Journal of Korea Multimedia Society Vol. 23, No. 8, August 2020(pp. 1030-1039)
https://doi.org/10.9717/kmms.2020.23.8.1030

블록체인 환경에서 Email 사용자 신뢰도 측정

김대한†, 서경룡††

Measuring Email User Reliability in a Blockchain Environment

Daehan Kim†, Kyungryong Seo††

ABSTRACT

The biggest feature of the online environment is anonymity. So it is difficult to identify the sender accurately in Email. So we use PGP to enhance the security of email. PGP is an e-mail encryption program that has become the standard for email security worldwide. But PGP has a weak point in security. PGP can identify users, but it is difficult to verify reliability. In PGP, the more reliable other users guarantee that user are, the more reliable they are. In the previous study, the PGP structure was implemented by utilizing the block chain to lay the foundation, and in this paper, the structure of the previous article is applied to the e-mail environment to measure up the sender's reliability, and a system is proposed that allows users to distinguish the reliability of the message.

Key words: Blockchain, PGP, Email, Reliability Distinguish, Evaluation

1. 서 론

PGP(Pretty Good Privacy)는 전 세계적으로 Email 보안의 표준으로 자리 잡은 전자우편 암호화 프로그램이다[1]. 사람들은 오래전부터 온라인 환경에서 서로 메시지를 주고받아왔다[2]. 우리가 알고 있는 온라인 환경의 가장 큰 특징 중 하나는 익명성이다. 발신자가 신뢰성이 높은 메시지를 보냈는지 아니면 발신자가 신뢰 가능한 사람인지 판단할 수 있어야 온라인 환경에서 개인의 정보를 보호할 수 있다. PGP는 메시지 암호화 기능과 전자서명 기능을 통해 Email의 보안의 표준으로 자리 잡았다.

PGP는 Web of trust[3]를 이용하여 키 관리를 한다. 사용자들이 신뢰 가능하다고 생각되는 사용자의 공개키에 서명을 해서 공개키의 신뢰도를 증가시키는 모델이다. 누구나 인증기관 역할이 가능하기 때문에 신뢰도의 정량화가 어렵다. 또한 새로운 공개키를 발급받았을 때 공개키에 서명을 받기가 힘들기 때문에 공개키의 신뢰도를 증가시키는 것이 어려운 일이다.

블록체인[4]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. 최종적으로 이 특성들은 신뢰성을 창출한다.

현재 Email의 메시지의 신뢰성 구분은 사용자의 스팸 설정으로 이루어지고 있어서 객관적인 구분은 힘들다. 스팸 설정은 자동 분류 옵션을 설정하여 분

※ Corresponding Author : Kyungryong Seo, Address: (48513) 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 : Jul. 10, 2020, Approval date : Jul. 24, 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)

류하고 있으며 제대로 분류되지 않을 가능성도 존재한다. 그래서 키워드 차단도 존재하지만 스팸 메일이 아닌 메일도 스팸으로 처리할 수 있는 문제점이 존재한다. 본 논문에서는 블록체인에서 키 관리를 하는 PGP 구조를 이용하여 발신자의 신뢰도를 측정할 수 있고 발신자의 신뢰도 수치에 따라 신뢰할 수 있는 메시지인지 구분할 수 있는 시스템을 제안한다. 블록체인은 본질적으로 데이터 무결성의 특징을 가지고 있다[5]. 그래서 신뢰성이 매우 높은 플랫폼이다. 제안하는 시스템에서 메시지를 작성하여 현재 상용화되고 있는 Email에 메시지를 전송한다. 전송할 때 메시지 내용 hash 값을 발신자의 개인키로 암호화를 한 서명 값을 전송하고 수신자는 발신자의 공개키로 서명 값을 복호화하여 메시지 내용의 hash 값과 같은지 비교하여 같다면 수신자의 신뢰도의 α% 수치만큼 발신자의 신뢰도를 증가시킨다. 같지 않다면 메시지는 전송되지 않는다. 즉 메시지 전송이 성공한다면 발신자는 수신자의 신뢰도 수치에 따라 자신의 신뢰도를 증가시킬 수 있다. 하지만 수신자가 메시지를 삭제한다면 삭제한 메시지로 인해 증가했던 신뢰도 수치에 고정 수치를 더하여 감소시킨다. 메시지를 삭제하는 행위는 그 메시지가 신뢰할 만한 메시지가 아니라고 수신자가 판단하기 때문에 발신자의 신뢰도를 감소시킨다.

Email뿐 아니라 현재 온라인 환경의 시스템은 익명성으로 인해 사용자들에 대한 신뢰도는 높지 않지만 매우 중요한 요소이다. 특히 금전적인 요소가 이동하는 시스템의 경우 신뢰도가 더욱 중요하다. 블록체인 환경에서 제안하는 시스템의 구조를 활용한다면 온라인 환경에서 신뢰도가 중요한 시스템에 적용하여 기존 시스템보다 신뢰도가 높은 시스템을 구현할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 블록체인과 이더리움, PGP에 대해 설명을 하고 최근 연구 동향에 대해 설명한다. 3장에서는 제안하는 시스템에서 구축한 키 관리 구조와 전체적인 시스템의 구조를 설계하고 사용자가 시스템에 정보를 등록하고 Email 메시지를 발신하고 수신하는 기능, 신뢰도가 증가하고 감소하는 기능을 구현하고 중간 결과물을 보여준다. 4장에서는 제안하는 시스템과 기존에 블록체인을 활용하여 구현한 인증시스템과 비교하여 평가한다. 5장에서는 결론과 향후 계획에 대해 서술한다.

