한국컴퓨터정보학회 하계학술대회 논문집 제26권 제2호 (2018. 7)

블록체인 기반 온라인 신분증명 스킴

최상용O
O한국과학기술원 전산학부
e-mail: csyong95@gmail.comO

Blockchain-Based Online Identity Certification Scheme

SangYong ChoiO
OSchool of Computing, Korea Advanced Institute of Science and Technology

● 요 약 ●

온라인 신분증명에는 공인인증서, I-PIN, 휴대전화 등이 사용된다. 서비스 제공자는 사용자의 신분을 증명한 후 사용자의 정보를 회원가입과 같은 절차를 통해 수집하고 저장한다. 이와 같이 중앙에서 관리하는 것은 관리적 측면의 편리성은 존재하지만 관리시스템 자체가 단일 실패 지점으로서의 위험성과 해킹 등으로 인한 개인정보 유출의 위험성이 상존한다. 최근 중앙관리의 한계를 급복하기 위해 분산 원장관리 기술인 블록체인 기술이 등장하였다. 블록체인 기술은 각각의 정보의 블록을 체인으로 연결하여 블록체인에 참여하는 각 노드에 의해 관리하는 분산관리 기술이다. 본 논문에서는 블록체인 기술을 기반으로 하는 온라인 신분증명 스킴을 제안한다. 블록체인을 기반으로 하기 때문에 개인의 정보를 중앙에서 관리할 필요가 없다. 또한 블록체인의 특성상 위변조로부터 안전하다는 장점이 있다. 마지막으로, 제안하는 방법에서 노드에 저장되는 개인정보는 암호화하는 방법을 사용하여 타인의 정보를 볼 수 없도록 하는 기밀성을 제공할 수 있어 노출에 대한 안전성을 제공한다.

키워드: 블록체인(Blockchain), 신분증명(Identity Certification), 인증(Authentication)

I. Introduction

최근 인터넷 환경의 변화는 생활에 많은 변화를 가져왔다. 특히, 인터넷을 이용한 민원업무, 쇼핑, 금융 등의 서비스는 더 이상 시간과 공간의 제약으로부터 사용자를 자유롭게 하였다. 인터넷을 이용한 이러한 서비스의 기반에는 공인인증서, 휴대전화, 신용카드 등을 이용한 인터넷 기반 사용자 인증기술이 자리하고 있다. 이와 같은 인증기반에서 서비스 제공자들은 신원확인 후 회원가입과 같은 절차를 거쳐 사용자의 개인정보를 자체적으로 저장하고 관리하는 중앙 집중 방식을 사용한다. 중앙집중식 저장관리는 서비스제공자의 측면에서는 긍정적으로는 고객에게 최적화된 서비스를 제공할 수 있는 방법이기는 하지만 개인정보유출 사고와 같은 사이버침해로부터 자유롭지 못하다. 최근 통계에 따르면 5년간 약 5천만 개 이상의 개인정보 유출사고가 발생하였다[1].

중앙 집중 관리방식의 한계점을 개선하기 위해 최근 등장한 기술이 블록체인 기술이다[2]. 본 논문에서는 블록체인 기술 기반 온라인 신분증명 스킴을 제안한다. 제안하는 스킴은 블록체인의 특성을 유지하고 있다. 즉, 신분증명 정보에 대해 중앙집중식 저장관리가 필요하지 않고 블록체인에 참여하는 개별 노드에서 신분증명 정보가 관리된다. 또한 블록체인 기반기술의 특성상 정보의 위변조가 어려워 무결성을 보장하며, 각 노드에 저장되는 개인정보는 소유자가 암호화하기 때문에 기밀성이 보장되고 유출로부터 안전하다.

