JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 5: 604~612, May 2019

PKI 인터넷 뱅킹과 블록체인 지불 거래의 비교 분석

박승철*

A Comparative Analysis of PKI Internet Banking and Blockchain Payment Transactions

Seungchul Park*

*Professor, School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam, 31253 Korea

요 약

PKI(Public Key Infrastructure) 인터넷 뱅킹은 서명 검증을 위한 공개키(public key)를 신원 정보와 함께 서버에 등록하고, 등록된 공개키를 사용하여 사용자 인증과 거래 인증을 위한 서명을 검증하는 데 활용한다. 반면, 비트코인 등 블록체인 기반의 금융 거래 시스템은 공개키 암호 기반의 디지털 서명에 근거한 인증 체계를 채택하고 있음에도 불구하고, P2P(peer-to-peer) 방식으로 지불 거래를 수행하므로 공개키를 등록할 수 있는 서버가 존재하지 않는다. 본 논문은 기존의 대표적인 인터넷 뱅킹 방식인 PKI 인터넷 뱅킹과 블록체인 지불 거래의 차이를 분석하고 블록체인 지불 거래의 장단점을 파악하는데 목적이 있다. 이를 통해 본 논문은 블록체인 지불 시스템이 보편적인 금융 거래에 활용되기 위한 구조적 측면과 보안성 측면의 개선방향을 제시하고자 한다.

ABSTRACT

PKI Internet banking is used to have users register their public keys with the banking server together with the identity information, and verify the signature for both user and transaction authentications by using the registered public keys. Although the Blockchain-based financial systems such as Bitcoin adopt similar digital signature-based authentication scheme, there is no server that participants can register public keys with because they perform P2P payment transactions. The purpose of this paper is to identify the advantages and disadvantages of the Blockchain-based payment transactions by analyzing the differences between the most common PKI Internet banking and Blockchain payment systems. Based on the analysis, this paper suggests the issues that need to be enhanced from the aspects of architecture and security in order for Blockchain payment transaction systems to be applied universally.

키워드 : 인터넷 뱅킹, PKI, 블록체인, 비트코인, 핀테크

Keywords : Internet banking, PKI, Blockchain, Bitcoin, FinTech

Received 11 February 2019, **Revised** 15 February 2019, **Accepted** 20 February 2019

*** Corresponding Author** Seungchul Park(E-mail:scpark@koreatech.ac.kr, Tel:+82-41-560-1492)
Professor, School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam, 31253 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.5.604 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

사토시 나카모토(Satoshi Nakamoto)에 의해 2008년 11월 비트코인[1]이 발표된 이후 블록체인(Blockchain) 기반의 전자 화폐 지불 거래(electronic cash payment transaction)에 대한 관심이 크게 고조되어 왔다. 블록체인 기반의 지불 거래 시스템은 모든 거래 내역을 안전하고 투명한 블록체인에 기록하고, 블록체인의 생성과 유지를 특정 기관에 의존하지 않고 분산적으로 수행하며, 모든 참여자가 블록체인을 유지하고 내용을 확인하고 검증할 수 있게 함으로써, 지불의 안전성을 담보하는 제3의 신뢰 기관을 경유하지 않는 P2P(peer-to-peer) 지불 거래를 가능하게 한다[2]. 따라서 블록체인 기반의 지불 거래 시스템은 제3의 신뢰 기관 구축과 경유 비용 회피를 가능하게 함으로써 저비용 금융 시스템 구축을 용이하게 하게하고, 제3의 기관에 의존하지 않는 참여자간의 자유로운 금융 거래 서비스 개발을 가능하게 할뿐만 아니라, 제3의 기관을 통한 거래 관련 프라이버시 노출로부터 자유로울 수 있는 장점을 제공한다. 그럼에도 불구하고 블록체인 기반의 많은 지불 거래 시스템들이 실생활에서 보편적인 지불 거래에 활용되기에는 기술적인 측면에서, 보안 관리 측면에서, 그리고 서비스 이용의 편의성 측면에서 아직 여러 가지 문제점을 노출하고 하고 있다[3].

기존의 디지털 서명 기반의 PKI 인터넷 뱅킹 시스템과 마찬가지로 블록체인 지불 거래 시스템은 공개키 암호(public key cryptography) 체계의 디지털 서명에 근거하여 거래 송신자와 거래 내용에 대한 인증 서비스를 제공한다. 즉, 거래 송신자의 서명 검증을 통해 송신자가 블록체인 상에서 해당 자금의 소유자임을 확인하고, 거래의 내용이 해당 소유자에 의해 작성되었음을 확인한다. 기존의 PKI 인터넷 뱅킹에서는 디지털 서명 검증을 위해 사용자 계좌(account)와 연결된 공개키를 사전에 서버에 등록하게 하게 한다. PKI 인터넷 뱅킹에서 공개키 등록 방법은 사용자 개인의 공개키 인증서를 등록하게 하는 PKI(Public Key Infrastructure) 기법과, 인증서는 인증 장치 제조 기관(예, 스마트폰 제조업체)에 대해 발행하고, 사용자의 공개키는 인증 장치가 생성하여 사용자를 대신하여 서버에 등록하는 FIDO(Fast IDentity Online) 기법이 사용되고 있다[4]. 이후 사용자가 인터넷 뱅킹 서버를 접근할 때 디지털 서명을 제시함으로써 사용자 인증을 수행한다. 그리고 거래를 확정하기 전에 사용자가 거래 결과에 대한 서명을 제시하고, 서버가 서명을 검증함으로써 거래를 승인하는 과정을 거친다. 승인 결과는 서버에 의해 통보됨으로써 거래 관련자가 거래 결과를 실시간으로 확인할 수 있다. 서버는 거래의 내용에 이상한 점이 발견될 때 이상 징후가 해소될 때까지 해당 거래 승인을 연기할 수 있다. 그리고 거래가 승인된 이후에도 송신자가 거래에 문제점을 발견하면 송신자와 은행과의 오프라인 협의를 통해 해당 거래의 취소 또는 변경을 추진할 수 있다. 또한 공개키와 대응되는 개인키에 문제가 발생하는 경우 새로운 키의 생성과 재등록이 가능하다.

