The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 1, pp.35-44, Feb. 29, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.1.35
JIIBC 2020-1-5

공용 블록체인 지갑을 위한 OTP 기반 계정 복구 문자열 관리 체계

Recovery Phrase Management Scheme for Public Blockchain Wallets based on OTP

송성한*, 김순태**, 신정훈**, 이정휴***

Seounghan Song*, Suntae Kim**, Jung-Hoon Shin**, Jeong-Hyu Lee***

요 약 공용 블록체인 기반 가상 암호화폐의 이용이 증가함에 따라 암호화폐 지갑 프로그램을 통해 관리되는 블록체인 계정 정보의 안전한 관리가 요구되고 있다. 기존에 제안된 블록체인의 계정 관리를 위한 지갑 프로그램은 계정의 개인키 관리 측면에서 높은 보안성을 가지지만 계정 복구 문자열 관리에 대해서는 낮은 보안성을 가지고 있다. 따라서, 본 논문에서는 사용자의 모바일 기기 정보와 OTP 기법을 이용한 새로운 사용자 인증법 기반의 블록체인 계정 복구 문자열의 안전한 관리 체계를 제안하여 기존 계정 복구 문자열 관리 방식의 문제점을 극복하고자 한다. 또한, 예상 행동 시나리오를 기반으로 제안된 블록체인 계정 복구 문자열 관리 체계에 대한 분석을 진행한다.

Abstract The growing use of public blockchain-based virtual cryptocurrency calls for secure management of blockchain account information managed through cryptocurrency wallet programs. The previously proposed wallet program has high security in terms of managing an account's private key, but low security in managing an account's recovery phrase. Therefore, in this paper, we propose a safe management system of blockchain account recovery string based on the new user authentication method using the user's mobile device information and OTP technique to overcome the problem of the existing account recovery string management method. It also conducts an analysis of the proposed blockchain account recovery string management system based on the expected behavior scenario.

Key Words : Blockchain Account Security, IPFS, OTP, Recovery Phrase, Smart Contract

Ⅰ. 서 론

Satoshi Nakamoto가 2008년 발표한 논문의 개념을 기반으로 2017년 출시된 가상 암호화폐인 비트코인이 블록체인에 대한 대중의 폭발적인 관심을 불러일으켰다.[1] 또한, 뒤를 이어 등장한 이더리움, 리플 등의 공용 블록체인 기반 암호화폐 또한 사람들의 관심을 불러일으키면서 해당 암호화폐들의 가격이 치솟는 현상을 자주 목격할 수 있다. 이러한 현상은 가상 암호화폐에 대한 대중의 관심이 증가하고 있다는 사실을 뒷받침해준다.

*준회원, 전북대학교, 소프트웨어공학과
**정회원, 전북대학교, 소프트웨어공학과
***정회원, 전북대학교, 소프트웨어공학과
접수일자: 2019년 10월 31일, 수정완료: 2020년 1월 4일
게재확정일자: 2020년 2월 7일

Received: 31 October, 2019 / Revised: 2 January, 2020 / Accepted: 7 February, 2020
***Corresponding Author: jhlee25@jbnu.ac.kr
Dept. of Software Engineering, Jeonbuk National University, Korea

블록체인은 기존 인터넷을 기반으로 한 서비스의 데이터가 중앙에 집중되어 관리되는 형태와는 다르게 P2P(Peer-To-Peer) 네트워크에 참여한 다수의 참여자가 동일 데이터를 소유하고 검증함으로써 데이터의 위조 및 변조 사실을 추적하여 무결성을 보장한다. 이러한 특징으로 인해 블록체인은 가상 암호화폐를 비롯한 데이터의 위조 및 변조 위험이 존재하는 영역에 유용하게 사용될 수 있다.

공용 블록체인 기반 가상 암호화폐를 이용하기 위해서는 암호화폐를 관리하기 위한 계정을 생성해야 하는데 다양한 형태의 지갑 프로그램을 통해 계정을 생성할 수 있다. 웹 또는 모바일 지갑 프로그램을 통해 생성되는 암호화폐 관리 계정은 암호학적 알고리즘을 통해 생성되고 해당 계정의 정보는 지갑 프로그램의 서버에 저장되어 사용된다.

이는 기존 인터넷 기반 서비스에서 사용자가 입력한 개인정보를 기반으로 계정을 생성하는 것과는 다르다. 또한, 블록체인에서 생성된 계정은 정보가 중앙 서버에 저장되어 관리되는 기존의 서비스와는 다르게 정보를 필수적으로 중앙 서버에 저장하지 않고 사용자마다 소지하고 있는 지갑 프로그램의 특성에 따라 사용자 PC 또는 별도의 물리적 장치에 계정 정보의 저장이 가능하다. 이를 통해 모든 계정 및 개인정보를 관리하는 중앙 서버 해킹으로 인한 정보의 유출에 대한 예방이 가능하다. 하지만 사용자의 지갑 프로그램 관리가 소홀할 경우 계정 정보의 유출 가능성이 존재하는 문제점이 존재한다.[2][3][4][5][6][20]

또한, 계정 정보가 유출되어 악의적인 사용자가 계정 정보를 이용해 트랜잭션을 발생시켰다면 해당 트랜잭션을 돌이킬 수 없다는 블록체인 생태계의 특징이 존재하여 계정 정보는 더욱 안전하게 관리되어야 한다.[7][8]

