Journal of The Korea Society of Computer and Information
Vol. 24 No. 8, pp. 59-66, August 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.08.059

Blockchain-Based Mobile Cryptocurrency Wallet

Gwyduk Yeom*

Abstract

As the monetary value of cryptocurrency increases, the security measures for cryptocurrency becomes more important. A limitation of the existing cryptocurrency exchanges is their vulnerability to threats of hacking due to their centralized manner of management. In order to overcome such limitation, blockchain technology is increasingly adopted. The blockchain technology enables decentralization and Peer-to-Peer(P2P) transactions, in which blocks of information are linked in chain topology, and each node participating in the blockchain shares a distributed ledger. In this paper, we propose and implement a mobile electronic wallet that can safely store, send and receive cryptocurrencies. The proposed mobile cryptocurrency wallet connects to the network only when the wallet actively is used. Wallet owner manages his or her private key offline, which is advantageous in terms of security. JavaScript based wallet apps were implemented to respectively run on Android and iOS mobile phones. I demonstrate the process of transferring Ethereum cryptocurrency from an account to another account through Ropsten, a test net for Ethereum. Hardware wallets, such as Ledger Nano S, provide a slightly higher level of security, yet have the disadvantages of added burden of carrying additional physical devices and high costs (about 80$).

▸Keyword: Blockchain, Mobile Cryptocurrency Wallet, Peer-to-Peer(P2P), Private Key, Ethereum

I. Introduction

2018년 1월 26일 일본의 암호화폐(가상화폐)거래소인 코인체크[1]가 해킹 공격으로 580억엔(약 5,700억 원) 상당의 암호화폐를 도난당했다. 이는 해킹으로 인한 가상화폐 피해로 사상 최대 규모이며, 피해자가 26만명에 달했다. 최초로 유출되기 시작한 지 19분 만에 피해액의 99%가 탈취당한 것으로 나타났다. 이러한 코인체크의 치명적인 실수는 암호화폐의 소유자 본인임을 증명하는데 필요한 개인 키(Private Key)를 인터넷과 완전히 분리된 오프라인 저장소인 콜드월렛(Cold Wallet)에 보관하지 않고, 항상 인터넷에 연결된 상태인 핫월렛(Hot Wallet)에 보관하고 있었을 뿐 아니라 키를 분산 보관하는 다중서명시스템을 갖추지 않은 것으로 보고되었다[2]. 또한, 2018년 6월 20일 빗썸 핫웰렛에 보관되었던 350억원 규모의 회사보유분 가상화폐가 탈취당했다. 고객이 보유한 가상화폐는 콜드월렛으로 옮겨진 상태였기 때문에 해킹으로부터 안전하였으나, 핫월렛에 저장되었던 회사보유분의 일부는 해킹 공격에 노출되었다. 개인 키가 저장된 온라인 서버의 네트워크가 해킹 공격에 의해 뚫린 것으로 보고가 되었다[2]. 이처럼 개인 키 관리의 미흡, 해킹에 취약한 핫월렛 저장소 사용 등 전자지갑 보안체계가 허술한 점을 대상으로 삼아 해킹된 사례가 압도적으로 많은 비율을 차지한다.

블록체인(Blockchain)은 암호화폐의 근간이 되는 기술로 여러 대의 컴퓨터에 데이터를 블록에 담아 체인 형태로 수많은 컴퓨터에 동시에 이를 복제해 저장하는 분산형 데이터 저장 기술이다. 중앙시스템을 없애고 P2P(Peer-to-Peer)방식으로 노드를 연결하여 수많은 해당 블록체인 네트워크에 참여한 모든 노드가 분산원장[3]을 소유한다. 네트워크에 참여한 참여자들은 모든 데이터를 공유하기 때문에 누구나 변경의 결과를 감지할 수 있는 분산컴퓨팅기술 기반의 데이터 위조와 변조방지 기술이다.

• First Author: Gwyduk Yeom, Corresponding Author: Gwyduk Yeom
*Gwyduk Yeom (yeom@sejong.ac.kr), Dept. of Software, Sejong University
• Received: 2019. 07. 10, Revised: 2019. 08. 23, Accepted: 2019. 08. 24.

최근 2019년 3월 출시된 삼성전자 스마트폰 갤럭시 S10[4]에 암호화폐 지갑 기능이 탑재되었다. 또한, 카카오 모바일 메신저 카카오톡[5]에서도 암호화폐 지갑을 지원할 예정이라고 밝혔다. 즉, 카카오톡을 통해서 등록된 친구에게 암호화폐를 송금할 수 있게 된다. 세계시장을 주도하는 대표적인 하드웨어 회사와 메신저 플랫폼이 모두 암호화폐 지갑을 지원함으로써 누구나 암호화폐에 접근할 수 있게 된다. 이에 따라 암호화폐 활용도가 더욱 확대될 것으로 보인다.

