Journal of Convergence for Information Technology
Vol. 9. No. 10, pp. 9-15, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.10.009

블록체인 환경에서 화이트박스 암호기반 키 보호 기법에 관한 연구

최도현[1], 홍찬기[2*]
[1]숭실대학교 컴퓨터학과 학생, [2]가톨릭관동대학교 의료IT학과 교수

A Study on Key Protection Method based on WhiteBox Cipher in Block Chain Environment

Do-Hyeon Choi[1], Chan-Ki Hong[2*]
[1]Student, Computer Science, Soongsil University
[2]Professor, Department of Medical IT, Catholic Kwandong University

요 약 최근 차세대 전자상거래 및 금융 분야에서는 비트코인, 이더리움 등의 블록체인 기반 기술에 관심이 크다. 블록체인 기술의 보안성은 안전하다고 알려졌지만, 가상화폐 관련 해킹 사건/사고들이 이슈화되고 있다. 가상화폐 지갑에 대한 로그인 세션 탈취, 악성코드 감염으로 인한 개인키 노출, 단순한 암호 사용 등 외부환경의 취약성이 주요 원인이었다. 그러나 개인키 관리는 전용 애플리케이션 활용 또는 로컬 백업, 문서 프린트를 통한 물리적 보관 등 일반적인 방법을 권장하고 있다. 본 연구에서는 화이트박스 암호 기반 개인키 보호 기법을 제안한다. 안전성 및 성능분석 결과 개인키 노출 취약점에 대한 안전성을 강화하고, 암호화키를 알고리즘에 내장하여 기존 프로토콜의 처리 효율성을 증명하였다.

주제어 : 인증, 블록체인, 비트코인, 핀테크, 화이트박스 암호

Abstract Recently, in the field of next-generation e-commerce and finance, interest in blockchain-based technologies such as Bitcoin and Ethereum is great. Although the security of blockchain technology is known to be secure, hacking incidents / accidents related to cryptocurrencies are being issued. The main causes were vulnerabilities in the external environment, such as taking over login sessions on cryptocurrency wallets, exposing private keys due to malware infection, and using simple passwords. However, private key management recommends general methods such as utilizing a dedicated application or local backup and physical archiving through document printing. In this paper, we propose a white box password-based private key protection scheme. As a result of safety and performance analysis, we strengthened the security against vulnerability of private key exposure and proved the processing efficiency of existing protocol.

Key Words : Authentication, Blockchain, Bitcoin, Fintech, Whitebox Cipher

1. 서론

블록체인(Block Chain) 기술은 가상화폐의 거래 장부 기술로 개발되었다. 신뢰 된 제3기관을 통한 상호인증 기술인 기존 PKI(Public Key Infrastructure)와 차이점이 있다. 완전한 P2P(Peer to Peer) 네트워크상에서 분산된 사용자 간의 상호인증을 통해 거래 신뢰성을 확보할 수 있으며, 이중 지불 방지와 사용자의 익명성을 보장한다[1]. 또한, 기존 다운로드 및 보안 프로그램 설치하는 윈도우 액티브 엑스(Active-X)나 추가 설치되는 플러그인(Plug-in)의 취약점을 해결하는 공인인증서 대체기술로써 기대되고

*Corresponding Author : Chan-Ki Hong(chankih@cku.ac.kr)
Received September 9, 2019
Revised October 2, 2019
Accepted October 20, 2019
Published October 28, 2019

있다[2,3]. 블록체인은 현재까지 안전한 기술로 알려졌지만, 암호 화폐 거래소가 해킹되어 보관 중이면 개인 암호를 유출하는 경우 큰 문제가 된다. 개인키(Private Key)를 통해 본인을 증명하고 거래를 수행하기 때문에 외부 경로에서 개인키 유출 및 비정상 거래에 관한 해결책이 없다. 중요 개인키를 저장하는 지갑 화폐 관리의 보안이 중요하다는 것을 의미한다[4,5].

본 논문에서는 블록체인 환경에서 안전한 화이트박스 암호기반 키 보호 기법에 대하여 제안한다. 핵심 목표는 개인키를 안전하게 보호하는 것으로 모두 5장으로 구성된다. 2장에서는 가상화폐 비트코인에서의 블록체인 동작 과정 및 구조, 블록체인 기술의 취약점에 관해 설명하고, 3장에서는 제안하는 화이트박스 기반 키 보호 기법을 설명한다. 4장에서는 안전성과 성능분석, 5장에서는 결론을 맺는다.

