PON 기반 블록체인의 고속 동기화 연구

김동오*, 오진태*, 김기영*
*한국전자통신연구원
dokim@etri.re.kr, showme@etri.re.kr, kykim@etri.re.kr

A Study on High-speed Synchronization of the PON-based Blockchain

Dong-Oh Kim*, Jin-Tae Oh*, Ki-Young Kim*
*Dept. of Blockchain & Big Data Research, Electronics and Telecommunications Research Institute

요 약

블록체인은 모든 참여자가 동일한 원장을 유지하는 분산 원장 기술로써, 신규로 참여하는 블록체인 노드는 원장을 동일하게 유지하기 위한 동기화 절차를 거쳐야 한다. 일반적으로, 동기화는 블록체인 상의 모든 블록을 순차적으로 적용하는 과정을 거쳐야 함으로 많은 시간이 걸리게 된다. 본 논문에서는 ETRI에서 자체 개발한 PON 기반 블록체인에서 동기화 성능을 개선하기 위해 비잔틴 환경에서 병렬적으로 동기화 요청하는 고속 병렬 동기화 모드와 최신 상태만 동기화하는 최신 상태 동기화 모드를 개발하였다. 성능 평가 결과 100,000 개 블록 동기화시 고속 병렬 동기화 모드가 기본 동기화 대비 5 배, 최신 상태 동기화 모드가 기본 동기화 대비 880 배 빠른 것을 확인하였다.

1. 서론

블록체인 기술은 블록체인 네트워크에 참여하는 모든 참여자가 동일한 원장을 유지하는 분산 원장 기술(Distributed Ledger Technology:DLT)의 하나로써, 변경 사항을 블록 단위로 연결하여 체인 형태로 구성하는 기술이다. 이때, 체인에 연결되는 블록을 결정하기 위해 합의를 거치게 되며, 블록체인 네트워크를 구성하는 노드들은 합의에 참여하여 블록을 검증할 수 있도록 동일한 원장을 가져야 한다[1,2].

따라서, 블록체인 네트워크에 신규로 참여하는 경우 분산 원장의 모든 블록을 순차적으로 적용하는 동기화 과정에 많은 시간이 걸리게 된다. 특히, 비잔틴 환경에서는, 동기화할 블록에 대한 검증 작업이 필요해 더 많은 시간이 요구된다[3].

특히, 분산 원장의 크기가 시간이 지날수록 점차 커지기 때문에, 동기화에도 점차 많은 비용이 요구된다[4]. 예를 들어, 21년 9월 기준으로 이더리움 Full Node 동기화시 Geth Archive 용량이 약 8,402GB로 동기화에 몇일이 소요될 수 있다[5]. 따라서, 동기화 문제를 해결하기 위해 최신 상태만을 동기화 하는 등 다양한 동기화 방법을 제시하고 있다[6].

ETRI 에서 자체 개발한 PON(Proof of Nonce) 기반 블록체인에서도, 동기화시 많은 시간이 요구된다. 따라서, 본 논문에서는 PON 기반 블록체인에서 동기화 성능을 개선하기 위해 비잔틴 환경에서 병렬적으로 동기화 요청하는 고속 병렬 동기화 모드와 최신 상태만 동기화하는 최신 상태 동기화 모드를 개발하였다.

본 논문의 구성은 다음과 같다. 2 장에서는 본 논문에서 사용한 PON 기반 블록체인에 대해 간략히 소개한다. 3 장에서는 본 논문에서 제시한 동기화 모드에 대해 간단히 설명한다. 4 장에서는 실험 환경 및 실험 결과에 대해서 기술한다. 마지막으로 5 장에서는 결론에 대해 간략히 언급한다.

2. PON 기반 블록체인

PON 기반 블록체인은 ETRI에서 자체 개발한 PON과 BADA(Byzantine Agreement among Decentralized Agents) 알고리즘을 적용한 블록체인이다. PON 기반 블록체인은 매 블록 마다 합의 참여 노드를 랜덤 선출하여 탈중앙성을 보장하고, BFT(Byzantine Fault Tolerance) 기반의 합의를 통해 최종성이 보장하며, 수~수만 노드까지 합의 참여를 지원함으로써 확장성을 지원한다[6].

PON은 해시 함수 기반으로 생성된 “넌스체인” 기반의 검증 가능한 넌스값을 활용해 합의체를 선출하는 알고리즘이다. BADA는 비잔틴 감내 가능한 다중 서명 기반의 PBFT 계열의 합의 알고리즘이다. PON은 VRF(Verifiable Random Function) 등에 비해 연산 비용이 작으며, BADA는 PBFT보다 낮은 합의 메시지 복잡도를 가지며 높은 TPS와 빠른 합의 시간을 갖는다.

3. PON 기반 블록체인의 고속 동기화 방법

PON 기반 블록체인에서 동기화는 다른 노드에 동기화를 요청하는 동기화 요청 단계와 수신된 블록을 활용하는 동기화 완료 단계로 나누어 처리된다.

동기화 요청 단계는 동기화에 필요한 정보를 블록체인 네트워크에 포함된 다른 노드에 요청하여 동기화 하는 단계이다. 동기화 요청 단계에서 요청하는 정보는 동기화 모드에 따라 다르며, PON 기반 블록체인에서 제공하는 3가지 동기화 모드는 다음 표 1과 같다.