암호화폐 전자지갑(Wallet)[6]은 핫월렛(Hot Wallet)과 콜드월렛(Cold Wallet)으로 나눌 수 있다. 핫월렛은 항상 네트워크에 연결되어 있는 암호화폐 전자지갑이며 항상 온라인 상태로 존재한다. 콜드월렛은 암호화폐 지갑이 사용되는 순간에만 네트워크에 연결되며 평소에는 오프라인 상태로 존재한다. 오프라인 상태로 암호화폐를 저장해 네트워크 해킹을 막아 보안성을 높인 암호화폐 하드웨어 지갑을 말한다. 시중에 나와 있는 하드웨어 지갑으로는 Ledger Nano S[13], Trezor[14], KeepKey[15] 등이 있다. 가장 유명한 콜드월렛 하드웨어 지갑은 레저(Ledger)사의 Ledger Nano S이다. 보안성은 높지만 부가적으로 하드웨어 장비 휴대의 불편함과 가격(약 $80 USD 이상)이 비싼 단점이 있다.

본 연구에서는 해킹의 위험없이 암호화폐를 안전하게 보관하고 거래할 수 있는 모바일 전자지갑을 제안하며 실제로 구현하였다. 제안한 모바일 전자지갑은 애플의 운영체제 iOS기반에서 자바스크립트(Javascrit)로 개발하여 아이폰에 앱형태로 탑재하였다. 구현한 암호화폐 모바일 전자지갑을 이더리움 공개 테스트넷인 Ropsten을 사용하여 내 계정에서 다른 계정으로 이더리움을 송금하는 과정을 보여준다. 개인키를 오프라인 상태로 각 개인이 직접 관리하므로 해킹의 위험없이 암호화폐를 안전하게 보관하고 거래할 수 있는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 이더리움 플랫폼의 세 개의 층인 이더리움 블록체인 층, 솔리디티 스마트 컨트랙트층, 그리고 이더리움 애플리케이션층에 관하여 살펴본다. 또한, 블록체인 해킹 공격을 유형별로 설명하고 대응방안을 알아본다. 3장에서는 제안한 모바일 전자지갑의 시스템 구성도와 화면구성을 설명한다. 또한, 전자지갑 작동을 위한 사용자 액션, 액션 조건, 그리고 지갑의 반응을 표로 보여준다. 4장에서는 이더리움의 지갑기능을 제공하는 메타마스크(Metamask) 설치방법을 보여준다. 메타마스크는 브라우저 확장 프로그램이며 이더리움 메인넷이나 테스트넷에 접속할 수 있는 기능을 제공한다. 본 논문에서 구현한 모바일 암호화폐 전자지갑을 이더리움 공개 테스트넷인 Ropsten을 사용하여 내 계정에서 다른 계정으로 이더리움을 송금하는 과정을 보여준다. 5장에서는 본 논문에서 제안한 모바일 암호화폐 전자지갑과 삼성 갤럭시 S10의 암호화폐 지갑기능인 블록체인 월렛, 그리고 하드웨어 지갑인 레저 나노스(Ledger Nano S)를 비교하여 설명한다. 그리고 마지막 6장에서는 결론과 향후 연구방향으로 마무리한다.

II. Related Works

본 장에서는 이더리움 플랫폼의 세 개의 층인 이더리움 블록체인 층, 솔리디티 스마트 컨트랙트층, 그리고 이더리움 애플리케이션층에 관하여 살펴본다. 블록체인 해킹 공격을 유형별로 설명하고 대응방안을 알아본다.

1. Ethereum platform

최초의 암호화폐인 비트코인은 암호화폐로서의 기능만 제공한다. 사토시 나카모토 (Satoshi Nakamoto)가 최초로 제안한 비트코인[7]은 화폐의 발행과 관리에 있어 기존 은행에서 사용하는 중앙은행 방식을 블록체인 기술을 사용하여 탈중앙화 방식으로 바꾼 최초의 시도이다.

이더리움[8]은 가치와 정보를 안전한 방식으로 서로 교환할 수 있는 어플리케이션을 만들어내는 강력한 플랫폼이다. 분산화된 플랫폼이며 전세계에 분산되어 있는 네트워크(노드)위에서 작동한다. 즉, 블록체인 위에서 움직이는 플랫폼이다. 해시값의 체이닝(Chaining)과 해쉬 트리(Hash Tree)[9]를 사용해 저장되므로 데이터의 무결성을 보장한다. 따라서 쉽게 해킹될 수 없다. 블록체인의 메커니즘 자체가 어렵게 만들어져 있기 때문이다. 이더리움은 그림 1과 같이 세 개의 층(Layer)로 이루어져 있다.

1.1 Ethereum blockchain layer

이더리움 블록체인 층은 가장 하위에 있는 층으로 트랜잭션을 처리하고 분산 공유원장(블랙체인)에 순서대로 기록하는 P2P(Peer-to-Peer) 네트워크이다. 네트워크에서 공유되는 모든 정보 즉, 발생하는 모든 트랜잭션을 기록할 수 있는 탈중앙화 된 데이터베이스를 구축한다. 네트워크에 있는 각각의 컴퓨터를 노드(Node)라고 부른다.

