Journal of Korea Multimedia Society Vol. 23, No. 5, May 2020(pp. 658-666)
https://doi.org/10.9717/kmms.2020.23.5.658

블록체인 환경에서의 PGP 인증 시스템

김대한†, 서경룡††

PGP Certification System in Blockchain Environments

Daehan Kim†, Kyungryong Seo††

ABSTRACT

PGP is an encryption software designed to provide information protection, security and authentication services for online communication systems. The characteristic of behavior done on the Internet is that you don't know the other person. It is very important to protect information from someone you cannot trust. So identification of the other person is an important task. PGP uses an digital signature algorithm to verify the identity of the other party. However, it is not accurate to check the other party's credibility. PGP increases trust as other users sign more on public keys of user. In other words, credibility is not perfect. In this paper, PGP certification system that key management in Ethereum blockchain, one of the blockchain platforms, is proposed. Key management in blockchain ensures data integrity, transparency and reliability.

Key words: PGP, Security, Digital Signature, Blockchain, Identification

1. 서 론

PGP(Pretty Good Privacy)는 온라인 통신 시스템의 정보 보호, 보안 및 인증 서비스를 제공하도록 설계된 암호화 소프트웨어이다[1]. PGP는 공개키를 사용하여 암호화를 하며 메시지 암호화와 전자서명 기능을 가지고 있다. 전자서명 기능의 경우 사용자 신원을 확인할 수 있다. 전자서명은 메시지에서 hash값을 추출하여 사용자의 개인키로 암호화한 뒤 원본 메시지와 함께 수신자에게 송신하면 수신자는 암호화된 hash값을 송신자의 공개키로 복호화하여 원본 메시지의 hash값과 비교하여 송신자의 서명이 맞는지 검증 가능한 알고리즘이다.

현재 인터넷상에서는 정보의 보호는 매우 중요한 일이다. 그래서 사용자는 상대방의 정보를 확인할 수 없고 신뢰 가능한 상대방인지 확신할 수 없다. 그래서 PGP의 전자서명 기능은 상대방이 정말 상대방인지를 확인할 수 있어 중요한 기능이라고 볼 수 있다. 하지만 상대방이 신뢰 가능한 상대방인지도 검증할 수 있어야 한다. 그래서 PGP는 Web of trust[2]를 이용하여 키 관리를 한다. 사용자가 상대방이 신뢰 가능하다고 판단되면 상대방의 공개키에 서명한다. 그리고 다른 사용자가 상대방의 공개키를 입수했을 때 상대방의 공개키 서명 중에 자신이 신뢰할 수 있는 사용자의 서명을 발견하면 상대방의 공개키를 신뢰할 수 있다. 이렇게 누구나 인증기관 역할이 가능하기 때문에 신뢰를 정량화하기 어렵다. 그리고 사용자가 새로운 공개키를 발급받았을 때 다른 사용자들

※ Corresponding Author : Kyungryong Seo, Address: DSLab, Pukyong National University at Daeyeon, 45, Yongso-ro, Nam-gu, Busan, Republic of Korea, TEL : +82-10-4545-6885, E-mail : krseo@pknu.ac.kr
Receipt date : Mar. 30, 2020, Revision date : Apr. 10, 2020
Approval date : Apr. 28, 2020

† Department of Computer Engineering, Pukyong National University at Daeyeon
(E-mail : kjs50458281@pukyong.ac.kr)
†† Department of Computer Engineering, Pukyong National University at Daeyeon
※ This work was supported by a Research Grant of Pukyong National University(2019)

에게 공개키에 서명을 받기가 힘들다. 그래서 해당 공개키의 신뢰도를 높이기가 힘들다.

블록체인[3]은 거래를 기록한 원장을 특정기관의 중앙 서버가 아닌 P2P(Peer to Peer) 네트워크에 분산해 공동기록 및 관리하는 기술로 정의한다. 즉 P2P 기반의 공유 원장 기술이다. 블록체인은 모든 참가자들 간에 모든 정보를 공유하기 때문에 무결성과 투명성이라는 특징을 가진다. 무결성과 투명성은 최종적으로 신뢰성을 창출한다.

