하이퍼레저 패브릭 오더링 서비스의 합의 알고리즘 개선 연구

이민형, 김기형, 김재훈
아주대학교

{quotia72, kkim86, jaikim}@ajou.ac.kr

A Study on the Improving Hyperledger Fabric Consensus Algorithm of Ordering Service

Min Hyung Rhie, Ki-Hyung Kim, Jai-Hoon Kim
Ajou University

요 약

P2P 기반의 4 차 산업 핵심기술 중 하나인 블록체인(Blockchain) 기술이 널리 사용되고 있지만, 성능 개선에 대한 요구사항이 높아지고 있다. 하이퍼레저 패브릭의 거래 흐름(Transaction Flow)에서 체인코드(Chaincode)를 시뮬레이트(Simulate)하는 부분과 보증 피어(Endorsing Peer)들이 서명하는 부분, 그리고 오더링 서비스(Ordering Service)를 하는 부분에서 병목 현상이 발생할 수 있다. 본 연구는 오더링 서비스의 Trade-off 관계인 속도와 안정성을 합리적으로 도출하기 위하여 RAFT 보다 더 안전한 BFT(Byzantine Fault Tolerance)계열을 사용하되, PBFT 보다 네트워크 오버헤드가 적은 개선된 오더링 서비스의 합의 진행 방식을 제안하였다. 제안하는 합의 알고리즘은 전체 네트워크를 최소한의 노드수로 구성된 여러 그룹으로 분리하고 여러 합의를 동시에 병렬 처리함으로서, 메시지 요구량을 줄이고 합의 알고리즘의 속도를 높일 수 있다.

Ⅰ. 서 론

블록체인(Blockchain)은 P2P 기반의 기술의 4 차 산업혁명의 핵심 기술로 익명성, 투명성, 보안성, 시스템 안정성, 확장성 등의 장점을 보유하고 있다. 행정 서비스, 당사자간 계약, 증명, 의료 정보 서비스, 에너지 판매, 자동차 생태계, 이력추적, 클라우드 융합, O2O, 콘텐츠 서비스 그리고 SCM, BPM 과 같은 기업 시스템 분야에서도 도입되고 있다[1]. 본 논문은 블록체인 기술을 활용한 리눅스 재단(Linux Foundation)에서 주관하고 있는 하이퍼레저(Hyperledger) 프로젝트의 일부인 하이퍼레저 패브릭(Hyperledger Fabric)을 연구하여 문제점을 파악하고 개선점을 도출하고자 한다.

Ⅱ. 본론

기존의 기술은 대부분 중앙집중형 서비스들이다. 만일, 데이터베이스에 수정 권한이 있는 사람이 악의적인 목적으로 접근하게 된다면 신뢰성과 안정성에 문제가 생길 것이다. 블록체인은 트랜잭션(Transaction)의 히스토리(history)를 기록해 데이터베이스의 감시하여 신뢰성을 확보하게 해준다.

그림 1 처럼 블록체인은 크게 Block Hash 값과 Header 와 Data 부분으로 나뉜다. Header 에는 이전에 생성된 Block Hash 값, Timestamp 등이 저장된다. 그리고, 이러한 블록들이 연결되어 블록체인이라고 한다. 블록체인의 유형은 네트워크 형태에 따라 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain) 그리고 컨소시엄 블록체인(Consortium Blockchain)으로 나뉜다.

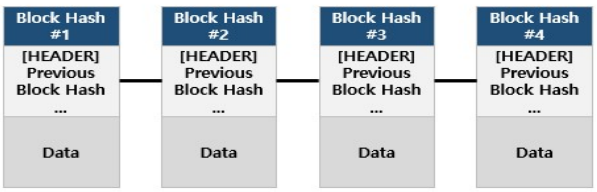

그림 1 블록체인 기술의 원리

본 논문은 이것들 중에서 하나의 조직이나 미리 선정된 주체들만 참여해 블록체인을 관리하는 책임을 공유할 수 있는 프라이빗 및 컨소시엄 블록체인 네트워크를 구현할 수 있는 하이퍼레저 패브릭을 다룬다[2][3].