블록체인 지불 거래 시스템은 PKI 인터넷 뱅킹의 클라이언트-서버(client-server) 방식의 거래가 아닌 P2P 방식의 지불 거래를 수행한다. 따라서 디지털 서명 검증과 거래 승인 과정에서 PKI 인터넷 뱅킹과 큰 차이가 있을 수밖에 없다. 블록체인 지불 거래에서 디지털 서명 검증은 블록체인을 유지하는 모든 P2P 노드(node)에 의해 가능해야 하고, 거래의 승인은 블록체인 생성에 참여하는 모든 P2P 노드(비트코인의 경우 블록 채굴자)들의 합의(consensus)를 통해 이루어진다. 디지털 서명 검증과 거래 승인을 담당하는 노드는 거래 송신자에게 알려지지 않는 다수의 익명 노드인 경우가 일반적이다[5]. 따라서 블록체인 지불 거래 시스템에서는 참여자가 서명 검증에 사용될 공개키를 등록할 서버가 존재하지 않기 때문에, 서버를 통한 공개키의 재등록, 거래의 취소와 변경, 그리고 거래 승인 정보의 통보 등의 서비스를 제공하기가 어려울 수밖에 없다. 블록체인 기반의 모든 지불 거래는 서버의 도움 없이 P2P 지불 거래 참여자의 전적인 책임 하에 이루어져야 하는 것이다. 그리고 블록체인 지불 거래의 승인을 위한 블록체인 생성자간의 합의 과정은 시간이 걸리는 작업이다. 그 결과로 거래 송신자는 승인 내역을 실시간으로 확인할 수가 없고, 거래가 승인되어 블록체인이 기록되고 나면 변경이 불가능하다.

본 논문은 새로운 블록체인 지불 거래 시스템을 현재 보편적으로 사용되고 있는 PKI 인터넷 뱅킹과 비교하여 분석함으로써, 블록체인 지불 거래의 장점과 단점을 파악하는 데에 일차적인 목표가 있다. 블록체인 전자 화폐 지불 거래는 현재 가장 널리 알려져 있는 비트코인을 중심으로 분석하고자 한다. 인터넷 뱅킹과의 비교 분석

과정에서 본 논문은, 블록체인 지불 거래가 보편적인 서비스로 발전하기 위해 개선되어야 할 사항들도 함께 제시하고자 한다. 본 논문은 안전하고 사용자 편의적인 블록체인 지불 거래 시스템의 개발과, 사용자들이 블록체인 지불 거래에 대한 정확한 이해를 바탕으로 서비스를 안전하게 활용하는데 기여할 것으로 기대한다.

Ⅱ. 관련 연구

비트코인 발표와 함께 블록체인 개념이 소개된 이후 블록체인 기반의 다양한 응용들이 개발되고 있지만, 가장 관심을 끄는 응용 서비스는 P2P 전자 화폐 지불 서비스이다. 비트코인 시스템은 내부 전자 화폐인 비트코인(BTC) 기반의 지불 서비스를 제공하고 있고, 이더리움 시스템[6]은 이더(ETH) 기반의 전자 화폐 지불 서비스를 스마트 계약과 연계하여 보다 다양한 형태로 제공할 수 있게 한다. 리플 시스템[7]은 내부 화폐인 리플(XRP)을 기반으로 전자 화폐뿐만 아니라 블록체인 기반의 법정 화폐(fiat currency) 지불 거래를 가능하게 한다. 이러한 블록체인 기반의 지불 거래 시스템들은 목표 응용에 차이는 있지만, 특정 서버에 의존하지 않는 P2P 지불 거래 서비스를 공개키 암호 체계에 근거한 디지털 서명 기반으로 제공한다는 점에서 공통점이 있다.

기존의 대표적인 지불 거래 시스템인 PKI 인터넷 뱅킹 시스템에도 공개키 암호 기반의 디지털 서명이 활발하게 적용되어 왔다. 초기 PKI 인터넷 뱅킹의 디지털 서명은 PKI 인증서를 통한 공개키 등록과 인증서의 공개키를 사용한 디지털 서명 검증 방식으로 적용되었으나, 최근 들어서는 개인의 인증서 발급이 불필요한 FIDO 인증 장치를 활용한 디지털 서명 방식이 활발하게 도입되고 있다[8]. PKI 및 FIDO 인터넷 뱅킹과 블록체인 지불 거래 시스템은 공개키 암호 기반의 디지털 서명에 기초한다는 공통점에도 불구하고, 각각 클라이언트-서버 구조와 P2P 구조에 근거한 지불 거래 서비스를 제공한다는 점에서 큰 차이를 가진다. 블록체인 P2P 지불 거래는 거래 안전성에 대한 책임을 전적으로 참여자 개인에게 의존하기 때문에, 거래 참여자가 보안 위협에 노출될 가능성이 커질 수밖에 없다. 실제로 한 조사보고서는 조사 대상자 중 22.5%가 보안 문제로 인해 자신의 비트코인 전자 화폐를 잃어버린 경험이 있는 것으로 보고하고 있다[9].