2. 관련연구

블록체인은 네트워크에 참가하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술이다. 간단히 말하면 정보를 변조하기 어려운 형태로 공유하는 시스템이다. 블록체인 네트워크는 중앙 관리 기관이 존재하지 않고 P2P 네트워크를 이용해 모든 참가자가 연결되어 있다. 기존 중앙에서 관리하는 네트워크의 구조는 중앙 기관을 멈추면 작동이 중단되었지만 블록체인 네트워크는 모든 참가자, 즉 모든 노드의 작동을 중단해야 한다. 또한 노드들이 공유하고 있는 정보는 블록 생성 이후 현재까지 모든 정보이다. 블록체인 네트워크에서 공유는 중앙에 있는 데이터를 복사해 공유하는 것이 아니라, P2P 네트워크를 이용해 각 노드가 정보를 복사해 가며 동기화하는 것을 의미한다. 그렇기 때문에 모든 노드들이 공유하고 있는 정보가 일치해야 하기 때문에 정보를 조작하기 위해서는 모든 노드의 정보를 조작해야 한다. 그래서 블록체인은 무결성의 특징을 가진다고 할 수 있다. 그래서 블록체인은 정보를 변조하기 어려운 형태로 공유하는 시스템이라고 할 수 있다. 예전에는 블록체인이 비트코인이라는 가상 화폐의 주요 기술로 사용되었다. 비트코인은 거래 내역을 모든 노드가 공유하는 응용 프로그램이다. 하지만 이제는 거래 내역뿐 아니라 다양한 정보를 모든 노드가 공유하는 기술로 진화하고 있으며 꾸준히 연구되고 있는 기술이다.

이더리움[6]은 블록체인 기술이 거래나 결제뿐 아니라 계약서, Email, 전자투표 등 다양한 분산 어플리케이션을 만들 수 있게 하는 플랫폼이다. 이러한 확장성을 제공할 수 있는 이유는 스마트 계약을 실행할 수 있기 때문이다. 스마트 계약은 개발자가 원하는 조건을 코딩할 수 있기 때문에 다양한 분야의 분산 어플리케이션을 만들 수 있게 한다. 그리고 Solidity라는 자바 기반의 독립적인 프로그래밍 언어를 통해 작성된다.

PGP는 온라인 통신 시스템의 정보 보호, 보안 및 인증 서비스를 제공하도록 설계된 암호화 소프트웨어이다. 크게 메시지 암호화와 전자서명의 기능을 가지고 있으며 공개키를 이용하여 암호화를 한다. 그리고 이때 사용되는 공개키와 개인키는 Web of trust에서 키 링(Key Ring)의 형태로 관리된다. Web of

trust는 웹 사이트 평판 및 검토 서비스이며 키 관리는 다른 사용자들의 평판에 의해 이루어진다. 어떠한 공개키에 다른 사용자들의 평판이 신뢰 가능하다고 여겨지면 신뢰 가능한 공개키이고 신뢰할 수 없다는 평판이면 신뢰할 수 없는 공개키이다.

예전부터 Email의 신뢰도를 증가시키기 위한 연구는 이루어져왔다[7]. 신뢰도가 낮다는 것은 발신자의 신원 확인이 어렵거나 신뢰도 측정이 어렵기 때문이다. 그래서 Email뿐 아니라 이전부터 온라인 환경에서의 신원 확인을 위한 인증 시스템에 대한 연구[8]가 이루어졌으며 최근에는 블록체인을 활용한 인증시스템 연구가 많이 이루어지고 있다[9, 10]. 그리고 블록체인을 이용해 PKI 구조를 구축하는 연구도 많이 이루어지고 있으며[11, 12, 13] PKI 구조의 단점을 보안한 PGP 구조를 블록체인을 이용하여 비트코인 기반 PGP 인증서를 구현하거나[14] 블록체인 관련 데이터를 PGP 인증서에 통합하여 PGP의 취약점을 개선하기도 하였다[15]. 다른 연구[16]에서는 블록체인을 사용하여 이메일의 무결성을 검증하는 효율적인 구조를 제안하였다. 그리고 Email뿐 아니라 차량환경에서 전달되는 메시지 내용의 신뢰성을 판단하기 위해 블록체인을 이용한 평판시스템의 연구도 이루어졌다[17]. 이처럼 최근에는 블록체인을 이용하여 기존 시스템의 신뢰성을 확보하거나 증가시키는 연구가 많이 이루어지고 있는 추세이다.

이전 연구[18]에서는 블록체인 환경에서 PGP 구조를 구축하여 인증시스템을 구현하였다. 본 논문에서는 이전 연구를 기반으로 확장하여 Email 환경에 적용시켜 Email 메시지의 신뢰성을 수신자가 구분할 수 있는 시스템을 제안한다.