본 논문에서는 블록체인 플랫폼 중 하나인 이더리움[4] 블록체인에서 키 관리를 하는 PGP 시스템을 제안한다. 사용자들 끼리 메시지를 주고받고 발신자가 신뢰 가능한 사용자인지 신뢰할 수 없는 사용자인지 검증이 가능하며 상대방의 정보와 신뢰도를 누구든지 확인할 수 있는 시스템을 구현하였다. 기존의 Web of trust가 아닌 블록체인에서 키 관리를 함으로써 신뢰성을 확보할 수 있다. 사용자의 키뿐만 아니라 기본 정보, 메시지 정보와 같은 정보들도 블록체인에 저장하여 누구든 확인 가능하여 사용자가 직접 신뢰도를 판단할 수 있다. 그리고 개인키와 같이 사용자 본인만 알아야하는 정보는 데이터베이스에서 관리하도록 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서 블록체인과 PGP에 대해 설명을 하고 최근 연구 동향에 대해 설명한다. 3장에서는 제안하는 시스템에서 구축한 키 관리 구조와 전체적인 시스템의 구조를 설계하고 블록체인에서 구현하였을 때의 이점을 설명한다. 그리고 사용자가 시스템에 정보를 등록하고 메시지를 발신하고 수신하는 기능, 신원을 확인하는 기능을 구현하고 중간 결과물을 보여준다. 4장에서는 제안하는 시스템과 기존에 블록체인을 이용하여 PKI 구조를 구현한 연구와 기존 PGP 시스템과 비교하여 평가한다. 5장에서는 결론과 제안하는 시스템의 활용성에 대해 서술한다.

2. 관련연구

블록체인은 네트워크에 참가하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술이다. 블록체인은 모든 데이터를 분산, 저장하기 때문에 모든 참가자들이 데이터를 공유한다. 그래서 블록체인은 투명성과 무결성의 특징을 가진다. 모든 참가자들이 공유하고 있는 데이터가 일치해야하기 때문에 데이터를 조작하기 위해서는 모든 참가자의 데이터를 조작해야한다. 그래서 블록체인은 무결성의 특징을 가진다고 할 수 있다[5].

PGP는 온라인 통신 시스템의 정보 보호, 보안 및 인증 서비스를 제공하도록 설계된 암호화 소프트웨어이다. PGP는 공개키를 사용하여 암호화를 하며 메시지 암호화와 전자서명의 기능을 가지고 있다. 사용자의 공개키와 개인키가 존재하며 모두 키 링(Key Ring)에서 관리된다.

위의 표는 공개키 링과 개인키 링의 구성요소를 보여준다. PGP에서는 Web of trust에서 키 링을 관리한다. Web of trust는 신뢰하는 사용자들을 통해서 키를 관리하는 방식이다.

이전부터 온라인 환경에서의 신원 확인을 위한 인증 시스템에 대한 연구[6]가 이루어졌으며 최근에는 블록체인을 이용하여 정보 보호, 보안 및 인증 서비스 분야에 활용하는 연구가 많이 이루어지고 있다. 그 중 하나는 메시지 전송을 필요로 하는 송신 노드에서 메시지 트랜잭션을 생성한 후, 서명을 하고 다른 노드에 전송한다[7]. 이를 수신한 노드는 수신한 메시지와 함께 전송된 공개키를 기반으로 송신 노드의 ID를 생성한 후, 해당 ID가 존재하는지 확인하고

Table 1. Private Key Ring Component

Component	Explanation
Timestamp	Date the key was created
Key id	Value to identify the key
Public key	Public key Contents
Private key	Private key Contents
User id	Value to identify the user

Table 2. Public Key Ring Component

Component	Explanation
Timestamp	Date the key was created
Key id	Value to identify the key
Public key	Public key Contents
Owner trust	Reliability in the owner
User id	Value to identify the user
Signature	Electronic signature
Signature trust	Reliability in the signature
Key legitimacy	It is set based on Owner trust and Signature turst

ID가 존재할 경우 송신 노드는 신뢰성 있는 노드로 구분되는 구조를 지닌다. 기본적인 블록체인 인증 구조이지만 단지 송신 ID 유무만 확인하기 때문에 신뢰성이 떨어진다. 본 논문에서는 전자 서명을 사용하여 송신자가 존재하고 송신자가 보낸 메시지가 맞는지 확인이 가능하여 신뢰성이 더 높다고 볼 수 있다. [8]의 연구에서는 스마트 계약을 이용해 PKI 구조를 구현 하였다. 이 구조에서는 사용자 누구든지 서명과 인증서 발급을 누구나 할 수 있게 구현되어있다. 기존 PKI 구조의 중앙 집중 형 구조를 벗어났지만 인증서의 폐기는 서명한 계정만 실행 할 수 있는 구조이기 때문에 누군가 의도적으로 인증서에 서명을 하면 의도적으로 서명한 계정만 서명을 해지 할 수 있기 때문에 취약한 점이 존재한다. 그 외에 [9, 10]연구에서도 블록체인을 이용하여 PKI 구조를 구축하였다. 다른 연구들[11, 12]에서는 중앙 집중 형 구조인 PKI가 아닌 PGP를 이용하여 PGP 인증서를 비트코인 기반으로 구현하거나 블록체인 관련 데이터를 PGP 인증서에 통합하여 기존의 PGP와 Web of trust에 대한 개선 사항을 제시하기도 한다. 본 논문에서는 인증서라는 구성요소가 없어도 신뢰성이 높은 구조를 구현하였기 때문에 다른 시스템에 적용하기 쉬운 범용성이 높은 구조라고 할 수 있다. [13]의 연구에서는 차량환경에서 전달되는 메시지 내용의 신뢰성 확보를 위해 블록체인을 이용해 메시지의 신뢰성을 판단하는 평판시스템을 제안하였다.

