스마트 컨트랙트를 이용한 사용자 중심 신원 관리 시스템

강민혁, 박민경, 권태경
서울대학교

{mhkang, mkpark}@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

User-Centric Identity Management System Using Smart Contact

Minhyeok Kang, Minkyung Park, Ted " Taekyoung" Kwon
Seoul National University Department of Computer Science and Engineering

요 약

사용자 신원을 관리하는 시스템은 신원 인증, 권한 부여 시스템 등에서 핵심적인 구성요소이다. 본 논문에서는 스마트 컨트랙트를 기반으로 탈 중앙화된 방식으로 안전하게 사용자가 신원을 생성, 관리하는 시스템을 제시한다. 사용자 신원은 스마트 컨트랙트를 통해 정의되며, N 개 중 k 개 임계치 서명 기법을 활용하여 비밀 키가 탈취된 상황에서도 안전하게 신원을 보호할 수 있는 기법을 제안한다.

I. 서론

사용자 신원을 관리하는 시스템은 신원 인증, 권한 부여 시스템 등에서 필요한 핵심적인 구성요소이다. 현재 신원 관리 시스템은 통합된 체계로 구성되어 있지 않고, 서로 다른 서비스 제공자가 각자 고유의 신원 관리 시스템을 구축하여 서비스를 제공하는 사일로 형태를 띄고 있다. 이에 따라 사용자는 각 서비스를 이용하기 위해 여러 신원을 생성하고, 그 정보를 기억하여야만 하는 불편함이 존재한다. 이에 대한 해결책으로 이더리움 시스템과 스마트 컨트랙트를 기반으로 신원을 정의하여 활용하는 시도들이 있었으나[1, 2], 신원을 정의하는 컨트랙트에 대한 접근이 비밀 키를 통해 제어되므로, 비밀 키가 탈취되었을 경우 신원에 대한 접근이 외부로 노출되거나[2] 통제권을 완전히 잃어버릴 수 있다는 위험이 존재한다[1].

본 논문에서는 스마트 컨트랙트(Smart Contract)를 기반으로 분산 환경에서 안전하게 사용자가 신원을 생성, 통제하는 시스템을 제시하며, 비밀 키가 탈취된 경우에도 N 개 중 k 개 임계치 서명(k-out-of-N Threshold Signature) 기법을 통해 안전하게 신원의 통제권을 복구하는 기법을 제안한다.

II. 배경지식

1. 블록체인

블록체인(Blockchain)은 개별 트랜잭션의 집합인 블록을 리스트 형태로 연결한 자료구조로, 블록 간 연결 관계는 다음 블록이 이전 블록의 암호기반 해시 값을 포함하는 것으로 정의된다. 블록체인은 분산된 노드들에 의해 유지, 관리되며, 정해진 프로토콜에 의해 전체 시스템에서 동일한 뷰를 가지도록 보장된다. 특히 각 블록이 유효한 블록으로 인정되기 위해서는 계산이 필요한 증명 과정이 필요하므로 기록된 정보에 대하여 임의 수정이 어렵다는 특징을 가진다.

2. 이더리움

이더리움(Ethereum)은 블록체인을 기반으로 한 암호화폐 시스템의 한 종류로, 스마트 컨트랙트를 효율적으로 배포, 실행시킬 수 있는 환경을 구축하고 있다. 이더리움에는 비밀키에 의해 통제되는 외부 소유 계정(Externally Owned Account)과 코드에 의해 통제되는 컨트랙트 계정(Contract Account)이 존재하며, 사용자는 외부 소유 계정을 통해 트랜잭션을 생성하여 스마트 컨트랙트를 배포하거나, 스마트 컨트랙트에 포함된 코드를 실행할 수 있다[3].

3. 스마트 컨트랙트

스마트 컨트랙트는 특정 조건을 실행 가능한 코드로 구현한 일종의 계약으로, 이더리움에서는 트랜잭션을 통해서 블록체인에 배포한다. 스마트 컨트랙트는 고유 주소를 가지고 있어, 해당 주소로 메시지를 전송하면 컨트랙트 코드가 실행된다. 코드를 실행함으로써 이더리움의 상태(State)를 변경하거나 다른 스마트 컨트랙트로 메시지를 전송할 수 있다.