2. 관련 연구

2.1 비트코인과 블록체인

비트코인은 제3기관의 검증 없이 사용자 간에 안전한 거래를 제공하는 가상화폐 기술이다. 기존 제3기관의 역할을 P2P 환경을 기반으로 '채굴자(Minor)'가 대신하여 신뢰 구조를 가진다[5]. 비트코인은 공개 소스로 공개되어 있으므로 누구나 개선 작업에 참여할 수 있고, 이를 활용해 개선된 비트코인 애플리케이션이나 새로운 가상화폐 거래가 가능하다. Fig. 1과 같이 송금할 대상인 받는 사람의 주소와 송금할 금액을 입력하고 보내기를 누르면 완료된다. 기본 원리는 거래내용을 시간 순서대로 기록(block)하고 이를 고리(chain)로 연결하여 분산된 거래내용에 대한 블록체인을 생성하여 검증하는 원리이다. 블록체인 기술을 이용한 비트코인의 거래 과정은 매우 간단하다. 지갑 프로그램을 설치하는 즉시 키 쌍(Key Pair)이 생성되며 바로 거래할 수 있다.

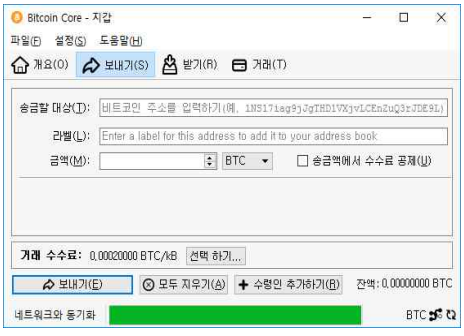

Fig. 1. Bitcoin Core Wallet Application

구조적인 측면에서 상세 프로세스는 아래 Fig. 2와 같다.

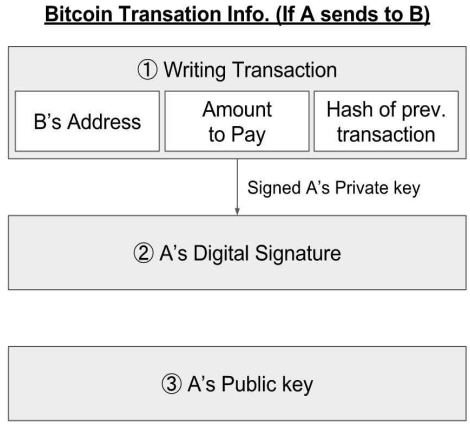

Fig. 2. Bitcoin Transaction Information

(1) A가 비트코인 지갑 프로그램에서 B에게 비트코인을 보낸다. (B의 주소와 보낼 금액을 입력)
(2) 입력한 B의 주소, 지급금액, 이전 거래내용의 해쉬값이 거래내용으로 작성된다. (해쉬값은 A가 보유하고 있는 비트코인 잔액 검증에 사용됨)
(3) 거래내용은 A의 개인키로 서명하며, SHA-256 등 256bit의 해쉬값으로 서명값을 생성하여 첨부한다.
(4) 마지막으로 A의 공개키값을 첨부한다. 작성된 거래내용 A의 서명값과 A의 공개키를 함께 전송하여 무결성 변조를 검증한다.

2.2 화이트박스 암호

화이트박스 암호 기술은 소프트웨어로 구현되어 PC, 모바일 등 장치에서 암호화 알고리즘이 실행되어도 암호키 분석이 어려운 장점을 제공하는 기술이다. 기존 TPM(Trusted Platform Module), 스마트카드, 하드웨어 OTP(One Time Password) 등 하드웨어는 보안성으로는 안전하지만, 비용증가와 설치의 어려움, 업데이트 및 패치의 어려움 등 다양한 문제가 존재한다. 화이트박스 공격(프로세스 내 모든 정보를 공격자가 알 수 있음)에 대해 암호키 유추가 어려운 것으로 알려져 있다. Fig. 3과 같이 전통적인 암·복호화 방식과 비교하여 암호키가 암호 알고리즘 속에 섞여 있어 (Obfuscation) 공격자가 키를 유추하기 어려운 구조로 설계되었다는 특징이 있다[6].

