공 학 석 사 학 위 논 문

블록체인에 기반한 PGP 설계와 구현

2021년 2월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

김 대 한

공 학 석 사 학 위 논 문

블록체인에 기반한 PGP 설계와 구현

지도교수 서 경 룡

이 논문을 공학석사 학위논문으로 제출함.

2021년 2월

부 경 대 학 교 대 학 원

컴 퓨 터 공 학 과

김 대 한

김대한의 공학석사 학위논문을 인준함.

2021년 2월 19일

위 원 장 공학박사 여 정 모 (인)

위 원 공학박사 한 영 선 (인)

위 원 공학박사 서 경 룡 (인)

목 차

그 림 목 차

표 목 차

블록체인에 기반한 PGP 설계와 구현

김 대 한

부 경 대 학 교 대 학 원 컴 퓨 터 공 학 과

요 약

현재 사회는 언택트 사회로 접어들고 있다. 언택트 사회에서 가장 중요한 요수중 하나는 신뢰다. 하지만 온라인 환경의 가장 큰 특징은 익명성으로 상대방을 신뢰하기 어렵다. 현재 상용화되고 있는 Email 에서는 보안을 강화하기 위해 PGP를 보안의 표준으로 하고 있다. PGP는 사용자를 식별할 수 있지만 사용자의 신뢰도를 판단하기에는 주관적인 구조다. 공개키에 다른 사용자의 서명이 많을수록 신뢰도가 높아지기 때문에 충분히 조작이 가능한 구조다. 블록체인은 근본적으로 무결성과 투명성을 가지고 있어 신뢰도가 높은 플랫폼이다. 그래서 본 논문에서는 블록체인을 활용하여 인증 구조중 하나인 PKI 구조를 설계하고 구현하여 인증 시스템에서의 신뢰성을 확인하고 PKI 구조의 단점인 중앙화를 보완한 PGP 구조를 설계하고 구현한다. 그리고 상용화되고 있는 Email 시스템에 블록체인을 활용한 PGP 구조를 접목하여 신뢰도를 증가시킨 Email 시스템을 제안한다.

Design and Implementation of a Blockchain-based PGP

Dae Han Kim

Department of Computer Engineering, Graduate School
Pukyong National University

Abstract

Now society is entering into an untact society. One of the most important factors in the untact society is trust. However, the biggest feature of the online environment is anonymity, making it difficult to trust the other person. Email, which is now commercialized, uses PGP as the standard for security to enhance security. PGP can identify users, but it is subjective to judge users' reliability. The more signatures other users have on the public key, the more reliable they are, so the structure is can fabrication. Blockchain is a highly reliable platform because it has fundamental integrity and transparency. So in this paper, we design and implement PKI structure, one of the certification structures, by utilizing the block chain, to verify reliability in the certification system and to design and implement the PGP structure which

complements the centralization, the disadvantage of PKI structure. then, we propose an email system that increases reliability by incorporating PGP structure using block chain into the email system that is being commercialized.

Ⅰ. 서론

1.1 연구의 개요

블록체인[1]은 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 데이터 분산 처리 기술이다. 블록체인의 특징은 분산 저장을 한다는 것이다. 블록의 내용을 위·변조하기 위해서는 모든 노드의 거래 데이터를 공격해야 하기 때문에 사실상 불가능에 가깝다. 그래서 블록체인은 근본적으로 무결성[2]과 투명성이라는 특징을 가진다. 최종적으로 이 특성들은 신뢰성을 창출한다. 현재 사회는 언택트 사회로 접어들고 있다[3]. 언택트 사회에서 중요한 요소 중 하나는 신뢰성이다. 그래서 신뢰성이 높은 플랫폼인 블록체인은 현재 주목 받는 기술이다.

공개키 기반 구조(Public Key Infra-structure)는 공개키 암호 방식을 바탕으로 인증서를 활용하는 구조이다. PKI 구조는 중앙 집중 형 구조이고 가장 큰 보안 약점은 중앙 기관인 인증기관(Certification Authority)을 신뢰해야 하고 인증기관은 무결성과 보안을 해칠 수 있는 강력한 능력을 가지고 있다는 것이다. 블록체인은 근본적으로 탈중앙화 되어있다. 그래서 PKI 구조를 블록체인 환경에서 구현하면 누구든 인증기관의 블록을 확인 할 수 있어 중앙 기관인 CA는 강력한 능력을 잃어서 PKI 구조의 보안 약점을 보완할 수 있다. PGP(Pretty Good Privacy)는 온라인 통신 시스템의 정보 보호, 보안 및 인증 서비스를 제공하도

록 설계된 암호화 소프트웨어이다[4]. 전 세계적으로 Email 시스템의 보안의 표준으로 자리 잡았다. 사람들은 오래전부터 온라인 환경에서 서로 메시지를 주고받아왔다[5]. 온라인 환경의 가장 큰 특징 중 하나는 익명성이다. 메시지를 보낸 발신자가 신뢰할 수 있는 사용자인지 메시지가 신뢰할 수 있는 내용인지 판단할 수 있어야 온라인 환경에서 개인의 정보를 보호할 수 있다. PGP는 메시지 암호화 기능과 전자서명 기능을 통해 Email의 보안을 담당하고 있다.

PGP는 Web of trust[6]를 이용하여 키 관리를 한다. 사용자들이 신뢰가능하다고 생각되는 사용자의 공개키에 서명을 해서 신뢰도를 증가시키는 구조이다. 모든 사용자가 인증기관의 역할이 가능하기 때문에 조작이 가능하여 신뢰도의 정량화가 어렵다. 또한 새로운 공개키를 발급받았을 때 공개키에 서명을 받기도 힘들어 공개키의 신뢰도를 증가시키는 것은 어렵다. 블록체인 플랫폼 중 하나인 이더리움[7]에서 키 관리를 하는 PGP 구조를 구축하여 사용자들 끼리 메시지를 주고받으면 수신자는 발신자가 신뢰 가능한 사용자인지 신뢰할 수 없는 사용자인지 검증이 가능하여 수신자가 직접 신뢰도를 판단 할 수 있다. 블록체인의 투명성으로 인해 발신자의 기본적인 정보와 신뢰도를 확인할 수 있기 때문이다.

1.2 연구의 필요성 및 목적

현재 Email의 메시지 신뢰성 구분은 사용자의 스팸 설정으로 이루어지고 있어서 객관적인 구분이 힘들다. 스팸 설정은 자동 분류 옵션을

설정하여 분류하고 있으며 제대로 분류되지 않을 가능성도 존재한다. 그래서 키워드 차단도 존재하지만 스팸 메일이 아닌 메일도 스팸으로 처리할 수 있는 문제점이 존재한다. 본 논문에서는 Email 보안의 표준인 PGP를 블록체인에 기반하여 설계하고 구현하였다. 그리고 Email 시스템에 활용하여 발신자의 신뢰도를 측정할 수 있고 발신자의 신뢰도 수치에 따라 신뢰할 수 있는 메시지인지 구분할 수 있는 시스템을 제안한다. 발신자는 메시지를 작성하여 수신자의 Email 주소로 메시지를 전송할 때 소량의 eth를 함께 전송한다. 그리고 수신자는 메시지를 확인하고 삭제하지 않는다면 소량의 eth를 획득하고 발신자는 수신자의 신뢰도 수치에 따라 신뢰도가 증가한다. 하지만 수신자가 신뢰할 수 없는 메시지라고 판단하여 메시지를 삭제한다면 수신자는 소량의 eth를 발신자에게 돌려주고 발신자는 신뢰도가 감소하는 구조이다. 수신자는 1차적으로 발신자의 정보와 신뢰도를 확인하고 신뢰할 수 있는 메시지인지 확인할 수 있다. 그리고 신뢰할 수 없는 메시지가 아닌 이상 소량의 eth를 획득할 수 있고 발신자는 자신의 신뢰도를 증가 시킬 수 있다.

Email뿐 아니라 현재 온라인 환경의 시스템은 익명성으로 인해 사용자들에 대한 신뢰도는 높지 않지만 매우 중요한 요소이다. 특히 언택트 사회로 접어들면서 온라인 환경에서의 신뢰도는 더욱 중요해지고 있다. 그리고 금전적인 요소가 이동하는 시스템의 경우 신뢰도는 더욱 중요하다. 블록체인에 기반한 PGP 구조를 신뢰도가 중요한 기존의 시스템에 적용한다면 기존의 시스템은 신뢰도가 증가할 것이다. 그리고 사용자들은 언택트 사회에서 좀 더 안심하고 온라인 환경을 활용할 수 있다.

1.3 연구의 환경 및 방법

본 연구에서는 블록체인 네트워크 환경을 구축하기 위하여 Ganache 2.1.0 프로그램을 이용하여 가상 계정을 생성하고 크롬 확장 프로그램인 MetaMask를 이용하여 웹에서 블록체인 지갑을 사용한다. 구현하기 위해 사용된 컴퓨터의 환경은 표 1 과 같다. 그리고 소스 코드 편집기는 Visual Studio Code를 사용하였고 사용된 프로그램 언어는 표 2 와 같다.

