로 재배치하여 노드가 부담하는 네트워크 부하를 줄이는 동적 샤딩(Dynamic Sharding) 기술 적용	BFT	lock/unlock
Monoxide[7]	샤드 내 합의 안정성을 위해 모든 샤드의 블록 내역을 저장하는 MPT 개념 도입	PoW	lock/unlock
Elastico[8]	샤드 내 합의 알고리즘으로 BFT 기반 알고리즘을 처음으로 사용	PBFT	고려하지 않음
OmniLedger[9]	Verifiable Random Function(VRF)을 사용하여 샤드를 나누는 기술 적용	BFT	lock/unlock
RapidChain[10]	악의적 노드에 대한 결함 내성을 50%까지 상승	BFT	lock/unlock
Ethereum 2.0[11]	BFT와 PoS 합의 알고리즘을 동시에 사용하여 더 높은 TPS 달성	BFT, PoS	lock/unlock
TEEChain[12]	신뢰 실행 환경(Trusted Execution Environment)을 도입하여 PBFT 합의 과정의 안정성을 높임	PBFT	2-phase lock/unlock

출처 Reproduced from [6-12].

때, UTXOs를 업데이트한 후 사용을 가능하게 하는 방식을 의미한다. 특히 TEEChain은 2단계 잠금/해제 방식을 사용하여 다른 방식보다 크로스 샤드 트랜잭션 처리 성능이 우수하다[12].

나. 샤딩 기술의 한계점

샤딩이 블록체인의 확장성을 높일 수 있지만, 그 대가로 보안성이 떨어진다는 분명한 단점이 있다. 모든 노드가 전체 장부를 가지고 있는 완전 복제 방식에서는 최대 49%의 노드가 악의적일 때도 블록체인의 무결성을 보장할 수 있지만, 샤딩 방식을 사용하면 한 샤드에 속한 노드의 절반 이상만 악의적이어도 블록체인의 무결성을 보장할 수 없다.

보안성을 유지하기 위하여, 특정 주기마다 노드를 샤드에 배정할 때, 샤드 내의 리더를 선출할 때, 여러 개의 샤드에 영향을 끼치는 트랜잭션을 담당하는 샤드를 정할 때 무작위로 노드를 설정하여 외부 공격에 강인하게 시스템을 설계하는 방법이 고려되고 있다[6-12]. 그러나, 노드 재설정 직후에 특정 샤드에 집중하여 공격이 가능한 강력한 공격자에 대해서 여전히 보안성이 떨어지는 문제점이 있다. 덧붙여서, 샤드 재할당 시 많은 통신 부담이 생겨 네트워크가 지연될 수 있다는 문제점도 존재한다.

2. DHT 기반 기술

DHT[1](Distributed Hash Table)는 P2P(Peer-to-Peer) 네트워크상의 노드 간에 O(log n) 시간에 통신할 수 있도록 노드 및 데이터를 분산하여 저장하고 관리하는 기술이며, 일관된 해싱(Consistent Hashing)을 통해 노드 가입/탈퇴가 자유로운 환경에서 확장성이 좋고, 빠른 검색을 지원하기 때문에 분산 노드 관리 시스템 또는 분산 KVS(Key-Value Store)를 구현하는 데 흔히 활용된다.

DHT의 특성을 활용하여 블록체인 노드의 트랜잭션 데이터 중복 저장 부하를 여러 노드에 분산하고자 하는 일부 연구들이(DHT Clustering, LightChain, Karakasa, VBG 등) 진행되었다(표 2 참조).

DHT 기반 트랜잭션 데이터 분산 저장 기술들은 대체로 설계 및 저장 확장성 등에 대한 시뮬레이션

1) DHT를 구현하는 다양한 프로토콜(Kademlia, Chord, Pastry 등)들은 네트워크컴퓨터 상의 노드/데이터를 빠르게 접근하기 위한 고유한 노드 관리 구조(XOR, 링, 트리 등), 룩업 테이블, 그리고 라우팅 테이블을 유지한다.

