블록체인 기반 자기주권 신원 시스템의 영지식 증명 기술 연구

황진주*, 김근형**
*동의대학교 응용소프트웨어공학전공
**동의대학교 게임공학전공
mfdo7722@gmail.com, geunkim@deu.ac.kr

A Study on Zero-Knowledge Proof Technology in Blockchain-based SSI System

Jin-Ju Hwang*, Geun-Hyung Kim**
*Applied Software Engineering Major, Dong-eui University
**Game Engineering Major, Dong-eui University

요 약

개인의 신원정보 보호에 대한 중요성이 높아지면서 개인이 직접 자신의 신원정보를 관리하고 데이터의 주권을 신원정보 소유자에게 부여하는 자기주권 신원 시스템에 대한 관심이 높아지고 있다. 자기주권 신원 시스템 내에서 개인은 스스로 자신을 식별할 수 있는 분산 식별자(DID: decentralized identifier)를 생성하고 분산 식별자 별 개인의 자격을 증명해주는 자격증명(VC: verifiable credentials) 정보를 발급받아 개인이 보유하며 자격증명의 검증을 요구하는 검증자에게 선택적으로 자격증명 정보를 제시한다. 개인의 프라이버시를 보호하기 위해 개인의 자격증명을 제시할 때 신원정보의 실제 데이터는 감추고 자격증명의 유효성은 입증시키는 영지식 증명의 개념을 적용하고 있다. 본 논문에서는 영지식 증명 기술을 살펴보고 하이퍼레저 인디(Hyperledger Indy) 기반 자기주권 신원 시스템에서 영지식 증명 기술 도입 예를 보인다.

1. 서론

우리가 사용하는 신원(identity)은 신원 사용자를 식별하는 식별자(identifier), 신원 사용자의 특성을 나타내는 속성(attribute), 신원의 사용자임으로 확인하는 인증 수단(authentication method), 신원을 발급하는 발급자(issuer)의 4 가지 요소로 구성된다. 신원을 검증하기 위해 검증자(verifier)에게 신분증을 제시하면 검증자는 신분증의 사진과 실물을 비교하여 신원의 소유자가 맞는지 확인한다.

온라인에서 기존의 신원 인증 기술은 중앙화 구조를 바탕으로 사용자가 자신의 신원을 관리하는 중앙기관에 신원 인증 요청을 보내면 중앙기관이 사용자의 신원을 대신 인증해주는 모델로 데이터의 주권을 중앙기관이 가진다. 이러한 모델에서는 사용자가 자신의 개인정보가 어떻게 사용되는지 알 수 없고 중앙기관이 자신의 정보를 악용하여도 사용자는 이를 알아채기 어렵다. 자기주권 신원(self-sovereign identity)은 탈중앙화 구조를 바탕으로 사용자가 직접 자신의 신원을 관리하고 데이터의 주권을 신원 소유자에게 부여하는 기술이다.

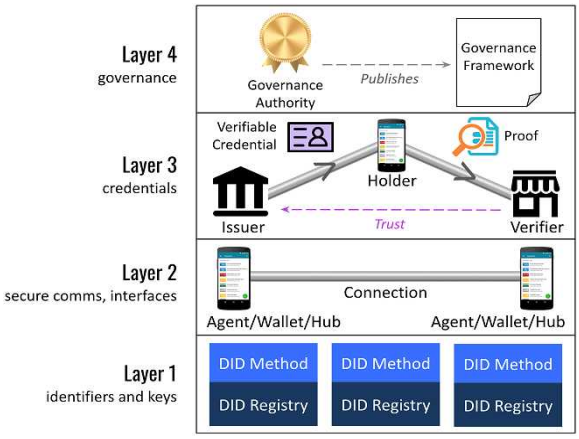
자기주권 신원의 증명은 분산 식별자(DID)와 검증가능 자격증명(VC), 검증가능 표현(VP: verifiable presentation)을 사용하여 구현한다. DID는 블록체인과 같은 탈중앙화 구조의 저장소를 기반으로 사람, 기관 및 사물을 식별하는 식별자이고 VC는 운전면허증, 학생증, 여권, 사원증, 졸업증명서, 재직증명서 등과 같이 사용자가 자신의 신원을 증명하기 위해 사용되는 신원증명이다.