최근에는 kakaopay에서 Hyperledger Fabric[14]으로 블록체인 인증 서비스를 구현하여 공인인증서를 대체 하고 있다. 그리고 의료 목적의 데이터를 분석하고 분석 결과를 의사에게 전송할 때 생기는 몇 가지 문제가 있는데 대표적으로 한 병원에서 데이터를 저장하면 사고가 날 경우 데이터가 손실되는 취약성 문제와 의료 데이터가 변조될 가능성이 있는 무결성의 문제가 존재한다. 그래서 [15]의 연구에서는 BSN(Body Sensor Network)과 블록체인을 병합하고 BSN의 바이오센서 노드를 사용하여 블록체인의 효율적인 키 관리 제도를 제안한다. 이렇듯 대기업이나 의료 분야에서나 다양한 분야에서도 현재 블록체인을 이용한 보안 및 인증서비스에 대한 관심이 매우 높은 상황이다.

3. 설계 및 구현

3.1 설계

본 논문에서는 투명하고 신뢰성이 높은 인증 시스템을 구현하기 위한 키 관리 구조를 제안한다. 제안하는 키 관리 구조는 Fig. 1과 같다. 사용자는 공개키와 개인키를 가진다. 그리고 공개키는 공개키 링에서 개인키는 개인키 링에서 관리된다. 그리고 기존의 공개키 링 구조에서는 공개키의 서명과 서명의 신뢰도, Key legitimacy를 관리 하였지만 제안하는 구조에서는 관리하지 않는다. 블록체인 환경은 이미 무결성과 투명성을 가지고 있기 때문에 굳이 다른 사용자가 공개키가 신뢰 가능하다고 서명을 할 필요가 없고 소유자의 신뢰도만 관리해도 충분하다.

공개키의 경우 누구나 확인 할 수 있어야하기 때문에 블록체인에서 관리하고 개인키의 경우 사용자 본인만 확인 가능해야 하기 때문에 데이터베이스에서 관리하도록 설계하였다. 그리고 블록체인 환경에서 발급되는 사용자 hash 값을 id 값처럼 사용하여 키 관리를 한다. 공개키 링에서 소유자 신뢰도를 관리하기 때문에 모든 사용자는 서로 간의 신뢰도를 확인 할 수 있게 설계 하였다.

본 논문에서 구현한 시스템은 메시지의 신뢰성 보다 사용자의 신원에 대한 신뢰성에 중점을 두고 설계를 했기 때문에 전자서명 알고리즘을 이용하였다. 메시지도 블록체인 환경에서 관리 하도록 설계를 해서 메시지가 변경되지 않았다는 것이 확인 가능하고 전자서명 알고리즘을 통해 신뢰 가능한 상대방인지 확인 한다면 메시지 무결성을 확보 할 수 있다.

본 논문에서 제안하는 시스템의 구조는 Fig 2와 같다. 사용자끼리 메시지를 주고받는 클라이언트를 설계하였다. 블록체인에서는 공개키 링 뿐 아니라 사

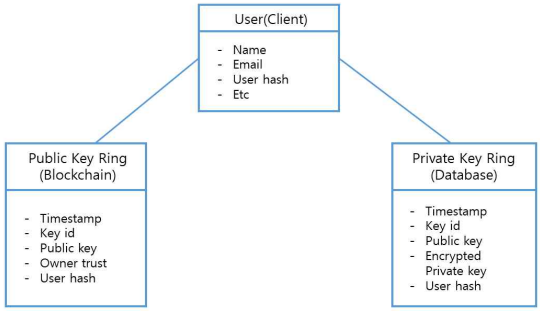

Fig. 1. Suggested key management structure.