표 2 DHT 기반 트랜잭션 데이터 분산 저장 기술

사례	특징	기반 DHT	한계점
DHT Clustering[13]	• 비트코인과 같은 PoW 합의 환경에 DHT 적용 • 메시지 전송 성능 평가	Kademlia	시뮬레이션만 수행
LightChain[14]	• IoT 등 자원이 제약적인 환경에 적용 • 공평한 블록 생성 기회 제공 • 통신/스토리지 성능 평가	Skip Graph	시뮬레이션만 수행
Karakasa[15]	• 비트코인 노드 부하 분산 • 스토리지 확장성, 메시지 부하 등 성능 평가	Chord	시뮬레이션만 수행
VBG[16]	• 연속된 블록 그룹 단위 분산 저장 • 프로토타입 구현 • 시뮬레이션 기반 성능 평가	Chord	BFT 보장 검증 필요

출처 Reproduced from [13-16].

단계까지만 수행되었고, 일부 구현까지 진행된 바가 있다. 하지만 트랜잭션 데이터의 분산 저장에도 여전히 비잔틴 장애 내성을 만족해야 하는데, 이에 대한 검증이 부족하여 향후 관련 연구가 필요한 상황이다.

가. DHT Clustering

일본 도쿄도립대학 연구팀은 비트코인과 같은 PoW 합의를 지원하는 블록체인 네트워크에서 모든 참여 노드를 구조가 없는 순수 P2P 네트워크의 마이너 노드와 트리 구조를 갖는 DHT 네트워크의 데이터 노드로 분리하여 데이터를 분산 저장하는 방법으로 DHT Clustering을 제안하였다[13].

트랜잭션이 발생되면 트랜잭션 풀에 수집되고, 마이너 노드들은 트랜잭션 풀의 트랜잭션들을 모아서 경쟁적으로 PoW를 수행하여 블록을 생성한다. 블록을 생성한 마이너 노드는 Kademlia 알고리즘을 적용하여 블록 해시의 prefix로부터 새로 생성된 블록을 저장할 데이터 노드 클러스터를 선정하고, 블록을 할당하게 된다.

DHT 클러스터 기술은 네트워크 부하, 저장 비용, 전파 지연 등의 관점에서 블록체인 네트워크의 확장성을 해결하는 방법으로서 DHT 활용을 제안하였다.

나. LightChain

터키 코치(Koc) 대학 연구팀은 IoT(Internet of Things)와 같이 컴퓨팅/저장 자원이 제한적인 노드 환경에서도 통신/스토리지 효율적으로 블록체인 네트워크를 운영하고 참여할 수 있도록 경량 참여 노드들로 구현된 DHT상에 블록 및 트랜잭션 데이터를 분산 저장하는 방법, 그리고 공평한 블록 생성 기회를 갖도록 PoV(Proof of Validation) 합의 기술을 포함하는 LightChain 기술을 제안하였다[14].

LightChain은 Skip Graph 방식의 DHT를 참여 노드상에 정의하였으며, 성능 평가 시뮬레이션을 수행하여 기존 중복 저장 방법 대비 저장 공간 66배, 부트스트래핑 380배의 향상을 예측하였다.

다. Karakasa

일본 게이오대학 연구팀은 비트코인 네트워크에서 각 노드의 독립성을 유지하면서 저장 용량을 줄이기 위해 Chord 방식의 DHT를 이용한 저장 부하 분산 방식인 Karakasa를 제안하였다[15].

Karakasa는 비트코인에서 실제 블록 데이터를 갖는 "BlockStorage"와 UTXO를 갖는 "ChainState" 중에서 BlockStorage를 DHT에 분산 저장한다. 일반적으로 새로운 트랜잭션이 발생하면, 각 노드의 메모리에 구축된 UTXOSet으로 검증하고, 만일 검증 시에 충돌이 발생하면 DHT에 관리되는 원본 블록을 검색하여 충돌 문제를 해결한다.

라. VBG(Virtual Block Group)

중국과학원 연구팀은 블록체인에서 연속되는 블록들을 가상의 그룹으로 묶고, 그룹 단위로 노드에 분산 저장하여, 각 노드가 일부 블록 데이터만을 저장하게 하는 방식으로 노드의 저장 부담을 줄이는 온체인 블록체인 저장 확장 모델인 VBG(Virtual Block Group) 기술을 제안하였다[16].