자기주권 신원의 증명 기술에는 VC/VP와 영지식 증명을 이용해 인증 필수 데이터만을 블라인드 형태로 제공한다. 영지식 증명(ZKP, zero-knowledge proff)을 이용한 검증은 영지식성(Zero-knowledgeness), 건실성(Soundness), 완전성(completeness)의 세 가지 속성을 기반으로 대상이 제시한 조건에 대한 결과값인 참, f 거짓의 값을 이용해 유효함을 입증한다. 이더리움의 경우 프로토콜의 어느 부분도 암호화되어 있지 않았다. 이후 보안 문제를 인지하고, 영지식 증명과 동형암호화 도구 적용을 위한 환경 구성은 끝냈지만 배포로는 이어지지 않아 적용은 어려운 상황이다 [1].

자기주권 신원 시스템에 영지식 증명 기술의 도입이 된다면, 기관 입증 시 개인의 신원정보가 아닌 제시한 조건에 대한 유효성을 증명하여 신원인증이 가능하다. 본 논문에서는 블록체인 기반으로 구현된 DID 시스템에 영지식 증명을 적용한 모델을 제시하고, 그 효용성과 특징에 대하여 기술할 것이다. 또한 하이퍼레저 프로젝트의 인디 블록체인 플랫폼을 이용하여 자기주권 시스템 구축을 도모한다.

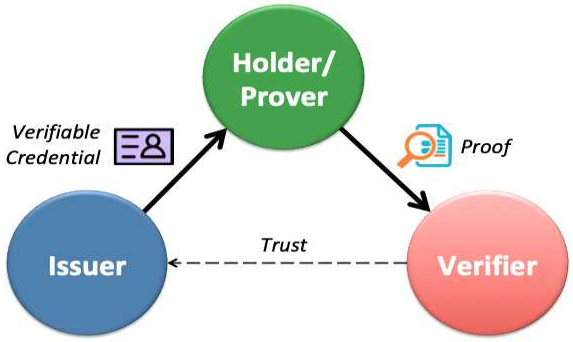
2. 자기주권 신원 시스템

자기주권 신원 시스템을 구성하는 모든 주요 핵심 요소에 대한 논의가 2018년 10월 IIW에서 처음 이루어졌고, 2019년 하이퍼레저 에리스 프로젝트 내에서 다음 (그림 1)과 같이 4계층으로 구성한 자기주권 시원 시스템 구조를 제안하였다.



(그림 1) 자기주권 신원 시스템 구조.

계층 1과 계층 2는 에이전트간 신뢰를 위해 암호화 신뢰가 설정되는 곳이며 계층 3은 (그림 2)에 나타낸 검증가능 자격증명 신뢰 삼각형 구축에 필요한 내용을 정의한다.



(그림 2) 검증 가능 자격증명 신뢰 삼각형

신뢰 삼각형은 비즈니스 거래의 한쪽 면만 설명한다. 많은 비즈니스 거래에서 양 당사자는 상대방에게 정보를 요청한다. 따라서 단일 거래에서 양 당사자는 보유자/증명자 및 검증자의 역할을 수행한다. 이 계층에서 해결할 문제는 교환할 검증가능 자격증명을 표현하는 형식과 자격증명 교환 프로토콜이다. 계층 4는 단순한 자기주권 신원 시스템 스택의 최 상위 계층이 아니라 강조점이 기계와 기술에서 인간과 정책으로 이동하는 곳으로 자기주권 신원 시스템 스택의 기술적 구현과 솔루션의 실제 비즈니스, 법률 및 사회적 요구사항을 연결하는 가교 역할을 한다. 모든 자기주권 신원 시스템의 궁극적인 목표는 온라인에서 상호작용하는 두 당사자 간에 상호 수용가능한 수준의 신뢰를 달성하는 것이다. 이 목표는 현재의 많은 형태의 거래에서 거의 불가능하다. 자기주권 신원 시스템을 사용하면 이 신뢰 계층의 기반이 암호화 신뢰에 의해 구축된다. 즉 탈중앙 네트워크에서 자격증명 발급자의 공개키와 공개적으로 확인할 수 있는 DID에 기반한다.