II. Preliminaries

1. Related works

1.1 블록체인

블록체인은 비트코인을 위해 개발된 기반 기술이다[2]. 블록체인의 기본적인 구조는 각각의 정보를 블록으로 만들고 각 블록에는 앞 블록의 해시 값이 포함되어 있다. 이러한 특성은 각 블록을 체인과 같이 연결시켜 준다. 따라서 블록체인 구조에서는 특정 블록을 변경하게 되면 연결된 하위 블록을 연속적으로 모두 변경해야 하며, 이 작업이 블록체인에 참여하는 모든 노드들 보다 빨리 이루어 져야하기 때문에 현실적으로 생성된 블록을 수정하는 것이 매우 어렵다. 블록체인은 그 사용처에 따라 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인(Consortium Blockchain) 3가지로 분류가 가능하다[3]. 각 블록체인은 구조적으로 유사하지만 다른 개념과 특징을 가지고 있으며, 블록체인을 정의 및 구현하기 위한 선결 요건 또한 존재한다. 이 중 퍼블릭 블록체인은 누구나 참여할 수 있으며, 참여자가 모두 블록을 생성하고 작업증명(Proof of Work)과정을 통해 검증할 수 있는 공개된 기반기술이다. 프라이빗 블록체인, 컨소시엄 블록체인은 블록체인을 다른 용도로 활용하기 위한 개념이다.

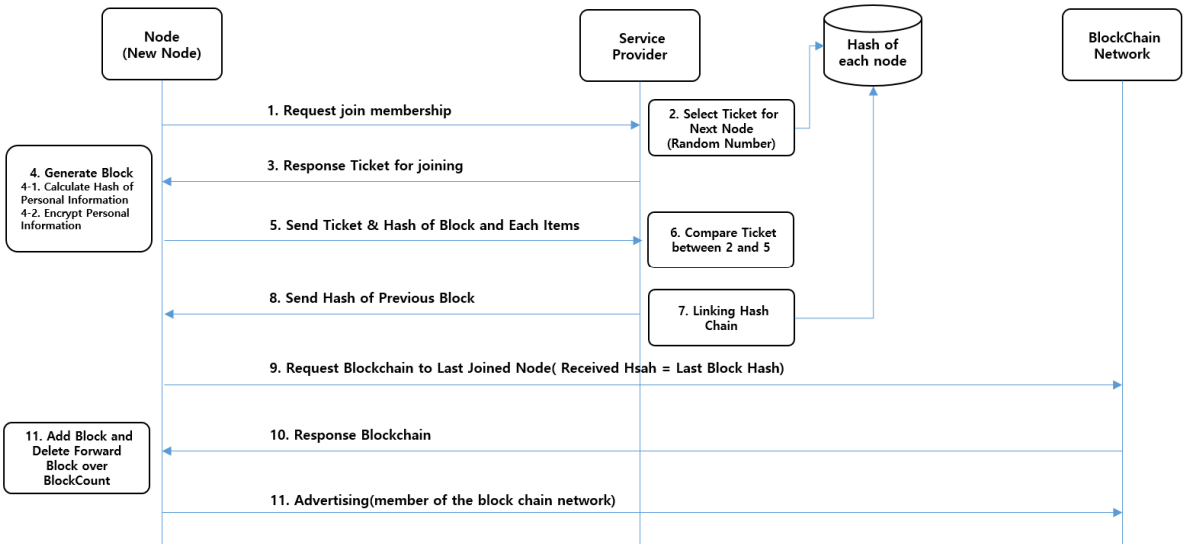

Fig. 1. BlockChain Network Join Process

1.2 온라인 신분증명

온라인 신분증명에 사용되는 정보는 크게 주민등록번호, 공인인증서, 휴대전화, I-PIN(Internet Personal Identification Number)등이 있으며, 주민등록번호를 사용하는 방법은 개인정보보호법[4][5]에 의해 대체 수단을 제공하도록 규제하고 있다. 이와 같은 방법의 공통적인 특성은 첫 째, 최초 발급 시 대면 또는 이와 유사한 방법으로 신원확인을 거친 후 발급된 정보를 사용하여 신원을 확인하며, 확인을 위한 정보가 특정 시스템에 데이터베이스화 되어 관리된다. 둘 째, 사용되는 정보에는 신원확인을 위한 정보만이 포함되어 있어 서비스제공자는 회원가입과 같은 절차를 통해 사용자의 정보 – 주소, 연락처 등 – 를 추가적으로 수집한다. 이렇게 수집된 정보는 각 서비스제공자의 내부에 데이터베이스로 관리된다.