3. 설계 및 구현

3.1 설계

본 논문에서는 Email 보안 표준인 PGP 구조를 블록체인 환경에서 구현하고 수신자의 신뢰도에 따라 발신자의 신뢰도가 증가하고 그 신뢰도에 따라 메시지의 신뢰성을 구분할 수 있는 시스템을 제안한다. 제안하는 시스템의 키 관리는 Fig. 1과 같이 블록체인 환경에서 공개키를 키 링의 구조로 관리하고 데이터베이스에서 개인키를 키 링의 구조를 관리하도록 설계하였다. 공개키 링은 Timestamp, Key id, Public key, Owner trust, User hash 값을 관리하고 개인키 링은 Timestamp, Key id, Public key, Encrypted Private key, User hash 값을 관리한다. 그리고 블록체인에서 발급되는 사용자 hash 값을 id 값처럼 사용하여 키 관리를 한다.

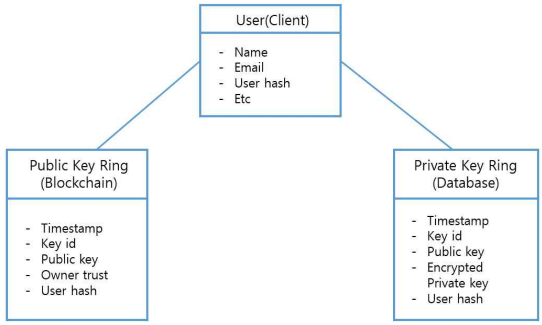


Fig. 1. Suggested key management structure.

제안하는 시스템의 구조는 Fig. 2와 같다. 발신자가 제안하는 시스템에서 메시지를 작성하고 전송 버튼을 누르면 발신자의 hash 값과 블록체인의 구조체에 저장되어 있는 신뢰도, 이름, 발신자의 Email, 수신자의 Email을 서버에 전송한다. 서버에서는 발신자의 hash 값을 이용해서 데이터베이스의 개인키 링에서 개인키를 구해서 서명 값을 만든다. 메시지 전송이 성공하면 수신자는 발신자의 공개키로 서명 값을 복호화하여 메시지 hash 값과 비교하여 같다면 수신자 신뢰도의 α% 수치만큼 발신자의 신뢰도를 증가시킨다. 그리고 수신자가 발신자의 메시지를 삭제한다면 발신자의 신뢰도는 그 메시지로 인해 증가했던 신뢰도 수치와 고정 수치가 더해져 감소시키도록 구현하였다. 이렇게 측정된 신뢰도가 β 미만일 경우에는 제목에 (unreliable) 이라는 문구를 추가해서 전송한다.

그리고 신뢰도가 증가하고 감소하는 구조는 Fig. 3과 같이 설계하였다. 메시지를 전송할 때 서명 값을 복호화하여 메시지 hash 값과 비교하여 같다는 것이 검증되면 수신자의 신뢰도 α% 수치 만큼 발신자의 신뢰도가 증가한다. 그리고 수신자가 메시지를 삭제한다면 서명 검증으로 인해 증가했던 신뢰도 수치와 고정 수치 γ을 합하여 발신자의 신뢰도를 감소시킨다. 즉 신뢰도가 높은 사용자가 메시지를 수신하여 신뢰할 수 있는 메시지라고 판단한다면 더 높은 신뢰도를 획득할 수 있는 구조이다. 신뢰도가 낮은 사용

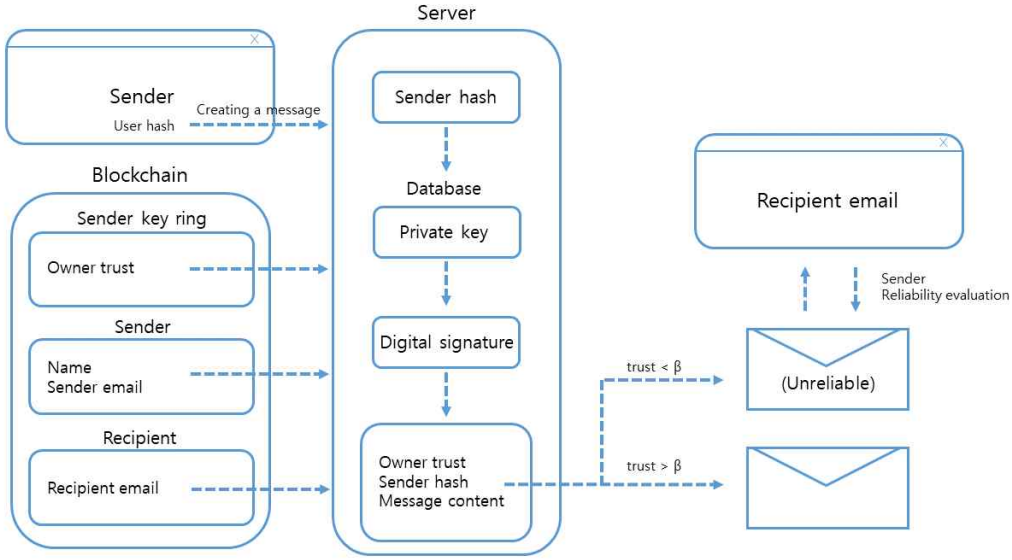


Fig. 2. Suggested system structure.