동일한 디지털 서명에 근거하고 있는 기존 PKI 인터넷 뱅킹과 블록체인 지불 거래의 비교 분석은, 블록체인 지불 거래의 보편적인 지불 서비스로의 발전 가능성 파악과, 안전한 블록체인 지불 거래 시스템 개발, 그리고 안전한 P2P 지불 거래 적용에 대한 큰 학습 효과를 제공할 수 있다. 그럼에도 불구하고 기존의 대표적인 지불 거래 시스템인 PKI 인터넷 뱅킹과 새로운 블록체인 지불 거래 시스템을 구체적으로 비교하는 연구는 거의 이루어지지 않았다. 이는 우리나라를 제외하고는 PKI 공개키 기반의 디지털 서명에 기초한 인터넷 뱅킹 경험이 많지 않고, FIDO 공개키 기반의 인터넷 뱅킹 서비스는 현재 초기 단계에 있기 때문인 것으로 여겨진다. 본 논문에서는 PKI 공인 인증서 기반의 인터넷 뱅킹 경험이 풍부하고, FIDO 공개키 기반의 인터넷 뱅킹 도입이 활발한 우리나라 인터넷 뱅킹 경험을 중심으로, PKI 인터넷 뱅킹과 블록체인 지불 거래를 비교하고자 한다.

Ⅲ. PKI 기반의 인터넷 뱅킹

3.1. 공개키 등록과 사용자 인증

디지털 서명 기반의 PKI 인터넷 뱅킹은 사전에 서명 검증에 필요한 공개키를 뱅킹 서버에 등록하도록 요구한다. 이 과정에서 뱅킹 서버는 공개키와 사용자 신원 정보(계좌 번호, 사용자 이름, 전화 번호, 주소 등)간의 결합 정보를 저장한다. 공개키 등록 방식은 PKI 인증서 방식과 FIDO 인증 장치 방식이 주로 사용되고 있다[4]. PKI 인증서 방식은 인증 기관(certification authority)에서 발급한 개인별 공개키 인증서(public key certificate)를 서버에 등록하고, 공개키에 대응되는 개인키(private key)는 사용자가 패스워드 등으로 자신의 저장 장치에 안전하게 보관한다. 반면 FIDO 방식은 FIDO 인증 기관이 인증 장치 제조업체(예, 스마트폰 제조사)에게 인증서를 발급하고, 인증 제조 업체가가 생산한 인증 장치가 사용자 등록 과정에서 공개키 생성과 등록 절차를 진행한다. 뱅킹 서버는 공개키와 함께 송신된 인증 장치 제조업체의 인증서와 인증 장치의 서명을 확인하고, 공개키와 사용자 신원 정보간의 결합 정보를 저장한다.

그림 1은 공개키 등록과 사용자 인증 과정을 보이고 있다. 공개키 등록이 완료된 이후 사용자가 뱅킹 서버에

접속하고자 하면, 서버는 서명에 사용될 챌린지(challenge) 정보를 클라이언트에게 제공하고, 클라이언트는 패스워드 또는 생체 인증 등을 통해 개인키 소유자 확인 과정을 거친 다음, 디지털 서명을 생성하여 서버에게 제공한다. 서버는 등록된 공개키를 사용하여 사용자의 서명을 검증함으로써 사용자 인증을 완료하고, 서버 접근 허용 여부를 결정한다. 이와 같은 사용자 인증 과정에서 핵심 역할을 하는 정보는 서명에 사용되는 개인키이다. 따라서 개인키의 안전한 보관이 PKI 인터넷 뱅킹 안전에 매우 중요한 문제임을 알 수 있다.

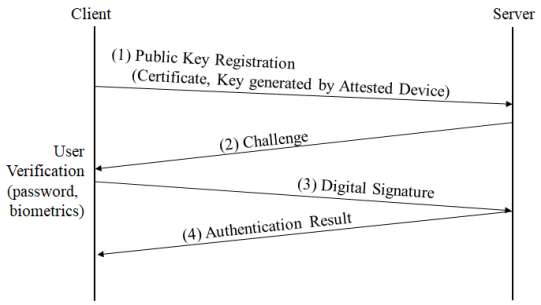

Fig. 1 Registration of Public Key and User Authentication

디지털 서명 기반의 PKI 인터넷 뱅킹이 활성화됨에 따라 개인키를 탈취하기 위한 사이버 공격들도 활발하게 시도되어 왔다. 표 1은 개인키 탈취를 목적으로 우리나라 PKI 인터넷 뱅킹에 대해 시도되어 왔던 사이버 공격 유형과 그에 대한 방어 대책들을 보이고 있다.