블록체인에서 계정 정보는 Seed Phrase와 이로부터 생성된 개인 키 및 공개 키를 지칭한다. 개인 키와 공개 키는 블록체인에 존재하는 데이터에 대한 소유권을 주장할 때 필수적인 값으로 256bit의 길이를 가진 문자와 숫자의 조합이다. 이러한 개인 키 및 공개 키는 암기하여 사용되기 어려운 점 때문에 선행 연구들에서는 해당 부분이 블록체인이 실생활에 적용되기 어려운 이유라고 말한다.[9][10][11] 또한, 생성된 Seed Phrase는 계정 생성 시에 사용되는 12자리 또는 24자리의 순서를 가지는 문자열 조합이다. 특히, 계정 생성 시에 사용된 Seed Phrase는 계정 정보의 분실 시 개인 키 및 공개 키 생성에 사용된다. 따라서 해당 문자열 소지 시 계정 자체를 복구할 수 있어 복구 문자열(Recovery Phrase)이라고도 불린다.

계정 복구 문자열은 사람이 보고 이해할 수 있는 문자들의 집합이다. 암기를 통해 관리할 수 있다고 생각할 수 있지만, 문자열의 수가 증가함과 동시에 문자 사이에 순서 또한 유지되어야 하는 특성이 있어 암기하기 쉽지 않다. 이 때문에, 여러 상용 지갑 프로그램에서는 사용자에게 계정 생성 후 반드시 물리적인 형태로 복구 문자열을 안전하게 보관하는 것을 권고하고 있다.

계정의 개인 키 분실 시에는 블록체인에 기록된 데이터 중 해당 계정과 연관된 모든 데이터에 대한 소유권을 주장할 수 없다. 이러한 이유로 최근 개인 키를 인터넷과 차단된 물리적인 저장장치에 저장하여 보관하는 하드웨어 지갑과 사용자의 개인 키를 중앙 서버에서 위탁하여 관리해주는 형태 등의 서비스가 제공되고 있다. 하지만 상대적으로 계정의 모든 정보를 생성할 수 있는 유일한 정보인 계정 복구 문자열에 대한 안전한 관리는 이루어지고 있지 않다.

그리하여 본 논문에서는 공용 블록체인 기반 가상 암호화폐 이용이 증가함에 따라 블록체인 계정 복구를 위한 복구 문자열의 분실 시 정보의 복구를 위한 안전한 복구 문자열 관리 방안으로써 사용자 모바일 기기의 정보를 활용한 OTP 기반 계정 복구 문자열 관리 체계를 제안한다.

II. 배경 지식

1. 기존 인터넷 서비스의 사용자 계정 관리

기존 인터넷을 기반으로 제공된 서비스는 아이디 및 패스워드를 이용한 사용자 인증을 통해 제공되었다. 사용자는 서비스를 이용하기 위해 개인정보를 제공하고 아래의 그림 1과 같은 절차를 거쳐 중앙 서버에 개인정보가 저장된다.

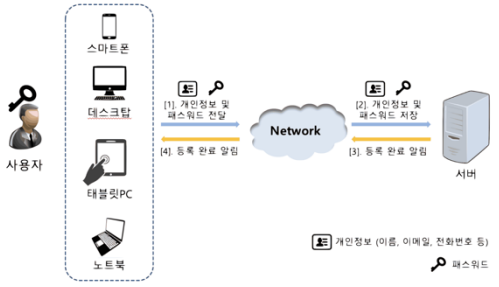

그림 1. 기존 인터넷 기반 서비스의 개인정보 보관
Fig. 1. Personal information storage for existing Internet-based services

이러한 구조는 사용자가 서비스 이용에 필요한 아이디 및 비밀번호를 분실하였을 때 유용하게 사용될 수 있다. 그림 2와 같이 사용자는 정보 복구 요청자가 자신임을 증명하기 위한 인증 수단으로써 계정 생성 시 입력했던 개인정보를 이용하여 인증할 수 있다. 또한, 선택적으로 보안 강도를 높이기 위해 OTP, 보안카드 등의 2차 인증 수단을 두어 인증하는 방법이 존재한다.

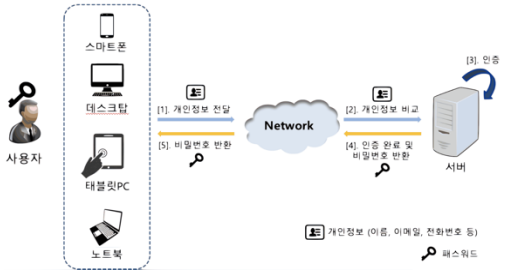

그림 2. 기존 인터넷 기반 서비스의 개인정보 반환
Fig. 2. Return of personal information for existing Internet-based service

하지만, 단일 또는 소수의 서버에 개인정보를 저장하여 보관하는 형태는 해킹의 대상이 되기 쉬워 SPOF(Single-Point of Failure) 문제로 인한 개인정보의 피해가 있을 수 있다.

2. 블록체인 키 생성 원리

공용 블록체인 기반 가상 암호화폐 계정은 기존 인터넷 기반 서비스와 달리 계정의 정보가 사용자 개인정보와 연관되어 있지 않고 계정을 관리하는 중앙 서버가 없다. 그러므로 공용 블록체인 네트워크에서는 개인정보를 바탕으로 계정을 복구할 수 없다. 이러한 특징은 아래의 그림 3에 나타낸 공용 블록체인 네트워크 계정 생성 방법에서 기인한다.