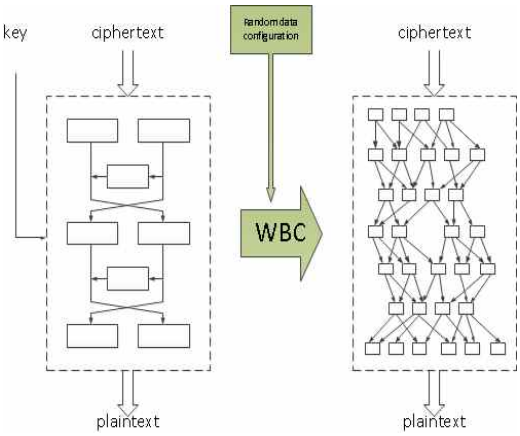

Fig. 3. Traditional and White-box(Encryption/Decryption)

테이블을 암호학적인 기법으로 적절히 분리하되 암호화 연산의 중간값이 노출되지 않도록 디코딩과 인코딩 과정을 수행한다. Fig. 4와 같이 인코딩 과정(Mi)과 디코딩 과정(Mi-1)이 별도의 테이블에서 계산된다. 중간값이 노출되지 않으면서 인코딩과 디코딩이 상쇄되고 원래의 암호화 동작(Xi)을 수행한다[7].

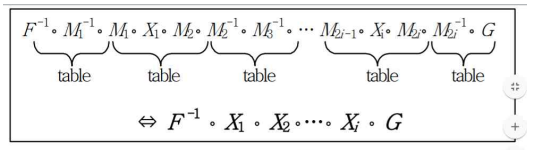

Fig. 4. White-box Cryptograph Internal Operation

결국, 화이트박스 암호 구현은 테이블 전체가 암호키로 볼 수 있으며, 화이트박스 암호 테이블 구성이 충분한 임의성을 가지고 있으므로 실행시간 또는 전력량 분석 등을 이용한 그레이박스(Gray-Box) 공격에도 상당한 강인성을 제공한다.

2.3 블록체인의 안전성과 취약성

기존 전통적인 은행이나 금융 기관 등의 중앙 집중화된 모델은 중앙 서버 해킹에 위험성이 매우 높다. 블록체인은 분산화 모델을 활용함으로써, 강력한 안전성을 제공한다. 채굴자들은 키체인(Key-Chain) 검증에 자원을 분산 처리 방식을 사용하고 있다. 해커 관점에서 정상적인 블록체인보다 큰 비용(51% 이상)이 요구된다. 2016년 12월 5일 기준으로 1년간 블록을 채굴하기 위한 Hash rate는 2,081,259,724 GH/s로 이에 대한 전력소비량은 600 Tera watt/hour가 넘는 양으로 환산된다. 이는 2011년 우리나라에서 사용되었던 총 전력량의 1.5배에 해당하는 천문학적인 전력량이다[8].

기존 중앙 집중형 체계보다 보안성과 관리의 효율성, 비용 절감 등 큰 이점이 있는 블록체인 기술에도 취약한 부분은 존재한다. 예로 비트코인은 개인 키에 거래에 대한 서명 검증과 소유권의 핵심 권한 제어를 해당 거래에 서명한 개인 키로 판단한다. 권장하는 개인키 관리 방법에는 PC에 백신 소프트웨어 설치, 개인키 파일의 주기적 백업, 키값을 문서로 직접 프린트(물리적 보관), 거래마다 새로운 주소(개인키, 공개키 한 쌍)를 발행하여 비트코인을 분산시키는 등 기초적인 방법을 권장하고 있다[9].

최근 비트코인과 유사한 다양한 가상화폐들이 안전한 거래 서비스를 제공한다고 소개하고 있지만, 안전성이 검증되지 않은 각 다른 개인키 저장관리 기법을 제공하고 있다. 일반적으로 사용자가 키를 저장/관리하는 방법에는 개인 PC 저장, 모바일 장비를 이용하거나 가상화폐 관리를 제공해주는 지갑(Wallet) 웹사이트 서비스 등을 이용할 수 있다. 그러나 지속해서 발생한 보안 문제점들이 개인키 노출 취약성의 원인이 되었다[10, 11]. 미국, 중국, 러시아, 일본 등 해외의 경우 은행이나 지급시스템 사용 제한, 외환 거래행위 금지, 자연인 또는 법인의 비트코인 사용 금지 등 규제 및 운영방안이 존재한다.