<표 1> PON 기반 블록체인의 동기화 모드

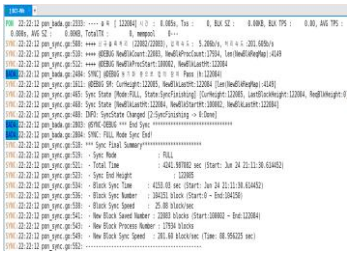
동기화 모드	동기화 범위	요청 정보 및 검증 방법
기본 동기화 모드 (FULL 모드)	모든 블록	모든 블록과 블록에 대한 검증 정보를 요청하여 블록 검증 및 동기화 수행
고속 병렬 동기화 모드 (PARALLEL 모드)	모든 블록	모든 블록을 다수 노드에 교차 병렬로 요청하여 블록 검증 및 동기화 수행
최신 상태 동기화 모드 (FAST 모드)	최신 상태	최신 상태에 대한 덤프와 이에 대한 검증 정보를 요청하여 검증 및 동기화 수행

동기화 완료 단계는 동기화 요청 단계 완료 이후 동기화 중 배포된 블록을 반영하여 동기화를 마무리하는 단계이다. 동기화 중에 블록체인 네트워크에서 배포되는 신규 블록들 중 일부를 임시 보관한 후, 동기화 완료 단계에서 순차적으로 반영하여 동기화를 마무리한다. 해당 단계에서 임시 저장된 모든 블록이 반영되면 동기화를 종료하고 합의에 참여 가능하다.

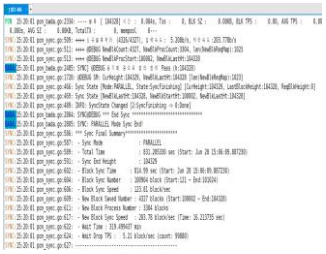
4. 성능 평가

PON 기반 블록체인의 고속 동기화 방법에 대한 성능 평가는 9개 노드로 구성된 PON 기반 블록체인 네트워크에서 100,000번째 블록에 신규 노드를 동기화하는 시험을 3가지 모드에서 각각 수행하였다. 블록체인 네트워크를 구성하는 각 노드의 사양은 Intel Xeon 3.0 GHz CPU, 256G 메모리, 256G SSD, 1G 이더넷, CentOS 7.6 이다.

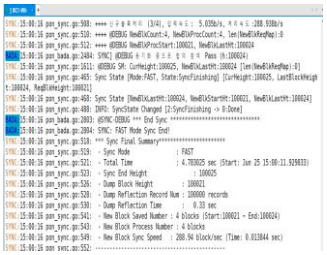
그림 1, 2, 3은 각각 Full 모드, PARALLEL 모드, FAST 모드로 동기화를 수행한 결과 화면을 보여준다. 각 그림의 "Sync Final Summary"에서 동기화 처리 결과에 대한 요약 정보를 확인할 수 있다.



(그림 1) FULL 모드 결과



(그림 2) PARALLEL 모드 결과



(그림 3) FAST 모드 결과

표 2는 신규 노드를 동기화 하는 3가지 모드의 동기화 시험 결과를 정리하였다.

<표 2> PON 기반 블록체인의 모드 별 동기화 결과

동기화 모드	동기화 수행 시간	동기화 완료 높이	임시 블록 처리 개수
FULL	4241.98 초	122,085	17,934
PARALLEL	831.2 초	104,329	3,304
FAST	4.78 초	100,025	4

표 2에서 동기화 수행 시간은 동기화 시작 후 완료까지 걸린 시간을, 동기화 완료 높이는 동기화가 완료된 블록의 높이를, 임시 블록 처리 개수는 동기화 완료 단계에서 처리된 임시 블록의 수를 의미한다.

5. 결론

본 문서에서는 PON 기반 블록체인에서 개발된 3 가지 동기화 모드에 대해 간략히 언급하고, 실험 결과 고속 병렬 동기화 모드가 기본 동기화 모드 대비 5 배, 최신 상태 동기화 모드가 기본 동기화 대비 880 배 빠른 것을 확인하였다.

본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음[No. 2018-0-00201, 블록체인(PON 알고리즘) 기반 고신뢰 정보거래 플랫폼 기술 개발]

참고문헌

[1] Scott Ruoti et al. "SoK: Blockchain Technology and Its Potential Use Cases" arXiv:1909.12454, 2019

[2] 진희상 김동오 김영창 오진태 김기영 "블록체인 분산합의 기술 동향" 전자공학회지 2021

[3] Michel Rauchs et al. "Distributed Ledger Technology Systems: A Conceptual Framework" Cambridge Centre for Alternative Finance, 2019

[4] Seoungkyun Kim et al. "Measuring Ethereum Network Peers" IMC '18: Proceedings of the Internet Measurement Conference 2018, 91-104, 2018

[5] Etherscan, https://etherscan.io/chartsync/chainarchive

[6] Péter Szilágyi "fast synchronization algorithm" https://github.com/ethereum/go-ethereum/pull/1889, 2018

[7] Jentae Oh et al. "Algorithm based on Byzantine Agreement among Decentralized Agents (BADA) " ETRI Journal, 42, 6, 872-885, 2020