2.1 영지식 증명 기술

영지식 증명(ZKP, zero-knowledge proof) 기술은 증명자(prover)가 검증자(verifier)에게 자신의 비밀과 관련해 어떠한 정보도 노출하지 않고 비밀의 유효성을 증명하는 방법으로 사전에 정의된 연산에 대해 비밀 입력 값은 공개하지 않고 입출력 값의 관계에 해당하는 비밀 입력 값을 알고 있음을 증명하는 암호 기술이다[a]. 증명자는 영지식 증명 기술을 통해서 해당 함수 및 입력 값과 출력 값의 관계를 증명하는 증명 값을 만들고 검증자는 증명 값만을 가지고 함수의 입력과 출력의 관계가 맞는지 확인하여 검증 시 비밀 입력 값이 필요하지 않고 유출되지 않는다.

영지식 증명 기술은 증명할 문장이 참이면 정직한 증명자는 정직한 검증자에게 이 문장이 사실임을 납득시킬 수 있는 완전성, 증명할 문장이 거짓이면 어떠한 거짓된 증명자도 정직한 검증자에게 사실이라 납득시킬 수 없는 건t성, 검증자는 증명할 문장의 참, 거짓 이외에 아무것도 알 수 없는 영지식성의 조건을 만족하여야 한다.

영지식 증명 기술은 성인 증명에 사용할 수 있는 범위 증명(range proofs), 특정 국가의 시민임을 증명할 수 있는 집합의 원소(set membership) 증명, 신원정보 중 성별이 남성인지 여성인지 증명할 수 있는 비교(comparison) 증명, 계산 무결성을 증명하는데 활용할 수 있다.

영지식 증명의 수학적 정의는 다음과 같다.

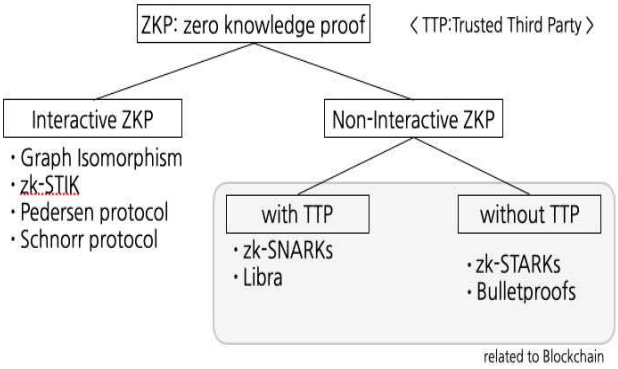
$$\forall x \in L, z \in \{0,1\}, \mathrm{View}_v[\mathrm{P}(\mathrm{x}) \leftrightarrow \mathrm{V}(\mathrm{x},\mathrm{z})] = \mathrm{S}(\mathrm{x},\mathrm{z})$$

$P(x)$는 증명자, z는 검증자의 질의 값, $V(x,z)$는 검증자, $View_v[P(x) \leftrightarrow V(x,z)]$는 검증자와 증명자 간의 상호증명 과정을 관찰하여 기록한 것이고 $S(x,z)$는 다른 컴퓨터에서 시뮬레이션한 결과로 검증자의 질의 값 0, 1에 대해 증명자와 검증자의 챌린지 증명과정을 다른 컴퓨터에서 똑같이 시뮬레이션할 수 있어야 한다는 것이다.

2.2 블록체인과 영지식 증명

영지식 증명은 블록체인의 프라이버시 문제 해결을 위해 사용된다. 영지식 증명 기술은 증거의 유효성을 검증하기 위해 증명자와 검증자간의 최종 증거 교환이 여러 번 이루어지는 대화식 증명 방법과 증명자가 최종 증거를 한번만 전달하는 비대화식 증명 방법으로 구분된다. 일반적으로 비대화식 증명방법이 좀 더 효율적이라 알려져 있다.