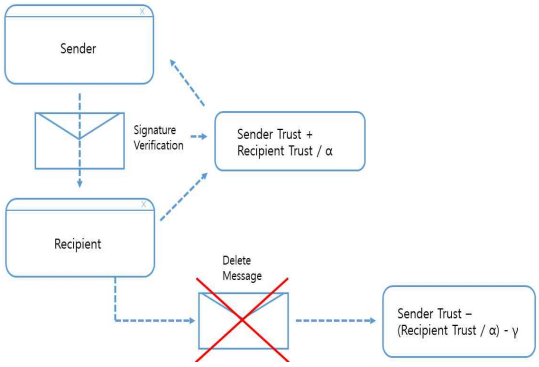


Fig. 3. Reliability increment, reduction algorithm.

자보다 신뢰도가 높은 사용자가 신뢰할 수 있는 메시지라고 판단하는 것이 더 신뢰성이 있기 때문이다. 하지만 감소하는 수치는 신뢰도가 높은 사용자가 삭제하든 낮은 사용자가 삭제하든 결국 고정 수치 γ만큼 감소한다. 신뢰도가 높은 사용자일수록 감소하는 수치도 증가한다면 한 번의 실수로 많은 신뢰도를 잃을 수 있기 때문에 상습적으로 신뢰할 수 없는 메시지를 보내는 사용자를 구분하기 위해서 감소 수치는 고정 수치로 설계하였다.

3.2 구현

본 논문에서 제안하는 시스템은 블록체인 환경에서 PGP의 전자서명 알고리즘을 이용해서 메시지를 상대방의 Email로 전송하고 수신자의 신뢰도 수치에 따라 발신자의 신뢰도가 증가하고 메시지를 삭제하면 발신자의 신뢰도가 감소하는 시스템이다. 시스템 클라이언트는 Javascript/React를 이용하여 구현하였고 서버는 node/express를 사용하여 구현하였다. 서버를 통해 MongoDB와 연동하였으며 블록체인 환경은 이더리움 플랫폼을 사용하였으며 스마트 계약은 Solidity 언어를 사용하여 구현하였다.

3.2.1 스마트 계약

Table 1은 제안하는 시스템에서 사용한 스마트 계약 함수이다. userAppend, keyRingAppend, trustAdd, trustSub의 4가지 스마트 계약 함수를 사용하였으며 userAppend는 블록체인 구조체에 사용자 정보를 등록하는 계약 함수이고 keyRingAppend는 사용자의 키 링 정보를 구조체에 등록하는 계약 함수이다. trustAdd와 trustSub는 신뢰도를 증가 또는 감소

Table 1. Smart Contract Function

Name	Explanation
userAppend	Register user information
keyRingAppend	Register user's key ring information
trustAdd	Increased reliability
trustSub	Reliability reduction

시키는 계약 함수이다. userAppend와 keyRingAppend는 사용자가 클라이언트에 처음 접속했을 때 사용자 정보를 등록할 때 사용된다. trustAdd와 trustSub는 수신자가 메일을 수신하거나 삭제할 때 발생한다. trustAdd는 메일을 수신할 때 수신자의 신뢰도 수치에 따라 증가하는 발신자의 신뢰도 수치가 달라진다. trustSub는 수신자가 메일을 삭제할 때 증가했던 수치와 고정 수치가 함께 감소된다. 즉 trustAdd와 trustSub는 신뢰도 측정에 사용되는 계약 함수이다.

3.2.2 주요 기능

처음 클라이언트 화면에서 회원 정보를 입력하면 데이터베이스와 블록체인에 Fig. 4와 같은 구조로 정보가 등록된다. 블록체인에 정보가 등록되기 위해서는 스마트 계약 함수가 실행되어야 하며 userAppend와 keyRingAppend 두 개의 스마트 계약이 실행된다. userAppend 계약은 사용자의 정보를 저장하는 계약이며 User라는 이름의 블록체인 구조체에 사용자가 클라이언트에 입력한 name, Email과 블록체인 계정인 hash값을 저장하는 스마트 계약이다. keyRingAppend 계약은 정보를 입력한 사용자에게 발급된 공개키의 정보를 저장하는 계약이며 Public key ring이라는 이름의 블록체인 구조체에 공개키 발급 시간, 공개키의 고유 ID, 공개키, 사용자의 신뢰도 그리고 블록체인 계정인 hash값을 저장하는 스마트 계약이다. 데이터베이스에도 블록체인과 마찬가지로 정보를 저장하며 User라는 테이블에 name, Email, hash값을 저장한다. 그리고 개인키는 사용자 본인만 확인 가능해야 하기 때문에 데이터베이스에 암호화를 해서 관리하며 Private key ring 테이블에 개인키 발급 시간, 개인키 고유 ID, 공개키, AES 알고리즘을 이용해 암호화한 개인키, hash 값을 저장하여 관리한다. 그리고 키의 고유 ID는 블록체인에서 관리하는 공개키의 ID는 스마트 계약을 통해 ID 값을 부여하고 관리하며 개인키의 ID는 데이터베이스에서 자동으로 지급하는 ID값으로 관리한다.

Fig. 5는 실제로 데이터베이스에 저장된 값의 형태이다. (a)는 사용자 정보, (b)는 개인키 링 정보이고 ObjectId가 데이터베이스에서 자동으로 지급하는 id로 개인키 링에서는 key id의 역할을 한다. 본 논문에서 사용한 데이터베이스는 MongoDB이며 NoSQL의 한 종류이다.

