블록체인 간 안전한 데이터 전송을 위한 영지식 증명 기반 데이터 공유 시스템 연구

유태훈, 김황남*

고려대학교 전기전자공학과

yth921@korea.ac.kr, *hnkim@korea.ac.kr

Research on a zero-knowledge proof-based data sharing platform for safe data transfer between blockchains

Taehoon Yoo, Hwangnam Kim*

School of Electrical Engineering, Korea University

요 약

본 논문에서는 영지식증명을 기반으로 한 블록체인 간 데이터 공유 플랫폼을 제안하여 블록체인 네트워크에서의 안전한 데이터 전송을 보장하는 연구를 서술한다. 제안하는 시스템에서는 서로 다른 블록체인 사이의 데이터 전송과정에서 영지식증명을 사용하여 데이터의 소유권을 증명하고, 데이터의 무결성을 검증하여 중간단계에서의 공격을 방지한다. 결과적으로 제안하는 시스템은 블록체인 간의 통신 과정에서 발생할 수 있는 보안 위협을 완화할 수 있고, 다수의 블록체인 네트워크로 구성된 환경에서 안전한 데이터 전송을 위한 기반 기술로써 동작할 수 있다.

Ⅰ. 서론

블록체인은 중앙 집중식 기록 보관 및 거래 시스템을 대체하며 연결된 블록의 체인으로 이루어진 분산된 데이터베이스 시스템으로, 각각의 블록은 이전 블록의 내용을 해시한 값과 새로운 데이터를 포함한다. 이 연결된 체인은 네트워크 상의 여러 참여자들에 의해 공유되며, 한 번 기록된 정보는 변경이 불가능하다. 이로써 블록체인은 탈중앙화, 신뢰성, 보안성, 그리고 투명성을 제공하며, 금융 거래부터 공급망 관리, 투표 시스템 등 다양한 분야에서 활용될 수 있다 [1]. 이러한 블록체인 기술은 스마트 계약에 기반한 변형 가능한 응용 프로그램의 구현과 다양한 비즈니스 모델의 등장으로 인해 점차 다양한 종류의 블록체인 네트워크가 등장하고 있다 [2] 하지만 이러한 서로 다른 블록체인을 연결하는 현재의 통신 방법은 중간 매개체 없이 직접적인 연결을 통해 이루어지는데, 이는 효율성과 보안성 측면에서 한계가 있다. 또한, 각각의 블록체인은 고유한 프로토콜과 특성을 가지고 있어 서로 다른 블록체인 간의 통신 과정에서 병목현상이 발생하거나 호환성의 문제가 발생한다. 이로 인해 블록체인 데이터 및 자산의 이동이 제한되고, 새로운 응용 프로그램의 개발이 지연되고 있다 [3, 4].

따라서 본 논문에서는 영지식 증명(Zero-knowledge proof, ZKP)에 기반한 새로운 데이터 공유 시스템을 제안한다. 영지식 증명은 데이터를 증명하거나 검증하는 과정에서 실제 데이터를 노출하지 않고 해당 데이터의 유효성을 검증할 수 있기 때문에 중간 단계에서 데이터의 검증 과정을 단순화할 수 있고, 서로 다른 블록체인 네트워크에서의 호환성 문제를 해결할 수 있다.