Table. 1 Attacks on Internet Banking PKI Private Keys and Countermeasures

attack types	countermeasures
offline phishing for certificate re-issuance	iTAN/OTP deployment
malware-based private key password cracking	iTAN/OTP deployment
online phishing/pharming	OTP, 2nd channel authentication
storage hacking	OTP, HSM/USIM deployment

FIDO 인터넷 뱅킹의 경우 인증 장치 제조업체에 대한 인증서 발급 과정에서 개인키 보호 메카니즘의 안전성을 확인하고, 뱅킹 서버는 인증 장치에서 생성된 공개키 등록과정에서 제조사의 인증서를 확인함으로써 대응되는 개인키의 안전성을 확인할 수 있다. 뱅킹 서버는 인증 장치의 안전성을 평가하여 이체 한도 등에서 차별적인 서비스 도입으로 위험도를 낮출 수 있다. 결과적으로 PKI 인터넷 뱅킹은 사용자와 뱅킹 서버가 상호 협력함으로써 안전한 인터넷 뱅킹 거래를 만들어 왔음을 알 수 있다.

3.2. 공개키 등록과 사용자 인증

PKI 인터넷 뱅킹은 사용자 인증과 별도로 거래 수행 내용에 대한 인증을 진행한다. PKI 인터넷 뱅킹 거래 인증 과정은 그림 2와 같다. 거래 인증 과정에서 사용자는 사용자 인터페이스를 통해 예비 거래의 결과를 확인할 수 있고, 확인한 거래 내용에 대해 거래 서명을 함으로써 뱅킹 서버에게 거래를 최종적으로 확정하도록 요청한다. 거래 서명을 수신한 뱅킹 서버는 해당 거래 결과를 원장(ledger)에 반영하고 거래를 확정한 후, 그 결과를 사용자에게 통보한다. 필요하면 확정된 거래 결과를 거래 송신자뿐만 아니라 수신자에게도 통보한다.

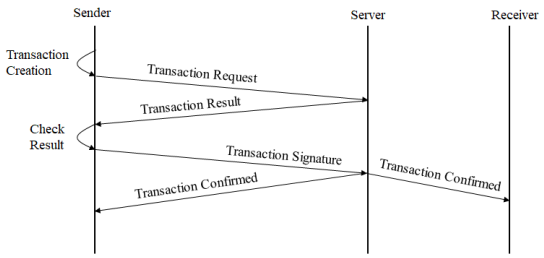

Fig. 2 PKI Transaction Authentication

PKI 인터넷 뱅킹 거래의 결과는 뱅킹 서버의 원장에만 기록되면 확정되기 때문에, 뱅킹 서버의 거래 확정 시점에서 거래가 완료된다. 따라서 사용자가 거래 서명을 제시하는 즉시 실시간으로 거래가 완료됨을 알 수 있고, 서버에 의해 거래 결과는 사용자에게 실시간으로 통보되는 시스템이다. 만약 실행한 거래에 이상이 발견되면 사용자는 즉시 오프라인으로 은행과 통신하고 대처할 수 있다.

오래전부터 디지털 서명 기반의 거래 인증 과정에서의 사이버 공격의 위험성이 예측되어 왔었고[10, 11], 2013년 말 실제로 PKI 서명 기반의 인터넷 뱅킹에서 거래 인증의 내용을 속이는 메모리 해킹(memory hacking) 공격이 발생하였다[12]. 브라우저의 응용으로 동작하는

클라이언트의 메모리상의 정보(계좌 번호, 금액 등)를 악성 소프트웨어를 사용하여 변경하는 공격이다. 표 2에서 보는 바와 같이 이 공격에 대한 대응책으로 키보드에서 입력된 거래 정보를 즉시 암호화하고, 암호화된 정보를 웹 메모리에서 거래 서명이 이루어진 정보와 함께 전송한 후 뱅킹 서버가 비교할 수 있게 하는 종단간 확장 암호화(end-to-end encryption extension) 기능이 구현되었다. 또한 거래 과정에서 수신 계좌 등이 변경될 때 2채널 인증을 통해 재확인하는 방법을 도입되었다[10]. 이상 거래 탐지 시스템(FDS – Fraud Detection System)의 도입도 메모리 해킹 공격 방어에 도움이 된다.

Table. 2 Attack on PKI Internet Banking Transaction Signature and Countermeasures

attack types	countermeasures
web memory hacking	extension of end-to-end encryption, 2nd channel authentication, fraud detection system

Ⅳ. 블록체인 지불 거래 시스템

4.1. P2P 시스템 구조

인터넷 뱅킹은 클라이언트-서버 방식으로 사용자 클라이언트(client)의 지불 거래 요청을 중앙의 뱅킹 서버(banking server)가 검증하고 한다. 그리고 거래 결과 정보는 뱅킹 서버가 비공개로 안전하게 유지한다. 반면, 블록체인 지불 거래 시스템은 거래의 검증과 승인을 중앙의 특정 서버에 의존하지 않고 기본적으로 P2P 방식으로 참여자들이 자발적으로 수행한다. 일정한 기간 동안 승인된 거래의 결과는 블록(block)으로 모아져 이전의 블록과 해시포인터(hash pointer)로 연결됨으로써 블록체인으로 저장된다. 그림 3에서 보는 것과 같이 블록체인 생성에 자발적으로 참여하는 참여자는 비트코인의 경우 채굴자(miner peer)로 불리고, 다수의 채굴자가 동일한 조건에서 합의를 통해 블록 생성에 참여한다. 생성된 블록은 채굴자들 포함한 모든 참여자들에게 전달되고, 원하는 참여자는 누구나 블록체인을 유지하고, 검색하고, 검증할 수 있다.