제안하는 시스템에는 메시지 발신, 수신 기능을 Fig. 6와 같은 구조로 구현하였다. 사용자가 상대방에게 메시지를 전송하기 위해서는 시스템에 정보가 등록된 사용자 리스트에서 전송하고자 하는 상대방을 선택하고 메시지를 작성하고 전송 버튼을 클릭하면 상대방의 메일로 메시지가 전송된다. 제안하는 구조에서의 서버는 클라이언트와 데이터베이스를 연동하고 클라이언트에서 데이터베이스로 정보를 전달하는 역할을 하고 nodemailer를 통해서 메시지를 수신자의 메일로 전송하는 역할을 하고 있다. 서버에서 발신자의 hash값을 이용해 데이터베이스 Private key ring에서 Private key를 이용하여 서명 값을 만든다. 그리고 데이터베이스의 Msg 테이블에 발신자의 Email 주소는 from_email 컬럼에 저장하고 수신

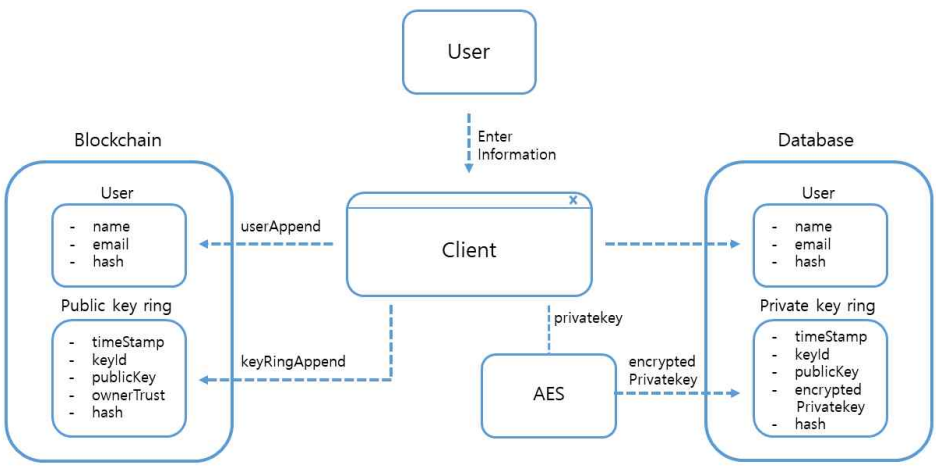


Fig. 4. Information registration structure.

```
_id: ObjectId("5ef019263a064f3f20717913")
name: "Recipient"
email: "kjs50458281@gmail.com"
hash: "0x0E8a06deEB323d1DDF3247598D6BD734982286aD"
reg_date: 2020-06-22T02:36:22.144+00:00
__v: 0
```


(a)


```
_id: ObjectId("5ef019263a064f3f20717914")
publickey: "-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKr7vlHQY6y..."
encrypted_prkey: "0¶ENF¥-º8á¥¶|7yC$m□□x&`□◀¯«dÃùµī□&(h9Û$U¶o·I└i¾>|□:WÉB&+û□¾®ñÿ□□2õ]¯ ..."
user_hash: "0x0E8a06deEB323d1DDF3247598D6BD734982286aD"
time_stamp: 2020-06-22T02:36:22.588+00:00
__v: 0
```


(b)

Fig. 5. Information stored in database (a)User info, (b)Private key ring info.

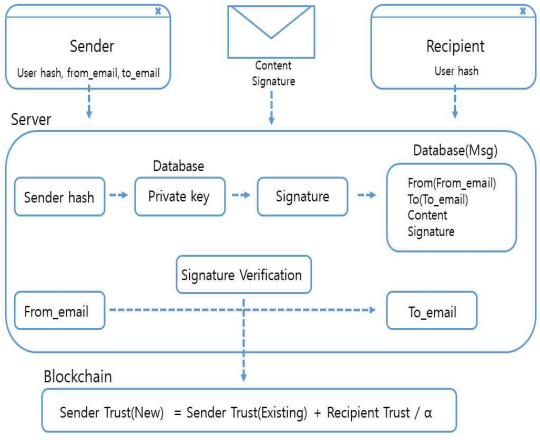


Fig. 6. Message sending structure.

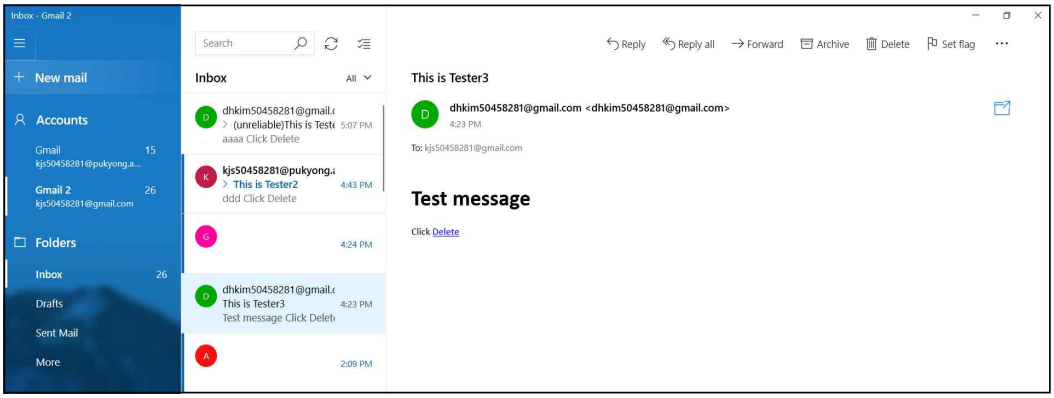
자의 Email 주소는 to_email 컬럼에 저장하고 메시지 원문 내용은 Content 컬럼에 저장하고 서명 값은 Signature 컬럼에 저장한다. 그리고 클라이언트에서 수신자와 발신자의 메일 주소를 받아와서 수신자의 메일로 메시지를 전송할 때 서명 검증을 하고 검증된 다면 발신자의 신뢰도를 수신자의 신뢰도 수치 α% 만큼 증가시킨다. Fig. 7은 실제로 Msg 테이블에 저장된 값의 형태이다.

