디지털산업정보학회 논문지 제13권 제4호-2017년 12월
http://dx.doi.org/10.17662/ksdim.2017.13.4.099

이더리움 기반 이메일 시스템 모델

김 태 경*

E-mail System Model based on Ethereum

Kim Taekyung

〈Abstract〉

With the advent of virtual money such as bit coins, interest in the block chain is increasing. Block Chain is a technology that supports Distributed Ledger and is a versatile technology applicable to various fields. Currently, the block chain is conducting research for various applications such as virtual money, trade finance, marketplace, power market, image contents service, and IoT. The technologies that make up the block chain are smart contract, digital signature/hash function and consensus algorithm. And these technologies operate on P2P networks. In this paper, we have studied e-mail system based on the ethereum which is one of the block chain based technologies. Most legacy mail systems use SMTP and the POP3/IMAP protocol to send and receive e-mail, and e-mail use S/MIME to protect the e-mail. However, S/MIME is vulnerable to DDoS attacks because it is configured centrally. And it also does not provide non-repudiation of mail reception. To overcome these weaknesses, we proposed an e-mail system model based on ethereum. The proposed model is able to cope with DDoS attack and forgery prevention by using block chain based technology, and reliable recording and management among block chain participants are provided, so that it is possible to provide a non-repudiation function of e-mail transmission and reception.

Key Words : Block Chain, E-mail, Ethereum, DDoS, SMTP

Ⅰ. 서론

IT 기술의 계속적인 발전으로 인해 우리의 생활은 급격하게 변화하고 있다. 핀테크, Healthcare, 클라우드 서비스 등의 기술들이 개발되어 다양한 분야에서 활용되고 있으며, ITS(intelligent transport systems) 기술도 자동차 등의 분야에 실제 적용되고 활용되고 있다. 그러나 e-mail에서는 여전히 SMTP(Simple Mail Transfer Protocol)를 사용하고 있다. 인터넷에서 전자 메일 전송은 SMTP를 지원하는 호스트 사이에 이루어지며, SMTP 호스트는 SMTP 명령과 그에 따른 응답 과정을 반복해 메일을 전송한다. 이 프로토콜은 그 이름에서도 알 수

* 명지전문대학 인터넷응용보안공학과 교수

있듯이 가능한 한 단순하게 설계되어 있다. SMTP는 메일을 보내는 사람에 대해 인증할 필요가 없으며 보내는 메시지도 평문으로 전송된다. 따라서 SMTP는 단순성과 개방성이라는 특성을 가지게 있어서 이에 따른 보안의 취약점을 가지고 있다.

이러한 보안 취약점을 보완하기 위하여 S/MIME (Security Services for Multipurpose Internet Mail Extension) 프로토콜이 등장하게 되었으며, S/MIME은 송신자의 인증과 메시지의 암호화 기능을 제공하지만, 메일 수신 부인방지 등의 기능은 제공을 하고 있지 않다. 본 논문에서는 블록체인 기술을 이용하고 있는 이더리움을 활용하여 이메일 시스템을 제안하고자 한다. 이더리움은 블록체인 기술에 기반을 둔 프로그래밍 언어, 클라우드 컴퓨팅 플랫폼이라 할 수 있다.

본 논문의 2장에서는 관련연구에 대해서 기술하였으며, 3장에서는 이더리움에 기반을 둔 이메일 시스템 모델을 제시하였다. 4장에서는 제안한 모델에 대해 성능평가를 수행하였으며, 마지막으로 5장에서는 결론에 대해서 기술하였다.

Ⅱ. 관련연구

2.1 S/MIME

S/MIME은 1995년에 개발되었으며, 메시지 보안을 위해 사용된다[1]. 유사하게 메시지 보안을 위해 사용되는 기술로는 PGP(Pretty Good Privacy)가 있다. PGP는 이메일에 필요한 보안 기능 중 수신 부인 방지와 메시지 부인 방지를 제외한 나머지 4개 기능을 지원한다. 메시지의 비밀성을 위한 암호화에는 RSA와 IDEA 등의 암호화 알고리듬이 사용되고, 메시지의 무결성을 보증하기 위한 메시지 인증과 메시지의 생성, 처리, 전송, 저장, 수신 등을 한 사용자 보증을 위한 사용자 인증의 디지털 서명에는 RSA가 사용된다. 또한 키 관리에는 RSA가 사용된다.