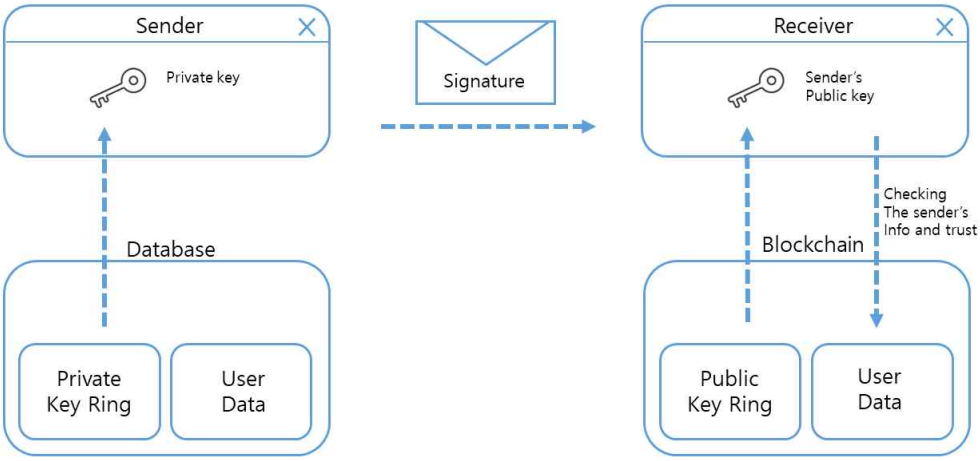

Fig. 2. System structure.

용자 정보와 발신자가 수신자에게 보낸 메시지와 메시지 hash값, 서명 값을 관리하도록 하여 수신자가 메시지의 내용이 변하지 않았다는 것을 직접 확인 할 수 있다. 데이터베이스도 마찬가지로 개인키 링뿐 아니라 사용자 정보와 메시지 정보를 함께 관리하도록 하였다. 그리고 클라이언트에서는 누구든지 발신자의 정보 및 메시지의 서명, 발신자의 신뢰도 등을 alert 창을 통해 확인 할 수 있도록 구현하였다.

3.2 구현

본 논문에서는 블록체인 환경에서 PGP의 전자서명 알고리즘을 이용해서 서로 메시지를 주고받고 상대방이 신뢰 가능한 사용자인지 확인 가능한 인증 시스템을 구현하였다. 시스템 클라이언트는 Java-script/React를 이용하여 구현하였고 서버는 node/express를 사용하여 구현하였다. 서버를 통해 Mongo DB와 연동하였으며 스마트 계약은 Solidity 언어를 사용하여 구현하였다.

3.2.1 블록체인의 이점

제안하는 PGP 인증 시스템에서 키 관리는 Web of trust가 아닌 블록체인에서 이루어진다. 공개키는 모든 사용자가 알 권리가 있어 키 링의 구조로 블록체인 환경에서 관리 된다. 블록체인은 이전 블록 hash 참조로 인해 공격자에 의해 데이터가 변경될 수 없다. 그래서 블록체인은 본질적으로 데이터 무결성을 가진다. 또한, 모든 블록 데이터를 참가자들이 공유하기 때문에 투명성을 가진다. 무결성과 투명성은 최종적으로 신뢰성을 창출해낸다. 인증 시스템에서 신뢰도는 중요한 요소라고 할 수 있다. 제안하는 시스템에서는 블록체인 환경을 이용함으로써 신뢰성을 확보할 수 있는 이점을 가진다.

3.2.2 주요 기능

처음 클라이언트 화면에서 회원 정보를 입력하면 데이터베이스와 블록체인에 Fig. 3과 같은 구조로 정보가 등록된다. 사용자 정보는 데이터베이스와 블록체인에 간단하게 이름과 이메일 hash 값이 등록되고 개인키 링 정보는 데이터베이스에 공개키 링 정보는 블록체인에 등록된다. 블록체인에 등록하기 위해서는 스마트 계약이 실행되어야 한다. 사용자 정보 등록은 전달인자들을 userAppend 계약을 이용해 블록체인 구조체에 저장한다. 공개키 링 정보 또한, 전달인자들을 keyRingAppend 계약을 이용해 블록체인 구조체에 저장한다. 개인키는 사용자 본인만 확인 가능해야 하기 때문에 데이터베이스에 암호화를 해서 관리한다. 본 논문에서는 AES 알고리즘을 이용한 암호화 값을 데이터베이스에서 관리한다. 그리고 keyId 경우는 데이터베이스에서 자동으로 지급하는 id 값으로 관리한다. 공개키 링은 스마트 계약을 통해 id 값을 부여하고 관리한다.