수신자 측에서는 Email에 접속하면 발신자의 신뢰도 수치에 따라 (unreliable)의 문구가 제목에 추가되거나 제목 그대로의 메시지를 확인할 수 있다. 본 논문에서는 발신자의 신뢰도가 β이하 일 때 (unreliable) 문구를 제목에 추가하여 전송하는 구조를 구현하였다. 또한 수신자는 Email 메시지에 포함된 링크를 통해 메시지를 삭제했다고 가정하고 신뢰도를 감소시킬 수 있다. 현재 상용화되고 있는 Email 클라이언트와 제안하는 시스템을 완전히 결합하기는 어려워 링크를 클릭하면 메시지를 삭제했다고 가정하여 발신자의 신뢰도를 감소시킨다.

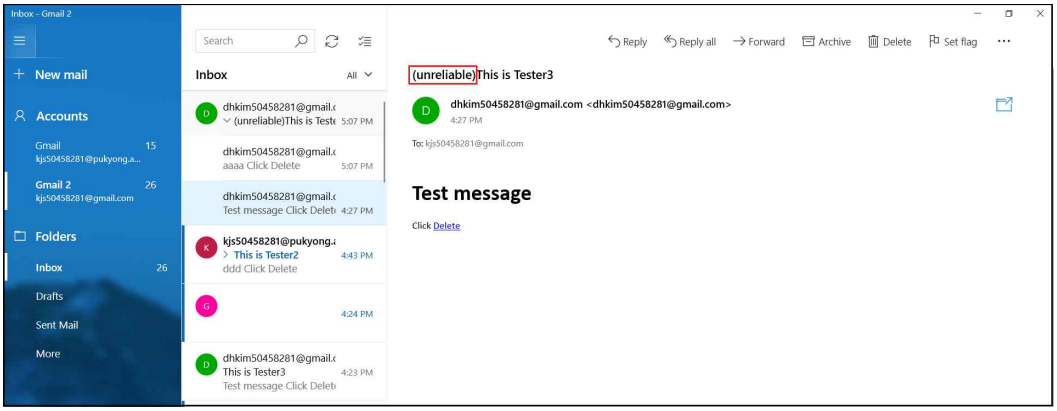
Fig. 8은 수신자의 Email 클라이언트에서 확인한 메시지이다. (a)는 신뢰도가 β이상일 경우 원문 그대로 수신한다. (b)는 신뢰도가 β미만일 경우이며 이 경우는 (unreliable)이라는 문구가 제목에 포함되어 수신되며 수신자는 이를 통해 스팸 메일뿐 아니라


```
_id: ObjectId("5ef01c4c50a02619604b3bcf")
from_email: "dhkim50458281@gmail.com"
to_email: "kjs50458281@gmail.com"
content: "This is a test message."
sign: "<r□ñM9rè>#-qi£uã#|¾¶W·ækOí□ý.+ã┐þ´¶Þ□~NW_□³x+□□'¹É=òv²z□Í!□¶Y."
date: 2020-06-22T02:49:48.347+00:00
__v: 0
```


Fig. 7. Message information stored in the database.



(a)



(b)

Fig. 8. Recipient's Email Screen (a) Confidenceable, (b) Unreliable.

신뢰 가능한 발신자인지 아닌지 판단할 수 있다.

Fig. 9는 메시지 전송이 성공했을 때 Client consol 창에 출력되는 정보이다. 수신자의 신뢰도에 따라 발신자의 신뢰도 증가 수치를 보여주고 있다. Fig. 9에서는 증가 수치 α %를 10%로 설정하였으며 위와 같은 결과를 출력하였다. 144의 경우 10%의 수치는 14.4지만 소수점 반올림, 반내림을 적용하여 구현하였다. Fig. 8 화면의 Delete링크를 클릭하면 메시지가 삭제된다고 가정하여 발신자의 신뢰도가 reliability increment value에 고정 수치 γ이 더해진 값이 감소된다.