표 1 PC 환경

CPU	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
Memory	8.00GB
OS	Windows 10 Pro

표 2 개발 환경

클라이언트	Javascript/React
서버	node/express
데이터베이스	MongoDB
블록체인	Solidity

연구는 Ganache를 통해 그림 1 과 같이 가상 계정을 생성한 후 MetaMask와 연동하고 구현한 시스템을 크롬에서 실행 시키고 각 계정마다 이름과 Email 주소를 입력하여 데이터베이스와 블록체인에 저장시킨다. 그리고 구현된 시스템에서 각 계정의 Email 주소로 메시지를 작

성하여 전송하는 작업을 반복한 다음 정보 확인과 신뢰도 측정이 올바르게 진행되었는지 분석한다.

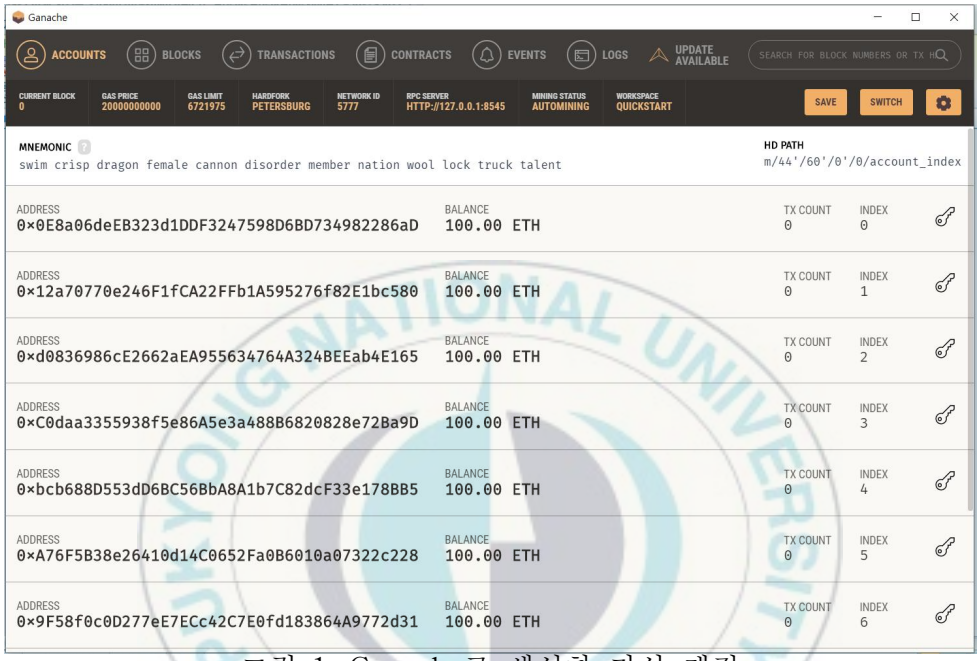


그림 1. Ganache로 생성한 가상 계정

Ⅱ. 관련 연구

2.1 PKI(Public Key Infra-structure)

공개키 기반 구조는 공개키 암호 방식을 바탕으로 인증서를 활용하는 구조이다. 인증기관의 전자 서명된 인증서 분배를 통해 공중망 상호인증을 기반으로 하는 전자 거래 인터페이스이다. PKI의 목적은 표 3 과 같다. 그리고 PKI 구조의 바탕인 공개키 암호 방식은 암호화를 하는 키와 복호화를 하는 키가 다른 방식을 의미한다. 즉 개인키와 공개키라는 두 개의 키로 구성이 되며 개인키로 암호화를 했다면 복호화 할 때는 공개키로 복호화하고 그 반대의 경우 반대로 암호화를 하고 복호화를 하는 방식이다.

표 3 PKI 목적

목적	주요 내용
인증	사용자 확인 및 검증
기밀성	송수신 정보 암호화
무결성	송수신 정보 위/변조 방지
부인봉쇄	송수신 사실 부인방지
접근제어	허가된 수신자만 접근 가능
키 관리	공개키 발급, 등록, 관리

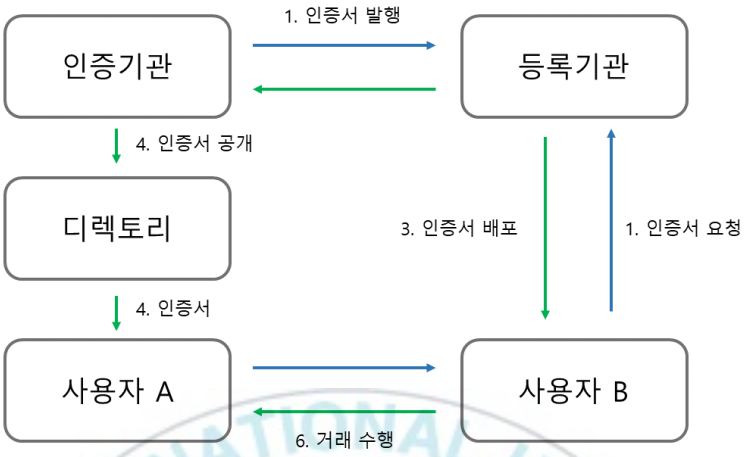


그림 2. PKI 구성도

그림 2 는 PKI의 구성도이다. 여기서 사용자는 등록기관(Registration Authority)에 인증서를 신청하면 신분을 검증 후 등록기관은 인증기관에 인증서 발급을 요청하고 인증기관은 공개키와 개인키를 생성하여 사용자에게 개인키를 발급하고 공개키와 인증서는 인증서 저장소에 저장한다. PKI는 인증기관, 등록기관, CRL(Certificate Revocation List), 디렉토리, X.509, 암호키로 구성되며 인증기관은 인증서 관리와 폐기를 하고 등록기관은 신원을 확인하고 인증서 발급 요청을 한다. CRL은 인증서 폐기 목록이고 디렉토리는 인증서, 암호키 저장과 관리를 한다. X.509는 공개키 인증서 표준 형식이고 암호키는 공개키와 개인키를 뜻한다.

2.2 PGP(Pretty Good Privacy)

PGP는 온라인 통신 시스템의 정보 보호, 보안 및 인증 서비스를 제공하도록 설계된 필 짐머만이 개발한 암호화 소프트웨어이다. Email 보안의 표준으로 자리 잡았다. 메시지 기밀성을 위한 암호화에는 IDEA, CAST, Triple-DES 등의 암호화 알고리즘을 사용하고, 메시지의 무결성을 보증하기 위한 전자서명에는 RSA 등이 사용된다. 해시 함수에는 MD5를 사용하고 키 관리에서도 RSA를 사용한다.

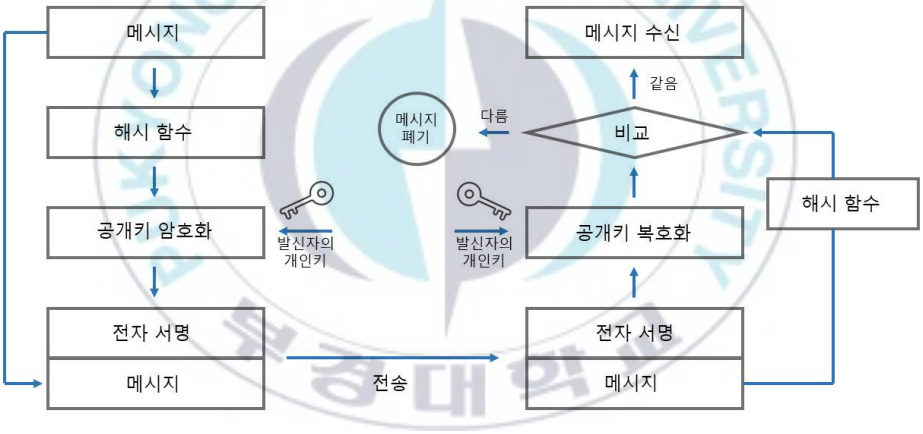


그림 3. 전자서명 알고리즘

메시지의 무결성을 보증하기 위한 전자서명 알고리즘은 그림 3 과 같다. 발신 측에서 메시지를 작성하고 메시지 내용을 해시화 한 다음 공개키 암호화를 통해 전자서명 값을 생성한 후 메시지와 함께 전송한다. 그 다음 수신 측에서는 서명 값을 복호화 한 다음 메시지 해시 값과 비

교하여 같다면 메시지가 성공적으로 전송되고 다르다면 메시지 내용이 변경된 것으로 간주하고 폐기가 되는 알고리즘이다.

PGP는 사용자 자신이 가지고 있는 개인키와 다른 사용자들에게 공개되어 있는 공개키 2개를 사용하여 안정성을 제공한다. 2개의 키는 모두 키 링(Key Ring)에 보관된다. 키 링은 사용자들이 소유하는 공개키, 개인키들을 저장하기 위한 자료 구조이다. 표 4 는 개인키 링의 구성요소이고 표 5 는 공개키 링의 구성요소이다.