VBG에서 연속되는 블록들을 하나의 VBG 그룹으로 묶어서 VBG의 블록 데이터를 일부 노드에만 저장하고, 인센티브 메커니즘과 블록 데이터의 저장 검증 및 감사 메커니즘을 통해 신뢰성을 보장한다.

블록 그룹이 어느 노드에 저장되었는지를 나타내는 VBG 저장 인덱스를 DHT에 관리하여 블록체인 플랫폼의 합의 메커니즘이나 네트워크 토폴로지를 변경하지 않고도 블록 데이터의 질의 효율성을 향상하는 방법을 제안하였다.

3. 이레이저 코드 기반 기술

블록체인은 다수의 노드가 동일한 트랜잭션 내역을 저장하는 복제 기반의 분산 저장 시스템이라고 볼 수 있다. 분산 저장 시스템에서 이레이저 코드(Erasure Code)를 사용하면 데이터의 신뢰도를 유지하면서 기존 복제 방식 대비 크게 노드 저장 부담을 줄일 수 있는데, 이에 착안하여 블록체인에 부호화 기술을 사용하여 스토리지 요구량을 줄이려는 연구가 진행되고 있다.

이 절에서는 먼저 이레이저 코드의 개념에 대해 알아보고, 기존 분산 저장 시스템에서 이레이저 코드를 사용하여 저장 효율을 높인 방법을 살펴본다. 마지막으로 블록체인에 이레이저 코드를 적용한 연구 동향을 살펴본다.

가. 이레이저 코드

이레이저 코드는 원본 데이터에 수학적 구조를 가진 패리티(Parity)를 추가하여 데이터 일부가 손실(Erasure)되는 상황에서 원본 데이터를 복구할 수 있도록 설계된 부호이다. 구체적으로, (n,k) 이레이저 코드는 k개의 메시지 심볼을 가진 원본 데이터를 활용하여 $n(>k)$개의 부호화 심볼을 구성한다. 여기서 부호화 심볼을 만드는 과정을 인코딩(Encoding)이라 하고, 메시지 심볼을 복구하는 과정을 디코딩(Decoding)이라 한다. 또, 메시지 심볼과 부호화 심볼의 비율 $r=k/n$을 부호율(Code Rate)이라 한다.

1) 체계적 부호

인코딩 방식에 따라 원본 데이터 전체가 부호화된 데이터에 변형 없이 포함될 수 있는데, 이러한 성질을 만족하는 이레이저 코드를 체계적 부호(Systematic Code)라고 한다. 체계적 부호를 사용하면 디코딩 과정 없이 원본 데이터 일부에 직접적으로 접근할 수 있다는 장점이 있다.

2) MDS 부호

이레이저 코드 중 인코딩된 데이터가 이론적 최대치의 데이터 소실을 견딜 수 있는 부호를 MDS 부호(Maximum Distance Separable Code)라 한다. (n,k) MDS 부호를 활용하면 n개의 부호화 심볼 중 임의의 k개의 심볼을 통해서 원본 메시지 심볼을 복구할 수 있다.

3) 고정 부호율/무율 부호

고정 부호율 부호(Fixed-Rate Code)는 메시지와 부호화 심볼의 수가 고정된 부호로써, 메시지 심볼을 고정된 개수의 부호화 심볼로 인코딩하는 부호이다. 반면 무율 부호(Rateless Code)는 주어진 개수의 메시지 심볼로 부호화 심볼을 무한히 만들어낼 수 있는 부호이다.

그림 3은 (3,2) 체계적 MDS 부호를 사용하여 메시지 심볼 A, B를 인코딩하는 과정과 부호화 심볼 중 일부가 손실되었을 때, 메시지 심볼을 디코딩하는 과정을 보여준다. 부호화 심볼 A의 정보가 소실되더라도 남아 있는 심볼 B, A+B의 차를 계산하여 메시지 심볼 A를 복구할 수 있게 된다. 이 부호는 메시지 심볼 전체가 변형 없이 부호화 심볼에 포함되므로 체계적 부호이고, 임의의 2개의 부호화 심볼을 통해서 메시지 심볼 전체를 복구할 수 있으므로 MDS 부호임을 알 수 있다. 또한 n, k값이 사전에 결

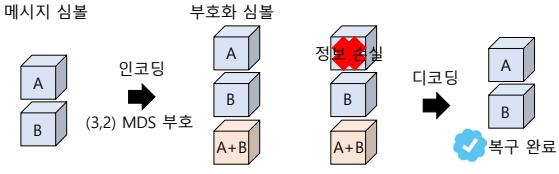

그림 3 (3,2) 체계적 MDS 부호

정되어 있으므로 고정 부호율 부호이다.