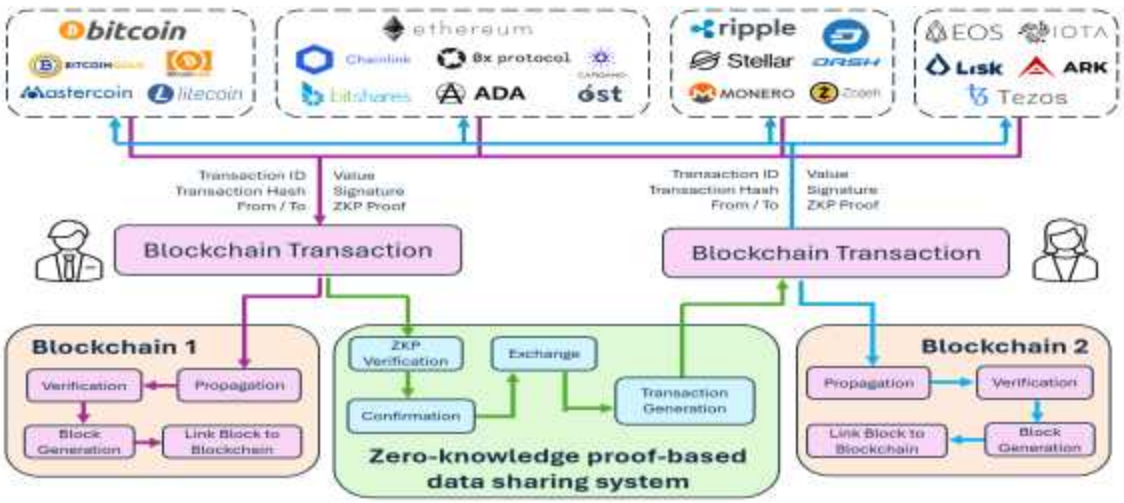

그림 1. 영지식 증명 기반 블록체인 데이터 공유 시스템

Ⅱ. 영지식 증명 기반 데이터 공유 시스템

2.1 시스템 구성 및 영지식 증명 과정

그림 1은 본 논문에서 제안하는 영지식 증명 기반 블록체인 데이터 공유 시스템의 전체 구조에 대한 개요를 보여준다. 제안하는 시스템은 서로 다른 블록체인 시스템 간의 데이터 전송에 대하여 중간 단계에서 동작하며, 영지식 증명에 기반하여 트랜잭션의 데이터를 직접 확인하지 않아도 해당 트랜잭션의 검증을 수행할 수 있다. 제안하는 시스템에서 영지식 검증을 수행하기 위해서 트랜잭션 데이터에 기반하여 영지식 증명을 생성해야 한다. 또한 다른 블록체인 네트워크로의 데이터 전송 과정은 각각의 블록체인 네트워크의 블록 생성 과정과 상관없이 트랜잭션이 생성된 순간 병렬적으로 수행되기 때문에 거래를 수행하려는 거래 금액만큼을 보증금으로 시스템에 제출해야만 한다.

제안하는 시스템에서 영지식 증명 검증을 수행하여 다른 블록체인 네트워크로 데이터를 전송하는 과정은 다음과 같다. 먼저 트랜잭션을 생성하는 송신자는 트랜잭션 데이터와 영지식 증명 알고리즘을 사용하여 해당 트랜잭션에 대한 영지식 증명을 생성한다. 제안하는 시스템은 생성된 영지식 증명을 수신하여 생성된 증명의 유효성을 검증한다. 또한, 이 과정에서의 중간자 공격과 이중지불 공격 등을 방지하기 위하여 해당 데이터 전송에 대하여 서명, 거래 내용 등의 확인 과정을 수행한 뒤, 전송하려는 블록체인 시스템에서 해당 트랜잭션 데이터에 합당한 가치의 트랜잭션을 생성한다. 각각의 블록체인 네트워크에서는 생성된 2개의 트랜잭션을 각각의 합의 알고리즘에 기반하여 트랜잭션의 유효성을 검증하여 블록 생성 과정에 포함시켜 거래를 확정한다. 거래가 확정된 후 트랜잭션 생성 과정에서 제출된 보증금은 송신자에게 반환된다.

2.2 시뮬레이션 결과

제안하는 시스템의 데이터 전송 속도를 측정하기 위하여 시뮬레이션 환경에서 비트코인, 이더리움, 이오스 블록체인 네트워크를 모델링하여 각각의 네트워크에서 생성된 트랜잭션에 대한 전송 시뮬레이션을 진행하였다.

그림 2는 비트코인에서 생성된 트랜잭션을 이더리움 네트워크로 전송하는 시나리오를 구성하여 시뮬레이션을 진행한 결과를 나타낸다. 비트코인 트랜잭션이 체결 완료된 후 이더리움 네트워크로의 전송이 진행되는 일반적인 전송보다 제안하는 시스템이 트랜잭션 수의 증가와는 상관없이 평균적으로 28% 빠른 속도로 진행되는 것을 확인할 수 있다.