Fig 4는 실제로 데이터베이스에 저장된 값의 형태이다. (a)는 사용자 정보, (b)는 개인키 링 정보이고 ObjectId가 데이터베이스에서 자동으로 지급하는 id

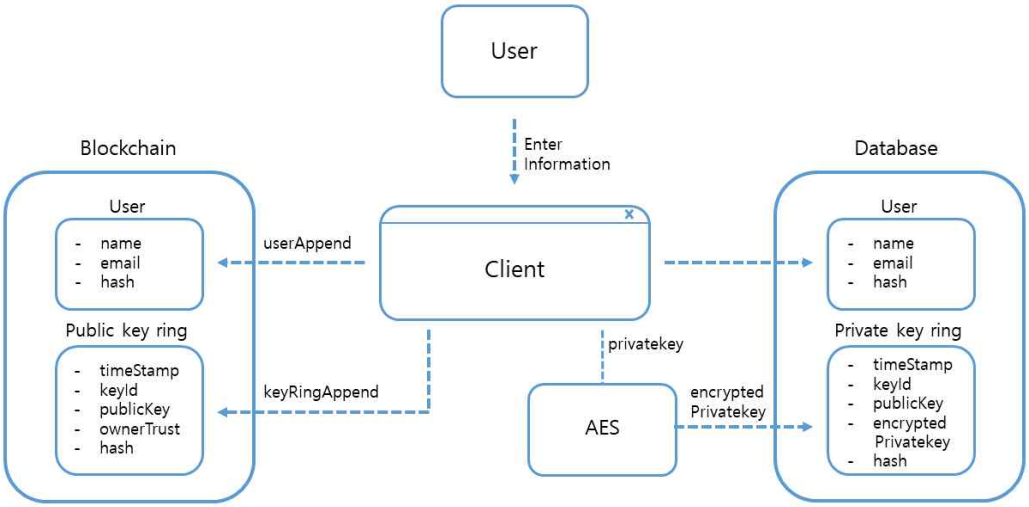

Fig. 3. Information registration structure.


```
_id: ObjectId("5e562000aef76229100bbf82")
name: "Kim Daehan"
email: "kjs50458281@gmail.com"
hash: "0x12a70770e246F1fCA22FFb1A595276f82E1bc580"
reg_date: 2020-02-26T07:36:32.550+00:00
__v: 0
```


(a)


```
_id: ObjectId("5e562000aef76229100bbf83")
publickey: "-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDmhZuYouw..."
encrypted_prkey: "0¶ENF¥-º8á¥¶¦7yC$m□□x&` □◀¯«dÃùµ¶ÍÙ%2|UøaðTÀÎ□x3ãtÜD□ª□┐oì┐ulà□┐▲kµ®Ç..."
user_hash: "0x12a70770e246F1fCA22FFb1A595276f82E1bc580"
time_stamp: 2020-02-26T07:36:32.870+00:00
__v: 0
```


(b)

Fig. 4. Information stored in database (a)User info, (b)Private key ring info.

로 개인키 링에서는 Key id의 역할을 한다. 본 논문에서 사용한 데이터베이스는 MongoDB이며 NoSQL의 한 종류이다.

제안하는 시스템에는 메시지 발신, 수신 기능을 Fig. 5와 같은 구조로 구현 하였다. 사용자가 상대방에게 메시지를 전송하기 위해서는 시스템에 정보가 등록된 사용자 리스트에서 전송하고자 하는 상대방을 선택하고 메시지를 작성하고 전송 버튼을 클릭하면 메시지가 전송된다. 제안하는 구조에서의 서버는 클라이언트와 데이터베이스를 연동하고 클라이언트에서 데이터베이스로 정보를 전달하는 역할을 하고 있다. 서버에서 발신자의 hash값을 이용해 데이터베이스 Private key ring에서 Private key를 이용하여 서명 값을 만든다. 그리고 데이터베이스의 Msg 테이블에 발신자의 hash는 from 컬럼에 저장하고 수신자의 hash는 to 컬럼에 저장하고 메시지 원문 내용은 Content 컬럼에 저장하고 서명 값은 Signature 컬럼에 저장한다. Fig. 6은 실제로 Msg 테이블에 저장된 값의 형태이다. 그 다음 블록체인의 Message 구조체에 메시지 정보를 msgAppend 계약을 통해 저장한다. 메시지 원문 내용 Content와 서명 값 Signature와 Msg 테이블에서 자동으로 생성하는 ObjectId값