4) 수식적 표현

이레이저 코드의 인코딩 과정을 다음과 같은 행렬의 곱 형태로 표현할 수 있다.

$$\mathbf{m}G = \mathbf{c}$$

여기서 $\mathbf{m}$은 k개의 메시지 심볼로 구성된 $1 \times k$ 크기의 메시지 벡터를 의미하고, $\mathbf{c}$는 n개의 부호화 심볼로 구성된 $1 \times n$ 크기의 부호화 벡터를 나타낸다. $k \times n$ 크기의 행렬 G는 메시지 벡터를 부호화 벡터로 변환해 주는 기능을 하며, 생성 행렬(Generator Matrix)이라 부른다. 그림 3의 부호화 과정을 행렬 곱 과정으로 나타내면 다음과 같다.

$$\mathbf{m}G = [\mathrm{A\ B}]\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix} = [\mathrm{A\ B\ A{+}B}] = \mathbf{c}$$

나. 분산 저장 시스템의 적용

분산 저장 시스템은 대용량의 데이터를 다수의 저장 디스크들을 활용하여 신뢰성 있게 저장하고 읽을 수 있게 하는 시스템이다. 하지만 분산 저장 시스템에 종종 사용되는 개별 저장 디스크들은 일반적으로 신뢰성이 떨어져서 원하는 시기에 저장된 데이터를 읽지 못할 수 있다.

1) 복제 방식

Hadoop 등 초기 대용량 데이터 저장소를 활용하는 기업들은 개별 디스크의 신뢰성이 떨어지는 문제를 해결하고자 초기 단계에 여러 개의 저장 디스크에 정보를 복제하여 저장하는 방식(예를 들어, Hadoop Distributed File System은 같은 데이터를 3번 복제하여 저장하는 방식을 사용함[17])을 사용하였다. 하지만 복제 방식은 같은 데이터를 중복하여 저장함으로써 많은 저장 오버헤드가 발생한다는 단점이 있다.

표 3 복제 방식과 소거 부호 기반 방식의 장단점

접근방법	장점	단점
복제 방식	저장 노드에 결함이 생겼을 때, 복구 과정에 적은 통신이 필요	저장 효율성이 낮음
이레이저 코드 기반 방식	저장 효율성이 높음	저장 노드에 결함이 생겼을 때, 복구 과정에 많은 통신이 필요

2) 이레이저 코드 기반 방식

복제 방식의 저장 부담 문제를 해결하기 위하여, 현재 Google, Facebook 등 다수 기업이 이레이저 코드를 분산 저장 시스템에 활용하고 있다[18,19]. 예를 들어, Facebook은 원본 데이터를 (14,10) RS 부호를 사용하여 인코딩하고, 부호화된 데이터를 14개의 노드에 분산 저장하는데, 원본 데이터 대비 저장 공간을 1.4배 활용하면서 최대 4개의 노드 결함에 내성을 갖게 데이터를 분산 저장할 수 있다[19].

하지만, 이레이저 코드를 적용하면 노드에 결함이 생겼을 때 많은 대역폭 자원이 필요하다는 단점이 있다. 분산 저장 시스템은 개별 저장 디스크에 결함이 생겼을 때 기존 디스크에 저장된 정보를 복구하는 과정이 요구되는데, 이레이저 코드는 다수의 노드에 저장된 부호화 데이터를 받아와 소실된 데이터를 복구해야 한다. 예를 들어, (14,10) RS 부호를 사용하면 결함이 있는 노드의 데이터를 복구하고자 기존 복제 방식 대비 10배의 통신 대역폭이 요구된다. 분산 저장 시스템에서 복제 방식과 이레이저 코드 기반 방식의 장단점은 표 3과 같이 정리할 수 있다.