표 4 개인키 링 구성요소

구성요소	설명
Timestamp	키가 생성된 날짜
Key id	개인키 식별을 위한 값
Public key	공개키
Private key	개인키 부분(암호화)
User id	사용자 식별을 위한 값

표 5 공개키 링 구성요소

구성요소	설명
Timestamp	키가 생성된 날짜
Key id	공개키 식별을 위한 값
Public key	공개키
Owner trust	소유자에 대한 신뢰도
User id	사용자 식별을 위한 값
Signature	서명 값
Signature trust	서명에 대한 신뢰도
Key legitimacy	Owner trust 및 Signature trust를 기반으로 설정

PGP에서는 Web of trust 개념을 사용하여 키를 관리한다. Web of trust는 신뢰하는 사용자들을 통해서 키를 관리하는 방식이다. 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. 즉 사용자가 다른 사용자의 공개키가 신뢰 가능하다고 판단되면 서명을 하여 사용자가 서명한 사용자의 공개키를 보증하는 형태이다. 그래서 공개키 링 요소 중에 Signature가 존재한다.

2.3 블록체인

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.

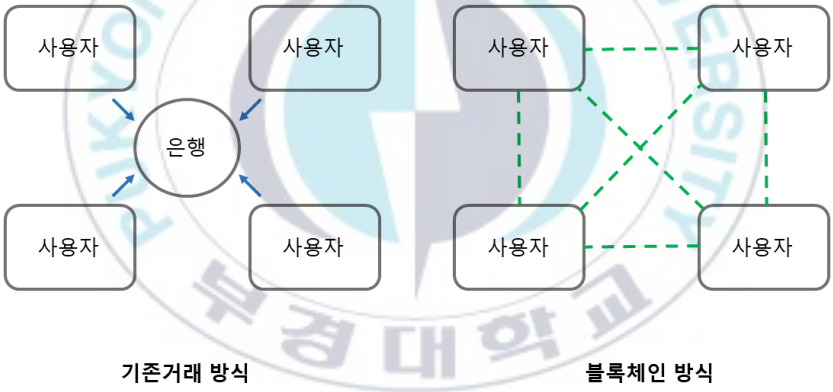


그림 4. 기존거래와 블록체인의 차이점

그림 4 는 기존 거래의 방식과 블록체인 방식의 차이점을 구조로 보여준다. 기존 거래 방식은 은행이라는 중앙기관에 의해 관리되고 블록체인 방식은 중앙기관이 없는 구조이다. 기존의 방식은 중앙 기관인 은행이 멈추면 작동이 중단된다. 하지만 블록체인 방식은 모든 사용자, 즉 모든 노드의 작동을 중단해야 작동이 중단된다. 또한 노드들이 공유하

고 있는 정보는 블록 생성 이후 현재까지 모든 정보이다. 블록체인에서 공유는 중앙에 있는 데이터를 복사해 공유하는 것이 아닌 P2P 네트워크를 이용해 각 노드가 정보를 복사해 가며 동기화하는 것을 의미한다. 그래서 모든 노드들이 공유하고 있는 정보는 일치해야한다. 정보를 조작하기 위해서는 모든 노드의 정보를 조작해야 한다. 그렇기 때문에 블록체인은 무결성의 특징을 근본적으로 가진다고 할 수 있다.

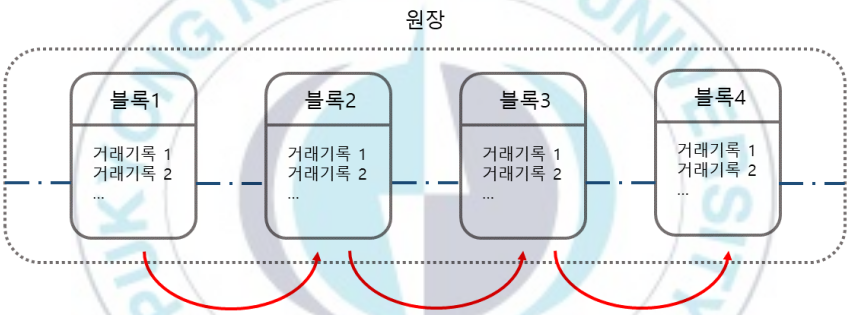


그림 5. 블록체인 구조

그림 5 는 블록과 블록이 체인형태로 연결되어 있는 블록체인의 기본 구조이다. 블록은 여러 개의 거래기록으로 묶여있는 형태다. 기존의 블록에 새로운 블록이 체인처럼 계속적으로 연결되는 데이터 구조가 블록체인이다. 그래서 모든 거래 기록을 포함하는 거대한 분산 장부라고 할 수 있다. 블록은 블록체인의 원소 개념이라고 할 수 있다. 블록은 TXID 라 불리는 블록의 해시 값을 이름으로 가지며 블록의 해시 값은 블록의

헤더 정보를 모두 합산한 후 SHA256으로 변환된 값이다. 블록은 크게 블록 헤더와 블록 바디로 구분된다. 블록 헤더는 블록 해시, 버전, 이전 블록 해시, 머클루트, 타임, bits, Nonce로 구성된다. 블록 해시는 헤더 정보를 모두 더하여 합을 구한 후 해시 함수인 SHA256으로 변환한 결과 값이고 버전은 해당 블록의 버전, 이전 블록 해시는 이전 블록의 주소 값을 가리키는 요소이다. 머클루트는 블록의 바디에 저장된 거래 기록들의 해시 트리, 타임은 블록의 생성시간, bits는 난이도 해시 목표 값을 의미하는 지표이고 Nonce는 블록을 만드는 과정에서 해시 값을 구할 때 필요한 재료 역할을 수행하는 요소이다. 블록 바디 부분에는 거래 기록들로 구성되어 있다.

2.4 이더리움

이더리움은 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. 스마트 계약이란 온라인상에서 특정 계약조건을 이행하는 것이다. 계약조건은 블록체인 위에 기록되면 처음 기록된 조건을 절대 수정할 수 가 없고 조건을 만족시킬 경우에 실행이 된다. 비트코인과의 차이점은 비트코인은 화폐역할을 하는 어플이고 이더리움은 다양한 서비스가 가능한 플랫폼이다.

Ⅲ. PKI 구조 설계 및 구현

3.1 PKI 구조에 블록체인 적용 연구 사례

이전부터 온라인 환경에서의 신원 확인을 위한 인증 시스템에 대한 연구[8]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[9]. 이를 수신한 노드는 수신한 메시지와 함께 전송된 공개키를 기반으로 송신 노드의 ID를 생성한 후, 해당 ID가 존재하는지 확인하고 ID가 존재할 경우 송신 노드는 신뢰성이 있는 노드로 구분되는 구조를 가진다. 기본적인 블록체인 인증 구조이지만 단지 송신 ID 유무만 확인하는 신뢰성이 떨어지는 구조이다. [10]의 연구에서는 스마트 계약을 이용해 PKI 구조를 구현하였다. 이 구조에서는 사용자 누구든지 서명과 인증서 발급을 할 수 있게 구현되었다. 기존 PKI 구조의 중앙 집중 형 구조를 벗어났지만 인증서의 폐기는 서명한 계정만 실행 가능한 구조이기 때문에 누군가 의도적으로 인증서에 서명을 하면 서명한 계정만 서명을 해지 할 수 있기 때문에 취약한 점이 존재한다. 그 외에 [11, 12]연구에서도 블록체인을 이용하여 PKI 구조를 구현하였다.

3.2 PKI 구조 설계

가. 스마트 계약 기능

블록체인에 기반한 PKI를 구현한 스마트 계약은 append, sign, revoke, isCertificateValid 기능들로 설계되었다. 표 6 은 스마트 계약 함수의 기능을 간단하게 설명하였다.

표 6 스마트 계약 함수 기능

기능 명	기능 설명
append	사용자의 정보로 만들어진 인증서를 블록체인 네트워크에 추가한다.
sign	블록체인에 추가된 인증서에 서명을 한다.
revoke	CA로 등록된 개체가 인증서를 취소한다.
isCertificateValid	인증서가 유효한지 체크한다.

나. 시스템 구조

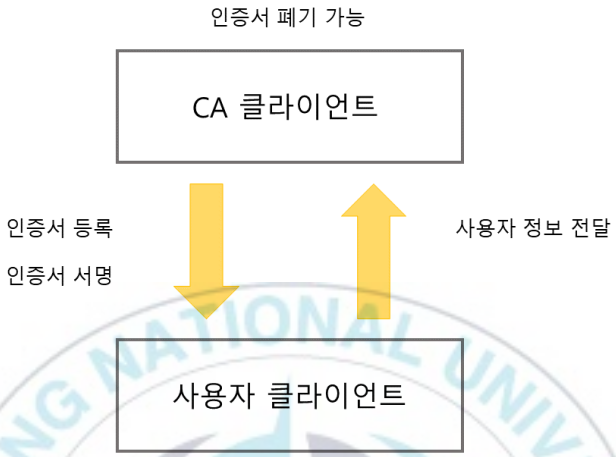


그림 6. 스마트 계약을 이용한 PKI 구조

그림 6 은 스마트 계약을 이용한 PKI 구조도이다. 우선 인증기관 역할을 하는 CA 클라이언트가 실행될 때 접속한 소유자 계정을 블록체인 네트워크에 등록한다. 등록된 계정은 사용자들에게 인증서를 발급하고 서명하고 폐기할 수 있다. 사용자 정보가 CA 클라이언트로 넘어왔을 때 append 함수를 이용해 블록체인 네트워크에 인증서 정보를 저장할 수 있다. 저장되는 정보는 사용자의 공개키가 포함된 인증서 데이터와 인증서 데이터를 해시한 값이다. 저장하면 인증서 ID 값이 반환된다. 반환된 인증서 ID 값을 이용해서 sign 함수로 블록체인에 서명 값을 등록할 수 있다. sign 함수로 추가되는 정보는 인증서 ID와 서명을 한 계정 주소, 인증서 만료 시간, 그리고 인증서 데이터를 해시한 값을 발급자의 개인키로 암호화 한 값이다. 그리고 인증서 폐기 목록에 서명 ID를 추

가 하고 false 값을 입력한다. revoke 함수는 사용자의 인증서를 폐기하는 역할을 한다. revoke 함수는 인증서 폐기 목록에 있는 서명 ID를 true 값으로 변경시킨다.