4. N 개 중 k 개 임계치 서명 기법

N 개 중 k 개 임계치 서명 기법은 하나의 공개 키와 이에 대응하는 비밀 키를 N 개로 나누어 구성하여, N 명의 나누어 가진 뒤, 각각 자신의 비밀 키로 특정 메시지를 서명하였을 때, k 개 이상의 서명이 있어야만 공개키를 통해 인증할 수 있는 서명기법이다[4].

III. 제안하는 사용자 중심 신원 관리 시스템

본 논문에서 제안하는 사용자 중심 신원 관리 시스템은 중앙화된 관리 기관 없이 사용자가 직접 자신의 신원을 생성, 관리할 수 있는 시스템이다.

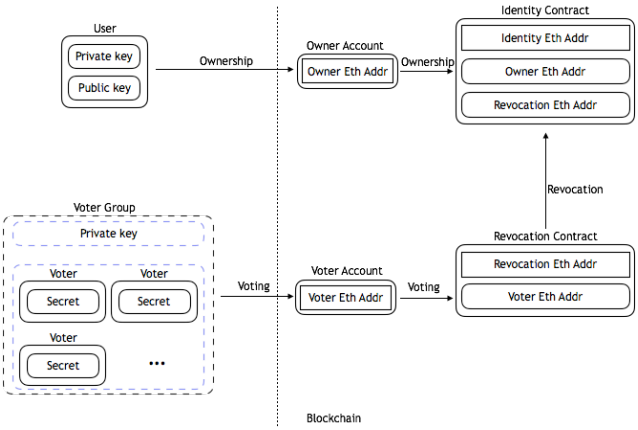

그림 1. 신원 관리 시스템 구조

그림 1 은 제시한 신원 관리 시스템의 구조를 나타낸 것으로 사용자 신원을 나타내는 신원 컨트랙트(Identity Contract), 신원 컨트랙트를 소유하는 소유자 계정(Owner Account), 소유자 계정을 통해 트랜잭션을 생성하는 사용자(User), 소유자 계정 주소를 폐지, 갱신할 수 있는 폐지 컨트랙트(Revocation Contract), 폐지 컨트랙트에 트랜잭션을 전달하는 투표자 계정(Voter Account), 투표자 계정을 통제하는 투표자 그룹(Voter Group)으로 구성되어 있다.

사용자는 비밀 키와 공개 키 쌍을 생성하고, 생성된 공개키를 이용해 고유한 소유자 계정의 이더리움 주소(Ethereum Address)를 만든다. 소유자 계정을 통해서 생성하는 트랜잭션은 대응하는 비밀키로 서명하여야 하기 때문에, 소유자 계정 주소를 통해 검증 가능하다.

신원 컨트랙트는 사용자의 신원을 나타내며, 신원 컨트랙트의 주소(Identity Eth Addr)는 사용자의 신원을 구분하는 일종의 식별자(Identifier)이다. 사용자가 신원을 생성할 때, 소유자 계정의 주소(Owner Eth Addr)와 폐지 컨트랙트의 주소(Revocation Eth Addr)를 지정한다. 신원 컨트랙트는 반드시 소유자 계정에 의해 생성된 메시지만 실행, 전달 하기 때문에, 사용자 신원을 인증하며 다른 응용 서비스의 스마트 컨트랙트를 구동할 수 있다. 소유자의 비밀 키가 탈취되거나, 새로운 키로 갱신하고자 하는 경우에 신원을 유지한 채, 지정된 소유자 계정의 주소만 폐지, 갱신 할 수 있다. 이는 폐지 컨트랙트를 통해서만 가능하다.