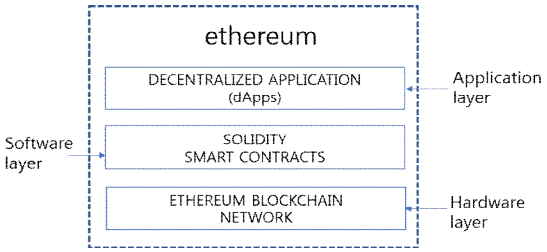

Fig. 1. The structure of ethereum platform

1.2 Ethereum smart contracts

스마트 컨트랙트[10]는 1994년 닉 사보(Nick Szabo)가 최초 제안한 개념으로 문서로 작성된 기존의 계약서는 서면으로 되어 있어 계약조건을 이행하려면 사람이 직접 수행해야 하지만 스마트 컨트랙트는 디지털 계약(Digital Contract)이므로 조건이 맞으면 자동으로 실행된다. 스마트 컨트랙트는 이더리움 가상머신(EVM)과 솔리디티(Solidity)[11]라는 프로그래밍

언어를 사용하여 이더리움 블록체인 플랫폼[12]에서 스마트 컨트랙트를 실행할 수 있게 한다.

블록체인은 다수의 노드가 데이터들을 검증하고, 검증된 것들을 기반으로 노드들끼리 공유하는 방식을 통해 디지털 데이터의 신뢰를 생성한다. 스마트 컨트랙트는 블록체인에 포함되며 네트워크 상의 모든 노드들이 동일한 스마트 컨트랙트의 인스턴스(복사본)를 가지게 된다.

스마트 컨트랙트는 컴퓨터 명령어로 계약서를 작성하고 작성시 설정한 조건이 충족되면 즉시 계약이 시행되므로 시간절약, 계약결과의 명확성, 그리고 신속하게 진행된다는 장점이 있다. 최초의 스마트 컨트랙트는 비트코인에서도 가능했으나, 계약의 반복이 불가능하며(반복문 사용불가) 비트코인 거래내역 잔고 외 다른 정보 관리가 안 되는 단점이 있다. 그러나, 이더리움 스마트 컨트랙트은 반복문 사용이 가능하고 네트워크상에서 수수료의 한계를 설정하여 무한루프를 막을 수 있다. 이러한 기능으로 인하여 이더리움은 블록체인 기술의 새로운 강자로 급부상했다.

1.3 Ethereum application layer: DApps

마지막 세 번째 층은 이더리움 사용자들에게 다양한 서비스를 제공하는 애플리케이션으로 스마트폰의 앱과 비슷하다. 이더리움 하드웨어와 소프트웨어 층을 활용하여 탈중앙화된 애플리케이션을 만들고 중앙화로 인해 생겨나는 오류들을 제거하며 계속해서 운영될 수 있게 만든다. 누구든 함부로 중단시킬 수 없다. 즉, 블록체인에서 운영되는 모든 애플리케이션(DApps)의 제작과 실행까지 가능하게 하는 종합 플랫폼이다. 이 기술은 스마트 컨트랙트를 기반으로 실행된다. 이더리움에서 가장 중요한 부분이고 이더리움이 큰 주목을 받는 이유 중의 하나이기도 하다. 그림 2는 이더리움의 생태계를 보여준다.

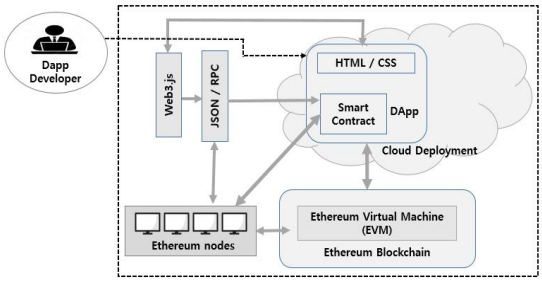

Fig. 2. Ethereum ecosystem

개발자는 스마트 컨트랙트 기술을 활용하여 솔리디티(Solidity) 프로그래밍 언어를 사용하여 댑(DApp)을 개발하며 개발된 소스코드는 이더리움 가상머신에서 실행시키며 수수료를 지불한다. 이더리움 가상머신을 동작시키는 원동력은 이더리움 노드들이며 채굴자(miner)는 이더리움 가상머신을 동작시키며 발생한 수수료를 지급받는다. 즉, 이더리움 가상 머신은 스마트 컨트랙트를 처리해주는 컴퓨터라고 말할 수 있다.

2. Cryptocurrency and types of attacks on blockchain networks

블록체인 네트워크는 해킹의 공격을 받을 수 있다. 블록체인 네트워크의 해킹 공격은 크게 네 가지 유형인 블록체인 인프라 공격, 블록체인 코드 공격, 블록체인 노드 공격, 그리고 블록체인 월렛 공격으로 나눌 수 있다. 공격을 유형별로 정리하면 표 1과 같다. 그리고, 구현 측면의 대응 방안은 다음과 같다.

