동형암호와 영지식 기반의 블록체인 동향

김현지*, 강예준*, 김원웅*, 서화정*†

*한성대학교 (대학원생)
*†한성대학교 (교수)

Trend of homomorphic encryption system and zero-knowledge-based blockchain

Hyun ji Kim*, Yea jun Kang*, Won woong Kim*, Hwa jeong Seo*†

*Hansung University(Graduate student)
*†Hansung University(Professor)

요 약

블록체인은 모든 트랜잭션을 체인에 기록함으로써 무결성을 보장할 수 있는 탈중앙화된 분산 원장 네트워크이다. 그러나 이러한 특성으로 인해 데이터 프라이버시 보호 측면에서 문제가 발생할 수 있다. 이를 위해 최근에는 동형암호와 영지식 증명을 활용하여 데이터 보호가 가능한 블록체인에 대한 연구들이 진행되고 있다. 본 논문에서는 이러한 연구 사례에 대해 살펴보았다. 동형암호를 활용하여 개인 정보 데이터를 노출하지 않고 데이터 연산이 가능 (e.g. 스마트 컨트랙트 상에서 금액 및 계좌 정보를 숨김)하며, 영지식 증명을 통해 올바른 데이터인지에 대한 검증이 가능하도록 할 수 있다. 이처럼 동형암호와 영지식 증명은 블록체인 상에서의 프라이버시 보호에 적절히 활용될 수 있다.

I. 서론

블록체인은 데이터에 대한 무결성을 검증할 수 있는 탈중앙화된 분산 원장 네트워크이다. 그러나 모든 트랜잭션이 체인 상에 기록되기 때문에 데이터 프라이버시 보호 측면에서 문제가 발생한다. 이를 극복하기 위해 영지식 증명 및 동형 암호 기반의 블록체인 기술이 다수 연구되고 있다. 본 논문에서는 영지식 증명 및 동형암호를 활용하여 프라이버시 보호가 가능한 블록체인 기술 동향에 대해 살펴본다.

II. 관련 연구

2.1 블록체인 (Blockchain)

블록체인은 모든 네트워크 참가자들이 peer-to-peer (p2p)로 구성되어 동일한 원장을 공유하고 있는 분산 원장 네트워크이다 [1]. 원장에는 네트워크 내의 모든 거래에 대한 데이터가 블록에 저장되어 체인 형태로 구성되어 있으므로 완료된 거래의 데이터를 변경할 수 없다. 따라서 데이터에 대한 위변조가 불가능하므로 무결성을 제공한다. 또한 네트워크 참여자들이 검증, 승인 그리고 합의를 이루기 때문에 중앙서버 없이 거래가 가능해지므로 탈중앙화를 이룰 수 있다. 따라서 추가적인 중앙 시스템을 구축할 필요가 없다는 장점이 있다. 그러나 블록체인에는 모든 트랜잭션이 기록되기 때문에 데이터 프라이버시에 대한 문제가 발생한다.

2.2 동형 암호 (Homomorphic Encryption)

동형암호화 (Homomorphic Encryption)는 평문을 연산하여 암호화한 결과와 평문을 암호화하여 연산한 결과가 동일하므로 비밀 데이터를 노출하지 않고 암호화한 채로 연산이 가능하다. 동형암호에는 연산의 유형이나 횟수 등에 따라 크게 3종류로 나뉜다. 먼저, 부분 동형 암호 (Partial Homomorphic Encryption, PHE)는

덧셈 또는 곱셈 연산 중에서 하나만 지원한다. 덧셈 및 곱셈 연산을 모두 지원하지만 제한된 연산 (차수가 낮은 다항식)만 가능한 Somewhat Homomorphic Encryption (SHE)는 SHE는 기밀성을 확보하기 위해 암호문에 노이즈를 삽입한다. 그러나 연산을 계속해서 수행하면 노이즈가 증가하면서 비밀 데이터를 훼손하게 되므로 횟수에 제한이 있다. 마지막으로 완전 동형암호 (Fully Homomorphic Encryption, FHE)는 덧셈과 곱셈을 모두 지원하고 부트 스트랩핑 (boot strapping)을 통해 노이즈를 제거함으로써 제한 없는 연산이 가능하다. 그러나 키크기가 증가함에 따라 데이터 크기가 매우 커지며 암호화된 데이터에 대한 연산을 수행하기 때문에 속도가 매우 느리다는 한계점이 있다. 최근에는 이러한 점을 극복하기 위한 연구들이 많이 진행되고 있다. 또한, 딥러닝 및 블록체인과 함께 사용되어 데이터 프라이버시를 보장하는 방법론들도 많이 연구되고 있다.