블록체인에 연결되는 블록에 거래들을 포함시키는 행위는 거래 결과를 원장(ledger)에 저장하는 거래 승인 작업에 해당한다. 어떤 거래들을 블록에 포함시켜 승인할 것인지는 블록 채굴자들의 합의(consensus)에 의해 결정된다. 합의 프로토콜은 블록체인의 유형에 따라 다를 수 있으나, 비트코인과 이더리움 같은 대표적인 블록체인 지불 거래 시스템은 작업 증명(proof of work)과 블록 인센티브(block incentive) 기반의 합의 프로토콜을 사용한다.

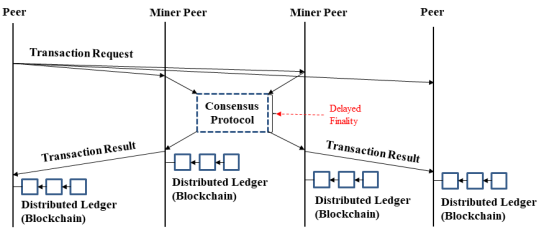

Fig. 3 Architecture of Blockchain Payment Transaction System

거래를 생성하여 네트워크로 송신하는 참여자는 누가 블록 생성자가 될 것인지 알지 못하는 상태에서 거래를 송신한다. 따라서 인터넷 뱅킹과 달리 블록체인 지불 거래 시스템에서는 서명 검증에 사용될 공개키를 사전에 등록할 방법이 없다. 그리고 합의 프로토콜은 채굴자들간의 통신을 통해 블록의 내용을 결정하기 때문에 합의 프로토콜을 통한 거래의 승인은 시간이 걸리는 작업이다. 비트코인의 경우 거래의 승인에 10분 이상이 걸리고 민감한 거래의 경우 거래의 승인에 60분 이상이 걸리기도 한다. 이더리움 같은 경우 14초에서 수분 정도가 걸린다[13]. 블록체인 지불 거래는 기본적으로 실시간 완료성(realtime finality)을 지원하지 않는 것이다. 블록체인의 각 블록이 채굴자들간에 합의되기 위해서는 블록을 상호 공유해야 한다. 블록의 크기가 너무 큰 경우 블록 전달 지연시간이 커지고, 이는 합의에 걸리는 시간의 상승 요인이 되기 때문에, 블록의 크기에 제약이 있을 수밖에 없다. 블록 크기의 제약은 단위 시간에 승인할 수 있는 거래 수의 제약으로 연결되고, 이는 블록체인 지불 거래 시스템의 거래 처리 용량 확대에 걸림돌로 작용하고 있다. 비트코인의 경우 초당 약 7 거래의 처리 용량을 지원한다[14].

4.2. P2P 시스템 구조

그림 4는 블록체인 지불 거래에서 주소 사용과 서명 검증 방식을 보이고 있다. 블록체인 지불 거래는 거래

참여자의 서명 검증을 위한 공개키를 등록하는 대신, 공개키로부터 추출되는 주소를 사용함으로써 공개키 등록 없이도 거래 송신자의 서명 검증을 가능하게 한다. 즉, 블록체인 참여자는 다음과 같이 자신의 공개키의 해시값(hash value)을 주소로 사용한다.

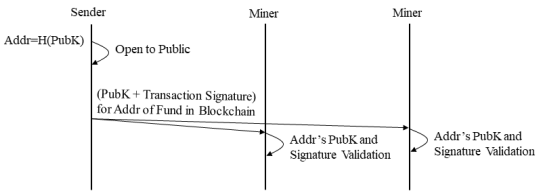

Fig. 4 Address Usage and Signature Validation of Blockchain Payment Transactions

Addr = H(public key), 여기서 H()는 해시함수.

거래 송신자는 블록체인 상에서 자신의 주소에 저장된 자금(fund)을 지불 거래에 사용하기 위해, 주소에 대응되는 서명과 공개키를 제시함으로써 해당 자금의 소유자 인증과 거래 인증을 동시에 시도하는 것이다. 거래 승인에 참여하는 채굴자들은 주소에 대응되는 공개키를 확인하고, 공개키를 사용하여 서명을 검증함으로써 해당 거래의 송신자가 해당 주소의 소유자임을 인증하고, 거래가 해당 주소의 소유자에 의해 송신된 거래임을 인증한다.

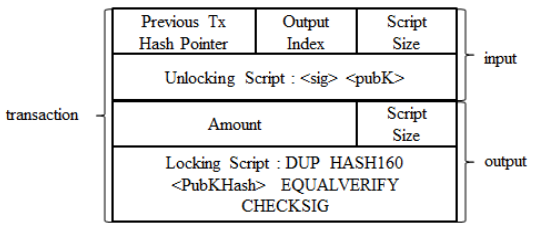

Fig. 5 Structure of Bitcoin Payment Transaction

그림 5는 비트코인 지불 거래의 자료 구조를 보이고 있다. 거래 송신자는 지불할 자금이 저장된 블록체인 상의 이전 거래(previous transaction)의 출력값 인덱스(output index)에 대한 서명(<sig>)과 공개키(<pubK>)를 제시함으로써, 이전 거래의 출력값에 저장된 금액(amount)의 소유자임을 증명하는 것이다. 해당 거래의 출력값에는 송신할 금액(amount)과 수신자의 주소가 (<PubKHash>) 포함된 소유자 증명 방법(잠금 스크립트, locking script)이 포함된다. 그림 5의 거래 자료 구조의 출력값의 잠금 스크립트는 서명과 공개키를 제시하도록 요구한다. 추후 해당 지불 거래의 수신자는 주소에 대응되는 서명과 공개키를 제시함으로써 해당 자금의 소유자임을 증명할 수 있는 것이다.