다. 블록체인 시스템의 적용

일반적으로 블록체인에서 그림 4와 같은 방법으로 이레이저 코드를 적용한다[20,21]. 먼저 포크(Fork)가 생길 확률이 매우 낮은 과거의 트랜잭션 블

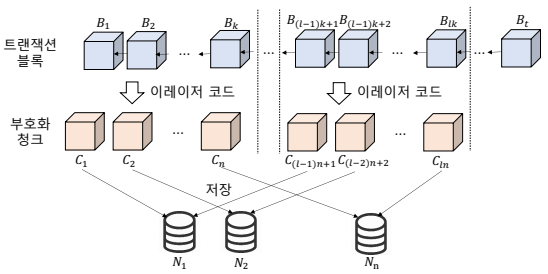

그림 4 이레이저 코드가 적용된 블록체인

록들을 k개 단위의 그룹으로 묶은 뒤, 각 그룹마다 이레이저 코드를 사용하여 인코딩 과정을 거친다. 그 후, 각 노드는 생성된 부호화 청크 중 일부만 저장한다. 이 방식을 통하여 각 노드가 저장할 데이터의 크기를 줄일 수 있다.

1) 이레이저 코드 적용 시 장단점

이레이저 코드를 활용하면, 자신과 동등한 역할을 하는 여러 노드를 활용하여 트랜잭션 검증을 진행할 수 있어서 블록체인의 탈중앙화 특성이 유지된다. 또한 이레이저 코드 기반 방식은 샤딩 방식과 비교하여 명확히 네트워크가 나뉘어 있지 않아 공격자가 블록체인을 공격하기 위해 더 많은 자원이 요구된다. 따라서, 블록체인의 보안성을 유지하는 데 유리하다.

반면, 트랜잭션 데이터에 이레이저 코드를 적용하여 다수의 노드에 분산 저장하면 전체 트랜잭션 내역을 복구할 필요가 있을 때 다수의 노드로부터 부호화 청크를 전송받아야 하고, 디코딩 과정이 필요할 수 있다. 여기서 많은 통신과 컴퓨팅 자원이 요구된다는 문제점이 있다.

2) 블록체인 활용 부호 종류 및 특징

표 4[22-27]와 같이, 블록체인의 트랜잭션 데이터를 분산 저장할 때 다양한 종류의 이레이저 코드를 적용할 수 있다. 사용되는 부호의 종류에 따라 블록체인 시스템 구축 시 세부적인 특징이 달라진다.

Reed-Solomon(RS) 부호는 MDS 부호의 한 종류

표 4 블록체인에 적용된 이레이저 코드의 종류 및 특징

이레이저 코드 종류	특징	고정 부호율/ 무율 부호 여부
Reed-Solomon(RS) 부호[22,23]	디코딩 과정에 필요한 노드의 수를 최소화하는 부호	고정 부호율 부호
Replication 부호[22]	디코딩 과정 없이 메시지 블록의 정보를 복구할 수 있는 부호	고정 부호율 부호
Luby Transform(LT) 부호[24]	새로운 노드가 블록체인 네트워크에 참여했을 때, 기존 노드에 저장된 부호화 청크를 재설정하지 않아도 되는 부호	무율 부호
Low-Density Parity Check(LDPC) 부호[25]	디코딩 과정에 필요한 노드의 계산 부담을 줄이는 부호	고정 부호율 부호
Raptor 부호[26]	블록체인 네트워크에 노드가 추가되는 상황에서 기존 노드에 저장된 부호화 청크를 재설정하지 않으면서, 디코딩 과정에 필요한 노드의 계산 부담을 줄이는 부호	무율 부호
PARE(Pattern Aware Redundancy for Erasure) 부호[27]	블록체인 노드가 소실되는 패턴이 반복적으로 일어난다는 사실에 착안하여, 노드가 해당 패턴에 최적화된 저장 용량을 가질 수 있게 하는 부호	고정 부호율 부호

출처 Reproduced from [22-27].

로써 최소한의 부호화 청크를 통해 원본 트랜잭션 내역 복구가 가능하다는 특징이 있다[22,23]. 화둥사범대학 연구팀은 체계적 RS 부호를 사용하여 트랜잭션 내역을 인코딩하고, 인코딩된 부호화 청크들을 복제하여 다수의 노드에 배치하는 방식을 제안하였다[22]. 이 방식을 사용하면 분할된 원본 트랜잭션 데이터가 복제되어 노드에 배포되기 때문에, 높은 확률로 디코딩을 하지 않고 트랜잭션 내역 전체를 복구할 수 있다. 하지만, RS 부호는 고정된 개수의 부호화 청크만을 만들 수 있는 고정 부호율 부호여서, 새로운 노드가 블록체인 시스템에 참여할 때마다 새롭게 인코딩을 진행하여야 한다는 단점이 있다.