2.3 영지식 증명 (Zero Knowledge Proof, ZKP)

영지식 증명은 자신이 가진 정보를 드러내지 않으면서 그것이 참이라는 사실을 증명하는 기법이다[3]. 영지식 증명은 다음과 같은 3가지 특성을 가진다. 먼저, 완전성 (Completeness)는 증명하고자 하는 정보가 참일 경우 정직한 증명자는 검증을 통과하는 것이다. 건전성 (Soundness)은 거짓인 정보에 대해서는 어떤 증명자도 검증을 통과할 수 없는 성질이며, 마지막으로 영지식은 검증을 수행하기 전과 후에 검증자가 가진 정보의 차이가 없다는 성질이다. 즉, 검증을 통해 자신이 가진 정보를 노출시키지 않는 것이다.

III. 연구 동향

본 논문에서는 개인 정보 보호를 위해 영지식 증명과 동형암호를 활용한 블록체인의 연구 동향에 대해 살펴본다.

블록체인 플랫폼 기반의 스마트 컨트랙트는 개인 정보 보호 측면에서 문제점이 있다. [4]에서는 완전 동형 암호화 (FHE)를 사용하여 입출력 개인 정보를 보호하는 스마트 계약을 지원하는 프레임워크인 smardFHE를 제안하였다. 이는 블록체인에서 완전 동형 암호를 처음으로 사용하였으며, 입출력 개인정보를 보호하면서 블록 체인 상의 여러 사용자에 대해 스마트 컨트랙트를 구축할 수 있도록 하는 최초의 사례이다. smartFHE는 contract owned와 externally owned라는 두 종류의 어카운트를 가지며, 그 중 externally owned는 프라이빗과 퍼블릭 어카운트로 나뉜다. 프라이빗 어카운트의 경우 프라이빗 트랜잭션을 초기화하고 프라이빗 스마트 컨트랙트에 참여가 가능하다. 프라이빗 트랜잭션 타입에는 다음과 같이 3가지가 있다. 퍼블릭 어카운트에서 프라이빗으로 금액을 전송하는 경우에는 거래 금액이 암호화되지 않으므로 영지식증명이 사용되지 않는다. 그러나 프라이빗 어카운트에서 다른 프라이빗 어카운트로 암호화된 금액을 전송하는 경우, 영지식 증명을 통해 전송되는 금액에 대한 검증을 해야할 필요가 있다. 마지막으로 프라이빗에서. 퍼블릭 어카운트로 금액을 전송할 경우, 영지식 증명을 통해 sender가 보내는 금액이 통장에 실제로 있는지 확인해야한다. 이때 공개된 어카운트로 전송되기 때문에 프라이빗 어카운트의 정보가 어느정도 유출될 수 있다. 이러한 프라이빗 어카운트를 쓰는 경우 프라이빗 모드로 동작하며 전송되는 금액과 잔액을 숨길 수 있다. 사용자는 프라이빗 데이터와 어카운트에 관련된 스마트 컨트랙트를 작성할 수 있으며, 해당 컨트랙트는 private 정보를 입력으로 받고 동형연산 (덧셈, 곱셈)을 수행하도록 한다. 이처럼 암호화된 형식으로 동작하는 컨트랙트에 사용자가 참여하기 위해서는 영지식 증명 시스템을 통해 특정 조건을 만족하는지 확인해야한다. 이때 채굴자들이 ZKP를 확인하고 요청된 동형 연산을 수행하는 역할을 한다. 이러한 과정을 통해 한명의 사용자에 대한 private 계산이 이루어질 수 있으며, 해당 기법에서는 이를 여러 사용자로 확장할 수 있는 시스템도 제안하였다. 즉, 채굴자가 암호화된 데이터 및 계정의 잔액에 대한 계산을 FHE를 통해 수행하고, 효율적인 영지식 증