4. 평 가

Email의 보안 표준인 PGP는 키 관리를 Web of trust에서 한다. Web of trust의 취약한 점은 신뢰관계가 주관적이라는 것이다. Web of trust에서 신뢰도를 증가시키기 위해서는 다른 사용자들이 사용자의 공개키에 서명을 해야 증가하는 구조이다. 신뢰도를 증가시키기 어렵기도 하고 다른 사용자들의 주관적인 판단에 의해 이루어지기 때문에 신뢰 관계가 주관적이라고 할 수 있다. 그래서 보안성이 뛰어난 플랫폼인 블록체인을 이용하여 신뢰 관계에 객관성을 증가시킬 수 있다. [10]의 연구에서는 블록체인을 이용한 메시지 인증 기법을 제안하였다. 블록체인 상에 저장된 정보를 기반으로 메시지의 유효성을 판별한다. 하지만 검증 노드에서 수신한 메시지에 함께 전송된 공개키를 기반으로 송신 노드의 ID를 생성한 후, 해당 ID의 유무로만 확인하기 때문에 신뢰성이 떨어진다. 본 논문에서는 수신자가 발신자의 hash도 확인할 수 있으며 수신자의 신뢰도에 따라 발신자의 신뢰도가 증가하고 수신자가 메시지를 삭제할 경우 신뢰도가 감소하는 구조를 구현하여 메시지의 유효성뿐 아니라 발신자의 신뢰도도 확인할 수 있으며

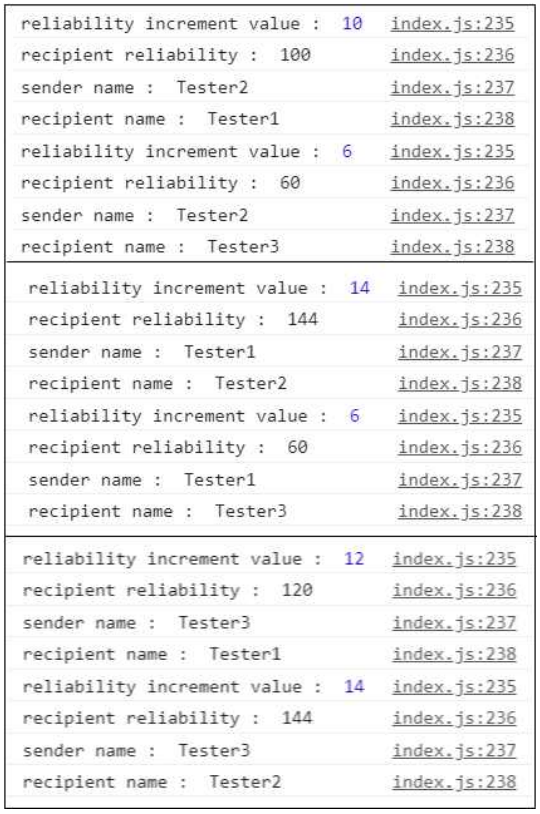


Fig. 9. Sender reliability increase by recipient reliability.

다른 시스템의 구조에서도 활용할 수 있는 유연성을 가진다. [9]의 연구는 전송된 hash 값과 저장된 hash 값이 일치한다면 해당 사용자와 암호채널을 생성하고 암호채널을 통해 개인정보를 전송하고, 수신한 개인정보의 hash를 계산한 후 저장된 hash 값과 비교해서 일치한다면 정당한 사용자로 인정하는 구조이다. 그래서 단순히 비교하는 방식 보다 발신자의 신뢰도를 수신자의 신뢰도에 따라 증가하고 수신자가 신뢰성이 없다고 판단하여 삭제하면 신뢰도가 감소하는 본 논문에서 제안하는 시스템이 신뢰성이 더 높고 활용성이 더 좋다. 그리고 더 나아가 PKI 구조를 블록체인을 이용하여 구현한 연구도 많이 이루어졌다. PKI 구조는 중앙 집중 형 구조로 인증기관을 무조건 신뢰해야 하는 구조라서 취약점이 명확하지만 [11]의 연구에서 중앙 집중 형 구조에서 벗어난 구조를 구현하여 기존 PKI 구조의 취약점을 보완하였다. 하지만 거래에 관련이 없는 사람들도 인증서를 발급하고 서명을 할 수 있고 인증서 폐기는 서명한 사용자만 실행할 수 있어서 누군가 의도적으로 인증서에 서명을 하면 의도적으로 서명한 사용자만 서명을 해지할 수 있기 때문에 여전히 취약점이 존재한다. 본 논문에서는 PGP 구조를 블록체인으로 구현하였기 때문에 중앙 집중 형인 PKI 구조의 취약점을 보완할 수 있고 인증서에 서명을 받지 않아도 블록체인의 투명한 특성 덕분에 모든 사용자가 신원을 확인할 수 있어 무결성이 확보된다. 그리고 신원 확인뿐 아니라 수신자 신뢰도에 따라 발신자의 신뢰도가 측정되어 사용자들이 직접 메시지의 신뢰성을 구분할 수 있는 장점이 존재한다. 그리고 기존 연구들 중에서도 PGP 구조를 블록체인으로 구현한 연구들이 존재한다[14, 15]. 비트코인을 기반으로 PGP 인증서를 구현하거나[14] 블록체인 관련 데이터를 PGP 인증서와 통합하기도 하였다[15]. 하지만 비트코인 플랫폼의 경우 거래 내역으로 한정되어 확장성이 떨어진다. 이전 연구[18]에서는 이더리움 환경에서 스마트 계약을 이용해 PGP 구조를 구현하여 인증시스템을 제안하였고 본 논문에서는 스마트 계약으로 구현한 PGP 구조를 Email 환경에 적용하여 확장시켰다.