폐지 컨트랙트에는 투표자 계정의 주소(Voter Eth Addr)가 명시되어 있어, 해당 투표자 계정만 폐지 컨트랙트로 메시지를 전달할 수 있다. 새로운 소유자 주소에 대한 메시지가 전달된 경우에 폐지 컨트랙트는 소유자 주소를 변경하도록 신원 컨트랙트를 구동한다. 투표자 계정의 주소(Voter Eth Addr)는 하나 이상의 투표자가 소유한 비밀 키에 대응하는 공개키로 생성된다.

투표자 그룹은 투표 계정을 통해 트랜잭션을 전달할 수 있는 비밀 키를 가진 개체들이며, 예를 들어 사용자가 소유한 기기가 될 수 있다. 각각의 투표자는 비밀 키를 구성하는 비밀을 나눠 가지며 k-out-of-N 임계치 서명기법을 사용하여 투표자 중 지정된 개체 수 이상이 서명하여야만 트랜잭션에 서명할 수 있다.

IV. 활용 시나리오

1. 사용자 공개키 신뢰 구축

신원 관리 시스템에 추가로 공개키 신뢰 정보를 매핑하는 스마트 컨트랙트를 구성할 경우, 사용자의 공개키 대한 신뢰 정보도 탈 중앙화된 방식으로 관리 될 수 있다. 이때 신뢰 체계는 신뢰 망(Web-of-Trust) [5]에서 자신이 신뢰하는 공개 키들의 셋인 열쇠고리(Key Ring) 또는 인증기관(Certificate Authority)이 발급한 인증서를 신원에 매핑하는 것으로 신뢰 정보를 관리/구축할 수 있다.

2. OpenID 형식 신원 인증

OpenID 에서 개별 사용자의 신원에 대한 식별자는 URL 또는 XRI 로 구성되며, 이에 대응하는 Yadis 문서에 사용자와 관련된 신원 서비스에 대한 정보가 저장된다[6]. 사용자의 신원을 확인하려는 의존 파티(Relying Party)는 사용자 신원 식별자를 통해 신원 제공자(Identity Provider)에 대한 정보를 확인하고, 사용자를 신원 제공자에게로 보내어 인증을 받게 하며, 인증 결과 제공된 토큰을 사용하여 신원을 확인한다. 이때, 신원 식별자로 본 논문에서 제시한 신원 컨트랙트의 주소를 사용하고, 이에 대응하는 Yadis 문서의 정보를 사용자 신원에 매핑하는 컨트랙트를 구성한다면, OpenID 형식의 신원 인증 시스템을 구축할 수 있을 것이다.

V. 결론

논문에서 제안한 사용자 신원 관리 시스템은 이더리움 기반의 스마트 컨트랙트를 통해, 사용자가 본인의 신원을 직접 관리할 수 있게 하여 개별 사용자의 신원에 대한 통합된 시각을 제공할 수 있다. 그뿐만 아니라, 임계치 서명 기법을 통해 사용자의 비밀 키가 탈취된 상황에서도 사용자의 신원 폐지를 가능하게 하여 기존 연구의 한계를 극복하였다. 향후 연구에서는 제안한 시스템을 기반으로 사용자 공개키 신뢰 구축 및 신원 인증을 위한 통합 인증 시스템을 제안/구축하고자 한다.

참 고 문 헌

[1] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, Michael Sena, "UPORT: A Platform for Self-Sovereign Identity 2017, (https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf).

[2] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." *Open and Big Data (OBD), International Conference on*. IEEE, 2016.

[3] Wood, Gavin. "Ethereum: A secure decentralized generalised transaction ledger." *Ethereum Project Yellow Paper* 151 (2014).

[4] Gennaro, Rosario, Steven Goldfeder, and Arvind Narayanan. "Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security." *International Conference on Applied Cryptography and Network Security*. Springer International Publishing, 2016.

[5] Caronni, Germano. "Walking the web of trust." Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000.(WET ICE 2000). Proeedings. IEEE 9th International Workshops on. IEEE, 2000.

[6] Recordon, David, and Drummond Reed. "OpenID 2.0: a platform for user-centric identity management." *Proceedings of the second ACM workshop on Digital identity management*. ACM, 2006.