비대화식 증명방법은 증명자와 검증자가 제 3의 신뢰 기관으로부터 증거 생성과 검증에 필요한 정보를 전달받아 영지식 증명 방법(ZKP with TTP)과 제 3의 신뢰 기관이 없는 영지식 증명 방법(ZKP without TTP)으로 분류한다. 신뢰 기관이 없는 영지식 증명 방법은 증거 생성과 검증에 필요한 정보를 증명자와 검증자가 메시지 교환을 통해 만들기 때문에 시스템의 효율성은 낮아지나 탈중앙화 특성은 유지한다[2].



(그림 3) 영지식 증명 방법과 블록체인과의 관계

zk-STARKs와 Bulletproofs는 신뢰기관이 없는 영지식 증명 방법에 해당된다. zk-STARKs 증명은 충돌저항성 해시 함수를 통해 더 희박한 대칭 암호화를 사용하기 때문에 초기 신뢰 설정이 필요하지 않다. zk-STARK는 계산이 증가하여도 증명자와 검증자 간의 통신 횟수의 양이 일정한데 zk-SNARK는 계산이 필요할 수로 증명자와 검증자 간의 통신 횟수의 양이 증가한다. 따라서 zk-SNARK의 전체 데이터 크기는 zk-STARK의 데이터보다 더 많다.

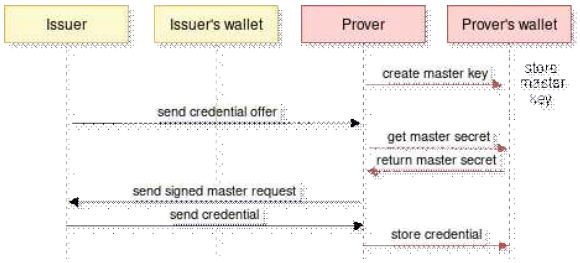
zk-SNARKs 증명은 신뢰할 수 있는 기관이 제공한 정보를 사용한 영지식 증명 방법이다.

2.2 하이퍼레저 영지식 증명 프로토콜

하이퍼레저 패블릭(Hyperledger Fabric)은 강력한 인증뿐만 아니라 신원을 드러내지 않고 거래할 수 있는 능력인 익명성(anonymity), 하나의 신원이 여러 번 사용되었을 때 동일한 신원으로 사용되었다는 것을 알 수 없도록 하는 불연계성(unlinkability) 등의 개인정보보호 기능을 제공하는 idemix 프로토콜을 제시한다.

하이퍼레저 인디(Hyperledger Indy)는 블록체인 또는 기타 분산 원장에 기반을 둔 디지털 신원을 제공하기 위한 툴킷, 라이브러리 등을 제공한다. 하이퍼레저 인디는 사용자 신원정보 보호를 위해 선택적 공개와 영지식 증명을 한다. 하이퍼레저 인디는 Idemix 프로토콜에 기반한 Indy-anoncreds를 사용하여 자격증명(Crednetial)의 주장(Claim)을 보호한다. 하이퍼레저 인디는 암호화 관련 API를 제공하는 하이퍼레저 울사(Hyperledger Ursa)의 Bulletproof 방법, Idemix 기반한 방법의 두 방식의 영지식 증명 방법을 사용할 수 있다. 보안과 암호화 관련하여 crypto, 선택적 정보제공, 대칭키 암호화 등 여러 방법을 결합하여 사용하여 보안에 주의를 두고 있다[3].

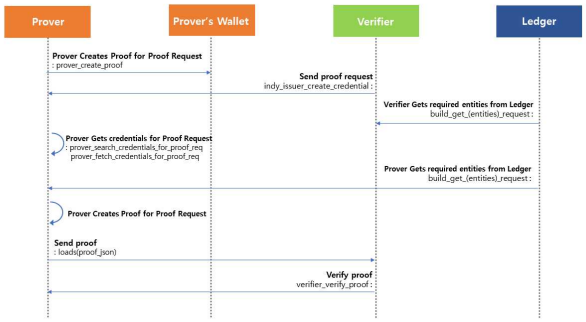
다음 그림은 Indy-annocreds를 사용하여 자격증명에 영지식 증명을 위한 기본적인 시퀀스이다.