3.3 PKI 구조를 이용한 인증 시스템 구현

본 논문에서는 이더리움 환경에서 스마트 계약을 이용해 PKI 구조를 설계하고 인증 시스템을 구현하였다. CA 클라이언트와 사용자 클라이언트를 구현하였고 CA 클라이언트에 접속한 계정을 CA로 등록한다. 사용자 클라이언트에서 사용자 정보를 CA 클라이언트로 넘겨주고 CA 클라이언트에서 사용자 정보를 받아 CA 클라이언트에 내장되어 있는 JSON 형태의 인증서 파일에 입력한다. 사용자 정보가 등록될 때 공개키와 개인키를 발급한다. CA 클라이언트에서 인증서 발급 버튼을 클릭하면 해당 사용자 인증서 데이터를 SHA512 함수를 이용해 해시 값을 구한다. 그리고 append 함수가 실행되어 인증서 데이터와 해시 값을 이더리움 네트워크에 추가한다. 그 다음 해시 값을 사용자의 개인키로 암호화 한다. 암호화한 값이 서명 값이고 서명 값 알고리즘은 그림 7 과 같다.

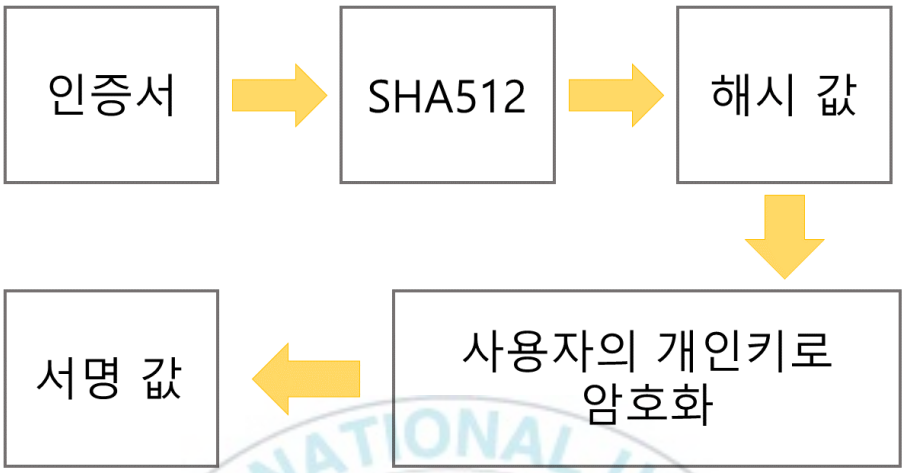


그림 7. 서명 값 생성 알고리즘

그림 8 은 구현한 인증 시스템을 통해 이더리움 네트워크에 추가된 사용자 인증서 데이터와 인증서 데이터를 SHA512 함수를 이용해 구한 해시 값과 그 값을 사용자의 개인키로 암호화한 서명 값이다.

그림 8. 블록체인에 저장되는 인증서 정보

그 다음 sign 함수를 실행해서 인증서 ID와 서명을 한 계정 주소, 인증서 만료 시간, 서명 값을 이더리움 네트워크에 추가하고 인증서 폐기 목록에 서명 ID 값을 추가하고 false 값을 입력한다. 그 다음 인증서 발급 버튼은 인증서 폐기 버튼으로 변경된다. 인증서 폐기 버튼을 클릭하면 revoke 함수를 실행하여 인증서 폐기 목록에 있는 해당 서명 ID를 true로 바꾸고 버튼은 다시 인증서 발급 버튼으로 변경된다.

CA 클라이언트에서 인증서 발급을 받은 사용자의 계정은 신뢰받는 계정이 된다. 신뢰받는 계정의 정보는 그림 9 와 같다.

그림 9. 인증된 사용자의 정보

이를 확인하기 위해서 사용자 클라이언트에 간단한 메시지 전송 기능도 구현하였다. 신뢰받는 계정이 다른 계정에 메시지를 전송을 하고 메시지를 전송받은 계정으로 사용자 정보에서 인증서 데이터 해시 값과 서명 값을 가져온 다음 사용자의 공개키로 서명 값을 복호화 한다. 그리고 복호화 한 결과 값과 hash 값을 비교해서 같은 isValid 속성에 true 값을 준다. 그리고 isCertificateValid 함수로 인증서 폐기가 안됐는지 만료시간을 초과하였는지 유효성 체크를 해서 유효하다고 판단되면 isCertValid 속성에 true 값을 준다. isValid 값과 isCertValid 값 모두 true 값이면 신뢰받은 계정이라고 확신할 수 있다. 복호화 한 결과 값과 해시 값을 비교하는 알고리즘은 그림 10 으로 간단하게 표현할 수 있다.

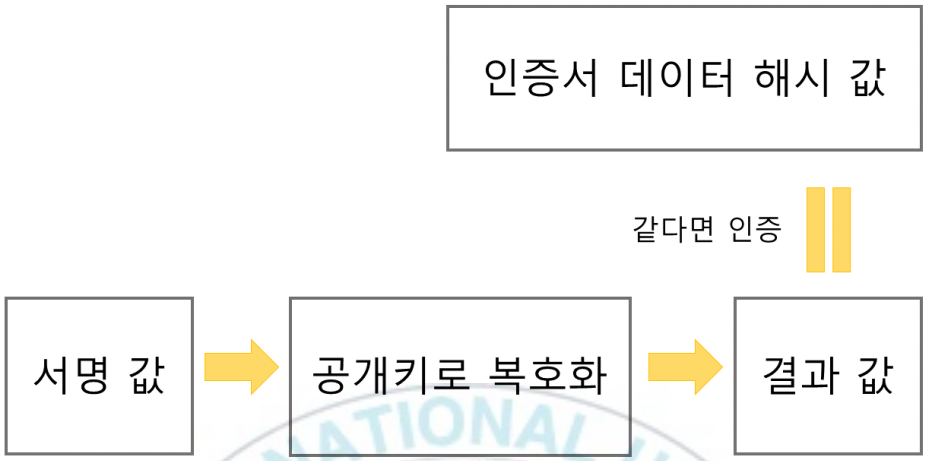


그림 10. 인증서 내용 인증 알고리즘

신뢰받은 계정이 보낸 메시지는 인증된 메시지 함에 추가하고 신뢰받지 않는 계정이 보낸 메시지는 인증되지 않은 메시지 함에 추가한다. 그리고 모든 사용자는 자신에게 메시지를 보낸 사용자의 이름을 클릭하면 그림 11 과 같이 인증서의 데이터 및 이더리움 네트워크에 등록된 정보를 alert 창을 통해 확인할 수 있다.

그림 11. 블록체인에 등록된 정보 alert창

Ⅳ. PGP 구조 설계 및 구현

4.1 PGP 구조에 블록체인 적용 연구 사례

블록체인을 이용해 PKI 구조를 설계하고 구현하여도 PKI 구조는 근본적으로 중앙 집중 형 구조이다. 또한 [10]의 연구처럼 블록체인을 적용해서 중앙 집중 형 구조를 벗어나도 누군가 의도적으로 인증서에 서명을 하면 서명한 계정만 서명을 해지 할 수 있는 취약한 점이 존재한다. 그래서 [13, 14]의 연구에서는 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 하였다. 그리고 PKI와 PGP 구조는 아니지만 [15]의 연구에서는 차량환경에서 전달되는 메시지 내용의 신뢰성 확보를 위해 블록체인을 이용해 메시지의 신뢰성을 판단하는 평판시스템을 제안하기도 하였고 [16]의 연구에서는 BSN(Body Sensor Network)과 블록체인을 병합하고 BSN의 바이오센서 노드를 사용하여 블록체인의 효율적인 키 관리 구조를 제안하여 의료 목적의 데이터를 분석하고 분석 결과를 의사에게 전송할 때 생기는 몇 가지 문제 중 하나인 한 병원에서 데이터를 저장하면 사고가 날 경우 데이터가 손실되는 취약성 문제와 의료 데이터가 변조될 가능성이 있는 무결성의 문제를 보완하기도 하였다. 이렇듯 대기업이나 의료 분야 등 다양한 분야에서도 현재 블록체인을 이용한 보안 및 인증서비스에 대한 관심이 매우 높은 상황이다.

4.2 PGP 구조 설계

가. 키 관리 구조

투명하고 신뢰성이 높은 시스템을 구현하기 위한 키 관리 구조는 그림 12 와 같다.

