영지식 증명 기반 합의알고리즘 연구 동향

김원웅*, 강예준*, 김현지*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Trends of Zero-Knowledge Proof Based Consensus Algorithm

Won-Woong Kim*, Yea-Jun Kang*, Hyun-Ji Kim*, Hwa-Jeong Seo*

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

최근 금융권에서 블록체인이 주목을 받고 있으며, 다양한 보안 이점을 제공하고 있다. 그러나 블록체인의 투명성에 의해 원치 않은 민감한 정보를 드러내게 되므로 프라이버시 문제를 야기 시킨다. 이러한 문제점을 해결하기 위한 다양한 연구가 진행되고 있다. 본 논문에서는 이러한 문제를 해결하기 위한 기법중 하나인 영지식 증명을 기반으로 하는 합의 알고리즘의 연구 동향에 대해서 조사하였다.

I. 서론

최근 암호화폐의 등장으로 블록체인은 금융권에서 많은 주목을 받게 되었다. 다양한 블록체인 기반 암호화폐가 존재하며 그 중 가장 유명한 것은 비트코인과 이더리움이다. 블록체인은 제 3의 기관이 존재하지 않고 사용자들끼리의 거래가 가능하도록 하는 분산 데이터베이스이며, 거래 기록 등과 같은 데이터들이 영구적으로 저장되어 자금의 흐름을 파악하기 용이하다. 또한 데이터에 대한 위변조가 불가능하도록 보장이 된다는 장점을 가지고 있어 금융권에서 주목을 받아왔다. 그러나 모든 사용자가 거래에 대한 검증이 가능해야 되는 블록체인의 특성상 계좌 잔액, 송수신자, 거래 내용 등의 정보가 드러나게 된다는 단점이 존재한다. 또한 p2p 네트워크의 특성상 각 사용자에 대한 신뢰 관계를 형성하는 것이 주요 쟁점으로써 자리잡아 왔다.

이러한 문제점을 해결하기 위한 다양한 시도들이 존재해왔으며 그 중 영지식(ZKP, Zero-Knowledge Proof)가 유력한 후보로써 각광받고 있다. 영지식은 둘 이상의 사용자가 각자의 어떠한 정보도 드러내지 않으며 신뢰 관계를 형성할 수 있는 증명 시스템으로, 1985년 Goldwasser에 의해 발표되었다.

본 논문에서는 블록체인의 투명성에 의한 문제를 해결하기 위한 ZKP 기반 합의 알고리즘의 연구 사례에 대해 조사하였다.

II. 관련연구

2.1 영지식 증명 (Zero Knowledge Proof, ZKP)

영지식 증명은 자신이 가진 정보를 드러내지 않으면서 그것이 참이라는 사실을 증명하는 기법이다[1]. 영지식 증명은 완전성 (Completeness), 건전성(Soundness), 영지식성(Zero-Knowledge)을 갖는다. 완전성은 증명하고자 하는 정보가 참일 경우 정직한 증명자는 검증에 성공하는 것이다. 건전성은 거짓 정보에 대

해서는 어떠한 증명자도 검증을 통과할 수 없는 성질이다. 마지막으로 영지식성은 검증을 수행할 때 증명자가 어떠한 정보도 드러내지 않는다는 성질이다.

III. 연구 사례

3.1 [2]

해당 논문은 블록체인, 스마트 컨트랙트 그리고 zk-SNARK를 결합하여 블록체인 및 ZKP를 통한 개인 정보 보호를 기반으로 하는 거래 시스템을 구축하여 개인 정보 보호 및 블록의 효율적인 검증이 가능하도록 하였다.

스마트 컨트랙트에서는 두 가지 제약 조건을 확인해야 한다. 이는 잔액의 소유권과 잔액 범위이다. 첫 번째로 잔액에 대한 소유권 문제는 악의적인 사용자가 다른 사람의 계정을 통해 거래를 하는 것을 방지하기 위해 거래를 위한 사용자 계정의 잔액은 본인의 소유여야 한다. 두 번째로 남아있는 잔액이 거래하고자 하는 금액의 양보다 많아야 한다. 소유권을 증명하기 위해서는 개인 키를 사용하여 공개 주소와 수신 주소를 생성한다. 그런 다음 공개 키와 난수를 기반으로 해시 값을 생성한다. 각 계정에는 난수가 존재하며 다른 노드들과의 난수를 해시하여 루트 해시값을 계산한다. 그 후 루트 해시값을 스마트 컨트랙트에 저장하게 되고, 사용자의 계정에서 거래가 발생하면 루트 해시값을 통해 소유권을 증명할 수 있다. 잔액 범위를 증명하기 위해서 소유권 증명 단계에서 사용자의 주소에 따른 전송 금액보다 계정 잔액이 더 큰지 확인한다. 이때 ZKP를 통해 증명의 여부만을 판단하고 주소와 송금 금액은 암호화되어 있기 때문에 값을 알 수 없다.

