# 오픈소스 블록체인 환경에서 리드 솔로몬 부호화 된 블록의 복구 성능 평가

이성현 [1], 이명철 [2]
[1] 인제대학교 컴퓨터공학과 학부생
[2] 한국전자통신연구원 스마트데이터연구실 책임연구원

slee000220@oasis.inje.ac.kr, mclee@etri.re.kr

# Performance Evaluation of Reed-Solomon Encoded Block Recovery in Open Source Blockchain Environments

Seong-Hyeon Lee[1], Myungcheol Lee[2]
[1]Dept. of Computer Engineering, Inje University
[2]Smart Data Research Section, ETRI

**요 약**

블록체인 원장의 용량이 폭증하면서 여러 확장성 문제들이 나타나고 있다. 이에 대한 해결 방법으로 원장에 Reed-Solomon 부호화를 적용하여 용량을 줄이려는 연구가 일부 진행 중이나, 피어에 장애가 발생하거나 악의적 행동이 있다면, 데이터 손실을 막기 위한 복구 과정이 필수적이다. 본 논문에서는 원장에 Reed-Solomon 부호화를 적용해 얻는 저장 공간의 감소 효과에 비해서 데이터를 복구할 시 어느 정도의 오버헤드가 발생하는지 성능 평가를 수행했다. 결과적으로, 많은 블록 복구가 필요한 상황에서 인코딩/디코딩 시간은 미미하였고, 대부분의 오버헤드는 청크 재전송 시간이었다.

## 1. 서론

비트코인 풀 노드의 원장 크기가 2022 년 1 월 380GB 에서 2023 년 9 월 491GB 로 2 년 반 만에 약 30% 증가하였고[1], 블록체인이 다양한 응용 분야에서 활용되기 시작하면 더 폭증할 것으로 예상된다.

블록체인 원장의 용량이 급증하면서, 블록체인 네트워크가 소수 마이닝 풀로 구성되는 중앙화의 위험성 문제가 제기되고 있고, 블록의 합의/저장 처리 속도 저하로 인해 트랜잭션의 검증 속도 또한 저하되는 등 많은 확장성 문제를 초래하는 블록체인 트릴레마 문제를 겪고 있다.[2]

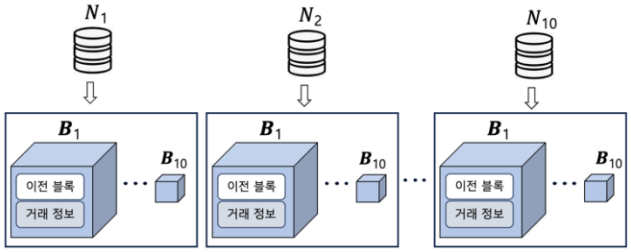
한편, Reed-Solomon (RS)은 통신 분야에서 먼저 사용되었으나, 최근 스토리지 시스템에서 가용성을 보장하면서 저장 공간을 줄일 수 있는 기술로서 관심을 받고 있다.

최근 블록체인 분야에서는 물리적 장애 또는 비잔틴 장애에 의해 발생하는 데이터 손실 오류를 RS 부호화를 적용하여 원장의 용량은 크게 줄이면서, 비잔틴 장애 내성 (BFT: Byzantine Fault Tolerance)을 가지도록 하는 연구를 수행하고 있다.[3]

본 논문에서는 이러한 연구에서 피어 장애 또는 사용자 요구에 의해서 발생하는 RS 부호화된 데이터의 복구 오버헤드를 성능 평가하는 연구를 수행하였다.

## 2. 본론

본 논문의 기반 시스템인 오픈소스 퍼블릭 블록체인 시스템[4]이 가정하는 블록체인은 그림 1 과 같이 모든 참여 노드들이 같은 원장을 가지도록 구성되어, 트랜잭션이 발생해 블록이 생성된다면 같은 블록을 노드들이 중복 저장해 저장 공간 낭비가 크다.




(그림 1) 블록체인 네트워크 원장 중복 저장 구조

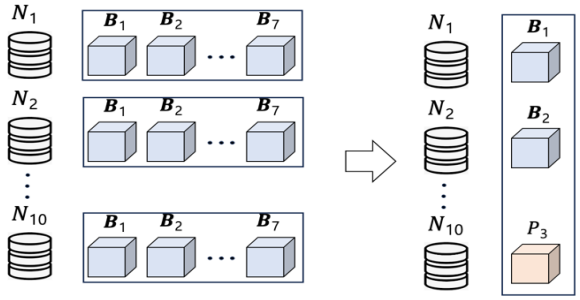
본 논문에서는 기반 시스템의 원장에 Reed-Solomon 부호화를 적용하여 피어 및 비잔틴 장애에 의해 발생하는 데이터 손실 오류를 방지하면서 저장 용량을 줄이도록 하였다.

이렇게 부호화된 블록에 대해, 사용자가 블록을 요구하거나, 피어의 장애 발생시 블록을 제공하기 위해서는, 복구 과정, 즉 분산 저장된 청크를 전송받아서 재인코딩을 수행해야 하는 오버헤드가 있다.