본 논문에서 제안하는 시스템은 키 관리를 Web of trust가 아니라 블록체인 환경에서 한다. 또한, P2P 네트워크 구조를 가지고 있는 블록체인 환경이라서 기존의 중앙 집중 형 구조의 단점을 보완할 수 있고 공개키에 대한 별도의 서명이 없어도 블록체인 특성상 신뢰성을 확보할 수 있다. 그리고 단지 신원 확인을 통한 신뢰성 확보뿐 아니라 수신자의 신뢰도가 높을수록 발신자의 신뢰도 증가 수치가 증가하도록 구현하였다. 신뢰할 수 없는 수신자가 신뢰할 수 있는 메시지라고 판단하는 것보다 신뢰도가 높은 수신자가 신뢰할 수 있는 메시지라고 판단하는 것이 더 신뢰성이 있기 때문이다. 그리고 신뢰도 수치의 감소는 수신자의 신뢰도에 상관없이 메시지를 삭제한다면 고정적인 수치가 감소하게 된다. 한 번의 실수로 인해 신뢰도가 대폭 감소하는 것보다 반복적으로 신뢰할 수 없는 메시지를 발신했을 때 신뢰할 수 없는 사용자로 판단하기 위함이다. 그리고 감소시키는 이유는 [19]의 연구에서 필요 없는 이메일을 정기적으로 삭제하는 사용자가 45%, 즉시 삭제하는 사용자가 33%로 78%의 사용자가 필요 없다고 생각하는 이메일을 정기적이든 즉시든 삭제를 한다는 결과가 나왔기 때문이다. 필요 없는 이메일에는 신뢰할 수

없는 메일도 있고 예전에는 필요했지만 현재는 필요가 없어진 메일도 있다. 그래서 신뢰할 수 없는 메일이 아니라 메일함을 정리하기 위해 삭제하는 경우도 존재한다. 그렇기 때문에 사용자들이 어느 정도 기간마다 메일함을 정리하는지 조사하고 적정기간을 기준으로 잡고 적정기간보다 빨리 삭제하게 될 경우 메일함을 정리하는 것이 아닌 메일 내용이 신뢰할 수 없다고 판단하여 삭제하는 것으로 간주하고 신뢰도를 감소시키는 것으로 보완할 수 있다.

5. 결 론

Email은 사용자들끼리 메시지를 주고받는 시스템이고 PGP 시스템을 사용하여 보안을 유지하고 있다. 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 주관적인 신뢰 관계를 가지고 있다고 볼 수 있다. 본 논문에서는 Web of trust 대신 블록체인 환경에서 키 관리를 진행하는 PGP 구조를 구현하여 Email에 접목시킨 시스템을 제안하였다. 그리고 발신자가 메시지를 전송하고 서명 검증이 된다면 수신자 신뢰도의 α%만큼 발신자의 신뢰도가 증가한다. 또한 삭제를 하였을 경우에는 증가시킨 신뢰도에 고정 수치가 더해진 만큼 발신자의 신뢰도가 감소한다. 이렇게 측정된 신뢰도에 따라 수신되는 메시지가 신뢰할 수 있는지 없는지를 사용자가 구분할 수 있게 구현하였다. 투명한 블록체인 환경에서 이루어지기 때문에 모든 사용자들은 신뢰도 증가, 감소 내역을 확인할 수 있어 신뢰성이 높은 구조이다. 향후에는 온라인 거래 시스템과 같이 상대방의 신뢰도가 중요한 시스템에 블록체인을 적용하여 신뢰도를 증가시키는 연구를 진행할 것이다.

REFERENCE

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

[2] The History of Electronic Mail(2001), http://www. multicians.org/thvv/mail-history.html (accessed October 23, 2008).

[3] G. Caronni, "Walking the Web of Trust," *Proceedings of IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 153-158, 2000.

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

[5] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring Data Integrity Using Blockchain Technology," *Proceeding of 2017 20th Conference of Open Innovations Association*, pp. 534-539, 2017.

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

[7] S. Garriss, M. Kaminsky, M.J. Freedman, B. Karp, D. Mazieres, and H. Yu, "RE: Reliable Email," In USENIX Conference on Networked Systems Design & Implementation (NSDI), 2006.

[8] 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.

[9] S.Y. Choi, "Blockchain-based Online Identity Certification Scheme," *Proceedings of the Korean Society of Computer Information Conference*, pp. 157-160, 2018.

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

[11] 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.

[12] L. Axon and M. Goldsmith, "PB-PKI: A Privacy-aware Blockchain-based PKI," *Proceedings of the 14th International Joint Conference on E-business and Telecommunications-Volume 4: SECRYPT*, pp. 311-318, 2017.

[13] A. Yakubov, W. Shbair, A. Wllbom, D. Sandra, and R. State, "A Blockchain-based PKI Management Framework," *Proceedings 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.

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

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

[16] Email Stamping: Gmelius Blockchain Architecture (2017), https://gmelius.com/email-stamping-blockchain.pdf (accessed October 06, 2018).

[17] 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.

[18] D.H. Kim and K.R. Seo, "PGP Certification System in Blockchain Environments," *Journal of Korea Multimedia Society*, Vol. 23, No. 5, pp. 658-666, 2020.

[19] S.K. Jeong and H.J. Kim, "A Survey Study of Internet Users Attitudes for Spam Mail in Busan," *The Journal of Internet Electronic Commerce Research*, Vol. 4, No. 2, pp. 49-72, 2004.

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