블록체인 시스템에서의 프라이버시 보호 기술 동향 분석

이태혁[1], 강명조[1], 김미희[2]
[1]한경대학교 컴퓨터응용수학부
[2]한경대학교 컴퓨터응용수학부, 컴퓨터시스템연구소
e-mail:[2017421041, rkdaudwh13, mhkim]@hknu.ac.kr

Analysis of Privacy Protection Technology Trends in Blockchain Systems

Tae-Hyeok Lee[1], Myung-Joe Kang[1], Mi-Hui Kim[2]
[1]School of Computer Engineering & Applied Mathematics, Hankyong National University
[2]School of Computer Engineering & Applied Mathematics, Computer System Institute Hankyong National University

요 약

최초 블록체인 시스템 비트코인이 나온 이후 현재 이를 활용한 다양한 기술들이 나오고 있다. 블록체인은 탈중앙성, 무결성, 보안성, 투명성 등 여러 가지 특성들을 가지고 있다. 블록체인의 투명성은 블록체인의 모든 데이터가 모두에게 공개된다는 특징으로 많은 관심을 가졌으나 이러한 특징은 블록체인이 실생활 도입의 활용도를 낮추고 있는 추세이다. 그래서 이를 보완하기 위해서 블록체인 시스템에서 프라이버시 보호 기술들 즉, 링서명, 영지식 증명, 프라이빗 샌드 등을 활용한 다양한 프로토콜이 등장하고 있다. 이에 본 논문에서는 이러한 기술들의 특징과 장단점을 분석하고자 한다.

1. 서론

블록체인(BlockChain)이란 데이터를 '블록'에 저장하여 P2P방식을 기반으로 그러한 블록을 체인 형태로 연결하는 분산 컴퓨팅 기술이다. 이러한 블록체인은 투명성이라는 특징을 가지고 있는데 이는 거래 내용 과정을 모두가 확인할 수 있다는 것이다. 다만 이러한 특징을 모두가 좋아하는 것은 아니다. 왜냐하면 자신의 거래 내용이나 계좌정보를 모두가 알 수 있기 때문이다.

이러한 특징은 현재 블록체인이 여러 실생활에 적용되는데 하나의 걸림돌이 되고 있다. 그래서 많은 연구자들은 블록체인의 내용을 모두가 알 수 없도록 보호하는 연구가 꾸준히 진행되고 있다. 본 논문은 현재 사용되고 있는 블록체인 시스템에서의 다양한 프라이버시 보호 기술에 대해 서술하고 이러한 기술들이 현재 적용되고 있는 사례에 대해서 알아보며 장점과 단점에 대해 분석하고자 한다.

2. 다양한 프라이버시 보호 기술과 장단점

2-1. 링서명

링 서명 기술[1]이란 하나의 링이라는 원형에 속해있는 그룹을 생각하면 좋다. 한 그룹에 속해있는 A가 거래를 원할 때 거래의 내용(m)을 자신의 개인키(S_i)로 암호화하고 그러한 거래내용을 그 그룹에 속하는 인원들(n)의 공개키(P_L)와 섞어서 사용자를 추적불가능하게 만드는 서명 기술이다. 이때 송신자는 링의 크기를 설정하는데 링의 크기가 클수록 거래의 크기도 커지고 이에 따른 수수료 또한 증가한다. 이를 통해 생성된 서명 값은 $\sigma = Enc(m, S_i, P_L, \cdot \cdot \cdot P_n)$으로 표현 가능하다.

이러한 기술은 생성자의 익명성이 보호되고 그룹으로 만들어지기 때문에 거래의 내용 또한 알 수 없지만 다만 거래의 생성자가 불분명하기 때문에 이중지불 공격에 대해 취약하다. 이러한 기술을 활용하여 만들어진 대표적인 코인으로는 모네로의 링CT 기술이 있다. 또한 이를 활용하여 의료, 투표 등 여러 분야에 적용하기 위한 기술들[2]이 현재 개발되어 지고 있으나 이는 복잡한 연산을 필요로 하여 거래의 크기가 커질 수밖에 없어 이를 보완하기 위한 성능 개선을 필요로 한다.

2-2. 영지식 증명(Zero Knowledge Proof, ZKP)

영지식 증명(ZKP)이란 증명자가 자신이 알고있는 지식이나 자신이 알고 있는 지식과 정보를 공개하지 않으면서 그 지식을 알고 있다는 사실을 검증자에게 증명하는 방식이다[3]. 즉, 검증자는 문제를 하나 공개해 만일 증명자가 자신을 공개하지 않고 이 문제의 정답을 말했을 경우 검증자는 다른 별도의 인증 없이 정당한 사용자임을 승인해 준다.