국내는 비트코인에 대한 투기척결 대책으로 합리적 규제 방안을 검토하고 있다[12, 13]. 따라서 무분별하게 거래소가 운영되고, 검증되지 않은 키 관리 기술들은 심각한 문제들을 발생시킬 가능성이 있다.

3. 화이트박스 암호 기반 키 보호 기법

3.1 기본동작 과정

Fig. 5는 제안하는 키 보호 구조의 기본동작 과정을 나타낸다.

3.2 키 교환 및 화이트박스 테이블 생성

화이트박스 테이블은 초기 회원 가입과정 또는 첫 거래 이전 한 번 이상 생성되어야 한다. 거래에 필요한 사용자 패스워드 즉, 개인키는 암호화되어 화이트박스 테이블 WT[1] 내부에 포함된다.

(1) 초기 가입과정에서 입력하는 패스워드를 파라미터로

사용한다. 타원곡선(ECC) 암호 알고리즘을 사용한다. 개인키 d를 패스워드 기반으로 2048bit 키를 생성한다. 이후 개인키 d를 이용하여 공개키 Q를 생성하여 공개한다.

$$Private\,Key = d(password)$$
$$Public\,Key = Q = d \times G(x, y)$$

(수식 1)

(2) 세션키는 PFS(Perfect Foward Secrecy)를 지원하는 ECDHE 기반 대칭키를 생성한다. 내부 대칭키 암호화 알고리즘은 AES256-CBC를 적용한다.

$$Session\,Key = ecdhe\_aes256(Q)$$

(수식 2)

(3) 화이트박스 테이블 WT^1에는 사용자 정보와 개인키, WT^2에는 서명 sign과 세션키를 포함하여 생성한다. 서명 sign은 공개키를 해쉬하고, 개인키로 서명하는 방법을 사용한다.

$$WT^1 = wb\_aes(user \parallel Private\,Key)$$
$$WT^2 = wb\_aes(sign \parallel Session\,Key)$$

(수식 3)

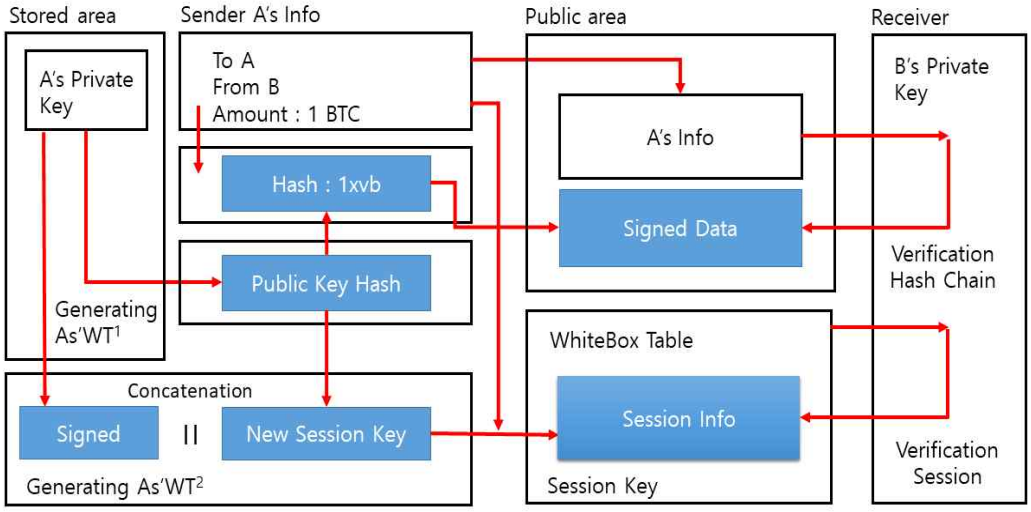

Fig. 5. White-box Cryptograph-based Key Protection Structure

3.3 화이트박스 테이블 검증

Fig. 6은 제안하는 키 보호 구조의 키 및 서명 검증과정을 나타낸다.