Luby Transform(LT) 부호[28]는 무율 부호로, 주어진 개수의 트랜잭션 블록을 임의 개수의 부호화 청크로 인코딩할 수 있다. 따라서, 블록체인 노드가 추가될 때 재인코딩 없이 새로운 노드에 저장할 수 있는 부호화 청크를 생성할 수 있다. 재인코딩을 하면 상당한 통신 및 연산 자원이 소모되기 때문에, 재인코딩이 필요 없는 LT 부호를 사용하면 블록체인 노드 수가 자주 변경되는 상황에서도 자원 효율적으로 시스템을 구축할 수 있다[24].

Low-density parity check(LDPC) 부호는 디코딩 과정에 필요한 연산량이 적다는 특징이 있는데, LDPC 부호를 트랜잭션 저장에 활용하여 빠르게 디코딩이 가능한 트랜잭션 분산 저장 방식이 설계되었다[25].

Raptor 부호는 LT 부호와 LDPC 부호를 연접한 부호이며[29], 이를 블록체인에 활용한다면 노드가 추가될 때 재인코딩이 필요 없는 무율 부호의 장점과 디코딩 과정에서 필요한 연산량이 적은 LDPC 부호의 장점을 모두 갖게 시스템을 설계할 수 있다[26].

미국 캘리포니아 대학 연구팀은 블록체인 노드가 소실되는 패턴을 분석하여, 각 노드가 패턴에 최적화된 스토리지 용량을 갖게 설계하는 부호인 Pattern Aware Redundancy for Erasure(PARE)를 제안하였다[27].

3) 이레이저 코드 활용 설계 시 고려사항

먼저, 새로운 블록에 포함된 트랜잭션을 부호화 블록을 보유하고 있는 노드가 효율적으로 검증할 수 있게 하는 방법이 필요하다. 이레이저 코드를 사용하면 다수의 노드에 저장된 정보를 전송받아 트랜잭션 내역을 복구한 후 트랜잭션 검증 절차를 거치는데, 이 과정에서 대역폭 자원과 컴퓨팅 자원이 많이 요구되어, 해당 시간에 블록체인 시스템이 안정적으로 동작하지 못할 수 있다. 이를 해결하기 위하여 원본 트랜잭션 데이터를 빠르게 얻기 위해 선택적으로 노드를 골라 부호화 청크를 전송받는 방법 등을 이용할 수 있다[25].

둘째로, 실제 블록체인의 트랜잭션 블록의 크기가 일정하지 않은 점도 고려할 필요가 있다. 이레이저 코드를 적용하기 위해 블록의 사이즈를 같게 만들어 주는 과정을 거쳐야 하는데, 사이즈가 작은 트랜잭션 블록에 0을 추가하는 제로 패딩(Zero-Padding)이나, 트랜잭션 블록 여러 개를 묶어서 비슷한 크기의 슈퍼블록을 만드는 방법 등을 사용할 수 있다[24].

마지막으로, 악의적인 비잔틴(Byzantine) 노드가 잘못된 정보를 전송할 때 정직한 노드가 이를 인지하는 방법을 고안해야 한다. 디코딩 과정에서 노드가 악의적으로 변형된 부호화 청크를 전송하는 것을 막기 위하여, 화둥사범대학 연구팀은 각 노드가 저장해야 할 부호화 청크 외의 나머지 청크에 대해서 해시값을 별도로 저장해 두는 방식을 제안하였다[22]. 이 방식을 통해 다른 노드가 전송해 온 부호화 청크의 해시값과 노드가 원래 저장하고 있던 해

시값을 비교하여 부호화 청크가 변조되었는지 쉽게 확인할 수 있게 된다. 또한 기존 블록체인의 블록 헤더의 정보를 이용하여, 디코딩 과정에서 잘못된 청크를 전송한 노드를 구별하는 방법이 사용될 수 있다[24].