그림 3. 공용 블록체인 계정 생성 방법
Fig. 3. Mechanism of blockchain account creation

먼저 랜덤하게 선정된 12개 또는 24개의 순서를 가진 문자열 집합의 이진값으로부터 개인 키를 생성하고, PKI(Public Key Infrastructure)를 기반으로 앞서 생성된 개인 키로부터 공개 키를 생성한다. 생성된 개인 키와 공개키는 블록체인 네트워크에 트랜잭션을 생성하는 과정에서 트랜잭션의 발신자와 수신자를 검증하기 위해 사용된다. 또한, 블록체인 네트워크에 검증되어 저장된 트랜잭션 데이터에 대한 소유권 증명에 필수적인 정보로써 이용되며 지갑 프로그램에 저장되어 사용된다.

3. 스마트 컨트랙트

1998년 닉 사보에 의해 처음으로 소개되었다. 스마트 컨트랙트는 여러 참여자가 존재하는 P2P 블록체인 네트워크에 계약을 프로그램 코드 형태로 배포하여, 언제든지 네트워크상에 배포된 계약을 누구나 실행할 수 있게 함으로써 제 3자의 개입 없이도 계약의 결과를 강제할 수 있다.[12] 따라서, 강제력 있는 계약의 이행을 담보로 계약의 신뢰도를 높일 수 있고 실생활에서 계약을 이행하기 위해 거래 과정 전반에서 발생하는 비용을 스마트 컨트랙트로 구현하고 실행하여 해당 비용을 줄일 수 있다. 이러한 특징 때문에 스마트 컨트랙트는 금융거래, 공증 및 부동산 계약 등의 분야에 활용될 수 있다.

4. IPFS

IPFS(Interplanetary File System)은 P2P 형태의 분산 환경에 파일을 저장할 수 있는 기술이며 네트워크상에 분산된 다수의 컴퓨팅 장치를 하나의 파일 시스템으로 연결하려는 분산 파일 시스템이다. 파일의 내용을 기반으로 해시 주소를 생성하여 분산된 환경 속에 저장되고 공유되도록 설계되었다. 내용이 각기 다른 파일들은 해시로 식별되어 관리된다.

블록체인 자체에 트랜잭션 데이터를 제외한 다른 데이터를 저장하게 된다면 엄청난 용량의 데이터가 네트워크의 참여자들에게 실시간으로 동기화되어야 한다. 이는 효율적인 블록체인 네트워크의 운영을 어렵게 한다. 또한, 인터넷 연결이 가능한 PC, 서버 등의 단일 저장장치에 데이터를 저장하여 보관하였을 때 악성 프로그램에 의한 지갑 데이터 탈취 사례가 존재하여 각별한 주의가 요구된다.[13]

본 논문에서는 블록체인 네트워크의 효율성과 보관데이터의 보안성을 높이기 위해 계정 복구 문자열 데이터의 저장소로써 IPFS 분산 파일 시스템을 이용한다.

5. OTP

OTP(One-Time Password)는 미리 정해진 패스워드가 아닌, 특정한 알고리즘에 따라 수시로 생성되는 비밀번호를 이용한 보안 시스템이다. 이는, 기존 패스워드

인증 진행을 위해 사용자의 기억에 의존하는 것과는 다르다. 대개는 주로 난수 발생기에 현재의 시간을 넣어 비밀번호를 생성하여 일회용 비밀번호로 사용한다. 흔히 사용되는 시간 기반 하드웨어 OTP 토큰의 경우 내장된 시계의 오차로 인한 발급 오류의 가능성과 분실 위험성이 존재한다. 해당 문제를 극복하기 위해 모바일 기기에서 사용 가능한 OTP 서비스도 존재하지만, 해당 서비스를 제공하는 서버에서 문제 발생 시 OTP를 이용한 인증이 불가능하다는 문제가 있다.

본 논문에서는 스마트 컨트랙트 내부에 사용자 인증을 위한 OTP 생성 알고리즘 및 입력 제한시간 설정 부분이 포함되도록 한다. 이로써 하드웨어와 인증 서버의 문제로 인한 OTP 발급 오류 및 별도의 하드웨어 OTP 인증 기기 분실 위험성을 제거할 수 있다.

6. AES

AES(Advanced Encryption Standard)는 2001년에 발행된 암호화 표준이며 동일 키로 암호화 및 복호화가 가능한 특징을 가진다. 기존의 암호화 표준인 DES(Data Encryption Standard)가 가진 56 bits 길이의 키에 비해 AES는 128, 192 bits 또는 256 bits 등의 키 길이를 선택적으로 사용할 수 있다는 주요 장점이 있다. 따라서, AES 암호화 사용 시 해커의 무작위 대입 방법을 통한 키의 해킹이 어렵다. DES 암호화 기법과 AES 암호화 기법의 주요한 차이는 아래의 표 1과 같다.