그림 12. 키 관리 구조

사용자는 공개키와 개인키를 가지고 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 공개키에 신뢰 가능하다고 서

명을 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.

나. 시스템 구조

제안하는 블록체인에 기반한 PGP 인증 시스템의 구조는 그림 13 과 같다. 사용자끼리 메시지를 주고받는 클라이언트를 설계하였다. 블록체인에서는 공개키 링 뿐 아니라 사용자 정보와 발신자가 수신자에게 보낸 메시지와 메시지 hash 값, 서명 값을 관리하도록 하여 수신자가 메시지의 내용이 변하지 않았다는 것을 직접 확인할 수 있다. 데이터베이스도 마찬가지로 개인키 링 뿐 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.

그림 13. PGP 시스템 구조

구현한 PGP 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.

4.3 PGP 구조 구현 및 주요 기능

가. 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 값 참조로 인해 공격자에 의해 데이터가 변경될 수 없다. 그래서 블록체인은 본질적으로 데이터 무결성을 가진다. 또한 모든 블록 데이터를 사용자들이 공유하기 때문에 투명성을 가진다. 무결성과 투명성은 최종적으로 신뢰성을 창출한다. 인증 시스템에서 신뢰성은 매우 중요한 요소이다. 제안하는 시스템에서는 블록체인 환경을 이용함으로써 신뢰성을 확보하는 이점을 가진다.

나. 정보 등록

처음 클라이언트 화면에서 회원 정보를 입력하면 데이터베이스와 블록체인에 그림 14 와 같이 정보가 등록된다.

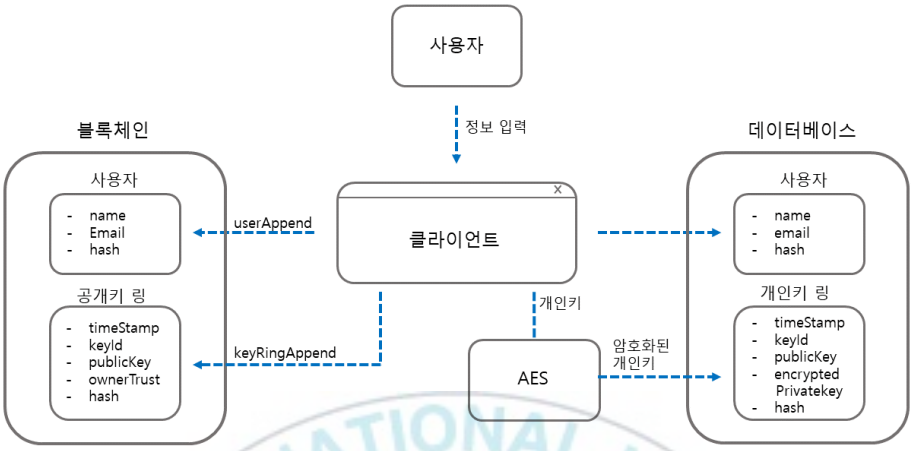
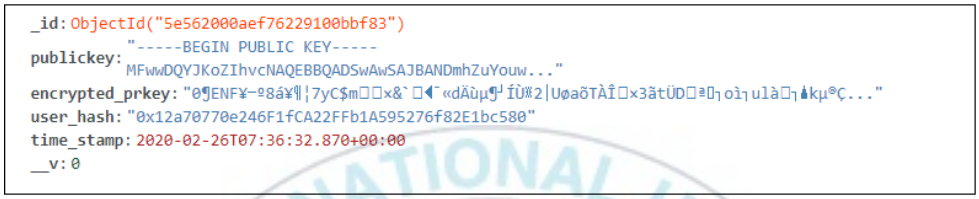


그림 14. 정보 등록 구조

사용자 정보는 데이터베이스와 블록체인에 간단하게 이름과 Email, hash 값이 등록하고 개인키 링 정보는 데이터베이스에 공개키 링 정보는 블록체인에 등록한다. 블록체인에 등록하기 위해서는 스마트 계약이 실행되어야 하며 userAppend 계약을 통해 공개키 링 전달 인자들을 블록체인 구조체에 저장한다. 개인키는 사용자 본인만 확인 가능해야 하기 때문에 데이터베이스에 AES 알고리즘을 이용해 암호화를 해서 관리한다. 그리고 keyId 경우는 데이터베이스에서 자동으로 지급하는 id 값으로 관리한다. 공개키 링은 스마트 계약을 통해 id 값을 부여하고 관리한다. 그림 15는 실제로 데이터베이스에 저장된 값의 형태이다.

(a)



(b)

그림 15. Database에 저장된 정보 (a) 사용자 정보 (b) 개인키 링 정보

(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.

다. 메시지 전송

PGP 인증 시스템의 메시지 발신, 수신 기능은 그림 16과 같은 구조로 구현하였다.

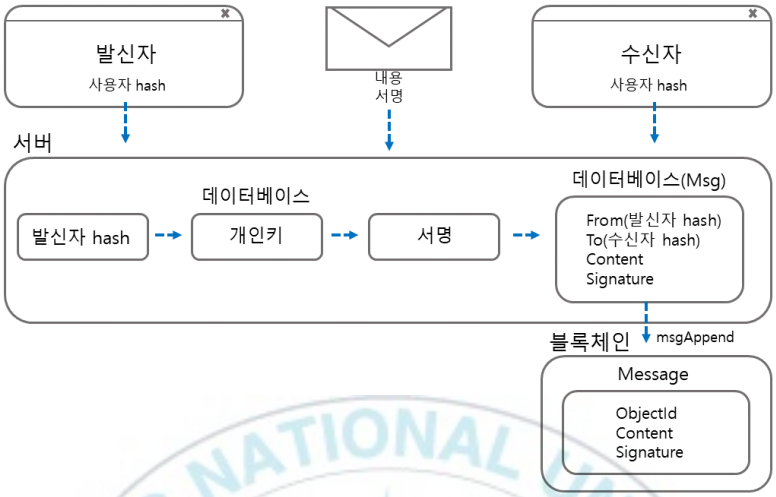


그림 16. 메시지 전송 구조

발신자가 수신자에게 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 한다. 서버에서 발신자의 hash 값을 이용해 데이터베이스 개인키 링에서 개인키를 이용하여 서명 값을 만든다. 그리고 데이터베이스의 Msg 테이블에 발신자의 hash는 from 컬럼에 저장하고 수신자의 hash는 to 컬럼에 저장하고 메시지 원문 내용은 Content 컬럼에 저장하며 서명 값은 Signature 컬럼에 저장한다. 그림 17은 실제로 Msg 테이블에 저장된 값의 형태이다.

그림 17. 데이터베이스에 저장된 메시지 정보

그리고 블록체인의 Message 구조체에 메시지 정보를 msgAppend 스마트 계약을 이용해 저장한다. 메시지 원문 내용은 Content와 서명 값 Signature와 Msg 테이블에서 자동으로 생성하는 ObjectId 값을 불러와서 id 변수에 저장한다. 그리고 id 변수는 Message 구조체에서 식별자 역할을 한다.

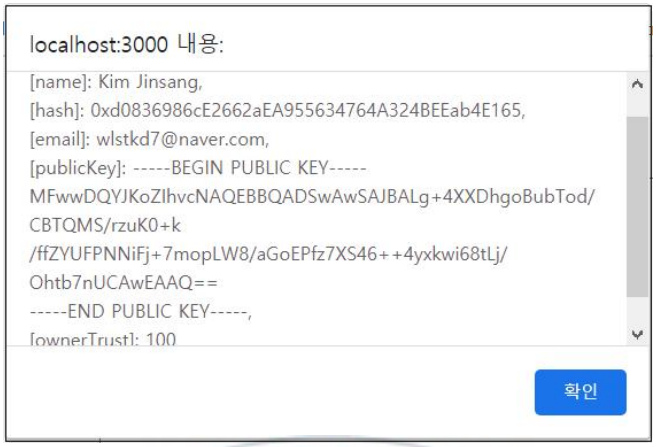
라. 신뢰도 판단

수신자 측에서는 클라이언트에 접속하면 전자서명 알고리즘을 이용해서 인증된 사용자 즉 신뢰 가능한 사용자가 전송한 메시지인지 검증한 후에 신뢰가능하다고 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 그림 18 과 같다.

그림 18. 검증을 위한 정보

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 hash 값을 이용해서 개인키 링에서 발신자의 공개키를 가져온 다음 서명 값을 복호화해서 메시지 hash 값과 비교를 한다. 비교해서 같다면 isValid 값에 true 값을 저장하고 다르다면 false 값을 저장한다. 그리고 isValid 값으로 인증된 메시지인지 인증되지 않은 메시지를 구별한다.

PGP 인증 시스템에서는 클라이언트에서 alert창을 통해 발신자의 신원을 확인할 수 있다. 메시지 리스트에 표시되는 발신자의 이름, 메시지 내용을 클릭하면 신원 확인이 가능한 창이 그림 19 와 같이 뜨도록 구현하였다.



(a)

(b)

그림 19. 신원 확인 가능한 alert 창 (a) 발신자 정보 (b) 메시지 정보

(a)창은 이름을 클릭했을 때 뜨고 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 비교하고 확인 할 수 있는 투명한 시스템이다.