2.1 Using hardware wallet

핫월렛은 스마트폰 앱이나 PC로 접속가능한 것이고 콜드월렛은 USB와 같은 하드웨어 형태나 개인키를 인쇄한 종이 등 인터넷에 연결되지 않은 오프라인 형태의 것이다. 콜드월렛 중 알려진 하드웨어 타입은 Ledger Nano S[13], Trezor[14], KeepKey[15] 등이 있다. 콜드월렛은 안전하지만 보관 및 휴대의 부담이 있다. 콜드월렛을 더욱 안전하게 사용하려면 다음과 같은 원칙을 따라야 한다.

- 안전한 오프라인 환경에서 개인 키 생성
- 개인 키 백업 만들기와 백업 키를 다른 장소에 보관
- 하드웨어 월렛을 도난당했을 때 실제 암호화폐를 도난당하는 것을 방지하기 위하여 월렛 암호화

2.2 Software key management methods with enhanced security

- Multi-factor[16]인증: 개인 키와 추가적인 인증기술을 활용하는 방안을 고려해야 한다.
- 다중 서명(Multi-Signature)[17]: n개의 개인 키 중에서 m개(m<=n)의 서명이 있어야 인증이 가능한 구조로 네트워크 사용자를 보호하는 방법으로 활용이 가능하다.

Table 1. Types of blockchain hacking attacks

유형	구분	위협	설명
블록체인 인프라 공격	DDos 공격	스팸거래생성 네트워크부하 발생	거짓거래의 유효성 검사로 처리시간이 늘어나고 이로 인한 부하발생
블록체인 코드공격	스마트 컨트랙트 취약점	코드버그로 인한 거래오류	스마트 컨트랙트가 복잡할수록 소프트웨어 오류발생 가능성 높음
블록체인 노드공격	합의 가로채기	51%공격을 통한 유효성 검사조작	퍼블릭 블록체인의 경우, 51% 공격자가 거래 완료된 자산을 재사용하고 특정 거래에 대한 거부가 가능함
블록체인 월렛공격	지갑관리 미흡	키 도용 취약한 권한 관리	지갑에 대한 접근 권한 상실시, 거래승인과 자산이동이 불가하며, 공격자가 키를 도용해도 시스템에서 이를 추적하는 것이 어렵고, 키 손상 여부도 인지하는데 상당한 시간이 소요됨

2.3 Transaction fees as a means for ensuring availability

특정 블록체인에서는 디도스(DDoS)[19]와 같은 네트워크 가용성을 무력화시키는 공격에 대응하여 프로그램 코드 실행

시 소요 실행자원(CPU 계산시간 혹은 메모리)에 비례하여 제한을 두고 있다. 실례로 이더리움은 코드 실행 시 가스(GAS)를 소비하도록 설계하여 블록체인 네트워크에서 디도스(DDoS)[19]의 가용성 공격을 방어하고 있다.

III. Proposed Mobile Wallet

본 장에서는 제안하는 모바일 전자지갑 시스템의 전체 시스템의 구성도를 보여주며 모바일 전자지갑의 메인화면 구성을 통해 전자지갑이 제공하는 기능들을 설명한다. 또한 전자지갑을 작동시키기 위한 각 메뉴별 사용자 액션(Action), 액션 조건, 그리고 지갑의 반응들을 설명한다.

1. Proposed system architecture for mobile wallet

본 논문에서 제안하는 모바일 전자지갑 시스템의 구성도는 그림 3과 같다. 블록체인에서 프론트엔드(front-end) 개발은 중요하다. 서비스와 사용자가 만나는 접점은 클라이언트에서 이루어지기 때문이다. web3.js는 JSON RPC(Remote Procedure Call, 원격 프로시저 호출) 스펙을 구현한 이더리움 자바스크립트 API로 주로 블록체인 프론트엔드 개발에 사용된다. 즉, JSON RPC 스펙에 대한 처리를 web3.js에 맡기고, JSON RPC가 아닌 자바스크립트로 Dapp(Decentralized application)을 개발할 수 있도록 지원하는 라이브러리이다.

이 모바일 전자지갑은 ERC(Ethereum Requests for Comment)-20 Token[18]을 지원한다. ERC는 이더리움 블록체인 네트워크에서 발행되는 토큰의 표준규약이다. 이더리움 네트워크내에서는 다양한 디앱(DApp, 탈중앙화애플리케이션)이 존재하고 이 디앱들은 각각 이더리움 기반의 서로 다른 토큰들을 발행하고 있다. ERC는 디앱 토큰을 개발하면서 준수하자고 합의한 개발자들의 기술표준 같은 것이다. 토큰 발행 시 지켜야 할 일종의 가이드라인이다. ERC-20의 장점은 이더리움의 스마트 계약(Smart Contaract)을 포함할 수 있다는 점이다. 토큰 거래에 특정한 계약조건을 추가함으로써 보다 안정적이고 범용성 높은 블록체인 활용이 가능해진다. 이 모바일 전자지갑은 지갑을 여는 역할을 하는 개인 키(Private Key)를 보관하는 키스토어(Keystore)를 가지고 있다.