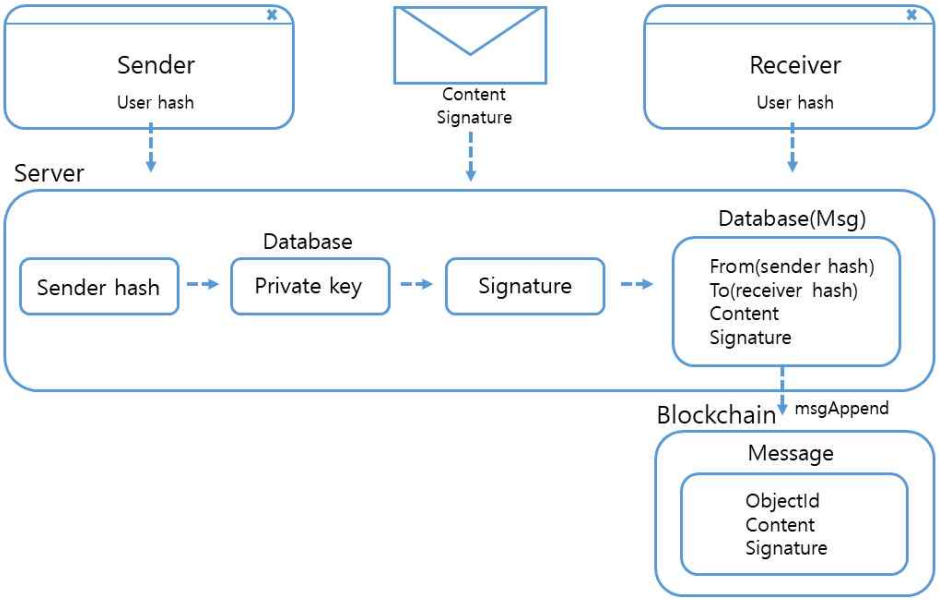

Fig. 5. Message sending structure.


```
_id: ObjectId("5e57677d7a03ab3b18c498dc")
from: "0xd0836986cE2662aEA955634764A324BEEab4E165"
to: "0x12a70770e246F1fCA22FFb1A595276f82E1bc580"
content: "Test Message"
sign: "¯0Sxõ¬<Þ¥âv}•Z¶ýÑ(ôÁ"□Û/T]oÄF*ómÞÑ4-ÿHåÎgV}M□Â[0dl%0□S□il└ÆtÑ-□&"
date: 2020-02-27T06:53:49.385+00:00
__v: 0
```


Fig. 6. Message information stored in the database.

을 불러와서 id 변수에 저장한다. 그리고 id 변수는 Message 구조체에서 식별자 역할을 한다.

수신자 측에서는 클라이언트에 접속하면 전자서명 알고리즘을 이용해서 인증된 사용자 즉 신뢰 가능한 사용자가 전송한 메시지인지 검증한 후에 신뢰 가능하다고 판단되는 메시지는 인증된 메시지 리스트에서 확인 가능하고 신뢰 가능하다고 판단되지 않는다면 인증되지 않은 메시지 리스트에서 확인 가능하다.

수신자 측에서 발신자가 신뢰 가능한 사용자인지 검증하기 위한 정보는 Fig. 7과 같다. 수신자 측 클라이언트에 접속했을 때 출력하는 정보를 consol에 출력한 그림이다. 첫 번째 정보는 발신자의 hash 값이고 두 번째는 발신자의 공개키 정보이다. 그리고 sign은 메시지에 대한 서명 값이다. 유저 hash값을 이용해서 개인키 링에서 발신자의 공개키를 가져온 다음 서명 값을 복호화해서 메시지 hash 값과 비교를 한다. 비교해서 같다면 isValid값에 true값을 저장하고 다르다면 false값을 저장한다. 그리고 isValid값으로 인증된 메시지인지 인증되지 않은 메시지를 구별하는데 사용한다.


```
0xd0836986cE2662aEA955634764A324BEEab4E165 index.js:208

publickey :  -----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALg+4XXDhgoBubTod/CBTQM
S/rzuK0+k
/ffZYUFPNNiFj+7mopLW8/aGoEPfz7XS46++4yxkwi68tLj/Ohtb7nU
CAwEAAQ==
-----END PUBLIC KEY-----
sign :
"0Sxõ¬<Þ¥âv}•Z¶ýÑ(ôÁ"□Û/T]oÄF*ómÞÑ4-ÿHåÎgV}M□Â[0dl%0□S
□il└ÆtÑ-□&
isValid :  true
```


Fig. 7. Information for Verification.

제안하는 시스템에서는 클라이언트에서 alert창을 통해 발신자의 신원을 확인할 수 있다. 메시지 리스트에 표시되는 발신자의 이름, 메시지 내용을 클릭하면 신원 확인이 가능한 Fig. 8와 같은 창이 뜨도록 구현하였다.

(a)창은 이름을 클릭했을 때 뜨는 창으로 발신자의 이름, hash, email, 공개키, 신뢰도를 확인 할 수 있다. (b)창은 메시지를 클릭했을 때 뜨는 창으로 메시지 내용과 메시지에 대한 서명 값을 확인 할 수 있다. 클릭 이벤트가 발생할 때 블록체인 구조체에서 필요한 정보들을 불러 온다. 누구든 상대방의 신원과 메시지의 서명을 확인 할 수 있게 구현하여 직접 비교하여 확인 할 수 있는 투명한 시스템을 구현 하였다.