V. 블록체인에 기반한 PGP 활용

5.1 블록체인 Email

본 논문에서는 제안한 블록체인에 기반한 PGP를 활용하여 메시지의 신뢰성을 확인할 수 있는 Email 시스템을 구현하였다.

5.2 시스템 구조

본 논문에서는 Email 보안 표준인 PGP를 블록체인 환경에서 구현하고 수신자의 신뢰도에 따라 발신자의 신뢰도가 증가하고 그 신뢰도에 따라 메시지의 신뢰성을 구분할 수 있는 시스템을 제안한다. 제안하는 시스템의 키 관리는 그림 12 와 같다. 시스템의 구조는 그림 20 과 같다.

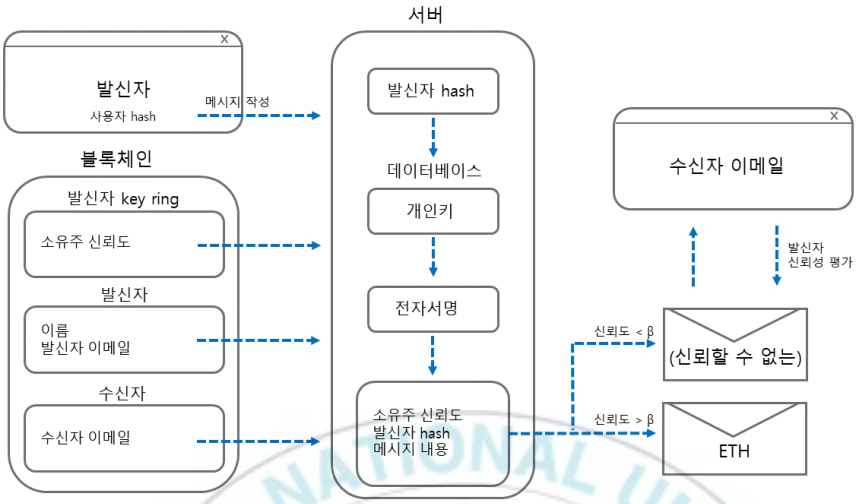


그림 20. 블록체인 Email 시스템 구조

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 (신뢰할 수 없는) 이라는 문구를 추가해 전송한다. 그리고 발신자가 메시지를 전송할 때 소량의 eth를 함께 보내고 수신자가 수신에 성공한다면 수신자가 소량의 eth를 획득한다. 하지만 수신자가 신뢰할 수 없는 메시지라고

판단하여 삭제를 한다면 소량의 eth는 발신자에게 다시 전송하는 구조이다.

5.3 신뢰도 측정

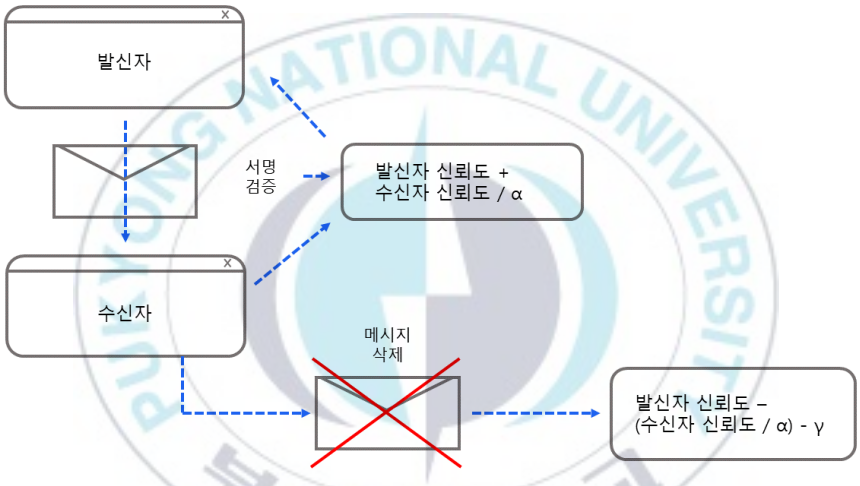


그림 21. 신뢰도 증가, 감소 알고리즘

신뢰도 측정 알고리즘은 그림 21 과 같다. 처음 메시지를 전송할 때 서명 값을 복호화하여 메시지 hash 값과 비교하여 같다는 것이 검증된다면 수신자의 신뢰도 α% 수치만큼 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

사용자보다 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 ɣ만큼 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 적용하였다.

그림 22. Eth 전송 구조

그림 22 는 블록체인 Email 시스템에서 eth를 주고받는 구조이다. 수신자가 발신자가 전송한 메시지를 성공적으로 수신했을 때 발신자는 수신자에게 소량의 δeth를 전송한다. 수신자는 소량의 eth를 획득하고 발신자는 신뢰도를 증가시키는 구조이다. 하지만 수신자가 메시지가 신뢰할 수 없다고 판단되어 삭제를 한다면 획득한 eth를 발신자에게 다시

전송하고 발신자는 신뢰도가 감소한다. 발신자는 자신의 eth를 소모하기 때문에 신뢰도를 조작하기 위해 다량의 메시지를 보내기 보다는 필요할 때 메일을 전송하게 되고 수신자는 신뢰할 수 있는 메시지라면 소량의 eth를 획득할 수 있고 신뢰할 수 없는 메시지라면 획득한 eth를 포기하고 발신자의 신뢰도를 감소시킬 수 있다. 그래서 신뢰할 수 있는 메시지를 고의적으로 삭제하기 보다는 소량의 eth를 획득할 것이다.

5.4 주요 기능

가. 스마트 계약

표 7 은 블록체인 Email 시스템에서 사용한 스마트 계약 함수이다.

표 7 블록체인 Email 시스템 스마트 계약

기능 명	기능 설명
userAppend	사용자의 정보를 블록체인 네트워크에 추가한다.
keyRingAppend	사용자의 키 링 정보를 블록체인 네트워크에 추가한다.
trustAdd	사용자의 신뢰도를 증가 시킨다.
trustSub	사용자의 신뢰도를 감소 시킨다.

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 감소시키는 계약 함수이다. 그림 23 은 실제로 구현한 스마트 계약 code이다.

```
function userAppend(string memory name, string memory email, string memory hash) public {
    users[hash] = User(name, email, hash);  //User 구조체에 정보를 저장하고 해시 테이블인 mapping 변수 users에 hash를 id 값으로 하고 User
                                            //구조체를 값으로 저장한다.
}

function keyRingAppend(string memory time_stamp, string memory publicKey, uint ownerTrust, string memory hash) public {
    nKeyRing++;  //키 링의 id 값 역할
    keyring[hash] = PuKeyRing(time_stamp, nKeyRing, publicKey, ownerTrust, hash);  //위의 함수와 같은 방식으로 키 링의 정보를 저장한다.
}

function trustAdd(string memory hash, uint increTrust) public {
    PuKeyRing storage updateTrust = keyring[hash];  //기존 키 링 정보에서 신뢰도를 증가 시킨다.
    updateTrust.ownerTrust += increTrust;
}

function trustSub(string memory hash, uint subTrust) public {
    PuKeyRing storage updateTrust = keyring[hash];  //기존 키 링 정보에서 신뢰도를 감소 시킨다.
    updateTrust.ownerTrust -= subTrust;
}
```

그림 23. 스마트 계약 code

userAppend와 keyRingAppend는 사용자가 클라이언트에 처음 접속했을 때 사용자 정보를 등록할 때 사용한다. trustAdd와 trustSub는 수신자가 메일을 수신하거나 삭제할 때 사용한다. trustAdd는 메일을 수신할 때 수신자의 신뢰도 수치에 따라 증가하는 발신자의 신뢰도 수치가 달라진다. trustSub는 수신자가 메일을 삭제할 때 증가했던 수치와 고정 수치가 함께 감소된다.

나. 정보 등록

블록체인 Email 시스템의 정보 등록은 블록체인에 기반한 PGP 인증 시스템의 구조 그림14 와 같다.

다. 메일 전송

블록체인 Email 시스템의 메일 전송 구조는 블록체인 PGP 인증 시스템의 메시지 전송 구조에서 변형되었으며 그림 24 와 같다.