표 1. DES, AES 암호화 기법 비교
Table 1. Comparison between DES and AES

	DES	AES
개발 시기	1977	2000
키 길이	56 bits	128, 192 or 256 bits
Cipher 종류	Symmetric Block cipher	Symmetric Block cipher
블록 크기	64 bits	128 bits
보안성	Proven inadequate	Considered secure

7. IMSI

IMSI(International Mobile Subscriber Identity)는 사용자의 스마트폰 단말기에 들어가는 USIM칩의 고유한 식별번호이다. 이는 통신기기의 단말기 식별번호(IMEI, International Mobile Equipment Identity)와는 다르다. IMSI는 셀룰러 망의 사용자를 식별하기 위해 사용되며, 모든 셀룰러 망에서 유일한 식별자이다. 총 64 bits 필드로 지정되며 그 구성은 다음의 표2와 같다.

표 2. IMEI 및 IMSI 구조와 형식
Table 2. IMEI and IMSI structure and format

구분		설명
IMSI	MCC	모바일 국가 코드
	MNC	모바일 네트워크 코드
	MSIN	모바일 구독자 식별번호
IMEI	TAC	IMEI 관리 기관에서 TAC가 할당된 그룹에 대한 고유코드
	MAC	스마트기기에 할당된 고유번호
	Check Digit	체크섬 디지트 (Checksum Digit)

2019년 퓨 리서치(Pew Research) 기관의 조사 결과에 따르면 대한민국의 휴대폰 단말 보급률은 99%에 가까우며 그 중 스마트폰이 차지하는 비율은 95%에 달한다는 것을 알 수 있다.[14] 따라서, 본 논문에서는 스마트폰의 IMSI를 사용자 식별자로 사용한다. IMSI를 개인 식별자로 이용한다면 모바일 기기 이외의 OTP 발급 기기와 같은 별도의 물리적 장치를 소지하여 사용자 인증을 진행할 필요가 없고, IMEI 값과 비교했을 때 더욱 전 세계적인 범위에서 유일한 값으로써 개인을 식별할 수 있는 값으로 사용될 수 있는 장점이 있기 때문이다.

Ⅲ. 관련 연구

사용자에게 중요한 데이터를 안전하게 보관해야 하는 문제와 이를 해결하기 위한 노력은 계속 존재해왔다. 특히 공용 블록체인 기반 가상 암호화폐를 사용자들이 안전하게 사용하게 하기 위한 다양한 지갑 관리 형태가 제안되었다.[2]

하지만 아래의 표 3과 같이 제안된 형태를 응용한 상용 지갑 프로그램의 형태 중 종이 지갑을 제외한 어떠한 지갑의 형태도 개인 키가 아닌 계정 복구 문자열의 안전한 관리를 위한 방안을 제시하고 있지 않다. 또한, 종이 지갑은 종이 문서에 사용자 계정 정보를 인쇄하여 안전한 곳에 물리적으로 보관해야 하는 특성으로 인해 종이 문서 분실 시 계정 복구가 불가능하다는 문제점이 있다.

표 3. 지갑 관리 형태 비교
Table 3. Wallet management from comparison

	웹 지갑	로컬 지갑	하드웨어 지갑	종이 지갑
저장 매체	중앙 서버	PC	Trezor, etc	종이
키 저장	O	O	O	O
복구 문자열 저장	X	X	X	O
사용자 인증 기법	비밀번호	비밀번호	특수장치정보 + 비밀번호	X
데이터 이동 방지	O	X	O	O

또한, 웹 지갑과 데스크톱 지갑 및 하드웨어 지갑 프로그램에서 사용하는 패스워드 기반 사용자 인증을 진행했을 때 존재하는 보안상의 문제로 인해 앞선 연구에서는 여러 다른 형태의 사용자 인증방법을 제안하였다.[15][16][17][18][19]

제안된 사용자 인증 기법으로는 사용자의 데이터를 저장할 물리 저장장치의 고유번호를 이용한 데이터 암호화를 통해 지정된 물리 저장장치만이 사용자 데이터에 접근 권한을 부여하는 기법과[15][16] 별도의 OTP 기기를 이용한 사용자 인증 기법[16], 사용자의 고유 정보인 지문, 홍채, 목소리 등의 고유 생체 정보를 이용해 중요한 데이터를 암호화하여 관리하는 기법 및 그 외 기법이 존재한다.[18][19]

각 기법에 대한 비교는 다음 표 4와 같다. 제안된 기법 중 물리 저장장치의 고유번호를 이용하는 기법의 경우, 물리 장치의 복구가 어려운 문제점이 존재한다. 생체 인증의 경우 제안된 기법 중 가장 보안성이 뛰어나다고 평가되는 반면 별도의 인증 서버에 저장된 사용자의 생체 정보가 유출될 가능성이 있다는 문제점이 있다. OTP를 이용한 사용자 인증 기법 또한 높은 보안성을 가지지만 OTP를 발급하는 기기를 항상 소지하고 다녀야 하는 불편함이 존재하고 OTP 발급 기기 분실 시 OTP 기기의 재발급 시점까지 사용자 인증을 진행할 수 없는 문제점이 존재한다.[17]

하지만 스마트 컨트랙트 안에서 OTP 발급이 가능케 하도록 한다면 위에 언급한 OTP 기법이 가진 문제점을 해결할 수 있다. 그리고 물리 저장장치를 이용해 데이터를 보관했을 때 발생할 수 있는 장치의 분실로 인한 데이터의 분실 문제는 데이터를 분산된 환경에 암호화하여 저장함으로써 일부 해결이 가능하다.