기존 PKI 인터넷 뱅킹은 공개키의 등록과 인증을 분리하고, 등록된 공개키를 사용하므로 사용자 인증과 거래 인증을 분리하여 수행할 수 있다. 또한 뱅킹 서버가 공개키에 결합된 신원 정보를 유지하고 있기 때문에 서명 검증의 안전성을 보완할 수 있는 OTP, SMS 등 제2, 제3의 채널을 사용한 인증을 추가할 수 있다. 반면, 공개키를 등록할 수 없는 블록체인 지불 거래의 경우 사용자(거래 송신자) 인증과 거래 인증을 통합하여 수행함을 알 수 있다. 그리고 채굴자들이 공개키와 결합된 사용자 신원 정보를 유지하고 있지 않고 사용자와의 통신 수단을 보유하지 않기 때문에 서명의 안전성을 보완할 수 있는 추가적인 인증 수단이 사용될 수 없다. 즉, 서명의 검증이 블록체인 지불 거래의 사용자 인증과 거래 인증의 유일한 수단으로 사용될 수밖에 없음을 알 수 있다.

Ⅴ. 비교 분석과 제언

5.1. 구조적 측면

표 3은 구조적인 측면에서 디지털 서명 기반의 PKI 인터넷 뱅킹과 블록체인 지불 거래의 비교 결과를 요약하고 있다. PKI 인터넷 뱅킹은 클라이언트-서버 모델에 근거하여 뱅킹 서버가 거래를 승인하고, 거래 결과 정보를 유지하고 관리한다. 클라이언트인 사용자는 전적으로 뱅킹 서버를 신뢰하고, 뱅킹 서버에 자신의 민감한 개인 정보를 제공한다. 반면 블록체인 지불 거래는 P2P(peer-to-peer) 모델에 근거하여 임의의 채굴자 피어들이 합의 프로토콜을 통해 거래를 승인하고, 거래 결과를 분산 블록체인에 안전하고 투명하게 유지하고 관리하며, 지불 거래 승인을 위해 사용자의 비밀 정보 등록을 요구하지 않는다. 따라서 블록체인 지불 거래는 서버 고장에 따른 전체 서비스 마비, 서버 해킹에 따른 전체 고객 비밀 정보 유출 등과 같은 단일 장애 지점(single point of failure)으로부터 자유롭고, 뱅킹 서버에 의한 개인 정보 검열의 우려로부터 자유로우며, 투명한 거래

서비스를 제공할 수 있는 장점이 있다. 그러나 P2P 블록체인 지불 거래는 거래 결과를 모니터링하고 책임지는 중앙의 서버가 존재하지 않기 때문에, 실행된 거래에 문제점이 발견되더라도 이를 되돌릴 수 있는 방법이 존재하지 않고, 거래 승인을 위한 참여자간 합의 프로토콜 수행에 시간이 많이 걸리기 때문에 실시간 거래 완료성(realtime transaction finality)을 지원하기 어려운 단점을 가진다. 또한 합의 과정에서 교환하는 거래 정보를 담은 블록(block)의 크기가 커질 경우 블록 전달 지연시간이 커지고, 이는 합의 프로토콜 수행 시간의 증가로 연결되기 때문에 블록 당 수용할 수 있는 거래의 수를 늘리는데 제약이 따를 수밖에 없다. 따라서 벵킹 서버가 자체적으로 처리 용량을 늘릴 수 있는 인터넷 뱅킹에 비해, 블록체인 지불 거래는 거래 처리율이 상대적으로 낮고 용량을 늘리는 데에도 제약이 많을 수밖에 없다.

Table. 3 Architectural Comparison of PKI Internet Banking and Blockchain Payment Transaction

items	PKI Internet Banking	Blockchain Payment
service model	client-server	P2P
single point of failure	yes	no
censorship	yes	no
transparency	no	yes
reversibility	yes	no
transaction finality	realtime	delayed
throughput	high(extensible)	low(constrained)
public key registration	yes	no
key renewal	yes	no
user and transaction authentication	separated	integrated

디지털 서명 기반의 PKI 인터넷 뱅킹에서는 기본적으로 공개키를 서버에 등록하고, 등록된 공개키를 서명 검증에 사용한다. 만약 서명에 사용하는 개인키가 노출되는 등의 문제가 발생하는 경우, 새로운 키 쌍(key pair)을 생성하여 등록된 공개키를 갱신할 수 있다. 그리고 뱅킹 서버와 대화 형식의 통신이 가능하기 때문에 거래 과정에서 등록된 공개키를 사용하여 사용자 인증을 먼저 수행하고, 최종적으로 사용자가 거래 내역을 확인한 후 거래 서명을 통해 거래 인증을 수행할 수 있다. 그러나 블록체인 지불 거래에서는 공개키 등록 대상인 중앙의 서버가 존재하지 않는다. 따라서 공개키 등록과 등록된 공개키의 갱신을 지원할 수 없고, 서버와의 대화를 통한 사용자 인증과 거래 인증의 분리 수행이 불가능하다. 사용자는 사용자 인증과 거래 인증에 필요한 모든 정보를 담은 거래를 네트워크로 한번 송신하는 것으로 모든 거래 행위는 종료된다.