따라서 ZKP의 주요 기능은 거래가 합법적인지에 대한 여부를 증명하기 위한 것이다. zk-snarks 알고리즘을 사용하여 증명 크기를 압축하고 스마트 계약을 검증할 때 이상적인 시간 비용을 달성할 수 있다. ZKP는 트랜잭션에 바인딩되어 영지식 증명이 받아들여지면 해당 트랜잭션도 받아들여지게 된다. 합법적인 트랜잭션은 클라우드 데이터베이스에 업데이트된다.

3.2 LiteZKP[3]

LiteZKP는 IoT 기술이 데이터 수집과 다양한 환경에서 유망한 기본 기술이 될 것이라고 판단하고 블록체인 기술의 최근 발전 및 익명의 탈중앙화 결제가 가능하도록 하는 분산 플랫폼이 IoT 및 MEC 시스템내에서 구현될 가능성이 높다는 것을 근거로 하여 블록체인을 IoT 및 MEC 시스템의 데이터 비용 지물 메커니즘으로 효율적으로 적용되도록 설계되었다.

해당 논문은 자원이 제한된 장치에서 스마트 컨트랙트 기반 영지식 증명 프로토콜을 사용하여 다중 익명 지불을 지원하기 위한 프레임워크인 LiteZKP를 제안하였다. 특히 연산 오버헤드를 최소화시키고 완전한 익명 시스템을 제공하기 위해 새로운 머클 트리 메커니즘을 포함함으로써 ZKP의 부담을 줄이고 지속적인 데이터 교환을 수행할 때 ZKP의 작업 양을 줄이기 위해 스마트 컨트랙트 기반 ZKP를 오프체인 결제 채널과 통합한다.

ZKP는 대규모 데이터 공유에 있어 여러 번의 빈번한 토큰 트랜잭션이 필요하므로 ZKP를 직접적으로 적용하면 IoT 및 엣지 장치에 계산 오버헤드가 발생한다. 이는 블록체인의 핵심 네트워크에서 빈번한 병목 현상을 야기할 수 있다. 또한 모든 트랜잭션은 블록체인 합의에 참여하는 모든 노드에 의해 검증되어야 하므로 주어진 시간에 블록체인이 처리할 수 있는 계산량은 매우 제한적이다.

이러한 기술적 문제를 해결하기 위하여 해당 논문에서는 IoT 및 MEC 장치가 ZKP 기반 작업을 수행하는 동시에 낮은 대기 시간, 낮은 에너지 그리고 저비용으로 다중 결제 교환을 지원하는 LiteZKP를 지원한다. 해당 논문의 핵심 아이디어는 여러 ZKP 기반 익명 지불을 사전에 발행하여 최종 데이터 교환 가격과 관련하여 지불을 완료하는 것이다. 이를 위해 총 세 가지의 핵심 아이디어가 존재하며 다음과 같다.

(1) 머클 트리 기반 익명성을 지원하기 위해 해시 계산을 줄이는 미니 머클 트리 구조

(2) 반복적인 ZKP 작업을 줄이기 위해 ZKP를 오프체인 결제 채널과 통합

(3) 증명 생성 및 검증 대기 시간을 최소화하

기 위한 최적화 체계

이를 통해 IoT 및 엣지 장치를 위한 분산형 ZKP 기반 프라이버시 보호 p2p 블록체인 기반 결제 시스템을 제안한다. 분산형 금융 서비스를 허용함으로써 자원이 제한된 장치는 제 3자의 개입없이 익명으로 지불을 교환할 수 있다. 또한 ZKP가 다양한 기능을 가진 디바이스에 적용할 수 있도록 지원하는 솔루션을 제시한다. 이러한 솔루션은 다중(연속) 결제의 특성을 활용하여 다양한 ZKP 변종 기술에 적용할 수 있다. 그리고 실제 구현을 사용하여 블록체인과 IoT 노드의 관점에서 제안된 시스템을 평가하고 LiteZKP가 지불 횟수에 상관없이 IoT 및 MEC 노드에서 ZKP 관련 작업에 일정한 시간만 필요함을 보여준다. 또한 블록체인의 관점에서 해당 접근방식은 오늘날 사용되는 전력에 비해 13배 향상시킬 수 있습니다. 결과적으로 LiteZKP는 사물 인터넷(IoT) 및 모바일 엣지 컴퓨팅(MEC) 플랫폼에서 대기 시간과 에너지 소비를 55% 이상 줄이며 단순한 ZKP 기반 체계에 비해 블록 처리 수수료의 8%만이 필요하다.