2. Limitations and improvement

기존 온라인 신원확인의 가장 큰 한계점은 중앙집중식 관리로 인한 해킹의 위협이다. 최근 다양한 해킹사례에서 보여주듯이 기업 내부의 개인정보를 유출하기 위한 시도가 빈번히 발생되고 있으며, 이에 대응하기 위한 컴플라이언스 준수 등 기업 내부의 관리적인 비용이 증가하고 있다. 이와 같은 한계점을 해결하기 위해 본 논문에서는 블록체인 기술을 제안한다. 블록체인 기술을 사용함으로 인해 개인정보를 서비스 제공자가 저장할 필요 없어 침해로부터 보다 안전하다고 말할 수 있다. 하지만 블록체인 기술의 특성은 각 블록의 모든 정보를 블록체인에 참여하는 각 노드가 모두 볼 수 있다는 점이다. 신분증명을 위한 정보를 블록체인으로 만든다면, 타인이 자신의 신원확인을 위한 정보 즉, 개인정보를 열람할 수 있기 때문에 이에 대한 보안책이 필요하다. 본 논문에서는 이에 대한 대책으로 블록에 포함된 각 개인의 정보를 소유자가 자신만의 키를 사용하여 암호화하는 방식을 제안한다.

III. Blockchain-Based Online Identity Certification

본 논문에서 제안하는 온라인 신분증명 스킴은 블록체인과 암호화 기술을 사용한다. 제안하는 신분증명 스킴의 구성요소는 사용자들로 구성된 퍼블릭 블록체인과 사용자에게 서비스를 제공하는 서비스 제공자이다. 제안하는 방법은 블록체인을 생성하는 단계, 즉 블록체인에 참여하는 단계와 서비스제공자와 상호작용을 통해 인증을 하는 2가지 단계로 진행된다.

1. 블록체인 참여(블록 생성)

첫 번째 단계는 블록체인을 생성하는 단계이다. 블록체인을 생성하기 위해서는 먼저 블록체인에 참여하여야 한다. 이는 회원가입과 유사한 절차를 거친다. 다만 일반적으로 회원가입을 할 때에는 개인정보를 서비스제공자에게 전달하지만 블록체인 네트워크에 참여하는 단계에서는 개인정보를 서비스제공자에게 전달하지 않는다. 세부적인 절차는 fig. 1과 같다. 먼저 블록체인에 참여하고자 하는 사용자는 참여 의사를 서비스제공자에게 전달한다. 서비스제공자는 작업증명 과정을 통제한다. 이는 각 참여자가 작업증명을 함으로 소요되는 시간을 절약하고 효율성을 높이기 위함이다. 서비스제공자는 참여를 요청한 사용자에게 티켓을 발행한다. 이 티켓은 다수의 요청자가 있을 때 블록체인의 중복생성을 방지하기 위한 순서를 정해준다. 티켓을 발급받은 사용자는 개인의 정보를 암호화하고, 각 정보의 해시를 머클해시트리로 만든다음 각 정보의 해시값과 Root 해시값 그리고 티켓을 다시 서비스제공자에게 전달한다. 서비스제공자는 티켓의 유효성을 확인한 후 현재 연결된 블록체인의 마지막 블록의 Root 해시를 요청자에게 전달한다. 요청자는 블록체인 네트워크에 수신한 Root해시를 마지막 블록으로 가진 노드에게 블록체인을 요청하고, 하위에 자신의 블록을 연결한다. 블록체인이 생성되면 각 노드는 자신의 노드를 기준으로 상위 N개의 노드에 대한 블록체인만을 보유한다. 통상적인 블록체인 구조에서는 각 노드가 모든 블록을 가지고 있어야 하며 이러한 방법이 가장 효과적이지만 무한정 커지는 블록의