S/MIME 버전 1이 나올 무렵에는 안전한 메시지를 위한 공식적인 단일 표준이 없었고 여러 개의 표준이 서로 경쟁하고 있었으며, 1998년 S/MIME 버전 2가 도입되었다. S/MIME 버전 2는 버전 1과는 달리 IETF(Internet Engineering Task Force)에 제출되어 인터넷 표준으로 고려되었다. 두 개의 IETF RFC(Request for Comments), 즉 메시지 표준을 지정한 RFC 2311과 인증서 처리 표준을 지정한 RFC 2312가 S/MIME 버전 2를 구성한다. 두 가지 RFC가 함께 결합하여 상호 운용 가능한 메시지 보안 솔루션을 전달하기 위해 공급업체가 준수할 최초의 인터넷 기반 프레임워크를 형성했다. S/MIME 버전 2가 도입되면서 S/MIME은 메시지 보안의 표준으로 자리를 잡게 되었다. 1999년에 IETF는 S/MIME 기능을 강화하기 위해 S/MIME 버전 3을 제안했다. RFC 2632는 RFC 2311을 기반으로 S/MIME 메시지 표준을 지정했고 RFC 2633은 RFC 2312의 인증서 처리 사양을 향상시켰다. RFC 2634는 보안 확인 메일, 보안 레이블 등의 추가 서비스를 S/MIME에 더하여 전체 기능을 확장했다[2]. 2004년 S/MIME는 버전 3.1 RFC 3851로 향상되었고, 가장 최근의 버전은 2010년 버전 3.2 RFC 5751이다.

S/MIME은 크게 디지털 서명과 메시지 암호화 기능으로 구분할 수 있다. 디지털 서명은 이메일을 보낸 사람이 이메일을 보낸 사실과 일치하는지 확인하기 위해 MIME 데이터 서명, 인증, 부인방지의 목적으로 디지털 서명을 사용한다. 메시지 암호화는 메시지를 받은 사용자가 메시지를 읽기 전까지 정보를 읽거나 이해할 수 없도록 암호화해야 한다. 따라서 비밀성을 유지할 수 있으며, 외부 공격자로부터 이메일을 보호할 수 있다. 즉 공개키 암호화, 메시지

무결성, 데이터 보안 등의 기능을 수행한다.

동작 원리는 메일 송신자가 자기 자신임을 인증하고 메시지를 보냈음을 부인 방지하기 위해 개인키를 암호화하여 메일 수신자에게 전송한다. 메일 수신자는 메일 송신자의 공개키를 이용하여 개인키를 추출하여 메일 송신자임을 확인한다. 즉 디지털 서명을 수행한다. 또한 파일과 메시지를 암호화하는데 속도적인 측면을 고려하여 대칭키 암호화를 사용하여 암호화를 수행하고, 대칭키 암호화하는 과정에 사용된 비밀키는 공개키 기반의 암호를 통해 암호화되어 수신자에게 전송한다. 이때 비밀키의 암호화에 사용되는 키는 수신자의 공개키를 이용한다. 자신의 공개키로 암호화되어 전달받은 비밀키를 자신의 개인키로 암호를 해제한 다음 추출된 비밀키로 암호화된 메시지나 파일의 복호화를 수행한다.