5.2. 보안 측면

PKI 인터넷 뱅킹과 블록체인 지불 거래 모두 디지털 서명을 사용하여 거래의 보안을 유지하지만, 보안 침해의 결과와 대응의 관점에서는 많은 차이가 있다. 표 4는 거래 보안 측면에서 디지털 서명 기반의 PKI 인터넷 뱅킹과 블록체인 지불 거래의 비교 결과를 요약하고 있다.

Table. 4 Security Comparison of PKI Internet Banking and Blockchain Payment Transaction

items		Internet Banking	Blockchain Payment
protection for key thefts	password	○	○
	biometrics	○	○
	HSM	○	○
protection for transaction	iTAN/OTP	○	×
	extended encryption	○	×
	2nd channel	○	×
	FDS	○	×
	HSM with transaction signature	○	○
key loss		key renewal	money loss

기본적으로 디지털 서명 생성을 위한 개인키(private key)를 안전하게 유지하는 것은 PKI 인터넷 뱅킹과 블록체인 지불 거래 모두에서 전적으로 사용자 개인의 몫이다. PKI 인터넷 뱅킹에서와 마찬가지로 블록체인 지불 거래의 클라이언트 장치는 안전한 장소에 개인키를 저장하고 패스워드(password), 생체 정보(biometrics) 등을 사용하여 개인키 접근을 차단함으로써 개인키 도난을 방지할 수 있다. 그리고 악성 소프트웨어 접근을 원천적으로 어렵게 만드는 HSM(Hardware Security

Module)을 이용하여 개인키를 보호할 수도 있다. 이와 같이 개인키의 보호 측면에서 보면 PKI 인터넷 뱅킹과 블록체인 지불 거래는 동일한 보호 메카니즘을 사용할 수 있다.

개인키가 공격자에게 도난되어 사용자 인증이 도용되는 경우를 대비하여 뱅킹 서버는 보안 카드(iTAN), OTP 등의 추가적인 사용자 인증 수단을 제공할 수 있고, 거래 정보의 조작을 탐지하기 위해 키보드 입력에 대한 확장된 종단간 암호화, 제2 채널을 이용한 거래 인증, 그리고 이상 거래 탐지 시스템(FDS)등을 도입할 수 있다. 그러나 블록체인 지불 거래의 경우 사용자가 추가적인 인증 정보를 제공하거나, 사용자 거래를 모니터링 할 수 있는 신뢰할 수 있는 서버가 존재하지 않기 때문에 이러한 추가적인 인증 수단 사용이 적용될 수가 없다. 즉, 디지털 서명을 위한 개인키가 공격자에게 도난되는 경우 블록체인의 피해자의 자금이 공격자의 접근에 완전히 노출되는 것이다. PKI 인터넷 뱅킹에 대한 메모리 해킹 공격의 경우 개인키 보호를 위한 인증 정보의 노출이 없는 경우에도 공격자가 거래 정보 조작을 통해 피해자의 자금을 가로챈다. 거래 정보 확인과 거래 서명 기능을 가진 하드웨어 보안 모듈(거래 서명 가능 HSM)은 개인키 보호와 메모리 해킹 공격 방어에 효과적인 수단이 된다. HSM을 통한 거래 서명은 블록체인 지불 거래에서도 안전한 거래를 위한 효과적인 수단이 될 수 있다.

만약 사용자가 어떤 이유로 개인키를 분실하는 경우 어떤 결과가 발생할까? PKI 인터넷 뱅킹의 경우 기존 공개키 등록 과정에서 등록된 신원 정보를 활용하여 뱅킹 서버에 등록된 공개키를 갱신함으로써, 자신의 개인키를 갱신할 수 있다. 반면 공개키 갱신 방법이 없는 블록체인 지불 거래의 경우 개인키 분실은 블록체인 상의 해당 자금에 대한 소유권 증명 방법의 상실로 연결되고, 결과적으로 해당 자금의 분실로 이어지게 된다.

5.3. 블록체인 지블 거래 개선을 위한 제언

앞의 비교 분석에서 살펴본 바대로 P2P 블록체인 지불 거래가 중앙 집중형 PKI 인터넷 뱅킹에 비해 여러 가지 장점이 존재한다. 그럼에도 불구하고 구조적인 측면과 보안 측면에서 여러 문제점도 안고 있다. 여기서는 본 연구 결과를 토대로 블록체인 지불 거래에서 개선되어야 할 사항들을 요약하고, 각 항목에 대한 구체적인 해결 방안의 제시는 향후 과제로 제시하고자 한다.

① 승인 지연시간 단축 및 거래 처리율 제고 : 실시간 고효율 합의 프로토콜 개발을 통해 실시간 거래 완료성을 지원하고, PKI 인터넷 뱅킹과 같은 수준의 확장성 높은 거래 처리율을 지원할 수 있어야 한다.