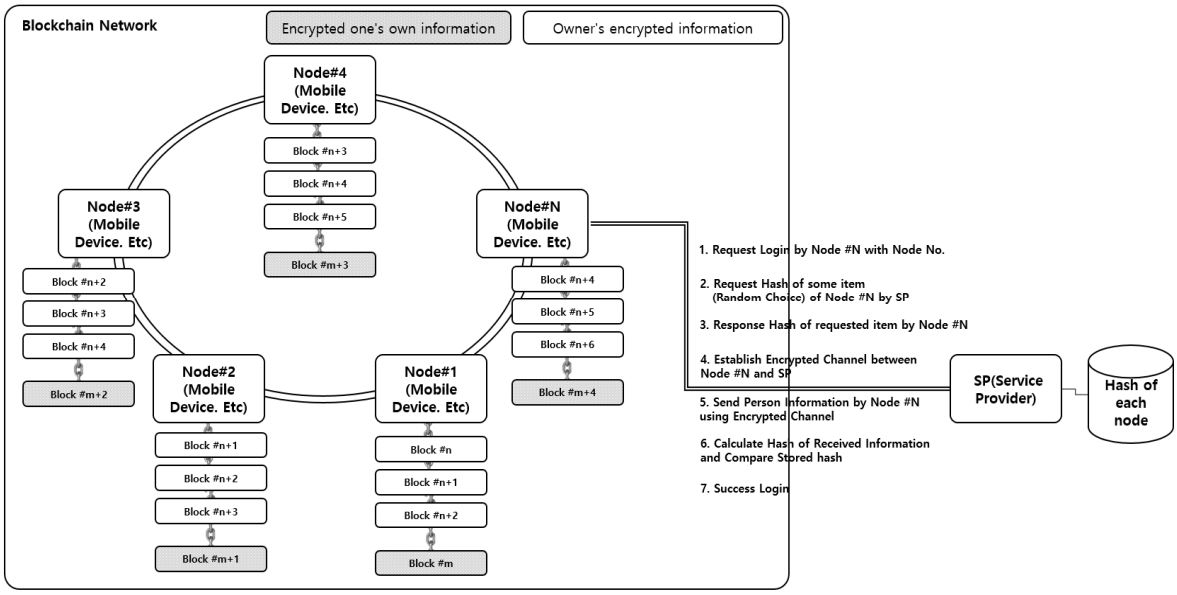

Fig. 2. Authentication Process using BlockChain

크기와 참여노드의 성능, 분산화 효과 등을 고려하여 N을 선정한 후 각 노드는 자신의 정보 상위 N개의 노드의 정보만을 가지고 있어도 수학적으로 하나의 노드 정보는 최소 N개, 최대는 노드의 수 $M_{(Node)}$만큼 분산 저장된다.

2. 블록체인을 이용한 인증

두 번째 단계는 인증단계이다. 인증 단계에서는 사용하는 방법은 시도응답 방법이다. 즉, 특정 사용자가 로그인을 요청하면 서비스제공자는 해당 사용자가 생성한 블록내에 포함된 특정 필드의 해시값을 요청한다. 이때, 필드의 선택은 랜덤 선택을 사용하여 재상용을 방지한다. 사용자로부터 해당 필드의 해시값이 전송되면 서비스제공자는 저장된 해시값과 전송된 해시값을 비교하여 일치할 경우 해당 사용자와 암호채널을 생성한다. 이후, 사용자는 암호채널을 통해 개인정보를 전송하고, 서비스제공자는 수신한 개인정보의 해시를 계산한 후 저장된 해시값과 비교한다. 만약 해시값이 일치한다면 정당한 사용자로 인정하고 로그인이 성공한다. 블록체인 네트워크에서 관리되는 블록과 서비스제공자와의 인증 과정은 fig. 2와 같다.

