블록체인 기법의 확장가능성을 위한 병행 수행 제어 기법에 대한 연구

강용혁*

*극동대학교

A Study of Concurrency Control Scheme for Scalability of Blockchain Technology

Yong-Hyeog Kang*

*Far East University

E-mail : yhkang@kdu.ac.kr

요 약

비트코인에 기반한 블록체인 기술은 익명성이 있는 스마트 계약, 저렴한 송금, 온라인 거래 등을 가능하게 하는 하부구조를 제시하고 있다. 하지만, 비트코인을 구현하는 블록체인 기술은 처리량과 지연시간 간의 트레이드오프 관계에 있는 확장가능성 제한을 갖고 있다. 이러한 문제를 해결하기 위한 비잔틴 고장 감내 기반 블록체인 기술이 제안되었다. 이 기법은 리더를 선출하고 리더에 의해 기존 블록 내에 작업증명을 포함하지 않는 많은 마이크로 블록을 구성하여 지연시간 증가 없이 처리량을 향상시켰다. 하지만 이 기법은 리더를 선출하는 부분에서 기존 기법보다 보안성이 떨어질 수 있다. 본 논문에서는 마이크로 블록기술과 병행수행 기법을 통해 블록체인 기술의 확장가능성을 위한 기법을 제안한다. 하나의 마이크로 블록 내에는 여러 개의 거래에 대한 정보가 있다. 제안 기법에서는 이러한 마이크로 블록들은 병행 수행함으로써 기존 기법보다 처리량을 증가시킬 수 있다.

ABSTRACT

Bitcoin-based blockchain technology provides an infrastructure that enables anonymous smart contracts, low-cost remittances, and online payments. However, the block-chain technology that implements the bitcoin has scalability constraints in tradeoffs between throughput and latency. To solve these problems, the Byzantine fault tolerant block-chain technique has been proposed. This technique improves throughput without increasing latency by selecting a leader and constructing many microblocks that do not contain proofs of work within the existing block by the leader. However, this technique may be less secure than existing techniques in selecting the reader. In this paper, we propose a technique for scalability of the blockchain technology by using microblock technology and parallel execution technique. Within one microblock there is information about several transactions. In the proposed scheme, the throughput of the microblocks can be increased by performing concurrently.

키워드

블록체인 기술, 마이크로블록, 병행 수행 제어, 비트코인, 확장성

Ⅰ. 서 론

암호 화폐(Cryptocurrency)는 익명의 온라인 지불, 저렴한 송금, 스마트 계약(smart contract)를 지원하는 하부 기술이다[1]. 하지만, 비트코인에 의해 유래된 블록체인 기술은 본질적으로 처리량과 지연시간 사이에 균형을 맞춰야 하는 확장성(scalability) 문제가 있다. 또한, 트랜잭션 처리 속도를 높이는 것은 비트코인과 같은 암호 화폐에는 가장 중요한 고려사항 중에 하나이다[2].

분산 원장을 사용하는 디지털 화폐에서 가장 큰 위협은 이중 지불 문제이다. 임의의 사람이 두 개의 트랜잭션을 동시에 수행하여 동일한 자금을 다른 수신자에게 전송할 경우 쉽게 발생할 수 있

다[3]. 본 논문에서는 이러한 문제점들을 해결하기 위한 기법을 제안한다.

Ⅱ. 관련 연구

트랜잭션의 처리 속도는 비트코인은 10MB 블록의 크기 기준으로 약 7tps 정도이다. 이는 1초에 7개의 트랜잭션이 수행이 가능하다는 의미이다. 페이팔은 115tps이며, VISA는 약 45000tps가 가능하다[2]. 이중 지불 문제와 속도 문제 및 확장가능성 문제점들을 해결하기 위해서 많은 논문들이 제안되고 있다. 우선 이더리움의 핵심에 있는 Ghost 프로토콜이다. Ghost 프로토콜은 비트코인의 체인대신에 트리 자료구조를 사용한다[2].

포괄적인(inclusive) 블록체인 프로토콜인 경우에는 DAG(Directed acyclic graph)를 사용하여 더 높은 속도로 블록을 생성할 수 있도록 하였다[4]. 이 기법에서는 충돌나는 블록에 있는 트랜잭션들을 통합하는 규칙을 제공한다.