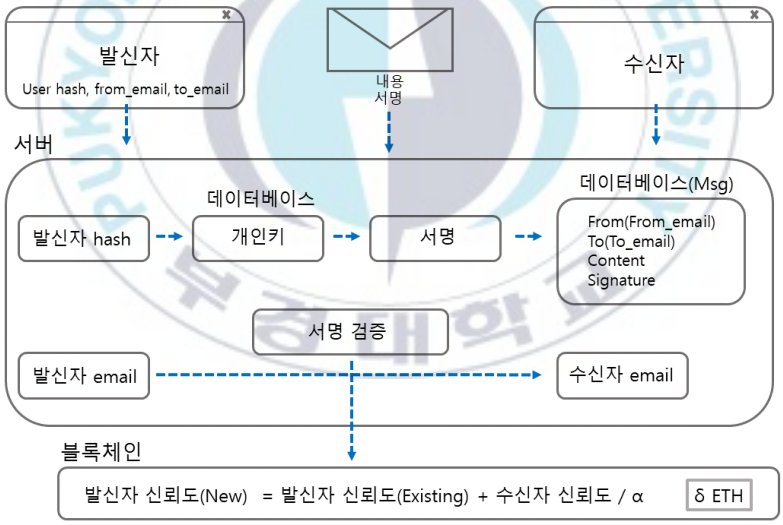


그림 24. 메일 전송 구조

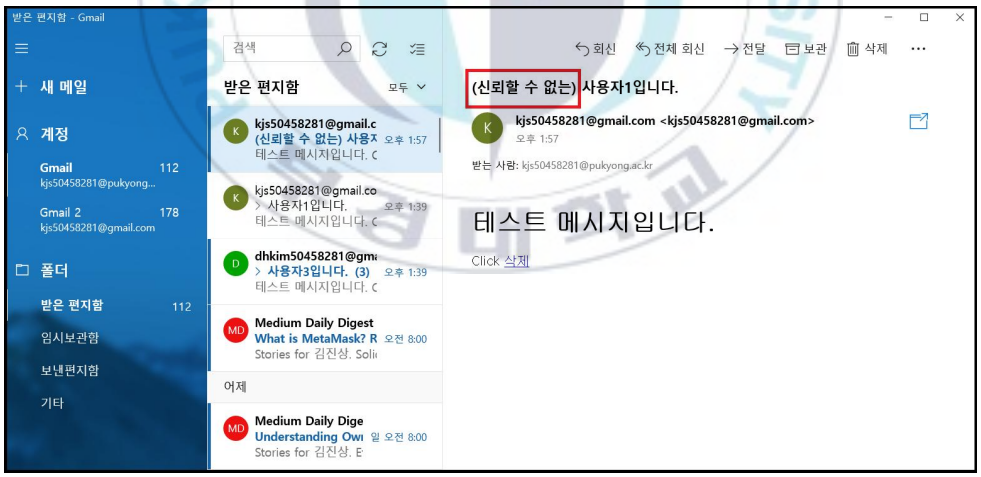
서버에서 발신자의 hash값을 이용해 데이터베이스 Private key ring 에서 Private key를 이용하여 서명 값을 만든다. 그리고 데이터베이스의 Msg 테이블에 발신자의 Email 주소는 From_email 컬럼에 저장하고 수

신자의 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 검증된다면 발신자의 신뢰도를 수신자의 신뢰도 수치 α%만큼 증가시키고 발신자의 계정에서 δ eth를 수신자에게 전송한다.

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

5.5 구현

(a)



(b)

그림 25. 수신자 Email 화면 (a) 신뢰할 수 있는, (b) 신뢰할 수 없는

그림 25 는 수신자의 Email 클라이언트에서 확인한 메시지이다. (a)

는 신뢰도가 β이상일 경우 제목 그대로 수신한다. (b)는 신뢰도가 β미만일 경우이며 이 경우는 (신뢰할 수 없는)이라는 문구가 제목에 포함되어 수신되며 수신자는 이를 통해 스팸 메일뿐 아니라 신뢰 가능한 발신자인지 아닌지 판단할 수 있다.

그림 26. 수신자 신뢰도에 의한 발신자 신뢰도 증가 수치

그림 26 은 메일 전송이 성공했을 때 클라이언트 Consol창에 출력되는 정보이다. 수신자의 신뢰도에 따라 발신자의 신뢰도 증가 수치를 보여주고 있다. 본 논문에서는 증가 수치 α %를 10%로 설정하였으며 위와 같은 결과를 출력하였다. 134와 156과 84의 경우 10%의 수치는 13.4와 15.6과 8.4지만 소수점 반올림, 반내림을 적용하여 구현하였다. 그림 25 화면의 삭제 링크를 클릭하면 메시지가 삭제된다고 가정하여 발신자의 신뢰도가 그림 27 과 같이 증가했던 신뢰도 수치에 고정 수치 ɣ가 더해진 값이 감소된다. 본 논문에서 고정 수치 ɣ는 10으로 설정하였다.

그림 27. 신뢰도 감소 수치

그림 28 은 메일을 전송하고 삭제할 때 계정 간의 eth 거래내역이다. 맨 오른쪽 value 값이 전송된 eth이며 본 논문에서 δ 값은 1로 설정하였다. 즉 전송하고 삭제할 때 계정 간 1eth를 주고받는다.

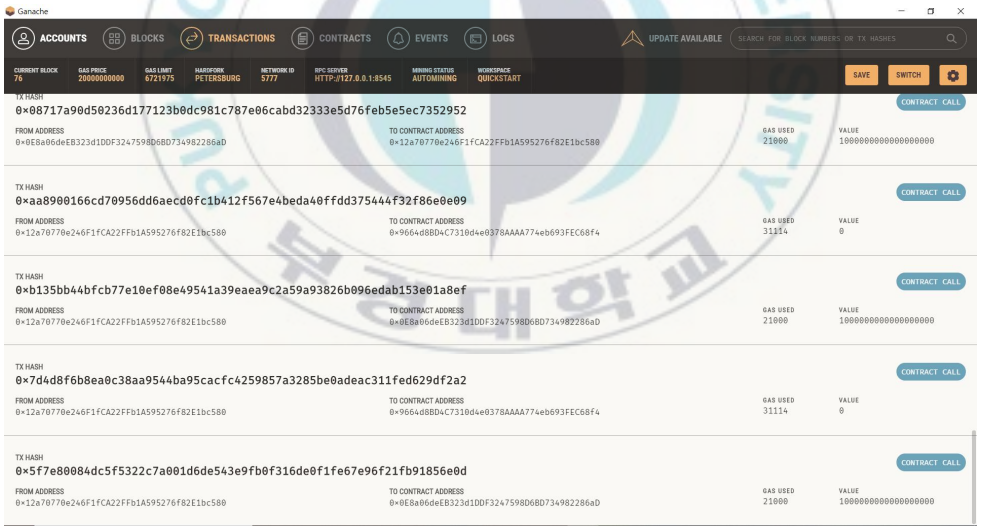


그림 28. eth 거래 내역

Ⅵ. 분석 및 평가

본 논문에서는 블록체인에 기반한 PKI 구조와 PGP 구조를 설계하고 구현하였고 구현한 PGP 구조를 활용하여 상용화된 Email 시스템에 적용하여 블록체인 Email을 구현하였다. 블록체인은 보안성이 뛰어난 플랫폼이다. 그래서 [9]의 연구에서는 블록체인을 이용한 메시지인증 기법을 제안하였다. 하지만 단지 송신 ID 유무로 확인하기 때문에 신뢰성이 떨어진다. 본 논문에서는 발신자의 ID가 실제 존재하는지 뿐만 아니라 발신자의 신원을 확인할 수 있는 신뢰성이 더 높은 구조를 구현하였다. 그리고 기존의 스마트 계약으로 구현한 PKI 구조[10]에서는 서명과 인증서 발급을 누구나 할 수 있게 구현하였다. 그래서 거래에 관련이 없는 사람들도 인증서를 발급하고 서명을 할 수 있다. 하지만 인증서 폐기는 서명한 계정만 실행할 수 있다. 누군가 의도적으로 인증서에 서명을 하면 의도적으로 서명한 계정만 서명을 해지할 수 있는 취약점이 존재한다. 본 논문에서 구현한 PKI 구조는 발급과 서명은 CA에서만 처리하도록 하였다. 기존의 구조에 비해 CA의 권한이 강하지만 기존의 취약점을 해결하여 보안을 강화하였다. [12]의 연구는 CA를 유지하지만 상위 CA가 존재한다. 하지만 블록체인 투명성으로 인해 모든 사용자들이 상위 CA들을 감시할 수 있다. 본 논문에서는 상위 CA들을 제거하여 단순한 구조로 인증 시스템을 구현하였다. 단순한 구조는 다른 시스템에도 적용 가능한 확장성을 높여준다. 하지만 PKI 구조는 근본적으로 중앙 집중 형 구조로 인증기관을 신뢰해야하는 구조이다.