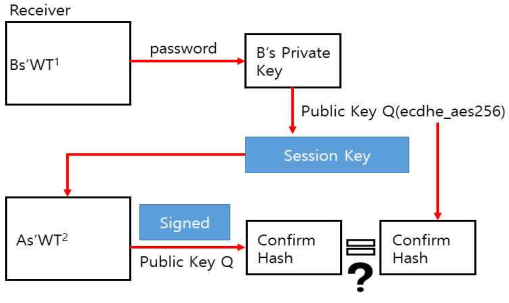

Fig. 6. White-box table Key and Signature verification

(1) 양방향 모두 로컬 저장소에 화이트박스에 접근하기 위한 추가 패스워드를 사용한다.

(2) 초기 생성(가입과정) 또는 이전 거래 종료에서 저장된 WT^1의 개인키를 확인한 후, 공개키 Q로 세션키를 생성한다. WT^2의 서명을 추출하여 기존 서명과 비교한다.

(3) 블록체인 내부 트랜잭션에 WT^2 검증에 대한 요청을 옵션을 추가하여 전파한다. (기존 해쉬체인 검증과정 포함)

(4) WT^2로부터 세션키(공개키 포함)를 확인 후 서명을 추출한다. 이후 암호화된 트랜잭션을 전체 노드로 전파한다.

3.4 세션의 갱신과 종료

Fig. 7은 통신 세션의 갱신 및 종료과정(정상)을 나타낸다.

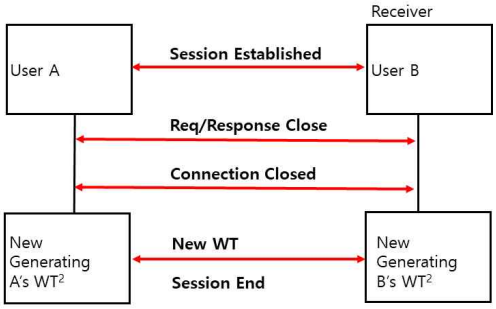

Fig. 7. White-box table Key and Signature verification

Fig. 8은 통신 세션의 갱신 및 종료 과정(에러)을 나타낸다.

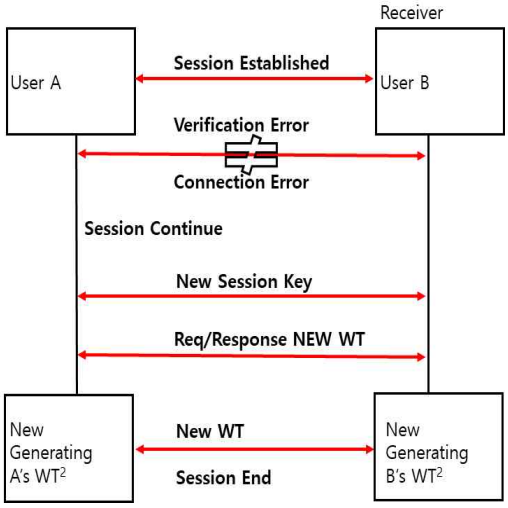

Fig. 8. White-box table Key and Signature verification

(1) 정상 통신과정은 종료 요청 이후 새로운 화이트박스를 생성하여 각 로컬에 저장한 후 세션을 종료한다. 종료 이후 세션키는 폐지된다.

(2) 비정상적인 통신은 기존의 세션을 유지하면서 새로운 화이트박스를 생성한다. 이후 화이트박스 검증 과정을 재시작한다.

4. 안전성 및 성능분석

4.1 안전성 분석

(1) 로컬에서 내부 키가 유출되어도 이를 악용할 수 없도록 키 자체를 암호화한다. 화이트박스 암호기반으로 키가 메모리에 적재된 순간을 해킹에 대한 높은 안전성을 제공한다.

(2) 블록체인 인증 노드에 강화된 암호화 키 복잡도를 제공한다. AES-256 대칭 블록암호의 선택 평문과 암호문에 대한 연관키 공격 복잡도(약 2126) × 세션 암호화키 복잡도(2126)에 추가적인 화이트박스 암호 복잡도를 제공한다.