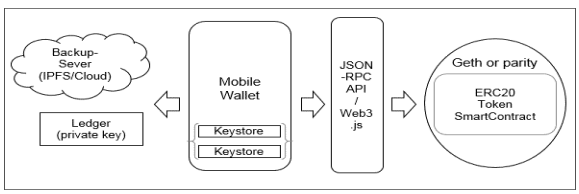

Fig. 3. Proposed mobile wallet architecture

2. Proposed main user interface for mobile wallet

제안하는 모바일 전자지갑의 화면구성은 표 2와 같다. 그림 4와 같이 메인화면을 통하여 전자지갑의 다양한 기능들에 접근할 수 있다. 지갑기능을 작동시키기 위한 사용자 액션(action), 액션 조건, 그리고 지갑의 반응은 표 3과 같다.

Table 2. The UI layout of proposed mobile wallet

모바일 전자지갑의 화면 구성	
메인	6. 이더리움 계정 가져오기
2. 이더리움 보내기	7. 계정 캐시
3. 토큰 보내기	8. 거래내역 조회
4. 이더리움 계정 만들기	9. 로그인
5. 이더리움 계정 내보내기	10. PIN 설정

Table 3. Definitions of conditions and responses for user interactions

사용자 액션 (전자지갑기능)	액션(Action) 조건	전자지갑의 반응
이더리움 보내기 버튼 클릭 (이더리움 전송)	정상적인 이더리움 수량(>=0) 및 수신할 이더리움 주소를 지정한 경우	약 5초 이내에 보내기 요청에 대한 알림메시지가 나타남(“보내기 요청에 대한 영수증을 받았습니다”)
토큰 보내기 버튼 클릭 (토큰전송)	정상적인 토큰수량(>=0) 및 수신할 이더리움 주소를 지정한 경우	약 5초 이내에 보내기 요청에 대한 알림메시지가 나타남(“보내기 요청에 대한 영수증을 받았습니다”)
액션없음 (토큰잔액표시)	네트워크 연결되고 활성화된 계정이 있는 경우	활성화된 이더리움 계정의 토큰잔액이 표시됨
	네트워크 연결되고 활성화된 계정이 없는 경우	잔액이 나타나지 않음
거래내역 버튼 클릭 (거래내역조회)	네트워크 연결되고 기존 거래내역이 있는 경우	거래내역이 표시됨
계정 만들기 버튼 클릭 (계정만들기)	조건 없음	약 5초 이내에 알림화면이 표시됨 (“새 계정이 생성되었습니다”)
계정 내보내기 버튼 클릭 (계정내보내기)	“개인키저장형식” 버튼 클릭	알림메시지가 표시됨(“개인키가 복사되었습니다”)
	“키저장형식” 버튼 클릭	알림메시지가 표시됨 (“Json키스토어가 복사되었습니다”)
계정 가져오기 버튼 클릭 (계정가져오기)	“클립보드”형식지정	알림메시지가 표시됨(“개인키가 복사되었습니다”)
로그아웃 버튼클릭 (로그아웃)	없음	지갑에서 로그아웃되어 PIN 입력화면이 나타남

Fig. 4. Main user interface for mobile wallet

Ⅳ. Implementation Result

본 장에서는 이더리움의 지갑 기능을 제공하는 메타마스크(metamask) 설치방법을 보여준다. 메타마스크[20]는 사용자들의 이더리움 계정과 개인 키를 안전하게 관리할 수 있도록 하는 브라우저 확장 프로그램이며 이더리움 메인넷이나 테스트넷에 접속할 수 있는 기능을 제공한다. 또한, 구현한 모바일 전자지갑을 이더리움 공개 테스트넷인 Ropsten을 사용하여 이더리움을 송금하는 과정을 보여준다.

1. Installation of Metamask

메타마스크는 구글 크롬(Chrome)에 플러그인 형태로 설치되기 때문에 운영체제(windows, mac, android)에 상관없이 모두 설치된다는 장점이 있다. 먼저, https://metamask.io에 접속한다. 이때, 인터넷 익스플로러나 사파리 브라우저가 아닌 구글의 크롬(Chrome) 브라우저로 접속해야만 한다. 그림 5와 같이 GET CHROME EXTENSION을 클릭해서 크롬에 추가한다. 크롬 브라우저 상단 오른쪽에 여우 모양 아이콘이 새로 설치된 것을 확인할 수 있다.

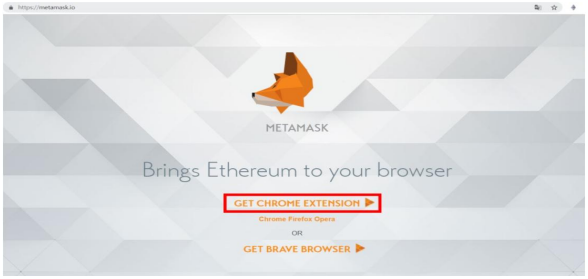

Fig. 5. Metamask installation

2. Sending ethereum

구글 크롬 오른쪽 상단에 플러그인 형태로 설치되어 있는 여우 모양 아이콘을 클릭하면 아래와 같은 이더리움 메인 넷이 실행된다. 이더리움 메인 넷 옆 버튼을 클릭하면 그림 6과 같이 이더리움 메인 넷, Ropsten 테스트넷, Kovan 테스트넷, 그리고 Rinkeby 테스트넷으로 구성된다.