따라서 본 논문에서는 계정 복구 문자열의 반환을 위한 사용자 식별자로써 사용자 모바일 기기의 USIM 고유정보를 사용하고 사용자 인증방법으로 OTP 기법을 사용한다. 모바일 기기에 내장된 USIM의 고유 정보인 IMSI는 글로벌 유일한 식별자로써 개별 사용자 식별에 사용될 수 있고 스마트 컨트랙트를 통한 OTP 사용자 인증을 진행하여 더욱 안전한 데이터의 관리가 가능하다.

표 4. 사용자 인증 기법 비교
Table 4. User authentication technique comparison

	OTP	**USB**	**모바일 기기**	**생체 인증**
저장 매체	전용 OTP 장치	USB 메모리	기기 식별 번호	중앙 서버
인증 요소	패스워드 + OTP 장치정보	패스워드 + USB 정보	USIM 고유번호 + IMEI	생체 정보
데이터의 이동/복사 방지	O	O	O	O
패스워드 필요성	O	O	X	X
저장 매체 분실취약성	O	O	O	X

Ⅳ. OTP 기반 계정 복구 문자열 관리

1. OTP 기반 계정 복구 문자열 관리 체계

본 논문에서는 계정 복구 문자열의 안전한 관리를 위한 OTP 기반 계정 복구 문자열 관리 체계를 제안하고자 한다. 본 논문에서 사용할 표기법은 표 5와 같다.

OTP 기반 계정 복구 문자열 관리 체계는 저장 요청자[A], 반환 요청자[B] 및 공용 블록체인 네트워크와 IPFS 네트워크에서 피어 노드로써 동시에 존재하는 복구 노드[R]로 구성되며, 저장 요청자의 요청으로 계정 복구 문자열의 저장을 처리하는 저장 시스템과 반환 요청자의 요청에 의한 계정 복구 문자열 반환 과정에서 사용자 인증을 진행하여 정당한 반환 요청자에게 복구 문자열을 전달하는 반환 시스템으로 구분할 수 있다.

저장 요청자와 반환 요청자는 반드시 모바일 기기를 통해 저장 및 반환 요청을 해야 하며 저장 및 반환 요청 시 블록체인 네트워크 및 IPFS 분산형 파일 시스템 네트워크에 복구 노드의 접근이 가능해야 한다. 또한, 사용자의 요청을 수행하는 복구 노드는 전달된 사용자 모바일 기기 정보를 저장하지 않으며 복구 노드의 개인 키는 유출 및 분실의 위협으로부터 안전하다고 가정한다.

표 5. 표기법
Table 5. Notations

표기	설명
A	저장 요청자
B	반환 요청자
C	악의적 사용자
R	계정 복구 노드
n	난수
Aimsi	저장 요청자의 USIM 식별번호
Anum	저장 요청자의 전화번호
Bimsi	반환 요청자의 USIM 식별번호
Bnum	반환 요청자의 전화번호
Bn	반환 요청자가 소지한 난수
Rpri	파일 복구 노드의 개인키
Rpub	파일 복구 노드의 공개키
File	계정 복구 문자열 파일
Phrase	계정 복구 문자열
*Phrase	암호화된 계정 복구 문자열
Addr	분산된 환경에 존재하는 파일 주소
*Addr	암호화된 파일의 주소
SC	OTP 생성 코드를 가진 스마트 컨트랙트
RSA(Key, *)	RSA를 이용하여 데이터를 암호화하는 함수 (대칭키 암호화 함수)
AES(Key, *)	AES 비대칭키 암호화 함수
DAES(Key, *)	AES 비대칭키 복호화 함수

가. 계정 복구 문자열 저장

계정 복구 문자열 저장은 복구 노드가 저장 요청자로부터 저장 요청을 받았을 때 실행되며 절차는 다음의 그림 4와 같다.

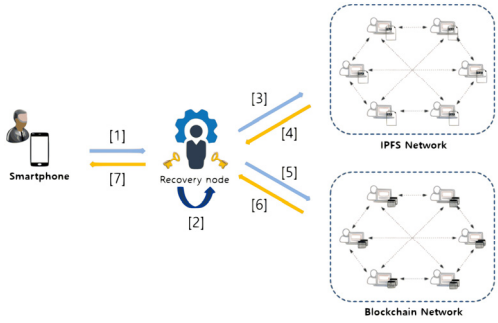

그림 4. 계정 복구 문자열 저장 절차
Fig. 4. Procedure for storing recovery phrase and encryption

1) A가 R에게 문자열의 저장을 요청
⇒ *info = (Aimsi + Anum)*

2) A의 정보와 R의 정보를 이용한 문자열 암호화 후 파일 생성
⇒ **Phrase ⟨= AES(info, Phrase)*
⇒ *File ⟨= RSA(Rpub, *Phrase)*

3) 암호화된 파일을 IPFS 네트워크에 저장

4) 파일 주소 변환
⇒ *Addr*

5) R의 정보를 이용해 파일 주소의 암호화 후 스마트 컨트랙트에 삽입하여 배포
⇒ **Addr = RSA(Rpub, Addr)*

6) 스마트 컨트랙트 배포 성공 메시지 반환

7) 계정 복구 문자열 저장 성공 메시지 반환

나. 계정 복구 문자열 반환

계정 복구 문자열 반환은 복구 노드가 반환 요청자로부터 계정 복구 문자열 반환 요청을 받았을 때 실행되며 그 절차는 다음의 그림 5와 같다.