Ⅳ. 결론

블록체인은 외부 기관의 개입 없이 거래 당사자 간의 신뢰 있는 거래를 가능하게 하는 파급력이 큰 기술이다. 본고에서는 개별 노드가 탈중앙성을 만족하며 적은 용량으로 블록체인 시스템에 참여하기 위한 트랜잭션 분산 저장 기술 동향에 대해 살펴보았다.

"어떠한 블록체인 시스템도 탈중앙성(Decentralization), 보안(Security), 확장성(Scalability) 모두를 만족할 수 없다."라는 잘 알려진 블록체인 트릴레마(Trilemma)가 있다[30]. 먼저 트랜잭션 내역을 저장하지 않고 다른 풀 노드에 의존하여 트랜잭션 검증을 수행하는 라이트 노드 기반의 방식은 탈중앙성이 떨어진다는 단점을 갖고 있었다. 트랜잭션을 분산 저장하는 샤딩과 DHT 기반 기술은 탈중앙성은 만족하지만, 일부 노드에만 트랜잭션 내역이 저장되면서 외부 공격에 취약하다는 문제점이 존재하였다. 세 가지 성질을 동시에 만족할 수 있는 솔루션으로 이레이저 코드를 활용하는 방식이 주목받고 있는데, 트랜잭션 내역을 복구하는 데 통신 및 계산 자원이 타 방식보다 많이 요구된다는 한계점이 있지만, 저장 공간 효율성이나 비잔틴 공격에 강한 특성으로 인해 이를 보완하기 위한 연구들이 활발히 진행되고 있다.

대규모 트랜잭션 데이터를 블록체인 노드에 효율적으로 저장하고 관리하는 기술은 가용성, 무결성, 소유권 보장이 요구되는 데이터를 다루는 다양한 산업에서 중추적으로 활용할 수 있는 사업화 가능성이 매우 높은 기술이니만큼, 핵심적인 기술 확보를 통해 산업 전반의 경쟁력을 확보하는 것이 중요하리라 여겨진다.

용어해설

Consistent Hashing 분산 데이터 관리 시스템에서 노드 가입/탈퇴가 빈번하게 발생하더라도 기존 데이터 분산 방법이 변경되지 않는 해싱 기술

Erasure Code 부호화 심볼 중 일부가 손실되는 상황에서 전체 메시지 심볼 복구가 가능하도록 하는 부호

Simple Payment Verification 모든 블록체인 거래 내역을 활용하지 않으면서 트랜잭션을 간편히 검증하는 방법

약어 정리

BFT	Byzantine Fault Tolerance
DHT	Distributed Hash Table
IoT	Internet of Things
KVS	Key-Value Store
LDPC	Low-Density Parity Check
MDS	Maximum Distance Separable
MPT	Merkle Patricia Trie
P2P	Peer-to-Peer
PoV	Proof of Validation
PoW	Proof of Work
SPV	Simple Payment Verification
TPS	Transaction Per Second
UTXO	Unspent Transaction Output

참고문헌

[1] BitInfoCharts, "Cryptocurrency statistics," Available from: https://bitinfocharts.com/

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Bus. Rev., 2008.

[3] E. Developer Team, "Electrum," 2017, Available from: electrum.org

[4] E. Palm et al., "Selective blockchain transaction pruning and state derivability," in Proc. IEEE Crypto Vall. Conf. Blockchain Technol. (CVCBT), (Zug, Switzerland), June 2018.

[5] R. Matzutt et al., "CoinPrune: Shrinking bitcoin's block-

chain retrospectively," IEEE Trans. Netw. Service Manag., vol. 18, no. 3, 2021.

[6] Locuschain, "Locus chain technical whitepaper," Nov. 2019, Available form: https://www.locuschain.com/upload/file/20211118_113627_445.pdf

[7] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in Proc. USENIX Symp. Networked Syst. Des. Implementation (NSDI), (Boston, MA, USA), Feb. 2019, pp. 95–112.

[8] L. Luu et al., "A secure sharding protocol for open blockchains," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., (Vienna, Austria), Oct. 2016.

[9] E. Kokoris-Kogias et al., "Omniledger: A secure, scale-out, decentralized ledger via sharding," in Proc. IEEE Symp. Secur. Priv. (S&P), (San Francisco, CA, USA), May 2018.