그림 3은 서로 다른 블록체인 네트워크에서 형성된 트랜잭션의 데이터를 전송하는 시나리오를 구성하여 각각의 트랜잭션이 전송되는 시간을 측정한 결과를 나타낸다. 비트코인, 이더리움, 이오스 블록체인이 초당 처리하는 트랜잭션의 수(Transaction Per Second, TPS)가 각각 약 7개, 30개, 4000개임을 고려하면, TPS가 높은 블록체인 네트워크 간의 통신에서 더욱 빠른 트랜잭션 처리가 일어나는 것을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 블록체인 간 안전한 데이터 전송을 위한 영지식 증명 기반 데이터 공유 시스템에 대한 연구를 수행하였다. 기존의 블록체인 간의 통신 방법의 한계를 극복하고 보안성과 프라이버시를 강화하기 위해 영지식 증명 기술을 활용하였다. 제안하는 시스템은 서로 다른 블록체인 네트워크 간의 상호 운용성을 증가시키고 확장성을 향상시킬 수 있고, 데이터의 안전한 전송을 보장하여 다양한 다중 블록체인 네트워크를 활용하는 응용 분야에서 사용될 수 있다.

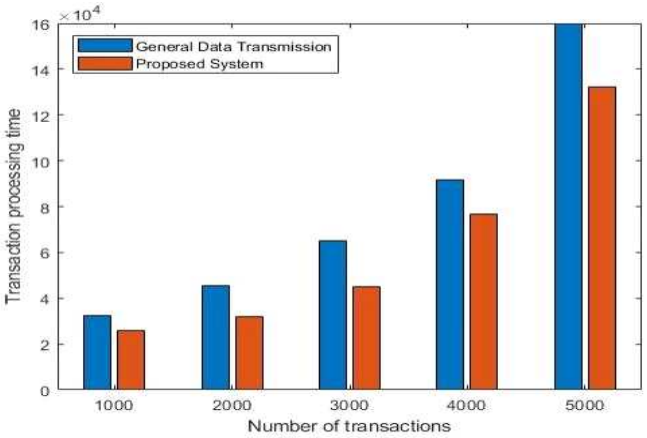

그림 2. 트랜잭션 처리 시간 시뮬레이션 결과

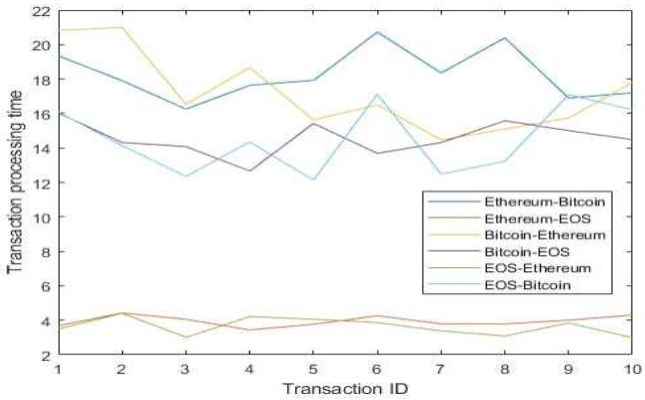

그림 3. 송수신 블록체인 네트워크에 따른 트랜잭션 처리 시간 시뮬레이션 결과

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2024-2021-0-01835). 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1A2C1012389).

참 고 문 헌

[1] Abou Jaoude, Joe, and Raafat George Saade, "Blockchain applications - usage in different domains." IEEE Access, 7 45360-45381, March 2019

[2] Guo, Ye, and Chen Liang. "Blockchain application and outlook in the banking industry.", Financial innovation, 2 pp.1-12, December 2016.

[3] J. Lee, B. Lee, J. Jung, H. Shim, and H. Kim, "DQ: Two approaches to measure the degree of decentralization of blockchain." ICT Express, 7.3 pp.278-282, August 2021.

[4] Park, Seongjoon, and Hwangnam Kim. "Dagmap: Multi-drone slam via a dag-based distributed ledger." Drones 6.2 (2022): 34.