4. 평 가

블록체인은 보안성이 뛰어난 플랫폼이다. 그래서 [7]의 연구에서는 블록체인을 이용한 메시지인증 기법을 제안 하였다. 하지만 단지 송신 ID 유무로 확인하기 때문에 신뢰성이 떨어진다. 본 논문에서는 발신자의 ID가 실제 존재하는지 뿐만 아니라 발신자의 신원을 확인할 수 있게 하여 신뢰성이 높은 구조를 구현하였다. 그리고 더 나아가 최근 블록체인을 PKI 구조와 결합하는 연구[8, 9, 10]가 많이 이뤄지고 있다. 하지만 PKI 구조는 중앙 집중 형 구조로 인증기관을 무조건 신뢰해야하는 구조이다. 공격자는 인증기관만 공격에 성공한다면 사용자들을 속일 수 있다. 본질적으로 보안에 취약점을 가지고 있다. 하지만 [8]의 연구는 중앙 집중 형 구조와는 벗어난 구조를 구현하였다. 하지만 거래에 관련이 없는 사람들도 인증서를 발급하고 서명을 할 수 있다. 그리고 인증서 폐기는 서명한 사용자만 실행 할 수 있다. 누군가 의도적으로 인증서에 서명을 하면 의도적으로 서명한 사용자만 서명을 해지 할 수 있기 때문에 여전히 취약한 점이 존재한다. 본 논문에서는 중앙 집중 형 구조가 아닌 P2P 형태의 PGP구조를 블록체인으로 구현하였기 때문에 중앙 집중 형 구조의 단점인 인증기관을 무조건 신뢰해야한다는 점을 보완할 수 있다. 또한, [8]의 연구처럼 인증서에 서명을 받지 않아도 모든 사용자가 신원을 확인할 수 있어 신뢰성이 확보되기 때문에 의도적인 서명 문제에 대해 자유로울 수 있다.

(a)

(b)

Fig. 8. Identification window (a)Sender info, (b)Message info.

PKI 구조의 단점을 보완하는 PGP 시스템에도 취약한 점은 존재한다. PGP 시스템은 Web of trust 환경에서 키 관리를 한다. Web of trust 환경에서 사용자들 간의 신뢰 관계는 주관적이다. Web of trust에서 사용자의 신뢰도는 다른 사용자들이 신뢰 가능하다고 판단될 때 사용자의 공개키에 서명을 함으로써 신뢰도가 올라간다. 사용자의 공개키에 서명이 많이 추가될수록 사용자의 신뢰도 또한, 올라가는 구조이다. 따라서 신뢰도의 수준을 정량화하기 어렵다. 또한, 사용자가 새로운 키를 생성했을 때 키의 신뢰도를 높이기 위한 승인자를 찾기 어려운 점이 존재한다. 그래서 [11, 12]연구에서는 블록체인 환경을 이용하여 Web of trust에 대한 개선 사항을 제안한다. [11]연구는 비트코인을 기반으로 PGP 인증서를 구현하였고 [12]연구에서는 블록체인 관련 데이터를 PGP 인증서와 통합하였다. 하지만 비트코인 플랫폼의 경우 거래 내역으로 한정된다. 제안하는 시스템은 이더리움 플랫폼에서 스마트 계약을 이용하였고 거래 내역뿐만 아니라 다른 분야에서도 사용할 수 있는 확장성을 가지고 있다. 또한, 인증서의 형태는 서명이 필요하며 중앙 기관이 없는 P2P 구조이기 때문에

서명자도 신원과 자격이 있는 사용자인지 판단해야 한다. 그래서 본 논문에서는 인증서를 사용하지 않고 사용자들이 직접 상대방의 신원을 확인하고 판단할 수 있도록 구현하였다. 그래서 문제가 생겼을 경우 문제에 대한 책임도 복잡해지지 않는다.

본 논문에서 제안하는 시스템은 Web of trust 대신 블록체인 환경에서 키를 관리한다. 블록체인 또한, P2P 네트워크 구조를 가지고 있어 중앙 집중 형 구조의 단점을 보완할 수 있고 기존 Web of trust의 장점도 보존 할 수 있다. 그리고 블록체인 환경에서 키 관리를 함으로써 별도의 서명이 없어도 공개키의 신뢰성을 확보할 수 있다. 그래서 기존 Web of trust에서 관리되는 PGP 시스템의 단점인 신뢰성을 보완할 수 있고 사용자가 새로운 키를 생성했을 때 별도의 승인 자를 찾지 않아도 된다. 그리고 사용자가 직접 상대방의 신원을 확인하고 신뢰도를 판단할 수 있다. 그래서 별도의 인증서는 필요하지 않은 구조이다. 또한, 이더리움 플랫폼에서 스마트 계약을 이용하였기 때문에 거래, 메시지뿐 아니라 다양한 분야에 적용할 수 있는 확장성도 가지고 있다.