2.2 이더리움

이더리움은 2015년 출시된 차세대 스마트 계약 분산 응용프로그램 기술이며 스위스를 거점으로 하는 Ethereum Foundation에서 개발이 진행되고 있는 오픈 소스 프로젝트이다[3]. 블록체인은 분산형 원장 기술이며, 데이터를 일련의 블록 형태로 기록하는 분산 데이터베이스로써 해시 트리[4]와 같은 기술을 통해 블록체인 데이터의 무결성을 보장하게 된다. 비트코인[5]은 2008년 11월 암호화 기술과 관련된 메일링 리스트에 발표된 논문에서 시작 되었다. 비트코인은 P2P 네트워크상에서 구현된 최초의 가상화폐로 2009년 1월에 제시된 논문을 바탕으로 비트코인 소프트웨어가 배포되어 운영이 시작되었으며, 2009년 1월 3일 최초의 블록이 만들어진 후 현재까지 계속 가동되고 있다. 이더리움은 비트코인과 마찬가지로 P2P 네트워크상에서 거래 이력을 블록체인에 기록하는 한편 스마트 계약 그 자체나 실행 이력도 기록할 수 있는 특징이 있으며, SNS, email, 전자투표[6] 등 여러 분야에서 사용자 스스로가 개발 및 운영할 수 있도록 개발되었다. 다른 플랫폼들과 비교되는 가장 큰 특징은 스마트 계약[7]이 가능하다는 점이다. 데이터를 실행 가능한 코드 형태로 블록체인에 업로드하여 일정 조건이 만족될 경우에 자동으로 코드를 실행하고 데이터의 소유권에 대한 임의의 규칙도 사용자가 생성할 수 있도록 되어 있다. 또한 C++, Python, GO 등 다양한 프로그래밍 언어로 구현되어 있지만 Go 언어판이 가장 활발하게 개발되고 있다[8].

이더리움 기술의 응용은 P2P 네트워크상에서 분산화 된 형태로 운영되는데 그 분류는 다음과 같다[9].

- 결제 및 거래에서의 응용: 자산을 블록체인에 기록하고 스마트 계약의 대상으로 사용하는 응용 형태로 그 예로서는 가상 화폐, 송금·결제, 무역 금융, 자금 조달, 마켓플레이스 등이 있다.
- 서명 및 증명에서의 응용: 서명 및 증명과 관련된 분야로 저작권 관리, 고액 물품 거래 추적, 계약 관리 및 실행, 문서 공증 등이 있다.
- 신규 서비스 응용: 신규 분야에 사용되고 있으며 IoT, 투표, 분산형 SNS 서비스 등이 있다.

이더리움은 다양한 응용의 개발 및 운영을 지원하기 위해 분산화 되어 있는 데이터베이스를 제공하며, 각 노드에서 만든 블록의 정당성을 검토하고 네트워크 전체에서 공유하는 블록체인에 반영하기 위해 합의 알고리즘을 제공한다[10].

2.3 블록체인

블록체인의 개념은 P2P 네트워크에 사이버 거래 정보를 공동으로 관리하는 신개념 분산거래장부로, 네트워크에서 모든 참여자가 공동으로 거래 정보를 검증, 기록, 보관하는 보안기술을 의미한다. 이러한

블록체인의 가장 대표적인 특징은 디지털 정보의 보안 관리 이슈에 대해서 중재자가 필요 없이 신뢰 프로세스를 구축할 수 있으며, 모든 정보가 암호화되어 전송 및 기록됨으로써 데이터 조작 및 오류를 방지 할 수 있을 뿐 아니라 거래기록이 분산되어 보관되므로 중앙 중개기관이 필요하지 않고 다양한 데이터 저장에 블록체인 기술 활용이 가능하다. 블록체인의 원리는 모든 구성원들이 접속해있는 네트워크와 위·변조 방지 프로그램을 통하여 정보를 자동적으로 검증하는 방식으로 구현된다. 즉 특정 시간동안 발생한 모든 거래기록 정보에 대하여, 정보 집합(Block)을 디지털화하여 생성하고, 모든 구성원에게 데이터를 전송한다. 이렇게 전송된 데이터는 구성원들의 PC 등 다양한 전자기기에 저장되고, 이렇게 생성된 정보는 작업증명을 통해 유효성을 확인하고, 확인된 거래기록 정보를 기존 블록체인에 연결(Chain)하는 방식으로 이루어진다. 여기서 정보 집합(Block)은 거래내역 및 발생시간 등의 내용을 문자, 숫자형태로 암호화된 숫자로 일종의 데이터 패킷을 의미한다[11].

블록체인의 핵심기술은 P2P 네트워크, 암호화, 분산 장부, 분산 합의와 같이 크게 4가지의 기반 기술로 구성되어 있다[12, 13].