본 논문은 기반 시스템에 블록 저장, 인코딩, 장애 발생, 청크 전송, 디코딩, 재인코딩 등의 기능을 설계 및 개발하였고, 기반 시스템과 제안 시스템을 통해 RS 부호화 적용 전과 후의 블록 복구 성능을 비교 평가해 보았다.

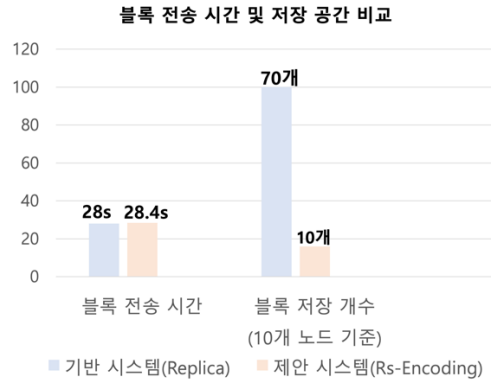
성능 평가를 위해, 비잔틴 장애 내성, $N = 3F + 1$ 공식을 만족하도록 $k = 7$, $m=3$ 인 (7,3) RS 부호화 환경을 구축하여 시험했다. 예를 들면, 10 개의 데이터 중 3 개까지의 데이터에 장애가 있다면 $10 >= 3F+1$ 이기 때문에 비잔틴 장애 내성을 보장한다.

그림 2 에서 왼쪽은 RS 부호화가 적용되기 전에 피어들의 원장 저장 상태, 즉 모든 피어가 모든 블록(B1, …, B7)을 중복 저장하는 상태를 나타내며, 오른쪽은 (7,3) RS 부호화를 적용한후 원본 블록(B1, …, B7)과 패리티 블록 (P1, P2, P3)을 10 개의 노드에 분산 저장한 상태를 나타낸다.




(그림 2) Reed-Solomon 인코딩 전/후 피어 원장 상태

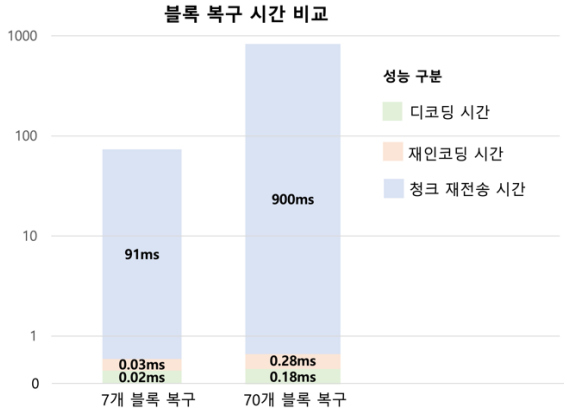
그림 3 은 기반 시스템에 부호화를 적용하지 않고 블록 마이너가 모든 피어에 블록을 전송하는데 걸리는 시간, 그리고 부호화가 적용된 제안 시스템에서 전송 시간을 비교하고, 각 시스템에서 블럭 저장 개수를 측정한 결과이다.




(그림 3) 블록 전송 및 저장 성능 비교

예상대로 본 논문의 시스템이 저장 공간은 약 7 배 적게 차지하는 것을 확인할 수 있었고, 총 70 개의 블록을 전송하는데 걸리는 시간은 큰 차이가 없어서, RS 인코딩 부하는 크지 않다는 것을 확인할 수 있었다.

그림 4 는 하나의 노드에 장애가 발생했을 때, 블록 7 개를 복구하는데 소요되는 시간과 70 개를 복구하는데 소요된 시간을 나타내며, 소요 시간은 블록 개수에 비례하여 증가하는 것을 알 수 있다. 대부분의 시간은 청크 재전송 시에 발생하고 디코딩, 재인코딩 오버헤드는 크지 않았다.




(그림 4) 블록 개수에 따른 블록 복구 시간 비교

## 3. 결론

본 논문에서는 오픈소스 블록체인에 RS 부호화를 적용하여 성능평가를 수행하였고, 원장에 RS 부호화를 적용하면 저장 공간을 많이 줄일 수 있다는 것을 확인할 수 있었다. 그리고, 복구 시에도 디코딩, 재인코딩 측면에서 큰 오버헤드가 발생하지 않는다는 것을 확인할 수 있었다.

그러나, 블록이 이미 많이 생성된 상태에서 복구를 위한 청크 재전송은 여전히 큰 비용이 발생할 수 있다. 향후 연구에는 노드의 추가, 삭제 장애에도 청크 전송을 최소화할 수 있는 방안을 고민해 볼 필요가 있다.

* 이 논문은 2021 년도 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).

## 참고문헌

[1] BitInfoCharts, “Cryptocurrency statistics,” Available: https://bitinfocharts.com/

[2] Q. Zhou, et al., "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020

[3] 최병준, 김창수, 이명철, “블록체인 트랜잭션 데이터 분산 저장 기술 동향,” 전자통신동향분석, 제 37 권 제 3 호, 085-096, 2022

[4] blockchain_go, “open source golang blockchain project,” Available: https://github.com/Jeiwan/blockchain_go

[5] Qi, X et al., "BFT-Store: Storage partition for permissioned blockchain via erasure coding," Proceedings of ICDE, pp. 1926-1929, April. 2020.