② 거래 불가역성과 사용자 및 거래의 통합 인증을 보완할 거래 내역 확인과 취소 방안 도입 : 참여자에 의해 송신된 거래를 이웃 노드가 송신자에게 피드백(feedback)하게 하고, 송신자가 자신의 거래 내역을 재확인하게 함으로써 거래 오류를 확인하고 오류 거래의 취소 등의 처리 방안을 도입할 수 있게 할 필요가 있다.

③ 키 도난과 메모리 해킹 위험성의 해소 방안 도입 : 거래 서명 기능이 포함된 HSM 기반의 클라이언트 장치 사용의 필수화 또는 강력한 장려를 통해 키 도난과 메모리 해킹의 위험성으로부터 사용자를 보호할 필요가 있다. 장기적으로는 인터넷 뱅킹 보다 키 도난의 위험을 획기적으로 줄일 수 있는 새로운 키 관리 메카니즘이 도입되어야 한다.

④ 키 분실 위험성의 해소 방안 도입 : 키 분실은 곧 블록체인 상의 자금의 분실로 연결되기 때문에, 장기적으로 인터넷 뱅킹 보다 키 분실의 위험을 획기적으로 줄일 수 있는 방안이 강구되어야 한다.

Ⅵ. 결 론

블록체인 지불 거래는 중앙의 서버에 의존하지 않는 P2P 방식의 지불 거래를 투명하게 제공한다는 점에서 큰 장점을 가지는 반면, 블록체인 지불 거래의 승인이 다수의 승인 처리 참여자(채굴자)들 간의 합의 프로토콜 수행을 통해 이루어지는 데서 오는 승인 지연시간 문제, 거래 처리율 저하 문제는 PKI 인터넷 뱅킹 대비 분명한 단점으로 파악된다. 또한 블록체인 지불 거래는 현재의 PKI 인터넷 뱅킹 등과 달리 중앙의 중재 기관의 개입 없이 P2P 방식으로 이루어지기 때문에, 키 관리, 거래 생성, 거래 내역 확인, 공격자에 대한 대응 등이 전적으로 참여자 개인의 책임 하에 이루어진다. 따라서 블록체인 지불 거래가 편리하고 안전한 거래 수단으로 받아들여지기 위해서는, 승인 지연시간 단축 및 거래 처리율 제고, 거래 불가역성과 사용자 및 거래의 통합 인증을 보완할 거래 내역 확인과 취소 방안, 키 도난과

메모리 해킹 위험성의 해소 방안, 그리고 키 분실 위험성의 해소 방안이 선결되어야 할 것이다.

ACKNOWLEDGEMENT

This paper was studied by the support of 2018 education and research promotion program for professors of Korea University of Technology and Education

References

[1] S. Nakamoto, “Bitcoin : A Peer-to-Peer Electronic Cash System,” White Paper, 2008[Internet]. Available: http://bitcoin.org/bitcoin.pdf.

[2] A. Kaushik, A. Choudhary, C. Ektare, and D. Thomas, “Blockchain - Literature Survey,” in *Proceeding of 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT)*, India, pp. 2145-2148, May. 19-20, 2017.

[3] I. C. Lin, and T. C. Liao , “A Survey of Blockchain Security Issues and Challenges,” *International Journal of Network Security*, vol.19, no.5, pp. 653-659, Sep. 2017.

[4] S. Park, “A Comparative Analysis of PKI Authentication and FIDO Authentication,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 7, pp. 1411-1419, Jul. 2017.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *Proceeding of 2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, USA, 25-30, Jun. 2017.

[6] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” White Paper, 2013 [Internet]. Available :http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[7] Ripple Labs Inc.. “Ripple: A Primer,” White Paper, 2018 [Internet]. Available:https://bravenewcoin.com/assets/Whitepapers/ripple-primer.pdf

[8] FIDO Alliance, “2017 State of Authentication Report,” White Paper, 2017[Internet]. Available : https://fidoalliance.org/wp-content/uploads/The-State-of-Authentication-Report.pdf

[9] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, “The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy,” in *Proceeding of International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, pp. 555-580, Feb. 22-26, 2016.

[10] H. S. Park, J. H. Lee, and S. C. Park, “Implementation, Security, and Usability Analysis of Accredited Certificate-based Internet Banking,” *Journal of Internet Computing and Services*, vol. 18, no. 4, pp. 69-79, Aug. 2017.

[11] A. Hiltgen, T. Kramp, and T. Weigold, “Secure Internet Banking Authentication,” *IEEE Security & Privacy*, pp. 21-29, Mar/Apr. 2006.

[12] Financial Services Commission, “Memory Hacking Related Press Release,” FSC Press Release, Jan. 2014[Internet]. Available : https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=88525

[13] F. M. Benčić, and I. P. Žarko, “Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph,” Cornell University Library, arXiv:1804.10013 [cs.DC], Apr. 2018.

[14] Financial Services Commission, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, Feb/Mar. 2016.

박승철(Seungchul Park)

1985.2 : 서울대 계산통계학과 졸
1987.2 : KAIST 전산학과 석사
1996.8 : 서울대 컴퓨터공학과 박사
ETRI 연구원, 한국IBM, 현대전자 네트워크연구소장, 현대네트웍스(주) 연구소장 역임
현재 한국기술교육대학교 컴퓨터공학부 교수
※관심분야 : 컴퓨터 네트워크, 네트워크 보안, 핀테크 보안