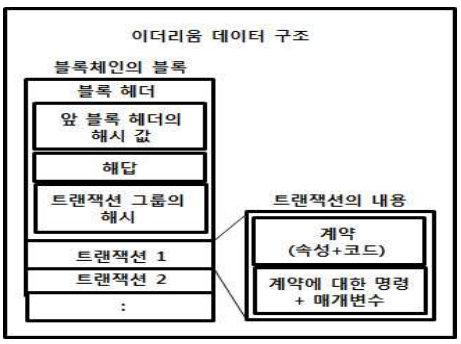
- P2P 네트워크: 탈중앙화 분산 네트워크를 위해 flooding 기반의 unstructured P2P 네트워크를 사용한다. 또한 P2P 네트워크의 통신은 TCP/IP를 사용하고 있으며, 블록체인의 참여자들은 자신과 물리적으로 가장 인접한 참여자들의 IP를 유지하고 있으며 이를 사용하여 메시지 및 데이터를 주고받는다.
- 암호화: 블록체인에서 사용되는 암호화 기술은 데이터의 무결성 검증을 위한 머클 트리(Merkle Tree), 거래의 부인방지를 위한 공개키 기반 디지털 서명 기법이 사용되고 있다.
- 분산 장부: 블록체인에서 분산 장부는 발생하는 모든 거래, 정보들을 참여자들의 검증과정을 거쳐 기록하며, 모든 참여자가 동일한 정보를 유지한다. 이러한 분산 장부는 블록체인이 제공하는 데이터 무결성 보장의 바탕이 된다.
- 분산 합의: 분산 합의는 분산 컴퓨팅과 멀티 에이전트 시스템 등의 분야에서 결함이 있는 프로세스가 있는 경우, 전반적인 시스템의 신뢰성을 달성하기 위하여 프로세스나 에이전트 간의 특정 데이터 값에 대한 동의를 이끌어내는 프로토콜이다.

Ⅲ. 이더리움 기반 이메일 시스템

3장에서는 이더리움을 통해 블록체인을 공유하는 분산 어플리케이션 기반의 안전한 이메일 모델을 제안하고자 한다. 이더리움은 P2P 네트워크상에서 동작하기 때문에 기존의 중앙 집중형 시스템보다 신뢰성과 보안 측면에서 안전한 시스템 구축이 가능하다.

3.1 이더리움 데이터 구조

일반적인 이더리움의 데이터 구조는 다음의 <그림 1>과 같다.



<그림 1> 이더리움 데이터 구조

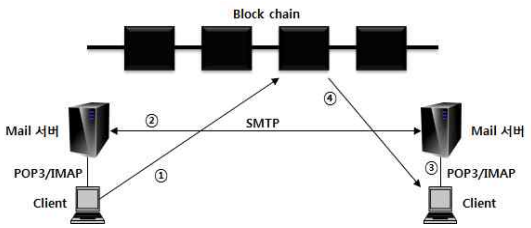
<그림 1>에서 블록체인은 복수의 트랜잭션을 모은 블록을 만들고, 블록에는 이전 블록의 해시를 포함시킨다. 그리고 해시 계산에 사용하는 해답(Nonce)과 해당 블록의 트랜잭션을 포함하는 트랜잭션 그룹의 해시 값을 포함하여 블록체인의 블록 헤더를 구성하게 된다. 따라서 어떤 블록의 내용을 위조하거나 변조하면 해시 함수의 특성에 따라 그 다음의 블록에 포함된 해시값이 변하게 되고 동시에 이후의 모든 블록에 포함된 해시값이 변하게 되므로 위조나 변조를 하기 어렵다는 특징이 있다. 또한 트랜잭션에 스마트 계약을 포함시켜 가상화폐 이외에도 다양한 범용의 목적으로 이더리움을 사용할 수 있도록 구성되어 있다.

블록체인은 P2P 네트워크에서 구축된 시스템으로 주요 기술로는 스마트 계약, 전자 서명 및 해시 함수 그리고 합의 알고리즘이 있다. P2P 네트워크란 컴퓨터끼리 같은 목적으로 연결해 네트워크를 형성하는 방식이다. 어떤 컴퓨터에서도 같은 처리를 수행할 수 있으므로 1대가 정지해도 시스템 전체에 영향을 주지 않는다는 특징을 가지고 있다. 스마트 계약은 블록체인 네트워크에서 동작하는 프로그램이다. 이 스마트 계약을 이용해서 블록체인을 가상화폐 이외에도 범용적인 목적으로 사용할 수 있도록 할 수 있다. 전자 서명 및 해시 함수는 트랜잭션을 발생시킨 사람(ex. 이메일 송수신자)의 정당성을 보증하거나 트랜잭션과 블록체인의 변조 방지, 암호화 등의 보안과 관련된 기능을 수행한다. 마지막으로 합의 알고리즘은 P2P 네트워크와 같은 분산 네트워크에서 합의 형성을 수행하기 위한 알고리즘이다.