(3) 최종 거래에 대한 세션정보와 화이트박스를 검증하기 때문에 개인키를 저장한 장치 자체를 분실하여도 내부 개인키의 유출에 대해 비교적 안전하다.

(4) 세션종료 과정에서 로컬에 암호화된 화이트박스는 지속해서 갱신되고 저장된다. 해킹을 위해서는 최근 통신에 대한 양방향(클라, 서버) 해킹이 모두 성공해야 하는 어려움을 제공한다.

(5) S/W 기반으로 구현되어 동작하기 때문에 모바일 장치 등 타 플랫폼에서 추가적인 2차 인증기술로 연동할 수 있고, 암호 알고리즘 설정을 쉽게 변경하여 보안 강도를 조절/강화할 수 있다.

4.2 성능분석

테스트 환경은 윈도우 10 Pro 64bit, Intel(R) Core I7-5700HQ CPU(2.70GHz)에서 Microsoft Visual C++ AES 암호 라이브러리 클래스를 활용했다. 기본설정은 128bit 블록, 256bit 키, CBC mode, 화이트박스 암호는 128bit 블록, 128bit 키를 사용한다. Table 1은 용량별 암호화(E:)/복호화(D:) 성능 비교분석 결과(ns:nano second)를 나타낸다.

Table 1. AES256 vs WB-AES256 Comparison(ns)

	AES256	WB-AES256
1MB (9 Round)	E : 0.001978300	0.002728462
	D : 0.001436845	0.013720294
10MB (9 Round)	E : 0.338940249	0.549147799
	D : 0.251424411	0.386428914
25MB (18 Round)	E : 0.206509811	0.451025427
	D : 0.191112787	0.338516515
25MB (36 Round)	E : 0.186428914	0.751025469
	D : 0.151424417	0.386428015
50MB (90 Round)	E : 1.486146537	1.751026117
	D : 1.725771018	1.635001919
100MB (90 Round)	E : 2.362501986	5.610616541
	D : 2.651004417	7.186428914

1, 10MB 크기의 문자열 암/복호화 성능은 기본 라운드 연산(9회) 기준으로 AES256 평균 0.0034(ns), 화이트박스 적용 이후 평균 0.0164(ns)로 약 0.013(ns)의 지연이 추가 발생함을 확인하였다. 거래 발생 순간 인증 목적으로써의 내부 해쉬 연산 지연 0.013(ns)은 실제 체감상 큰 영향이 없음을 알 수 있다. 이는 암호화 문제셋 용량의 증가에 대한 성능 차이 영향이 더 크다. AES256은 기본적으로 문자열 용량이 증가하면 추가적인 암/복호화 성능을 요구한다. 라운드 연산 차이에 대한 성능 변화를 살펴본다. 동일 25MB 문자열 기준 라운드 연산(18라운드-> 36라운드)을 증가시킨 후 비교하였다. 10MB에서 25MB 용량증가는 성능에 큰 차이가 없는 것으로 나타났다. 총 평균 지연은 약 0.2102(ns)로 라운드 증가(암호화 강도 변경)는 용량증가로 인한 추가 연산보다 영향을 적게 받는 것으로 나타났다. 문자열 50, 100MB 기준 90라운드로 증가시킨 이후 지연을 비교하였다. 50MB 기준부터 평균 지연 차이 0.2649(sec)로 전체 암/복호화 시간이 약 2.1~2.3초 추가되었고, 100MB 기준에서 암/복호화 시간이 지연 차이 3초 이상 지연이 발생하고 있다. 사용자 인증과정에서 발생하는 화이트박스 인증 문자열 용량은 실제 수십 바이트 크기이다. 비교분석을 위해서 비교적 큰 용량의 문자열을 사용했다. 결론적으로 문자열 크기에 비례하는 화이트박스의 생성 크기는 성능에 영향을 주지만, 실제 1MB 이하 크기로 생성되는 화이트박스 테이블은 사용자에게 체감상 큰 영향을 끼치지 않으리라고 예측할 수 있다.