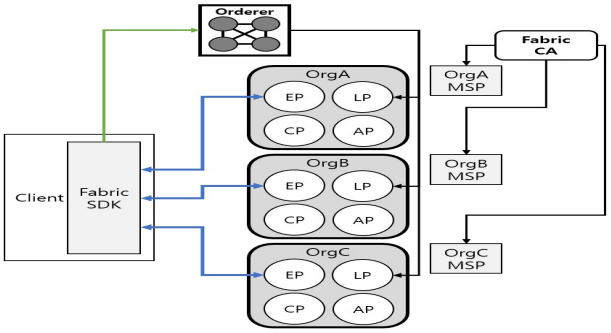

그림 2 하이퍼레저 패브릭 구조

그림 2 에서 EP 는 Endorsing Peer, AP 는 Anchoring Peer, LP 는 Leader Peer, CP 는 Committing Peer 를 의

미한다. 각 피어(Peer)들은 원장(Ledger)을 가지고 있으며 원장은 World State 와 Blockchain 을 가지고 있고, 각각 현재의 상태를 갱신하는 데이터베이스의 역할과 거래의 Log 및 History 의 역할을 담당하고 있다[4]. 또한 체인코드(Chaincode)를 가지고 World State 에 대한 put, get, delete 를 진행하거나 임의적 변경이 불가능한 (immutable) 블록체인에 쿼리(query)도 가능하다[5].

거래 흐름(Transaction Flow)은 EP 가 gRPC 프로토콜을 이용해 Tx(Transaction)형식을 확인하고 서명이 유효한지 MSP 를 이용해 Policy 를 확인하며 체인코드를 실행한다. 체인코드로부터 반환된 형태를 R/W set 으로 클라이언트에게 응답을 해주면 각 EP 로부터 Policy 에 따라 서명 받은 read-write set 을 Orderer 에게 보내어 Ordering Service 를 진행하는데 이 때 합의 프로세스가 일어나게 된다. 현재는 CFT(Crash Fault Tolerance)를 구현한 RAFT 가 쓰이고 있다[6]. 이렇게 생성된 블록은 해당 채널의 모든 피(CP)로부터 검증을 받아 블록체인에 추가하게 된다. 결론적으로 Endorsing-Ordering-Validating 이라는 3 단계를 거치게 된다[7].

문제는 하이퍼레저 패브릭의 거래 흐름에서 ①체인코드를 시뮬레이트(Simulate)하는 부분과 ②EP 들이 서명하는 부분, 그리고 ③오더링 서비스(Ordering Service)를 하는 부분에서 병목 현상이 발생한다는 점이다.

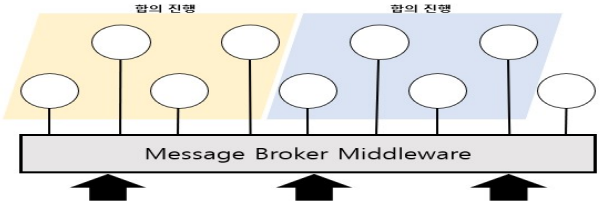

그림 3 Proposed Ordering Service Consensus Architecture

BFT(Byzantine Fault Tolerance)는 CFT 만 구현되는 RAFT 와 달리 AFT(Arbitrary Fault Tolerance)까지 구현하여 안정성이 RAFT 보다 높다. 그러나, 합의에 비용이 많이 요구되어 성능이 저하된다는 Trade-off 관계에 있다. 성능 저하를 줄이기 위해 그림 3 처럼 Message Broker 라는 미들웨어를 둘 것을 제안한다. 이 브로커가 하는 역할은 클라이언트로부터 오는 메시지를 조정(Coordinate)하여 우선순위를 만들고 무작위(Randomly)로 $3f+1$ (f: 최대 장애 발생 노드 수) 이상의 합의 노드(Leader 와 Follower)를 선출하여 PBFT 합의를 진행하는 것이다. 오더링 서비스의 문제는 순서대로 처리하기 때문에, 대규모 트래픽이 들어오면 대기 시간이 길어진 트랜잭션들이 취소될수 있다. $3f+1$ 이상 노드를 가진 합의 그룹(Consensus Group) 형태로 브로커에 의해 여러 그룹으로 나뉘어서 멀티 쓰레드(Multi-Thread)처럼 병렬적으로 합의를 진행하게 된다면, 노드 수가 증가함에 따라 성능이 줄어드는 것이 아니라, 오히려 대규모 트래픽에 강한 오더링 서비스를 진행할 수 있다.