명 시스템을 통해 사용자가 개인 입력 정보가 올바르다는 것을 증명해냄으로써 성공적으로 동작한다. Microsoft의 SEAL 라이브러리를 사용하여 RLWE (Ring-Learning with Errors) 기반의 FHE 체계인 BFV (Leveled Brakerski/Fan-Vercauteren scheme)를 벤치마크한 결과, private 거래와 스마트 컨트랙트는 사용자의 실행 시간 측면에서 높은 성능을 달성하였다.

[5]에서는 클라우드 데이터의 보안 및 무결성 검사와 안전한 다자간 계산을 함께 제공 블록체인 기반 엣지 컴퓨팅 기술을 제안하였다. 블록체인의 운영 효율성과 클라이언트의 컴퓨팅 부담을 덜기 위해 엣지 컴퓨팅 모델을 활용하였으며 여러 엣지 노드들이 데이터에 대한 계산을 수행하고 체인에 기록하는 등의 기능을 수행한다. 이러한 아키텍처를 기반으로 어떠한 작업을 실행해야 하는 경우, 실행 측에서는 모든 데이터를 암호화하고 엣지 노드에서는 해당 데이터를 수신하여 암호화된 상태로 연산한다. 이때 덧셈 동형을 지원하는 Paillier 시스템을 사용하였으며 암호화된 최종 결과를 얻은 후 이를 클라이언트에 반환하도록 한다. 이처럼 블록체인과 엣지컴퓨팅 그리고 동형암호화의 장점을 결합하여 블록체인 기반의 분산형 개인정보 보호 아키텍처를 설계하였다.

[6]에서는 스마트 그리드 시스템의 개인정보 보호 문제와 데이터 집계 작업에 대한 계산 및 통신 비용의 한계점을 극복하기 위해 딥 러닝 및 동형 암호화 기반의 개인 정보 보호 데이터 집계 모델을 제안하였다. 훈련을 위해 사용되는 딥러닝 모델은 모든 사용자가 동의한 통합된 모델이 있다. 로컬 데이터를 사용자가 암호화한 후 클라우드 서버에 업로드하면, 서버 A와 B는 데이터들을 집계한 후 로컬 모델에 전송한다. 이때, 동형 암호를 사용하여 암호화 된 상태에서의 집계가 가능하도록 한다. 이후, 로컬에서는 각 사용자가 암호문을 복호화한 후 로컬 모델을 업데이트한다. 이러한 방식으로 사용자의 전기 사용량 데이터를 안전하게 집계하여 예측에 활용할 수 있는 집계모듈을 제공한다. 또한, 스마트 그리드 데이터 분석에서는 데이터 변조 위협이 존재하므로 이를 위해 집계 모듈을 블록체인에 배포함으로써 데이터를 집계하고 블록에 저장할 수 있도록 하였다. 해당 블록체인 모델은 동형 암호화 및 적절한 인증 메커니즘으로 모든 통신에서 개인 정보 보호 및 기밀성을 유지할 수 있다. 따라서 모든 과정에서 집계자는 데이터를 직접 볼 수 없지만 정확한 데이터를 전력센터에 제공할 수 있다. 또한, 데이터가 유효한 소스에서 전송되는 것인지를 인증하는 메커니즘을 통해 데이터 주입 공격 등을 방어할 수 있게 된다. 이외에도 블록체인의 해시함수를 활용하여 가로채기 후 데이터 패킷을 재생하는 공격도 막을 수 있다. 즉, 해당 연구에서는 스마트 그리드 환경에서 가능한 모든 유형의 공격을 차단할 수 있는 블록체인 기반의 개인 정보 보호가 가능한 데이터 집계 모델을 제공하였다. 실험 결과, 집계 계산 비용은 기존의 기술보다 20%~80% 저렴하며, 최소한의 계산 오버헤드를 달성하여 상당한 성능 개선을 보였다.