PKI 구조의 단점을 보완한 구조가 PGP 구조이다. 하지만 PGP 구조에도 취약한 점이 존재한다. PGP 구조는 Web of trust 환경에서 키 관리를 한다. Web of trust 환경에서 사용자들 간의 신뢰 관계는 주관적

이다. Web of trust에서 사용자의 신뢰도는 다른 사용자들이 신뢰 가능하다고 판단될 때 사용자의 공개키에 서명을 함으로써 신뢰도가 올라간다. 사용자의 공개키에 서명이 많을수록 사용자의 신뢰도 또한 높은 구조이다. 따라서 신뢰도의 수준을 정량화하기 어렵다. 또한 사용자가 새로운 키를 생성했을 때 키의 신뢰도를 높이기 위한 승인자를 찾기 어려운 점이 존재한다. 그래서 [13, 14]연구에서는 블록체인 환경을 이용하여 Web of trust에 대한 개선 사항을 제안한다. [13]연구는 비트코인을 기반으로 PGP 인증서를 구현하였다. 그래서 인증서를 발급하고 해지할 때 비용이 발생한다. 또한 공개키에 대한 서명도 존재한다. 그리고 비트코인 UXTO 데이터베이스를 사용하여 화폐의 역할에 중점을 두었다. [14]연구에서는 블록체인 관련 데이터를 PGP 인증서와 통합하였다. 본 논문에서 제안한 PGP 구조는 개인키 링은 데이터베이스에서 관리하고 공개키 링은 이더리움에서 관리하여 사용자에게 공개되어야 할 정보는 블록체인, 보호되어야 할 정보는 데이터베이스에서 관리하도록 하였다. 또한 인증서의 형태는 서명이 필요하며 중앙 기관이 없는 P2P 구조이기 때문에 서명자도 신원과 자격이 있는 사용자인지 판단해야한다. 그래서 블록체인 PGP 구조에서는 인증서를 제거하여 발급과 해지에 드는 비용도 발생하지 않게 하여 비용을 절감하였고 공개키 링 서명 관련 속성도 삭제하여 새로운 키의 신뢰도를 높이기 위해 승인자를 찾는 어려움도 제거하였다. 대신 사용자들이 직접 상대방의 신원을 확인하고 판단할 수 있도록 구현하였다. 그래서 문제가 발생하였을 경우 문제에 대한 책임도 복잡해지지 않는다. 그리고 [13, 14]의 연구는 비트코인 플랫폼을 사용하였다. 비트코인은 화폐의 역할에 충실한 플랫폼이다. 본 논문에서는 이더리움 플랫폼을 사용하여 다른 시스템에서도 사용 가능한 확장성을 확보하였다. 이더리움은 다양한 기능을 구현 가능한 플랫폼이

다.

예전부터 Email의 신뢰도를 증가시키기 위한 연구는 이루어져왔다 [17]. 신뢰도가 낮다는 것은 발신자의 신원 확인이 어렵거나 신뢰도 측정이 어렵기 때문이다. 그래서 본 논문에서는 블록체인에 기반한 PGP를 활용하여 Email에 적용시켜 블록체인 Email 시스템을 구현하였다. 블록체인 Email 시스템은 메일을 전송할 때 eth를 함께 전송하고 수신자가 수신한 메일을 삭제할 때 eth를 발신자에게 다시 전송한다. 그리고 수신자가 수신을 성공하면 수신자의 신뢰도에 따라 발신자의 신뢰도 수치가 증가한다. 수신자의 신뢰도가 높을수록 발신자의 신뢰도 증가 수치가 증가한다. 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 [18]의 연구에서 필요 없는 이메일을 정기적으로 삭제하는 사용자가 45%, 즉시 삭제하는 사용자가 33%로 78%의 사용자가 필요 없다고 생각하는 메일을 정기적이든 즉시든 삭제를 한다는 결과가 나왔기 때문이다. 또한 블록체인 Email 시스템에서는 수신을 성공한다면 수신자는 eth를 획득하고 삭제를 할 경우 eth를 다시 발신자에게 전송해야한다. 즉 삭제하는 메시지는 수신자가 eth를 포기해서라도 삭제해야 할 만큼 신뢰성이 떨어지는 메시지이다. 하지만 필요 없는 메일에는 신뢰할 수 없는 메일도 있고 예전에는 필요했지만 현재는 필요가 없어진 메일도 있다. 즉 사용자가 메일을 정리할 경우가 존재한다. 그렇기 때문에 사용자들이 어느 정도

기간마다 메일을 정리하는지 조사하고 적정기간을 기준으로 잡고 적정기간보다 빨리 삭제하게 될 경우 메일을 정리하는 것이 아닌 메일 내용이 신뢰할 수 없다고 판단하여 삭제하는 것으로 간주하고 신뢰도를 감소시키는 것으로 보완할 수 있다. 블록체인에 기반한 PGP를 Email에 활용하여 기존의 Email에서 신뢰도를 측정하고 구분할 수 있는 기능을 추가시켜서 스팸메일이나 신뢰할 수 없는 메일을 사용자들이 더 잘 구분할 수 있도록 구현하였다.

Ⅶ. 결론 및 향후연구

PKI 구조는 중앙 집중 형이고 인증기관을 다른 상위 인증기관이 인증하는 복잡한 구조이다. 본 논문에서는 블록체인 환경에서 스마트 계약 기능을 이용해 탈중앙화된 PKI 구조를 설계하여 인증기관도 누구나 확인 가능하여 상위 인증기관이 없어도 신뢰할 수 있는 구조를 구현하였다. 하지만 PKI 구조는 근본적으로 중앙화된 구조이다. 그래서 PKI 구조의 단점을 보완한 PGP 구조를 블록체인 환경에서도 구현하였다. 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 어렵다. 또한 사용자가 새로운 키를 생성하였을 때 새로운 키에 서명을 해줄 승인자들을 찾기가 어려워서 키의 신뢰도를 높이는 것에 어려움이 존재한다.

블록체인은 본질적으로 데이터 무결성과 투명성을 가지고 있어서 신뢰성이 높다. 그래서 기존 PGP 시스템보다 본 논문에서 구현한 블록체인 환경에서 키 관리를 진행하는 PGP 구조가 신뢰성이 높다. 또한 블록체인 기반으로 구현한 PGP 인증 시스템에서는 메시지 발신, 수신자들 간의 신뢰도를 확인할 수 있다. 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. 그래서 본 논문에서는 블록체인에 기반한 PGP를 활용하여 블록체인 Email 시스템을 구현하였다.

Email은 사용자들끼리 메시지를 주고받는 시스템이고 PGP 시스템을

사용하여 보안을 유지하고 있다. 본 논문에서는 보안을 담당하는 PGP 시스템을 블록체인에 기반한 PGP로 대체하였다. 그리고 발신자가 메시지를 전송하고 서명 검증이 되어서 수신자가 메일을 성공적으로 수신한다면 수신자 신뢰도의 α%만큼 발신자의 신뢰도가 증가하고 발신자가 수신자에게 δeth를 전송한다. 또한 삭제를 하였을 경우에는 증가시킨 신뢰도에 고정 수치가 더해진 만큼 발신자의 신뢰도가 감소하고 수신자가 발신자에게 δeth를 다시 돌려준다. 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 금전적인 요소가 들어가 신뢰도가 더욱 중요한 시스템에 블록체인을 적용하여 신뢰도를 증가시키는 연구를 진행할 것이다.

참고문헌

[1] S.Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash System" Technical report, bitcoin.ort,2008.

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

[3] 전승화, 김정호. "언택트 (Untact) 산업 확산의 이론적 배경과 전망." 신산업경영저널 38.1, pp. 96-116, 2020.

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

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

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

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

[8] 박영호, 공병운, 이경현, "전자신분증 기반의 개인 신분확인을 위한 인증시스템 설계." 멀티미디어학회논문지 14.8, pp. 1029-1040, 2011.

[9] 박준호, 윤문형, 김용호, 이정훈, 정오균, "지상 무기체계에서 블록체인 기반의 메시지 인증 기법." 한국콘텐츠학회 종합학술대회 논문집, pp. 405-406, 2019.

[10] 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.

[11] L.Axon, 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.

[12] A.Yakubov, W.Shbair, A.Wlbom, D.Sandra, 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.

[13] D.Wilson, 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.

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

[15] 이경모, 이경현, "VANET 환경에서의 협력적 메시지 전달을 위한 블록체인 기반 평판 시스템." 멀티미디어학회논문지 21.12, pp. 1448-1458, 2018.

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

[17] S.Garriss, M.Kaminsky, M.J.Freedman, B.Karp, D.Mazieres, H.Yu, "RE: Reliable Email." In USENIX Conference on Networked Systems Design & Implementation (NSDI), 2006.
[18] 정석찬, 김현정, "부산지역 인터넷 이용자의 스팸메일 대응형태에 관한 조사연구." 인터넷전자상거래연구 4.2, pp. 49-72, 2004.

감사의 글

길지도 않고 짧지도 않은 2년의 석사과정의 마침표인 학위 논문을 제출하게 되었습니다. 처음 회사를 그만두고 학사 전공이 아닌 다른 전공의 대학원의 진학을 앞두었을 때 정말 막막했습니다. 하지만 막막했던 석사과정을 별 탈 없이 끝낸 나 자신이 자랑스럽습니다. 돌이켜 보면 주위에 많은 사람들의 도움과 희생이 있어 별 탈 없이 끝낼 수 있었기에 여기에 감사의 글을 남깁니다.

가장 먼저 석사과정 시작부터 지금까지 세심한 지도와 많은 가르침으로 이끌어 주신 서경룡 교수님께 진심으로 감사의 인사를 드립니다. 처음 비전공자였던 저를 잘 이끌어주시고 현명한 지도와 조언을 아낌없이 해주셔서 정말 감사합니다. 그리고 전공의 지식들을 쉽게 배울 수 있게 질 좋은 강의를 해주신 컴퓨터 공학과 대학원 모든 교수님께도 깊이 감사드립니다.

같이 학교를 다니면서 어려울 때 조언과 격려를 해준 컴퓨터 공학과 동기생들에게 감사의 인사를 전하고 싶습니다. 그리고 힘들 때 고민을 들어주고 조언을 해주고 격려와 웃음으로 응원을 주었던 친구들에게도 감사의 인사를 전하고 싶습니다.

마지막으로 저를 낳아주시고 길러주시고 2년 동안 믿고 응원해주신 부모님께 감사의 인사를 전합니다.

2021년 01월 04일

김대한 드림