3. 검증 및 분석

3.1 기밀성 보장

제안하는 방법은 각 노드가 자신의 암호키를 사용하여 암호화하기 때문에 자신의 정보는 즉시 확인이 가능하고, 타 노드의 정보는 블록체인 내에 포함되어 있지만 확인이 불가능하다. 또한 개인정보를 서비스제공자에게 전송하기 전 사용자 식별을 거쳐 암호화된 채널을 사용자별로 생성하기 때문에 기밀성은 알려진 암호화 방법의 안정성만큼 보장된다.

3.2 무결성 보장

제안하는 방법에서 각 노드가 보유한 블록 내의 개인정보를 머클해시트리의 개념을 사용하고 블록을 생성할 수 있는 권한은 서비스제공자에 의해 통제되기 때문에 노드가 임의로 블록의 내용을 변경하거나 인가되지 않은 블록을 연속적으로 연결하여 블록체인 자체를 변조할 가능성은 희박하다.

3.3 가용성 보장

제안하는 방법에서는 노드의 정보를 서비스제공자가 저장하지 않는다. 하지만 사용자가 서비스를 제공받기 위해 언제든지 온라인상으로 신원증명을 하게 되면 수신하는 블록에 개인정보가 포함되어 있기 때문에 활용이 필요할 때에는 언제든지 활용이 가능하다

3.4 블록체인 복사 등의 재사용 위험

블록체인 내의 자신의 블록을 인증을 위해 사용하기 위해서는 먼저 노드 내에서 블록의 암호화를 해제 하여야 한다. 따라서 복사와 같은 재사용은 기밀성 보장에서 언급한 수준으로 안전하다.

IV. Conclusions

본 논문에서는 퍼블릭 블록체인을 기반으로 하는 온라인 신원증명 스킴을 제안하였다. 제안하는 방법은 개인에 관한 정보를 서비스제공자가 저장할 필요가 없어 서비스 제공자의 입장에서는 개인정보 유출을 위한 사이버 해킹 등으로부터 안전하다. 개인의 측면에서는 자신의 정보를 서비스를 제공받을 시점에만 서비스 제공자에게 전송하기 때문에 개인정보 유출로 인한 추가적인 피해로부터 안전하게 된다. 또한, 개인정보를 각 노드에 저장할 때 암호화 하기 때문에 기밀성이 보장되고, 블록체인 기술을 기반으로 하여 무결성이 보장된다.

향후, 본 논문에서 제안하는 스킴을 실제 구현하여 모바일과 같은 휴대단말 환경에서 과연 얼마만큼의 분산저장이 효과적인지와 다양한 해킹의 방법으로부터 제안하는 인증 방법이 어느 정도 안전성을

보장하는지 등을 실험을 통해 검증할 계획이다. 또한 제안하는 방법을 오프라인에서도 적용할 수 있는 방안에 대한 연구를 지속할 것이다.

REFERENCES

[1] TaeJin Kim, “50 million personal information leaks in the last five years”, *http://www.zdnet.co.kr/news/news_view.asp?artice_id=20171002094311, 2017.10*

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.10.31.

[3] Byeong-ju Park, Tae-jin Lee and Jin Kwak., "blockcha in-Based IoT Device Authentication Scheme," Jourjal of The Korea Institue of Information Security & Cryptology, Vol. 27, No. 2, pp. 343-351, Apr. 2017.

[4] KISA, *https://www.i-privacy.kr/jsp/user4/support/help1.jsp*

[5] Hyung-Hyo Lee., "An Alternative Resident Registration Number System and Management Framework for Privacy Protection," The Journal of Korean Institute of Information Technology, Vol. 8, No. 6, pp. 49-58, June 2010.

[6] Song-yi Han, Kang Ryoung Park and So-Young Park.,. "A Study on Releasing Cryptographic Key by Using Face and Iris Information on mobile phones." Journal of the Institute of Electronics Engineers of Korea, Vol. 44, No. 6, pp.1-9, Nov. 2007.