[10] M. Zamani et al., "RapidChain: Scaling blockchain via full sharding," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., (Toronto, Canada), Oct. 2018, pp. 931–948.

[11] V. Buterin, "Ethereum: Platform review," Opportunities and Challenges for Private and Consortium Blockchains, 2016.

[12] H. Dang et al., "Towards scaling blockchain systems via sharding," in Proc. Int. Conf. Manag. Data, (Amsterdam, Netherlands), June 2019, pp. 123–140.

[13] Y. Kaneko et al., "DHT clustering for load balancing considering blockchain data size," in Proc. Int. Symp. Comput. Netw. Workshops, (Takayama, Japan), Nov. 2018, pp. 71–74.

[14] Y. Hassanzadeh-Nazarabadi et al., "LightChain: A DHT-based blockchain for resource constrained environments," arXiv preprint, CoRR, 2019, arXiv: 1904.00375.

[15] R. Abe et al., "Blockchain storage load balancing among DHT clustered nodes," arXiv preprint, CoRR, 2019, arXiv: 1902.02174.

[16] B. Yu et al., "Virtual block group: A scalable blockchain model with partial node storage and distributed hash table," Comput. J., vol. 63, no. 10, 2020, pp. 1524–1536.

[17] D. Ford et al., "Availability in globally distributed storage systems," in Proc. USENIX Symp. Oper. Syst. Des. Implementation (OSDI), (Vancouver, Canada), Oct. 2010, pp. 61–74.

[18] C. Huang et al., "Erasure coding in windows azure storage," in Proc. USENIX Annu. Tech. Conf., (Boston, MA, USA), June 2012, pp. 2–12.

[19] K.V. Rashmi et al., "A solution to the network challenges of data recovery in erasure-coded distributed storage systems: A study on the Facebook warehouse cluster," in Proc. USENIX Workshop Hot Topics Storage File Syst. (HotStorage), (San Jose, CA, USA), June 2013, pp. 1–5.

[20] M. Dai et al., "A low storage room requirement framework for distributed ledger in blockchain," IEEE Access, vol. 6, 2018, pp. 22970–22975.

[21] D. Perard et al., "Erasure code-based low storage blockchain node," in Proc. IEEE Int. Conf. Internet Things (iThings) & IEEE Green Comput. Commun. (GreenCom) & IEEE Cyber, Phys. Soc. Comput. (CPSCom) & IEEE Smart Data (SmartData), (Halifax, Canada), July 2018.

[22] X. Qi et al., "BFT-store: Storage partition for permissioned blockchain via erasure coding," in Proc. IEEE Int. Conf. Data Eng. (ICDE), (Dallas, TX, USA), Apr. 2020.

[23] S. Li et al., "Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously," IEEE Trans. Inf. Forensics Secur., vol. 16, 2020, pp. 249–261.

[24] S. Kadhe, J. Chung, and K. Ramchandran, "Sef: A secure fountain architecture for slashing storage costs in blockchains," arXiv preprint, CoRR, 2019, arXiv: 1906.12140.

[25] H. Wu et al., "Distributed error correction coding scheme for low storage blockchain systems," IEEE Internet Things J., vol. 7, no. 8, 2020, pp. 7054–7071.

[26] A. Tiwari and V. Lalitha, "Secure raptor encoder and decoder for low storage blockchain," in Proc. Int. Conf. Commun. Sys. Netw. (COMSNETS), (Bangalore, India), Jan. 2021.

[27] D. Mitra and L. Dolecek, "Patterned erasure correcting codes for low storage-overhead blockchain systems," in Proc. Asilomar Conf. Signals, Syst., Comput., (Pacific Grove, CA, USA), Nov. 2019.

[28] M. Luby, "LT codes," in Proc. Ann. IEEE Symp. Found. Comput. Sci., (Vancouver, Canada), Nov. 2002.

[29] A. Shokrollahi, "Raptor codes," IEEE Trans. Inf. Theory, vol. 52, no. 6, 2006, pp. 2551–2567.

[30] T. Ometoruwa, "Solving the blockchain trilemma: Decentralization, security & scalability," May 2018, Available from: https://www.coinbureau.com/analysis/solving-blockchain-trillemma