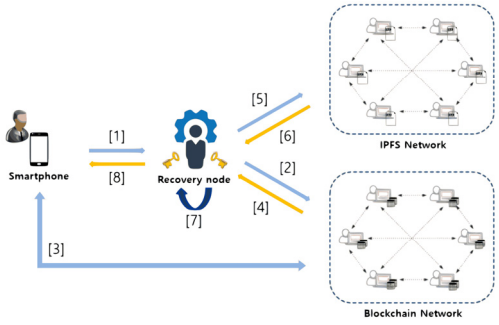

그림 5. 계정 복구 문자열 반환 절차
Fig. 5. Procedure for returning recovery phrase and decryption

1) B가 R에게 계정 복구 문자열의 반환을 요청
⇒ info = (Bimsi + Bnum)

2) SC를 실행하여 내부에서 난수 n을 생성하여 사용자에게 전달

⇒ *SC에서 난수 n 생성*

3) 생성된 난수 n과 사용자가 가진 난수를 비교하여 사용자 인증을 진행
⇒ *n <=> Bn*
⇒ *If False, quit SC*

4) 사용자 인증 성공 후 SC에 저장된 암호화된 계정 문자열 파일 주소 반환
⇒ *Addr = RSA(Rpri, *Addr)*

5) 파일 주소 값을 이용하여 IPFS로부터 파일 요청

6) 파일 주소에 대응되는 파일 반환
⇒ *File*

7) R의 개인 키를 이용해 파일의 복호화 진행
⇒ **Phrase = RSA(Rpri, File)*

8) 파일 내용 복호화
⇒ *info = (Bimsi + Bnum)*
⇒ *Phrase = DAES(Key, *Phrase)*

V. 안전성 평가

본 논문에서 제안한 OTP 기반 계정 복구 문자열 관리 체계와 상용 지갑 프로그램의 형태에 대한 안전성 평가를 선행 연구에서 소개된 개인 키 관리 안전 기준에 따라 진행되었다.[2] 또한, OTP 기반 계정 복구 문자열 관리 체계에 존재하는 두 시스템인 계정 복구 문자열 저장 시스템 및 계정 복구 문자열 반환 시스템에 대한 안전성 평가를 진행하였다.

본 평가에서는 실제 발생 가능한 외부의 공격에 대한 저항성을 평가 항목으로 사용한다. 예를 들어, 데이터를 소유한 저장 매체의 분실 위험성과 패스워드 분실 위험성 및 악성코드 저항성 등의 평가 항목을 통해 제안된 체계와 기존 상용 지갑 프로그램을 비교한다. 또한, 평가 항목에 해당하는 키 데이터는 본 체계의 복구 문자열에 해당한다고 간주하며 해당 항목을 만족할 경우 O로 표기한다. 그 결과는 아래의 표 6에 나타내었다.

제안된 체계는 인터넷과 완전히 분리된 매체를 통해 계정 정보를 관리하는 것과는 달리 분산된 환경에 저장하여 관리하기 때문에 제안된 평가 항목 중 일부를 만족하지 못한다. 하지만 이는 인터넷과 분리된 저장 매체의 분실 또는 훼손 시 계정 정보를 복구할 수 없다는 문제점을 해결할 수 있다.

또한, 제안된 체계는 블록체인과 IPFS에서 동시에 노드로 존재하는 복구 노드가 항상 정상적으로 작동한다고 전제한다. 이는 사용자 기기의 정보가 외부의 공격으로 인해 탈취당하더라도 계정 문자열의 복구를 위해 필요한 정보 중 일부이기 때문에 복구 노드의 안전한 키 관리를 통하여 기존 종이 지갑 형태의 계정 정보 관리 방법과 비교하였을 때 복구 문자열의 탈취 또는 분실 위험성을 낮출 수 있다.

표 6. 제안 기법 안전성 평가
Table 6. Evaluation framework for security

	제안 기법	웹 지갑	로컬 지갑	하드웨어 지갑	종이 지갑
Malware Resistant	O			O	O
Key Kept Offline			O	O	O
No Trusted Third Party			O	O	O
Resistant to Physical Theft		O			
Resistant to Physical Observation	O				
Resilient to Password Loss	O			O	O
Resilient to Key Churn	O	O			O
No New User Software	O	O			O
Cross Device Portability		O			

1. 계정 복구 문자열 정보 저장 시스템의 안정성

OTP 기반 계정 복구 문자열 저장 시스템에 대한 공격은 계정 복구 문자열 저장에 필요한 정보인 계정 복구 문자열 저장 요청자 기기의 USIM 식별번호 및 전화번호를 추출하는 것이며, 그 과정은 그림 6과 같다.