Bitcoin-NG 기법에서는 그림 1과 같이 사각형 형태의 키블록을 생성하여 리더를 선출하고 리더에 위해 원형태의 마이크로블록들을 수행하는 기법을 제안하였다[1]. 이 기법은 비잔틴 고장 감내 프로토콜로 비트코인과 동일한 신뢰 모델이지만 확장가능성을 고려한 프로토콜이다.

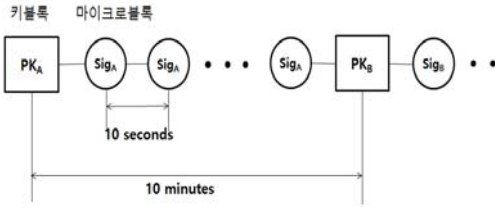

그림 1. BitCoin-NG 체인의 구조

Ⅲ. 제안 기법

본 논문에서는 데이터베이스의 병행수행 제어 기법을 이용하여 트랜잭션의 속도 및 확장성을 높이는 기법을 제안한다. 기본적인 원리는 병행 수행 제어 기법을 이용하여 트랜잭션의 수행을 병행 수행하도록 하여 속도를 높이고 제어기법을 통해 보안 또는 신뢰 문제를 해결하는 기법이다. 병행 수행 제어 기법은 크게 다음과 같이 두 가지 기법으로 나눌 수 있다. 잠금(locking) 기법과 낙관적(Optimistic) 기법이 있다. 낙관적 기법은 공유되는 자원이 적고 트랜잭션 수행 시간이 짧고 전체적인 사용 사항을 제어할 수 있어야 하는 환경이므로 블록체인에는 적합하지 않다.

잠금 기법을 사용하여 병행 수행 제어를 하는 기법은 이중 지불 문제를 해결하기 위해 먼저 사용하려는 트랜잭션이 잠금을 요청하여 수행하면 된다. 잠금 기법으로 인해 이중 지불이 허용되지 않으며 잠금이 없는 출력들은 잠금 후에 병행 수행하여 사용할 수 있다. 하지만 분산 환경에서 잠금 기법을 구현하기 위해서는 공유메모리가 있어야 하며 해당 자원을 접근하는 통일된 인터페이스가 있어야 한다. 블록체인 환경에서는 위와 같은 기법이 적용되지 않아서 공개키 기반구조를 이용하여 접근해야 한다.

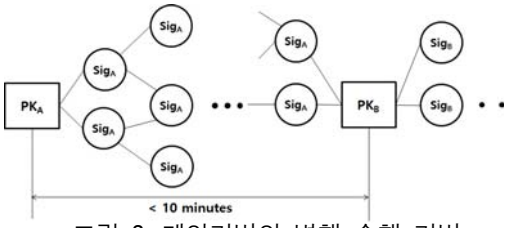

그림 2. 제안기법의 병행 수행 기법

제안 기법에서는 마이크로블록들을 키블록 리더에 의해 서명이 되므로 리더에 의해 잠금과 같은 역할을 할 수 있다. 동일한 출력에 대해 두 번째 서명할 때는 서명하지 못하도록 함으로써 병행 수행 제어의 잠금 기능을 구현할 수 있다

Ⅳ. 결론 및 향후 연구과제

본 논문에서는 데이터베이스의 병행 수행 제어 기법을 이용하여 이중 지불 방지 기법과 속도 및 확장가능성을 갖는 블록체인 기술을 제안하였다. 향후 연구과제로는 제안 기법에 대한 상세 설계와 검증을 수행하고 성능평가를 수행하는 것이다.

참고문헌

[1] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, Bitcoin-NG: A Scalable Blockchain Protocol. In 13th USENIX Symposium on Networked Systems Design and Implementation, 2016.

[2] A. Kiayias and G. Panagiotakos, Speed-security tradeoffs in blockchain protocols, IACR Cryptology ePrint Archive, 2015.

[3] F. Tschorsch and B. Scheuermann, Bitcoin and Beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surveys Tuts., 2016.

[4] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, Inclusive block chain protocols, In Financial Cryptography and Data Security, 19th International Conference, 2015.