이더리움 데이터모델은 비트코인의 데이터 모델과 많이 유사하나 스마트 계약이라는 기능이 가장 큰 차이점이라고 할 수 있다.

3.2 이더리움 기반 이메일 시스템 모델

현재 대부분의 이메일 시스템은 SMTP 프로토콜과 POP3/IMAP 프로토콜을 이용하여 이메일 서비스를 제공하고 있다. 따라서 본 논문에서는 기존의 이메일 시스템 구조에서 이더리움 기반의 블록체인을 활용하는 이메일 시스템 모델에 대해서 제안하고자 한다. 본 논문에서 제안하는 이메일 시스템의 모델은 다음과 같다.

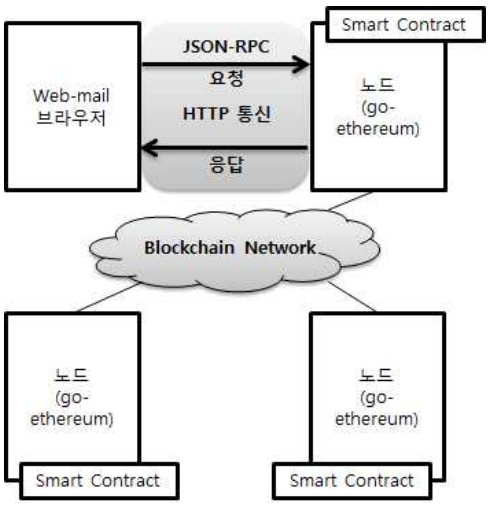


<그림 2> 이더리움 기반 이메일 시스템 모델

사용자는 일반적으로 메일을 작성하여 보내는 방식과 동일하게 메일을 작성하여 전송하면 되며, 전송 버튼을 클릭하면 메일의 내용이 이더리움 기반 스마트 계약을 이용하여 블록체인에 기록(①)된다. 블록체인에 저장시에는 메일 송수신자 사이에 세션 협상 과정에서 생성된 세션 키를 이용하여 메일 내용을 암호화 할 수 있다. 즉 암호화 된 메일 내용을 블록체인에 기록하게 된다. 기존의 메일 시스템을 이용하여 수신자에게는 보내지는 내용은 블록체인에서 해당 메일을 확인할 수 있는 정보를 메일 내용에 담아 수신자의 메일 서버에 전송한다(②). 메일 서버는 전달받은 메일을 해당 계정의 사용자에게 전송하며(③), 메일을 받은 사용자의 PC에서는 전송받은 메일의 식별자 값을 이용하여 이더리움 기반 스마트 계약을 통해 수신자에게 전송된 메일을 수신(④)하고, 세션 키로 메일 내용을 복호화 한다. 여기

서 메일의 내용을 블록체인에 기록하는 것과 블록체인에 기록된 내용을 가져오는 동작은 이더리움의 전용 개발언어인 Solidity를 이용하여 개발을 수행하며, 또한 소스 코드는 Ethereum Virtual Machine(EVM)이라는 가상 머신에서 동작하기 때문에 플랫폼에 의존하지 않는 특성을 가지고 있다.

전송하고자 하는 메일을 블록체인에 기록하고, 기록된 이메일을 가져오는 동작은 다음의 <그림 2>와 같다.



<그림 3> 메일을 블록체인에 저장 및 조회 구조

웹 메일 브라우저에서 메일을 작성한 후 전송 버튼을 클릭하게 되면 메일의 내용들이 JSON-RPC를 통해 이더리움 클라이언트의 이더리움 가상 머신(Ethereum Virtual Machine) 안에 있는 스마트 계약에 전송되며, 스마트 계약은 이메일의 내용을 블록체인에 기록하는 역할을 수행한다. 마찬가지로 수신자의 PC에서도 스마트 계약을 이용하여 자신에게 전달된 메시지를 블록체인으로부터 가져올 수 있다.