- 이더리움 메인 넷: 우리가 실제로 사용하는 이더리움 네트워크이다.
- Ropsten 테스트넷: 메인넷 이더리움은 작업 증명(POW, Proof of Work)[21]으로 채굴이 되는데 Ropsten 테스트넷 또한 작업 증명(POW, Proof of Work)으로 채굴이 되는 구조이다. 이더리움 메인넷과 가장 비슷한 테스트넷이라고 할 수 있다. 본 논문에서도 이 테스트넷을 사용하여 코딩을 진행한다.
- Kovan 테스트넷: 권위 증명(POA, Proof of Authority)[22] 방식으로 채굴이 되며 Ropsten이 가끔 대량의 트랜잭션 거래 발생으로 블록체인 네트워크가 고장나는 경우가 있는데 그 경우를 방지하기 위해 다른 방식으로 채굴이 되고 있다. 블록이 생성되는데 시간이 짧기 때문에 솔리디티(Solidity) 코드를 빠르게 컴파일할 수 있다.
- Rinkeby 테스트넷: Kovan과 마찬가지로 POA 방식을 활용하고 있지만 블록 생성이 빠르지가 않다. 장점은 이더리움 재단 자체적으로 만든 POA 알고리즘으로 작동하고 있다는 것이다. 다른 이더리움 클라이언트에 코딩을 적용할 때 호환성이 좋다.

본 논문에서는 그림 7과 같이 이더리움 메인넷을 Ropsten 테스트넷으로 바꾸어 준다. Ropsten 테스트넷을 사용하여 내 계정에서 다른 계정으로 이더리움을 송금하는 화면은 다음과 같다. Ropsten 테스트넷이므로 이더리움은 무료로 입금받을 수 있다.

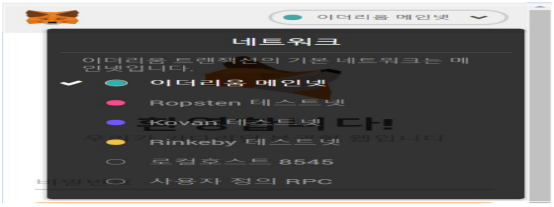

Fig. 6. Selection of ethereum mainnet

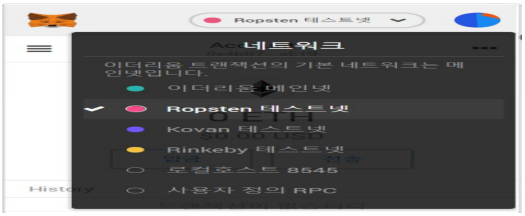

Fig. 7. Selection of ropsten testnet

이더리움 전송자 계정과 수신자 계정은 그림 8과 그림 9와 같이 설정할 수 있다.

이더리움 전송자는 Accounts2(0x9bc7eo77ac88c394로 시작)이며 수신자는 그림 9와 같이 0xf577abb96로 시작한다. 전송자가 현재 보유하고 있는 이더리움(ETH)은 4.9684ETH이며 전송수수료(Transaction Fee)는 0.1ETH이다. 그림 10을 통해 이더리움 전송이 성공했음을 알 수 있다. 이더리움 전송을 하면 트랜잭션이 생성되며 Ropsten 테스트넷 전용 ERTHERSCAN 화면을 통하여 그림 11과 같이 트랜잭션별 전송거래 내역을 확인할 수 있다.