영지식 증명은 다음과 같은 수학적 정의를 사용한다. $\forall x \in L, z \in 0,1^*, View_v[P(x) \leftrightarrow V(x,z)] = S(x,z)$

P(x): 증명자

V(x, z): 검증자

←→: 검증자와 증명자간의 검증 과정

View: interactive proof 과정을 관찰하여 기록한 것

z: 검증자의 질의 값

이를 알리바바의 동굴에 대입하면 다음과 같다. 증명자가 A혹은 B 입구로 들어가면 검증자는 증명자를 A로 나오게 할지, B로 나오게 할지를 z 값으로 결정한다. 이 과정을 반복하고 이를 기록하여 같은 결과가 나오도록 한다. 이렇게 보면 과정이 단순한 것 같지만 이는 매우 엄격한 수학적 증명을 요구하기에 시스템이 매우 복잡해질 수 있다. 또한 시스템 설정이 조금만 변경되어도 이를 유지하지 못하게 된다.

2-3 프라이빗샌드

프라이빗샌드[4]는 대시코인에서 사용되는 프라이버시 보호 기술로 여러 개의 거래를 모아서 하나의 익명거래로 병합하는 믹싱 기술을 사용한다. 믹싱기술이란 어디에서 코인을 받고 누구에게 코인을 보내는지에 대한 정보를 알 수 없도록 숨기는 기술을 의미한다. 이때 모든 정보는 풀노드인 마스터 노드만 알아 볼 수 있도록 마스터 노드의 공개키를 이용한 암호화를 통해 익명성을 보장한다. 또한 이 암호화된 정보를 한 곳에 모아 믹싱 과정을 수행하여 거래 과정 또한 감추게 된다.

이러한 기술은 전자투표에서 익명성을 보장하기 위한 방법으로의 사용이 연구되고 있다[5]. 링서명이나 영지식 증명은 투표 시 송금액이 일정하고 수신자도 쉽게 특정할 수 있기에 적용이 쉽지 않다. 대신 프라이빗 샌드의 믹싱기술은 마스터노드에 동일한 프라이빗 샌드를 요청하는 사람들을 하나로 묶어 이를 믹싱하는 방식이기에 누가 누구에게 해당 투표를 했는지 알 수 없다. 또한 마스터노드도 송신자의 개인정보를 식별할 수 있는 어떠한 내용도 전송되지 않는 방식으로 익명성을 보장하게 된다.

<표1>은 지금까지 소개한 프라이버시 보호 기술의 장단점을 비교한 표이다.

	장점	단점
링 서명	신원이나 공개키 등의 노출 없이도 다른 구성원들로부터 트랜잭션 검증 가능	그룹원의 수가 많아지면 서명 값도 이에 비례하여 길어짐
영지식 증명	증명 값만으로 데이터의 참 거짓 확인 가능	복잡한 수학적 증명을 요구하기 때문에 시스템이 복잡해짐
프라이빗 샌드	마스터 노드로 신속성과 익명성이 보장된다.	같은 단위로 전송되는 코인이 있어야 해당 과정이 수행됨

<표1> 프라이버시 보호 기술별 장단점

3. 결론

블록체인 기술은 2009년 개발된 비트코인 기반 암호화폐 기술로, 제3의 신용기관 없이도 네트워크 참여자들 간에 신뢰할 수 있는 거래가 가능하게 함으로써 디지털 인프라에 탈집중화, 수평적인 디지털 비즈니스의 기반이 될 수 있다. 오늘날 인터넷이 가진 문제점들을 해결할 수 있는 강력한 기술이라는 점에서 현재의 중앙집중식 거래 및 기록 관리 메커니즘에서 근본적으로 벗어나 기존 시장경제의 생태계에 혁신적인 플랫폼으로 불리고 있다.

다만 거래에 대한 기록 및 저장하는 과정에서 거래내역, 과정, 금액 등 모든 것이 노출된다는 것이 현재 블록체인이 실생활에 적용되는데 많은 걸림돌이 되고 있다. 이를 해결하기 위해 다양한 보호기술들 또한 아직은 높은 컴퓨팅 기술을 요구하거나 이를 악용할 경우 그에 대한 대처가 취약하다는 단점이 여전히 존재한다. 이러한 측면이 개선이 된다면 블록체인은 앞으로 다양한 분야에서 활용될 수 있기에 블록체인 시스템에서 적절한 프라이버시 보호 기술 연구는 필수적이다.

4. Acknowledgement

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620), 교신저자 김미희.

참고문헌

[1] Ji-Sun Park, Sang Uk Shin “Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection" Journal of Internet Computing and Services, no.6, pp.105 - 117, 2019년

[2] Lee Deoksang. "MEXchange: Privacy-preserving Blockchainbased Framework for Health Information Exchange using Ring Signature and Stealth Address", 학위논문(석사)-포항공과대학교 일반대학원, 2020년

[3] 황진주, 김근형 “블록체인 기반 자기주권 신원 시스템의 영지식 증명 기술 연구”. 한국정보처리학회 학술대회논문집 28권2호,pp.355-358

[4] 프라이빗 샌드 : https://docs.dash.org/ko/0.12.3/introduction/features.html

[5] Jae-Han Cho, Lee-Sub Lee, Chang-Hoon Choi “Anonymous Blockchain Voting Model using the Master NodeNetwork”, Journal of the Korea Academia-Industrial cooperation Society v.22 no.5, pp.394 - 402, 2021년