여기서 Contract 프로그래밍은 Solidity라는 언어를 사용하며, Solidity는 일반적인 C언어나 자바로 구현할 수 있는 것은 대부분 구현할 수 있다. 노드(go-ethereum)에는 JSON-RPC 서버라는 기능이 있어 브라우저에서 HTTP 통신으로 스마트 계약(smart contract)을 조작하거나 블록체인의 다양한 정보를 취득할 수 있다.

Ⅳ. 성능평가

이더리움을 이용한 이메일 시스템은 블록체인을 이용하여 이메일 정보를 분산 원장에 기록하고 공유함으로써 이메일을 받는 사람에게 전달할 수 있으며, 해시함수를 이용하여 메일 내용의 무결성을 확보할 수 있다.

또한 데이터의 암호화를 위해서 ECIES, AES-256 암호 알고리즘을 이용하여 기밀성을 제공할 수 있으며, Secp256k1 ECDSA 디지털 서명을 이용하여 인증 및 데이터의 위변조를 예방할 수 있다[12].

4.1 메일 내용의 위변조 방지 및 배달 증명

블록체인의 특성이 블록이라는 단위로 시간별로 이어져 있으므로 한 블록에는 앞의 블록과 뒤의 블록과 연결되는 연결 정보가 포함되어 있으며, 앞의 블록의 내용을 변경하게 되면 뒤에 이어지는 모든 블록을 다시 생성해야 하므로 과거 블록의 내용을 변조하는 것이 거의 불가능 하다. 그러므로 이더리움 기반 이메일 모델은 이메일 내용에 대한 위변조를 방지할 수 있다. 또한 블록체인은 분산형 원장 구조이며, 그 블록체인에 네트워크에 참가한 모든 사람들이 모든 기록을 보유한 원장을 소유하게 되므로 메일 송수신에 대한 투명성이 높아지게 된다. 즉 메일 전송의 시점을 객관적으로 알 수 있으며, 이메일 전송에 대한 검증을 모든 참가자들에게 받

게 된다. 또한 메일의 내용은 세션키를 이용하여 암호화함으로 스푸핑 및 스니핑 공격 등을 예방할 수 있다.

4.2 메일 송수신자 인증

블록체인에서는 각 트랜잭션에 한 개씩 전자 서명이 부여되며, 전자 서명을 검증하기 위한 공개키 세트도 부여된다. 트랜잭션의 전자 서명을 검증하면 제3자가 도용 등을 통해 메일을 보냈는지의 여부 그리고 메일을 보낸 사람이 제대로 메일을 보냈는지의 여부를 검증할 수 있다. 블록체인에서 트랜잭션을 발행하려면 공개키와 비밀키의 쌍이 필요하며, 일반적으로 키 쌍의 생성에 타원 곡선 암호(ECDSA) 알고리즘을 사용하고, 키 길이는 256비트 이상을 사용한다.

4.3 성능 비교

제안한 이더리움 기반 이메일 시스템과 S/MIME의 성능을 비교하면 다음과 같다. 주로 보안성능 위주로 성능 비교를 수행하였으며, 제안한 모델의 경우 분산원장 기술을 이용하므로 이메일 전송과 수신에 신뢰성을 제공할 수 있다.

<표 1> 이메일 성능 비교

항목	S/MIME	제안모델
비밀성 제공	O	O
무결성 제공	O	O
사용자 인증	O	O
메일 전송 부인방지	O	O
메일 수신 부인방지	X	O
DDoS 공격 내구성	약함	강함

S/MIME과 제안한 모델 모두 전자서명과 해시를 이용함으로 사용자 인증과 비밀성 그리고 무결성을 제공할 수 있다. 그러나 이더리움 기반 이메일 시스템의 경우 블록체인 기반 시스템이므로 분산원장이라는 특성으로 원칙적으로 위변조가 불가능하며, 이더리움에 참가하는 각 노드가 동일한 데이터를 보유하고 있으므로 DDoS 공격 등 특정 서버를 공격하여 서비스 거부를 일으키는 공격에 대응할 수 있는 강한 특성을 가지고 있다. 또한 메일 전송 및 메일 수신 부인방지 기능을 제공하여 배달증명 등의 기능을 수행할 수 있다. 이외에도 블록체인을 이용하여 메일의 내용이 암호화하여 저장되므로 스푸핑 및 스니핑 공격에 위협을 받지 않고 이메일 송수신 기능을 안전하게 수행할 수 있다.