(그림 4) 마스터키 요청 생성 및 자격증명 발급

증명자는 자신의 자격증명의 소유권 증명을 위해 고유한 속성을 마스터 키를 통해 증명한다. 자격증명 발급자는 증명자에게 자격증명 제안(Credential Offer)을 보낸다. 그 후 증명자는 자격증명 요청을 생성하고 보낸다. 발급자가 서명된 자격증명 요청을

올바르게 수신하면 발급자는 증명자에 대한 자격 증명을 생성한다. 자격증명 생성 시 자격증명 발급자, 서명 방법, 폐기방법 등을 기술해야 한다.



(그림 5) 자격증명 검증 절차

발급자는 개인 키를 사용하여 전달받은 방식을 통해 서명한다. 서명된 자격증명은 검증자에게 전송된다. 검증자는 증명자에게 증거 요청을 보내서 소유권 증명을 요청하고 검증자는 그에 맞는 알맞은 증명을 생성해 응답한다. 검증자는 수신된 증명의 유효성을 기본적으로 indy_verifier_verify_proof를 통해 전달된 증명 기법을 이용하여 true값이 확인된다면 올바른 자격 증명이 됨을 알 수 있다.

이러한 시퀀스를 기반으로 실제 테스트를 진행하여 영지식 증명이 적용된 검증가능 자격증명(VC)을 이용하여 신원인증이 가능함을 검증한다. 시뮬레이션에서는 VC 발급 시 발급 내용을 영지식으로 생성하기 위해 자격증명 증명의 속성 값의 생성 타입 값을 CL로 설정하였다.

(그림 6)과 같이 서명 유형에 “CL”, Camenisch Lysyanskya 속성을 추가하면, Prover의 복수 자격 증명(이름, 나이, 주소 등)에서 정보 노출 없이 하나의 서명으로 Issuer를 제안하여 하이퍼레저 영지식 증명을 위해 사용되는 기본 메소드 유형을 적용할 수 있다.

```
certificate_cred_def = {
      ‘tag’ : ‘TAG1’,
      ‘type’ : ‘CL’,
      ‘config’ : {“support_revocation” : True}
}
```

(그림 6) creidential definition 생성 유형 정의

```
running 1 test
test medium_cases::prover_create_credential_req::prover_c
reate_credential_req_works_for_invalid_credential_def ...
 ok

test result: ok. 1 passed; 0 failed; 0 ignored; 0 measure
d; 370 filtered out; finished in 21.16s
```

(그림 7) VC 유효성 검증 시뮬레이션 결과

이러한 방식으로 생성된 자격증명를 기반으로 한 개의 발급자와 한 개의 검증자 간의 영지식 증명 방법의 검증 시뮬레이션 결과는 (그림 7)과 같이 올바르게 인증이 완료되어 트랜잭션이 기록된다.

3. 결론

영지식 증명 모델을 이전에 도입하기 위해서는 하드웨어적 성능 혹은 그 이외의 성능의 한계로 증명을 위한 특성 중 하나가 결여되었다. 그러나 기술의 발전을 통하여 해당 문제가 소멸에 가까워졌다. 이러한 이유로 기업의 기술적인 능력이 따라준다면 영지식 증명 시스템의 도입은 개개인의 중요한 인적 사항이 오가는 DID 시스템에서는 필수불가결한 사항이 될 것으로 사료된다.

감사의글

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1047573).

참고문헌

[1] Andreas M. Antonopoulos / Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps, Sebastopol, CA, O'Reilly Media, pp. 67-70, Nov. 2018.

[2] 오현옥 “영지식 증명 연구 동향”, 정보통신기획평가원, 주간기술동향 1953호, 2020, 07.

[3] Chul Park, Jonghyun Kim, Dong Hoon Lee, "Privacy-Preserving Credit Scoring Using Zero-Knowl", Korea Institute Of Information Security And Cryptology, Vol. 29, No. 6, pp. 9-14, Dec. 2019