5. 결 론

제안하는 키 보호 기법의 핵심은 통신세션이 생성된 후 암호화된 개인키의 로컬 메모리 유추 가능성 방지가 목적이다. 기존 AES256 암호화에 사용자 사이 양방향 화이트박스 암호를 적용하여 로컬에 저장된 개인 키에 대한 안전성을 높이는 특징이 있다. 성능분석 결과 화이트박스 크기 증가는 연산에 영향을 주었지만, 최근 사용하는 일반적인 PC 사양으로 1MB 이내 문자열을 사용한다는 가정했을 때 0.0012(ns) 체감 성능은 사람이 큰 차이를 못 느끼는 수준이다. 제안하는 키 보호 기법은 모든 블록체인 노드를 대상으로 해쉬 연산을 수행하지 않는다. 특정 이벤트에 대해 인증 용도로 수행해야 하는 단점이 있으므로 블록체인 전체 노드를 보호할 수는 없다. 보안 기능의 관점에서는 실시간 블록체인 연산에 대한 거래 이상 감지 기능으로 적용될 수 있을 것으로 예상한다.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system.* BITCOIN(Online). http://bitcoin.org

[2] A. M. Antonopoulos. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies.* BOSTON : O'Reilly Media.

[3] H. R. Jung & J. W. So. (2018). Security of Password Vaults of Password Managers. *Korea Institute of Information Security & Cryptology, 28(5),* 1047-1057. DOI : 10.13089/JKIISC.2018.28.5.1047

[4] J. H. Kim. (2013). *Next Money Bitcoin-The emergence of digital currency to change the game.* Seoul : Bookie.

[5] H. Y. Kim. (2018). Analysis of Security Threats and Countermeasures on Blockchain Platforms. *Korean Institute of Information Technology, 16(5),* 103-112. DOI : 10.14801/jkiit.2018.16.5.103

[6] W. Brecht. (2012). *White-box cryptography: hiding keys in software.* NAGRA Kudelski Group Switzerland.

[7] W. Michiels. (2010). Opportunities in white-box cryptography. *IEEE Security & Privacy, 8(1),* 64-67. DOI : 10.1109/MSP.2010.44

[8] H. J. Lee, D. H. Won & Y. S. Lee. (2019). Protection Technologies against Large-scale Computing Attacks in Blockchain. *Korea Information Assurance Society, 19(2),* 11-19. DOI : 10.33778/kcsa.2019.19.2.011

[9] M. S. Kim et al. (2016). Effective Vitalization Plan of Electronic Cash using Bitcoin. *Jouranl of Information and Security, 16(4),* 79-90. UCI : G704-001662.2016.16.4.008

[10] T. Bamert, C. Decker, R. Wattenhofer & S. Welten. (2014). Bluewallet: The secure bitcoin wallet. *In International Workshop on Security and Trust Management*, 65-80, Springer. DOI : 10.1007/978-3-319-11851-2_5

[11] M. Gentilal, P. Martins & L. Sousa. (2017). TrustZone-backed bitcoin wallet. *In Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems,* 25-28, ACM. DOI : 10.1145/3031836.3031841

[12] H. K. Kim. (2014). Bitcoin Regulation : Legal and Regulatory Issues of the Virtual Currency System. *Korea Securities Law Association, 15(3),* 377-431. DOI : 10.17785/kjsl.2014.15.3.377

[13] S. J. Park. (2018). A study on the compatibility of Korean financial system and blockchain. *HUFS Law Research Institute, 42(4),* 133-151.
DOI : 10.17257/hufslr.2018.42.4.133

최 도 현(Do-Hyeon Choi) [정회원]

· 2008년 2월 : 동서울대학교 컴퓨터 소프트웨어학과 졸업
· 2010년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
· 2016년 3월 : 숭실대학교 컴퓨터학과 (공학박사)

· 2019년 3월 ~ 현재 : 성결대학교 미디어소프트웨어 객원교수
· 관심분야 : Mobile, Network Security, PKI, Virtualization
· E-Mail : cdhgod0@ssu.ac.kr

홍 찬 기(Chan-Ki Hong) [정회원]

· 1986년 : 중앙대학교 전자계산학과 (이학사)
· 1988년 : 중앙대학교 대학원 전자계산학과 (공학석사)
· 1992년 : 중앙대학교 대학원 전자계산학과(공학박사)

· 1992년 3월 ~ 현재 : 가톨리관동대학교 의료IT학과 정교수
· 관심분야 : 정보보안, PKI, 블록체인
· E-Mail : chankih@cku.ac.kr