Ⅴ. 결론

비트코인 등의 가상화폐의 등장으로 블록체인에 대한 관심이 높아지고 있다. 블록체인은 분산원장을 지원하는 기술로 여러 분야에 적용 가능한 범용성이 높은 기술이다. 현재 블록체인은 가상 화폐, 무역 금융, 마켓플레이스, 전력시장, 영상 콘텐츠 서비스, IoT 등 다양한 분야에서 활용을 위한 연구를 수행하고 있다. 블록체인을 구성하는 기술로는 스마트 계약, 전자 서명 및 해시 그리고 합의 알고리즘이 있으며, 이러한 기술들이 P2P 네트워크에서 동작하게 된다.

본 논문에서는 블록체인 기반 기술 중 하나인 이더리움을 이용한 이메일 시스템에 대한 연구를 수행하였다. 기존의 메일에서는 대부분 SMTP와 POP3/IMAP 프로토콜을 이용하여 이메일을 주고받고 있으며, 이러한 이메일에 대한 보안을 위해 S/MIME을 사용하고 있다. 그러나 S/MIME의 경우

메일 수신 방지 기능을 제공하지 못하고 서버가 중앙 집중적으로 구성되어 있기 때문에 DDos 공격에 취약한 특성을 갖고 있다. 이러한 취약점을 보완하기 위하여 이더리움 기반 이메일 시스템 모델을 제안하였으며, 제안한 모델은 블록체인 기반 기술을 활용하여 DDoS 공격 및 위변조 방지에 대응이 가능하고, 블록체인 참여자 간에 신뢰성 있는 기록 및 관리가 제공되므로 메일 송수신 부인방지 등의 기능을 제공할 수 있다.

참고문헌

[1] https://www.ietf.org/rfc/rfc5751.txt

[2] https://technet.microsoft.com/library/aa995740

[3] Ethereum: White paper, A next-generation smart contract and decentralized application platform, Sept. 2014.

[4] 이부형, 이성범, 문지연, 이종혁, “해시 트리 기반의 경량화된 DTLS 메시지 인증,” 한국통신학회, 한국통신학회논문지, 40(10), 2015. 10, pp. 1969-1975.

[5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Oct. 2008.

[6] K. Lee, et al., “Electronic voting service using block-chain,” JDFSL, Vol. 11, No. 2, June. 2016, pp. 123-135.

[7] C. D. Clack, V. A. Bakshi, and L. Braine, “Smart contract templates: foundations, design landscape and research directions,” arXiv preprint arXiv:1608.00771, Aug. 2016.

[8] K. Delmolino, et al., “A programmer’s guide to ethereum and serpent,” University of Maryland, May. 2015.

[9] 이부형, 이민영, 고현서, 명소희, 김미옥, 이종혁, “Ethereum Whisper 기반의 안전한 모바일 메신저,” 한국통신학회, 한국통신학회논문지, 42(7), 2017. 7, pp. 1477-1484.

[10] Ethereum Github Wiki(2016), Retrieved Mar., 27, 2017, https://github.com/ethereum/wiki/wiki.

[11] 김태형, “블록체인 개념 및 분야별 활용사례 분석,” 대한전기협회 전기저널, 제487호, 2017. 7, pp. 58-65.

[12] 이동영, 박지우, 이준하, 이상록, 박수용, “블록체인 핵심 기술과 국내외 동향,” 한국정보과학회, 정보과학회지, 35(6), 2017. 6, pp. 22-28.

[13] 아카하네 요시하루 외, 블록체인 구조와 이론, 위키북스, 2017년 6월.

■ 저자소개 ■

김 태 경
(Kim Taekyung)

2017년 9월~현재
명지전문대학 인터넷응용보안공학과 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학 정보전자과 교수
2005년 8월 성균관대학교
전기전자및컴퓨터공학과(공학박사)

관심분야 : 네트워크보안, IoT 보안, 개인정보보호
E-mail : tkkim@mjc.ac.kr

논문접수일 : 2017년 10월 19일
수 정 일 : 2017년 10월 31일
게재확정일 : 2017년 11월 01일