[7]에서는 데이터 소유자, 클라우드 서비스 제공자, 반신뢰 클라우드 서버 간의 안전한 데이터 공유를 실현하기 위해 영지식 증명에 기반한 블록체인 개인 정보 보호 기법을 제안하였다. 해당 시스템에는 데이터 소유자, 개인 데이터를 소비하는 클라우드 서비스 조직, 반신뢰 클라우드 서버, 개인키 생성자, 스마트 컨트랙트, 블록체인이라는 총 6개의 엔터티가 있다. 각 엔터티는 블록체인에 등록된 후, 개인키 생성자가 공통 개인키 쌍을 사용자에게 할당한다. 클라우드 서비스 제공자는 데이터 소유자가 제공한 데이터가 자신의 요구 사항을 충족하는 것을 믿을 수 없으므로 스마트 계약을 사용하여 데이터 요구 사항에 대한 일관성과 효율성을 보장하고자 한다. 따라서 zk-SNARK를 통해 필요한 데이터의 영지식 증명을 생성하고 계산결과와 해시 값을 스마트 컨트랙트에 보내고 필요 키워드를 블록체인에 업로드한다. 데이터 소유자는 클라우드 서비스 제공자가 업로드한 블록체인의 키워드를 보고 그들이 요구하는 개인 데이터를 암호화한 후 반신뢰 서버에 암호화된 데이터를 전송하고, 서명된 해시 값을 블록체인에 기록한다. 이와 동시에 스마트 컨트랙트에 영지식 증명, 계산 결과, 해시값이 전송되며, 컨트랙트 실행을 통해 클라우드 서비

스 제공자가 전송한 값과 자동 비교가 수행된다. 영지식 증명이 검증된 후에는 데이터 소유자가 클라우드 서비스 조직의 공개키를 사용하여 재암호화를 위한 재암호화 키를 생성한다. 그리고 반신뢰 서버는 재암호화를 실행하여 데이터 소유자로부터 받은 암호문을 중간 암호문으로 변환한 후 클라우드 서비스 제공자에게 전송한다. 이후, 클라우드 서비스 제공자는 개인키를 사용하여 복호화함으로써 필요로 하는 개인 데이터를 얻고 블록체인의 데이터와 비교하여 무결성을 검증한다. 이처럼 영지식 증명에 기반한 블록체인을 활용하여 각 엔터티 간의 신뢰할 수 있고 안전한 데이터 공유가 가능하도록 한다.

IV. 결론

본 논문에서는 영지식 증명과 동형암호 체계를 활용한 블록체인 시스템 동향에 대해 살펴보았다. 동형 암호를 적용할 경우 개인 정보를 드러내지 않은 채로 연산이 가능하므로 블록체인 기반의 스마트 컨트랙트 거래에서 금액 또는 계좌 정보를 숨긴 채로 데이터 연산이 가능하도록 하는 등과 같이 활용할 수 있다. 그러나 이처럼 암호화된 상태로 데이터를 처리하면 실제 사용자의 데이터를 알 수 없으므로 그에 대한 검증 과정이 필요해진다. 이를 위해 영지식 증명이 사용되며, 스마트 컨트랙트를 통해 거래되는 금액 검증, 공유되는 데이터가 옳은 데이터인지에 대한 확인 등이 가능해진다. 이처럼 영지식 증명과 동형암호 모두 블록체인 상에서의 개인 정보 보호의 측면에서 활용되고 있다.

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, 100%).

[참고문헌]

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[2] G.Y.Lee, “Trends in Personal InformationProtection and Management Technology for BigData Utilization,” Information &CommunicationsMagazine, 37(1), pp. 32-39, 2019.

[3] 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.

[4] Solomon, R., & Almashaqbeh, G. (2021). smartfhe: Privacy-preserving smart contracts from fully homomorphic encryption. Cryptology ePrint Archive.

[5] Yan, Xiaoyan, Qilin Wu, and Youming Sun. "A homomorphic encryption and privacy protection method based on blockchain and edge computing." Wireless Communications and Mobile Computing 2020 (2020).

[6] Singh, Parminder, et al. "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid." Computers & Electrical Engineering 93 (2021): 107209.

[7] Feng, Tao, et al. "Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof." Wireless Communications and Mobile Computing 2022 (2022).