악의적인 사용자인 C는 다른 사용자의 모바일 기기를 갈취하여 정당한 사용자로 가장해 계정 복구 문자열 저장 요청에 사용되는 USIM 식별번호와 전화번호를 알아내어 향후 사용자가 계정 복구 문자열의 저장을 요청했을 때 추출정보를 이용할 수 있다. 이 같은 경우에 도난당한 USIM 정보를 가진 통신사에 통보하여 해당 기기의 정보로 요청된 OTP 인증을 거부하도록 할 수 있다. 이를 방지하기 위해 사용자는 자신의 기기에 별도의 사용자

인증 수단을 두어 기기가 분실되더라도 기기가 가진 정보의 이용 및 접근을 불가능하도록 해야 하고 기기 정보의 유출 위험이 있다고 의심되는 경우 다른 기기의 정보를 이용하여 계정 복구 문자열을 안전하게 관리해야 한다.

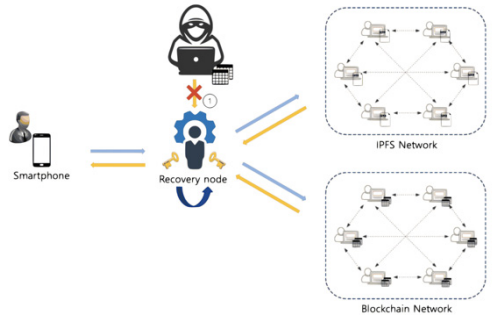

그림 6. 저장 요청자 기기 정보 추출 과정
Fig. 6. Procedure for extracting information from a requester

2. 계정 복구 문자열 정보 반환 시스템의 안정성

OTP 기반 계정 복구 문자열 반환 시스템에 가능한 공격은 IPFS 네트워크로부터 계정 복구 문자열 반환에 필요한 정보인 저장 요청자 기기의 USIM 식별번호 및 전화번호를 알아내는 것과 동시에 스마트 컨트랙트에 저장된 파일의 주소를 얻기 위해 복구 노드의 개인 키를 추출하는 것이다. 문자열 저장 요청자의 정보 추출 과정은 그림 6에 나타내었고 복구 노드의 개인 키 추출 과정은 다음의 그림 7과 같다.

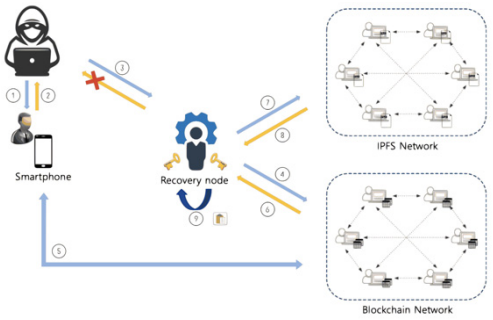

그림 7. 복구 노드 정보 추출 과정
Fig. 7. Procedure for extracting information from recovery node

악의적인 사용자인 C는 계정 복구 문자열의 AES 파일 복호화에 사용되는 키를 가진 복구 노드의 개인 키를 탈취하려 할 수 있다. 하지만 블록체인의 특성인 익명성으로 인해 블록체인에 존재하는 많은 참여자 중 어느 참여자가 복구 노드로써 동작하는지 분별하기 어렵다. 따라서, C의 입장에서 복구 노드의 개인 키를 탈취하는 것은 거의 불가능하다.

Ⅵ. 결 론

공용 블록체인 기반 최초의 암호화폐인 비트코인이 등장하고 10년이 지났지만, 암호화폐 계정 정보의 분실 및 해커에 의한 탈취 위협이 여전히 존재하는 상황에서, 계정의 개인 키 분실 시 계정 복구에 필수적인 계정 복구 문자열의 안전한 관리를 위한 연구가 미비하다. 사용자는 문자열의 유출을 방지하기 위해 계정 생성 후 계정 복구 문자열을 종이 문서로 작성하여 안전한 곳에 보관해야 했다, 이는 해당 종이 문서 분실 시 계정에 대한 소유권 증명이 불가능한 문제점이 있다. 이를 해결하기 위해서는 정보의 분실 위험이 낮고 해커의 정보 탈취가 어려우며 정당한 사용자에게만 접근이 허용되는 계정 복구 문자열 관리 방법을 생각해야 한다.

본 논문에서는 계정이 가진 계정 복구 문자열의 안전한 관리 및 정당한 사용자에게 계정 복구 문자열을 반환할 수 있는 OTP 기반 계정 복구 문자열 관리 체계를 제안하였다. 제안한 체계는 스마트 컨트랙트와 사용자 모바일 기기 사이의 메시지 교환을 통해 OTP 인증을 진행하여 정당한 사용자임을 인증하고 분산된 환경에 암호화되어 저장된 계정 복구 문자열 정보를 사용자에게 반환한다.

사용자는 모바일 기기의 정보와 복구 노드의 키로 복호화를 진행하여 계정을 복구하도록 한다. 이는 사용자가 가진 기기의 정보로 복호화를 시도하여 암호화하여 저장된 계정 복구 문자열의 소유권을 증명할 수 있어 정당한 사용자임을 인증하는 도구로 이용될 수 있다. 따라서 이는, 계정 복구 문자열 복구에 기여할 수 있다. 그러나 제안한 체계는 사용자 모바일 기기 분실 시 계정 복구 문자열의 복구 방안이 마련되어 있지 않다. 이러한 문제를 해결하기 위해, 향후 사용자 기기에 의존적이지 않은 안전한 사용자 인증방법에 관련된 추가적인 연구가 필요하다.

References

[1] Satoshi Nakamoto, “Bitcoin”: A Peer-to-Peer Electronic Cash System, Consulted, 2008.