3.3 P-CFT[4]

해당 논문에서는 Hyperledger Ursa 암호화 라이브러리를 사용하여 허가형 블록체인을 위한 영지식 충돌 장애 허용 합의 알고리즘인 P-CFT를 제안한다. 제안된 합의 알고리즘은 충돌 내결함성을 보장하면서 합의 계층에 직접 고유한 데이터 프라이버시를 제공한다.

해당 모델은 인증기관과 세 가지 유형의 노드(인증기관, 클라이언트 노드, 기본 노드, 복제 노드)가 포함된다.

합의 절차는 총 5단계로 설정, 요청, 포워드, 확인, 마무리로 이루어져 있다. 설정 단계에서는 인증기관이 거래 메시지에 대한 키 쌍을 발급하기 위한 알고리즘을 수행한다. 이 과정은 한 번만 수행하면 되며, 인증기관은 클라이언트 노드와 합의 노드(기본 노드, 복제 노드)에게 setup 메시지를 보낸다. 요청 과정에서 클라이언트는 원본 메시지를 기반으로 일회성 영지식 증명을 생성하고 시스템에 요청 메시지를 보낸다. 포워드 단계에서 기본 노드는 새 블록을 게시하고 클라이언트의 요청을 다른 복제 노드들에게 브로드캐스팅 한다. 확인 단계에서 복제 노드는 전달된 메시지를 수신하고 일회성 영지식 증명의 진위 여부를 확인한다. 검증이 성공적으로 완료되었을 경우 복제 노드는 검증 메시지를 다른 합의 노드들에게 전송한다. 마무리 단계에서 각 합의 노드는 적어도 (N - 1)/2 만큼의 다른 합의 노드로부터 메시지를 확인하고 블록을 커밋한다. 블록이 체인에 성공적으로 커밋된 후 각 노드는 요청에 대한 합의에 도달했다는 메시지를 클라이언트에게 전송한다.

P-CFT는 증명자 수준에서 5분 안에 10,000건의 트랜잭션을 처리할 수 있어 zk-SNARK 및 zk-STARK에 비해 수백 분, Bulletproof에 비해 수천분을 절약할 수 있다. 검증자 수준에서는 35분 만에 10,000건의 트랜잭션을 검증할 수 있으며 이는 zk-SNARK(1.7분) 및 zk-STARK(2.7)분보다 느리지만, Bulletproof에 비해서는 수백 분을 절약할 수 있다.

결과적으로 제안된 프로토콜은 기존 ZKP 프로토콜에 비해 낮은 검증 시간을 유지하면서 빠른 증명 생성 시간을 제공할 수 있음을 보여준다. 결과적으로 기존 허가형 블록체인 네트워크의 합의 수준에 프라이버시를 제공하기 위해 제안된 접근 방식의 타당성을 보여준다.

IV. 결론

본 논문에서는 블록체인의 투명성에 의해 발생하는 문제점을 해결하기 위해 ZKP를 적용한 합의 알고리즘에 대해 조사하였다. 기존 ZKP에 비해 짧은 검증 시간과 적은 블록 처리 수수료가 절감되지만, 증명이 블록에 담김으로써 블록에 포함될 수 있는 트랜잭션의 수가 감소하여 결과적으로 TPS(Transaction Per Sec)가 감소하는 문제가 존재할 수 있다. 이를 개선하여 TPS를 높일 수 있는 연구 또한 진행되어야 할 것으로 사료된다.

V. Acknowledgement

This work was supported by Institute of Information & communications Technology

Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%) and this work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%).

[참고문헌]

[1] Park, Chul, Jonghyun Kim, and Dong Hoon Lee. "Privacy-Preserving Credit Scoring Using Zero-Knowledge Proofs." Journal of the Korea Institute of Information Security & Cryptology 29.6 (2019): 1285-1303.

[2] Wang, Jin, et al. "Block Verification Mechanism Based on Zero-Knowledge Proof in Blockchain." Comput. Syst. Sci. Eng. 45.2 (2023): 1805-1819.

[3] Boo, EunSeong, Joongheon Kim, and JeongGil Ko. "LiteZKP: Lightening zero-knowledge proof-based blockchains for IoT and edge platforms." IEEE Systems Journal 16.1 (2021): 112-123.

[4] Li, Wanxin, et al. "P-cft: A privacy-preserving and crash fault tolerant consensus algorithm for permissioned blockchains." 2021 4th International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2021.