5. 결 론

PGP 시스템은 Web of trust에서 키 관리를 진행하는 구조이다. 그래서 다른 사용자들이 사용자의 신뢰도를 측정하고 판단하여 서명함으로써 다른 사용자들도 사용자가 신뢰 가능한지 판단한다. 그렇기 때문에 사용자 간의 신뢰 관계가 주관적이다. 주관적인 신뢰 관계는 사용자의 신뢰도를 실제 값으로 정량화하기 어려움이 존재한다. 또한, 사용자가 새로운 키를 생성하였을 때 새로운 키에 서명을 해줄 승인자들을 찾기가 어려워 키 의 신뢰도를 높이는 것에 어려움이 존재한다.

본 논문에서는 블록체인 환경에서 키 관리를 진행하는 인증 시스템을 제안하였다. 블록체인은 본질적으로 데이터 무결성과 투명성을 가지고 있어서 신뢰성이 높다. 그래서 기존 PGP 시스템보다 높은 신뢰성을 가지는 인증 시스템을 구현 하였다. 또한, 제안하는 시스템은 메시지 발신, 수신자들 간의 신뢰도를 확인할 수 있는 구조이다. 이 구조를 활용하여 스마트 거래 인증 시스템이나 전자메일 시스템에 적용하여 신뢰성을 높일 수 있다. 이처럼 신뢰성이 중요한 어떤 시스템이든 적용 가능한 범용성이 높은 구조라고 할 수 있다.

REFERENCE

[1] S. Garfinkel, *PGP: Pretty Good Privacy*, CA: O'Reilly Media, 1995.

[2] G. Caronni, "Walking the Web of Trust," *Proceeding of IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 153-158, 2000.

[3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, *Technical Report*, 2008.

[4] V. Buterin, A Next Generation Smart Contract & Decentralized Application Platform, *Ethereum White Paper,* 2014.

[5] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring Data Integrity Using Blockchain Technology," *Proceeding of Conference of Open Innovations Association IEEE*, pp. 534-539, 2017.

[6] Y.H. Park, B.U. Kong, and K.H. Rhee, "Design of an Authentication System Based on Personal Identity Verification Card," *Journal of Korea Multimedia Society*, Vol. 14, No. 8, pp. 1029-1040, 2011.

[7] J.H. Park, M.H. Yoon, Y.H. Kim, J.H. Yi, and O.K. Jeong, "A Message Authentication Scheme Based on Blockchain Techniquein the Ground Weapon System," *Korean Convertgent Contents on Future Innovations,* pp. 405-406, 2015.

[8] M.A. Bassam, "SCPKI: A Smart Contract-Based PKI and Identity System," *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 35-40, 2017.

[9] L. Axon and M. Goldsmith, "PB-PKI: A Privacy-aware Blockchain-based PKI," *Proceedings of the International Joint Conference on e-Business and Telecommunications-Volume 4:SECRYPT*, pp. 311-318, 2017.

[10] A. Yakubov, W. Shbair, A. Wllbom, D. San-

dra, and R. State, "A Blockchain-based PKI Management Framework," *Proceeding of The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain Colocated with IEEE/IFIP Network Operations and Management Symposium*, pp. 1-6, 2018.

[11] D. Wilson and G. Ateniese, "From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain," *Proceedings of International Conference on Network and System Security*, pp. 368-375, 2015.

[12] A. Yakubov, W. Shbair, and R. State, "Block PGP: A Blockchain-based Framework for PGP Key Servers," *Proceeding of International Symposium on Computing and Networking Workshops*, pp. 316-322, 2018.

[13] K.M. Lee and K.H. Rhee, "A Reputation System Based on Blockchain for Collaborative Message Delivery over VANETs," *Journal of Korea Multimedia Society*, Vol. 21, No. 12, pp. 1448-1458, 2018.

[14] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," *Proceeding of Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, pp. 4, 2016.

[15] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient Key Management Scheme for Health Blockchain," *Chinese Association for Artificial Intelligence Transactions on Intelligence Technology 3.2,* pp. 114-118, 2018.

김 대 한

2017년 2월 신라대학교 식품영양학과 학사
2019년 3월~부경대학교 컴퓨터공학과 석사과정
관심분야 : 블록체인, 정보 보안

서 경 룡

1983년 2월 부산대학교 전기기계공학과 공학사
1990년 2월 한국과학기술원 전기 및 전자공학과 석사
1995년 8월 한국과학기술원 전기 및 전자공학과 박사
1991년 10월~현재 부경대학교 컴퓨터공학과 교수
관심분야: 분산시스템, 컴퓨터 네트워크