Fig. 8. Inquiring balance of an ethereum account

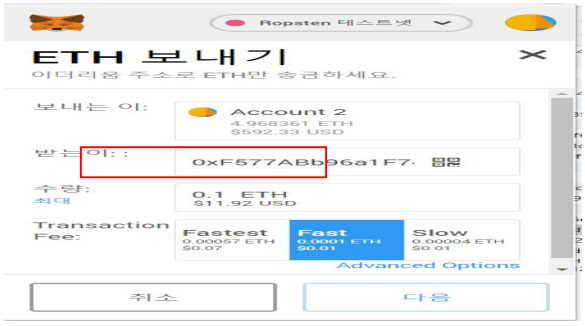

Fig. 9. Sending ethereum

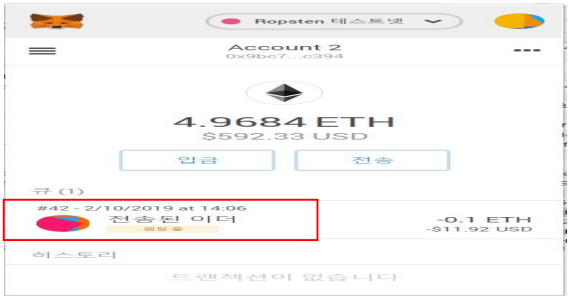

Fig. 10. Confirmation of transmission of ethers

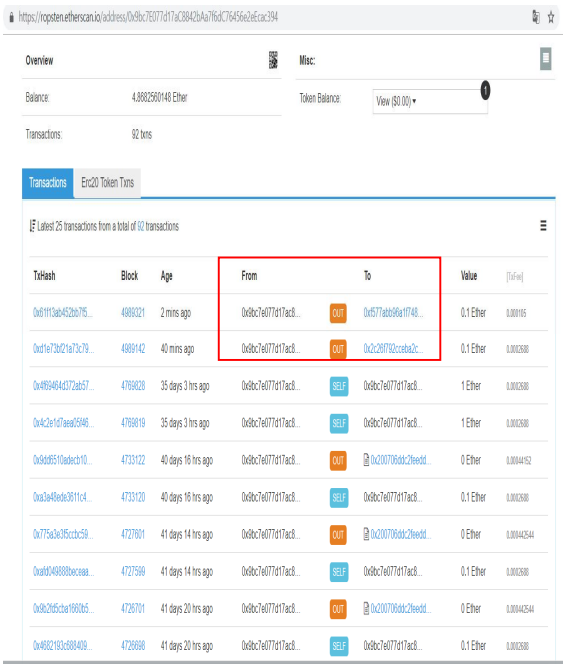

Fig. 11. Inquiring transaction history

Ⅴ. Performance Analysis

본 장에서는 본 논문에서 제안한 모바일 암호화폐 지갑, 삼성전자의 스마트폰 갤럭시 S10에 탑재된 암호화폐 지갑(블록체인 월렛), 그리고 암호화폐 하드웨어 지갑인 Ledger Nano S를 비교하여 설명한다. 콜드월렛 하드웨어 지갑은 Ledger Nano S[13], Trezor[14], KeepKey[15] 등이 있다. 그 중에서 선도적인 하드웨어 암호화폐 제조업체이자 개발자인 레저(Ledger)는 2017년에 1백만개 이상의 하드웨어 지갑을 판매하여 2900만 달러의 이익을 기록하였다[23]. Ledger Nano S는 레저(Ledger)사의 대표적인 콜드월렛 하드웨어 지갑이다. 갤럭시 S10[4]는 세계적인 제조업체인 삼성전자에서 2019년 3월에 출시한 스마트폰으로 암호화폐 지갑(블록체인 월렛)이 탑재되었다. 표 4는 제안한 모바일 지갑과 다른 지갑들과 비교한 것을 보여준다.

Table 4. Comparison our suggested wallet with other wallets

지갑 / 요소	Ledger Nano S	갤럭시 S10내 블록체인 월렛	제안한 모바일 지갑
종류	콜드월렛	핫월렛	핫월렛
형태	하드웨어	소프트웨어	소프트웨어
가격	약 80$	스마트폰 가격(약 60만원)에 포함	무료
보안성	높음	알려지지 않음	높음
네트워킹 여부	항상 온라인	항상 온라인	사용시에만 온라인
결제서비스	미지원	지원	미지원

하드웨어 지갑은 가격이 비싼 단점이 있지만 암호화폐를 저장하기 위한 가장 안전한 수단으로 각광받았다. 그러나 2018년 2월 레저(Ledger)에서 취약점이 발견되어 하드웨어 지갑이라도 암호화폐에 대한 안전을 보장할 수 없다는 점을 증명하였다. 범죄자들은 이미 해당 취약점을 이용하여 레저(Ledger) 사용자에게 피싱(Fising) 사이트가 포함된 지갑 주소를 전달하여 지갑에 보관되어 있는 가상화폐를 탈취하고 있는 것으로 확인되었다. 공격자는 사용자 컴퓨터에 침입한 후, 사용자 몰래 새로운 지갑 주소를 생성하고 레저(Ledger) 지갑은 개인용 컴퓨터에서 자바스크립트 형태로 동작하기 때문에 만약 컴퓨터가 악성코드에 감염된다면 (지갑 주소 코드를 공격자의 지갑 주소 코드로 수정해 놓으면 된다) 암호화폐들을 공격자 자신의 지갑으로 전달한다.

본 논문에서 제안한 모바일 암호화폐 지갑은 암호화폐 지갑이 사용되는 순간에만 네트워크에 연결되며 평소에는 오프라인 상태로 개인 키 및 암호화폐를 저장하므로 보안성이 높고 무료이므로 부담없이 사용할 수 있다.

Ⅵ. Conclusions

최근 2019년 3월에 출시된 삼성 스마트폰 갤럭시 S10[4]에 암호화폐 지갑 기능이 탑재되었다. 또한, 카카오[5] 모바일 메신저 카카오톡에서도 암호화폐 지갑을 지원할 예정이라고 밝혔다. 즉, 카카오톡을 통해서 등록된 친구에게 암호화폐를 송금할 수 있게 된다. 이러한 추세에 따라 다양한 블록체인 서비스가 개발될 것이며 암호화폐는 점점 대중화될 것으로 여겨진다.