[2] Eskandari, Shavan et al, "A First Look at the Usability of Bitcoin Key Management", In Proc, 2015.
DOI: 10.14722/usec.2015.23015.

[3] Conti, Mauro et al., "A survey on security and privacy issues of bitcoin", IEEE Communications Surveys and Tutorials, 2018.
DOI: 10.1109/COMST.2018.2842460.

[4] Om Pal, Bashir Alam et al., "Key management for blockchain technology), KICS ICT Express, 2019.
DOI: 10.1016/j.icte.2019.08.002.

[5] Xiaoyang Zhu et al., "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions", Sensors (Basel), 2018.
DOI: 10.3390/s18124125.

[6] S. B. Lee et al., "Security Analysis of Blockchain Systems: Case Study of Cryptocurrencies", Journal of The Korea Institute of Information Security & Cryptology, Vol.28, No.01, 2018.
DOI: 10.13089/JKIISC.2018.28.1.5.

[7] I. Miers, C. Garman, M. Green et al., "Zerocoin: Anonymous distributed e-cash from bitcoind", in proc. IEEE symp. Secur. Privacy, pp.397-411, 2015.
DOI: 10.1109/SP.2013.34.

[8] S. Suyn, M. Au, J. Liu et al., "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero", in proc. Eur. Symp. Res. Comput. Secur., pp.456-474, 2017.
DOI: 10.1007/978-3-319-66399-9_25.

[9] N. Unger et al., "SoK: Secure messaging." in Proc. IEEE Symp. Secur. Privacy, pp.232-249, 2015.
DOI: 10.1109/SP.2015.22.

[10] S. Sheng, L. Broderick, C. A. Koranda, J. J. Hyland, "Why Jonny still can't encrypt: Evaluating the usability of email encryption software.", in Proc. Symp. Usable Privacy Secur., pp.03-04, 2006.

[11] S. L. Garflinkel, D. Margrave, J. I. Schiller, E. Nordlander, R. C. Miller, "How to make secure email easier to use", in Proc. SIGCHI Conf. Hum. Factors Comput. Syst., pp.232-249, 2005.
ISBN: 1581139985.

[12] N. Szabo, "Smart Contracts: Building Blocks for Digital Free Markets", Extropy Journal of Transhuman Thought, 1996
DOI: 10.1200/JCO.2011.40.6546.

[13] N. Courtois, P. Emirdag, F.Valsorda, "Private key recovery combination attacks: On extreme fragility of popular Bitcoin key management, wallet and cold storage solutions in presence of poor RNG events", Cryptology ePrint Archive, 2014.

[14] "95% of South Koreans use smartphones and which country has the highest penetration rate?", 〈KBS〉, 2019. (2019. 10. 21 - Access Date)
http://mn.kbs.co.kr/news/view.do?ncd=4135732

[15] S. J. Kim, "Passwordless Protection for Private Key Using USIM Information", Jour. Of KoCon.a, Vol.17, No.06, pp.32-38, 2017.
DOI: 10.5392/JKCA.2017.17.06.032.

[16] J. H. Lee, I. J. Jo, S. J. Kim, "User Authentication System Using USB Device Information", Jour. Of KoCon.a, Vol.17, No.07, pp.276-282, 2017.
DOI: 10.5392/JKCA.2017.17.07.276.

[17] S. J. Kim, I. J. Jo, "Management Method to Secure Private Key of PKI using One Time Password", Jour. Of KoCon.a, Vol.14, No.12, pp.565-573, 2014.
DOI: 10.5392/JKCA.2014.14.12.565.

[18] J. B. Kim, J. E. Song, M. K. Lee, "Authentication of a smart phone user using audio frequency analysis", JKIISC, Vol.22, No.02, pp.327-336, 2012.
UCI: G704-001221.2012.22.2.017.

[19] H. J. Mun, "Biometric Information and OTP based on Authentication Mechanism using Blockchain", JCIT, Vol.8, No.03, pp.85-90, 2018.
DOI: 10.22156/CS4SMB.2018.8.3.085.

[20] Young-Seek Chung, Jae-Sang Cha, "The Security Risk and Countermeasures of Blockchain based Virtual Currency Trading", KIIECT, Vol.11, No.01, pp.100-106, 2018.
DOI: 10.17661/jkiiect.2018.11.1.100.

저 자 소 개

송 성 한(준회원)

- 2019.8~: 전북대학교 석사재학
- 2019: 전북대학교 학사
- Email: shak5643@gmail.com

김 순 태(정회원)

- 2014~: 전북대학교 소프트웨어공학과 부교수
- 2010: 서강대학교 공학박사
- 2007: 서강대학교 공학석사
- Email: stkim@jbnu.ac.kr

신 정 훈(정회원)

- 1992~: 전북대학교 소프트웨어공학과 교수
- 1999: 충북대학교 공학박사
- 1991: 충북대학교 공학석사
- Email: shinjh@jbnu.ac.kr

이 정 휴(정회원)

- 1993~: 전북대학교 소프트웨어공학과 교수
- 1993: 전북대학교 공학박사
- 1986: 전북대학교 공학석사
- Email: jhlee25@jbnu.ac.kr

※ 이 논문은 정부(정보통신기술진흥센터)의 재원으로 대학 ICT 연구센터 육성지원 사업의 지원을 받아 수행된 연구임.
(No. IITP-2019-2017-0-01628)