N 개의 노드중에서 최대 f 개의 노드까지 결함이 발생할 수 있다고 가정할 때, Leader 가 Follower(Replica)들에게 Heartbeat 를 전송하여 데이터 일치성을 유지하고 노드의 활성 여부를 확인하므로 RAFT 는 $2(N-1)$ 정도의 메시지 수가 발생할 것이고, N은 $2f+1$ 이상 있어야 한다. 만일 PBFT 를 적용하게 된다면 Pre-Prepare, Prepare, Commit 의 과정을 거쳐서 합의가 진행되는데, Leader 나 Follower 상관없이 각 노드는 합의를 위해 $N-1$ 개의 메시지를 2 번씩 보내기 때문에 $2N(N-1)$ 정도의 메시지 수가 발생하게 되어 네트워크 오버헤드가 급격히 증가하게 된다. 그리고 BFT 이기 때문에 N 은 $3f+1$ 이상이어야 하기 때문에 필요한 노드의 수도 RAFT 보다 많다.

그러나 본 논문에서 제시하는 PBFT 를 활용한 개선된 오더링 서비스의 합의 방식을 적용한다면 N 은 전체 노드 수, n은 각 합의 그룹의 노드 수, P는 병렬적으로 합의를 진행할 수 있는 그룹의 수, m 은 총 메시지 수라고 한다면 다음과 같은 식이 나온다.

$$n \geq 3f+1, \qquad P = \frac{N}{n}, \qquad m = \sum_{k=1}^{P} 2n(n-1)$$

각 그룹마다 PBFT 가 진행되니 n 은 $3f+1$ 이상이어야 하며, 전체 노드를 n 만큼 나누면 그룹의 수가 나오는데 그룹의 수는 합의 프로세스를 비동기적으로 진행할 수 있는 수이기도 한다. 각 그룹마다 $2n(n-1)$ 만큼의 메시지 수가 필요하고, 모든 그룹의 메시지 수를 모두 더하면 전체 네트워크의 총 메시지 수가 된다. 만일 f=2, N=8, n=4 라고 가정한다면, PBFT 와 개선된 오더링 서비스의 합의 방식은 각각 m=112, m=48 로 합의에 필요한 메세지수를 줄일 수 있다. 또한, 합의 프로세스도 2 개의 그룹이 동시에 처리하므로 2 배의 속도 개선 효과가 있다.

Ⅲ. 결론

각 합의 프로세스 방식의 네트워크 오버헤드를 최대 메시지의 수를 기준으로 비교했다. BFT 는 비잔틴 결함을 극복할 수 있는 장점이 있지만, 메시지 요구량이 많다. 이를 극복하기 위하여 제안하는 합의 알고리즘은 전체 네트워크를 최소한의 노드수로 구성된 여러 그룹으로 분리하고 여러 합의를 동시에 병렬처리함으로서, 메시지 요구량을 줄이고 합의 알고리즘의 속도를 높일 수 있음을 확인하였다.

ACKNOWLEDGMENT

이 논문은 2018 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업과(NRF-NRF-2018R1D1A1B07040573) 2020 년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2020 년 산업전문인력역량강화사업)

참 고 문 헌

[1]이승민 수석, 블록체인 관련 동향 및 시사점, 이슈리포트 2018-제 27 호, 정보통신산업진흥원, 2018.07.02

[2]국내외 금융분야 블록체인 활용 동향, 보안연구부-2015-028, 금융보안원, 2015.11.23

[3]블록체인 기술이란 무엇일까요: 블록체인 네트워크 유형, IBM, URL: https://www.ibm.com/kr-ko/blockchain/what-is-blockchain

[4]Key Concepts: Ledger, HYPERLEDGER FABRIC DOCS, URL: https://hyperledger-fabric.readthedocs.io/en/release-2.0/ledger/ledger.html

[5]Key Concepts: Smart Contracts and Chaincode, HYPERLEDGER FABRIC DOCS, URL: https://hyperledger-fabric.readthedocs.io/en/release-2.0/smartcontract/smartcontract.html

[6]Key Concepts: The Ordering Service, HYPERLEDGER FABRIC DOCS, URL: https://hyperledger-fabric.readthedocs.io/en/release-2.0/orderer/ordering_service.html

[7]Architecture Reference: Transaction Flow, HYPERLEDGER FABRIC DOCS, URL: https://hyperledger-fabric.readthedocs.io/en/release-2.0/txflow.html?highlight=Endorsing%20Peer#transaction-flow