본 논문에서는 블록체인 기반으로 해킹의 위험 없이 암호화폐를 안전하게 보관 및 거래할 수 있는 모바일 전자지갑을 제안하며 실제로 구현하였다. 제안한 암호화폐 모바일 지갑은 애플의 운영체제 iOS기반에서 자바스크립트(Javascript)로 개발하여 아이폰에 앱 형태로 탑재하였다. 개인 키를 오프라인 상태로 각 개인이 직접 관리하므로 네트워크 해킹을 막아 보안성이 높다. 구현한 모바일 지갑을 메타마스크를 설치하여 이더리움 공개 테스트넷인 Ropsten을 사용하여 내 계정에서 다른 계정으로 이더리움을 송금하는 과정을 보여주었다. 또한 제안한 모바일 지갑과 삼성 갤럭시 S10에 탑재된 암호화폐 지갑 기능인 블록체인 월렛, 그리고 하드웨어 지갑인 레저 나노스(Ledger Nano S)를 비교하여 설명하였다. 제안한 모바일 암호화폐 지갑은 보안성이 높고 무료인 소프트웨어 지갑이므로 부담없이 사용할 수 있다. 가장 유명한 콜드월렛 하드웨어 지갑인 레저 나노스(Ledger Nano S)는 보안성은 높지만 부가적으로 하드웨어 장비 휴대의 불편함과 가격이 비싼(약 80$) 단점이 있다. 삼성 갤럭시 S10내 탑재된 블록체인 월렛은 스마트폰을 구매해야 사용할 수 있으며 최근에 출시되었기 때문에 아직 보안성에 대한 정보가 미비하다.

향후 암호화폐 이더리움(Ethereum) 뿐만 아니라 비트코인(Bitcoin)[7], 리플(Ripple)[24] 등 다양한 암호화폐의 송금 기능과 결제서비스 기능을 추가할 예정이다.

REFERENCES

[1] Coin Check, *https://coincheck.com*

[2] Case Studies of Hacking Incidences, LG CNS IT Solutions, *https://m.post.naver.com*

[3] Park Sung Jun, “Blockchain Paradigm and Fin Tech Security”, Information And Communications Magazine, Vol.34, No.3, pp. 23-24, Mar. 2017.

[4] Samsung Electronics Galaxy S10, *https://www.samsung.com/sec/*

[5] KaKao, *https://www.kakaocorp.com/*

[6] Miraje Gentilal, Paulo Martins, and Leonel Sousa, “TrustZone-backed bitcoin wallet”, CS2 '17 Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, pp. 25-28, ,Jan. 2017.

[7] Bitcoin, *https://github.com/bitcoin/bitcoin*

[8] Ethereum, *https://ethereum.org*

[9] Pradip Kumar Sharma, and Jong-Hyuk Park, “Blockchain based hybrid network architecture for the smart city”, Future Generation Computer Systems, Vol.86, pp.650-655, Sep. 2018.

[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” Secuity and Privacy(SP), 2016 IEEE Symposium on, pp. 839-858, 2016.

[11] Santiago Bragagnolo, Henrique Rocha, Marcus Denker, and Stephane Ducasse, “SmartInspect: solidity smart contract inspector”, 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Mar. 2018.

[12] V. Buterin, “A next generation smart contract and decentralized application platform”, Ethereum White Paper, 2015.

[13] Ledger Nano S, *https://www.ledger.com/*

[14] Trezor, *https://github.com/trezor*

[15] KeepKey, *https://github.com/keepkey*

[16] Jun Ho Huh, and Kyungryong Seo, “Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing”, The Journal of Supercomputing, Vol. 75, Issue 6, pp. 3123-3139, June. 2019.

[17] Nurzhan Zhumabekuly Aitzhan, and Davor Svetinovic, “Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams”, IEEE Transactions on Dependable and Secure Computing, Vol.15, Issue 5, pp.840-852, Oct. 2016.

[18] Daejun Park, Yi Zhang, Manasvi Saxena, Philip Daian, and Grigore Rosu, “A formal verification tool for Ethereum VM bytecode”, ESEC/FSE 2018 Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pp. 912-915, Nov. 2018.

[19] Muhammad Saad, My T. Thai, and Aziz Mohaisen, “POSTER:Deterring DDoS Attacks on Blockchain-based Cryptocurrencies through Mempool Optimization”, Proceedings of the 2018 on Asia Conference on Computer and Communications Security, pp. 809-811, June 2018.

[20] MetaMask, *https://metamask.io/*

[21] Hong Liu, Yan Zhang, and Tao Yang, “Blockchain-Enabled Security in Electric Vehicles loud and Edge Computing”, IEEE Network, Vol.32, Issue 3, pp. 78-83, June 2018.

[22] S. Gupta, and M. Sadoghi, “Blockchain Transaction Processing”, Encyclopedia of big data technologies, pp. 1-11, 2019.

[23] Chain News, *https://www.chainnews.kr/*

[24] Ripple, *https://ripple.com/*

Authors

Gwyduk Yeom received the M.S. and Ph.D. degrees in Computer Science and Engineering from Yonsei University and Konkuk University, Korea, in 1996 and 2006, respectively. Before joining Sejong, She was a postdoctor research fellow in the Department of Computer Science at the Arizona State University, USA. She is currently a head researcher in the Department of Software at Sejong University, Korea. Her research interests include Mobile cryptocurrency wallet, Ethereum Blockchain payment, and Solidity Smart Contract.