ZK-SNARK 기반 온체인 VC 검증 체계에서 지갑 주소 바인딩을 이용한 소유자 인증 기법

하현재 [1], 류재철 [2]
[1] 충남대학교 컴퓨터공학과 석사과정
[2] 충남대학교 컴퓨터공학과 교수

redcurrantcluster@gmail.com, jcryou@cnu.ac.kr

Ownership Authentication via Wallet Address Binding in a ZK-SNARK-Based On-Chain VC Verification Scheme

Hyeon-Jae Ha[1], Jae-Cheol Ryou[1]
[1]Dept. of Computer Engineering, Chungnam National University

요 약

메타버스와 Web3 환경에서 프라이버시 보호를 강화하기 위해 영지식 증명을 적용한 자기주권 신원(Self-Sovereign Identity, SSI) 체계가 주목받고 있다. 이러한 접근은 DID 문서 조회 없이 증명만으로 검증을 수행할 수 있어 확장성과 프라이버시 면에서 이점이 있으나, 제출자가 제시하는 검증가능 자격증명(Verifiable Credential, VC)의 정당한 소유자인지 확인하는 절차가 미비하다는 한계가 있다. 본 논문은 VC 발급 단계에서 소유자(Holder)의 지갑 주소를 VC 에 바인딩하고, 온체인에서 검증 컨트랙트에게 제출되는 ZK-증명 검증과 트랜잭션 송신자 주소와의 일치 확인을 결합해 소유자 인증(Holder binding)을 달성하는 기법을 제안한다. 제안 기법은 VC 도용 · 탈취 · 비인가 양도를 억제하고, 발급기관이나 DID 문서 저장소 조회 없이 제시자와 소유자의 동일성을 보장한다.

1. 서론

자기주권 신원(Self-Sovereign Identity, SSI)은 정부 등 중앙 기관에 신원 정보의 보관 · 제출 권한을 위임하던 기존 방식에서 벗어나, 디지털 신원의 생성과 관리에 대한 통제권을 신원 주체(개인)에게 부여하는 패러다임이다. C. Allen 은 SSI 가 갖추어야 할 핵심 특성으로 존재성(Existence), 통제권(Control), 접근성(Access), 투명성(Transparency), 지속성(Persistence), 이식성(Portability), 상호운용성(Interoperability), 동의(Consent), 최소화(Minimization), 보호(Protection)의 10 가지 원칙을 제시하였고, 이후 Q. Stokkink 과 J. Pouwelse 가 증명가능성(Provable)을 추가하여 총 11 가지 원칙이 SSI 설계 · 구현 수준을 평가하는 기준으로 자리 잡았다[1][2].

본 연구는 이러한 요구를 충족하기 위해 영지식 증명 프로토콜 zk-SNARK 을 적용한 검증 가능 자격증명(Verifiable Credential, VC) 구조와 운용 방식을 제안하며, 특히 디지털 신원의 도용 및 비인가 양도 문제를 해결하기 위한 지갑 주소 바인딩 기반 소유자 인증(Holder binding) 기법을 함께 제시한다.

2. 관련연구

2.1 DID 기술 현황

자기주권 신원(Self-Sovereign Identity, SSI)과 탈중앙화 신원(Decentralized Identity)은 밀접한 개념으로, 실제 적용에서는 두 용어가 엄격히 구분되지 않고 혼용되는 경우가 많다. 일부 연구에서는 탈중앙화 신원을 제 3 자 중개자를 제거하는 기술적 방법론으로, 자기주권 신원을 그 기술을 전제로 사용자가 전 과정에서 신원에 대한 주권을 갖는 지향점으로 구분한다[3].

기존 다수의 SSI 솔루션은 탈중앙화 식별자(DID) 기술에 기반하며, DID 문서를 신뢰 가능한 저장소에 게시 · 조회하고 그 안의 공개키로 서명 검증을 수행한다. 여기서 DID 문서의 저장 · 해결(Resolve) 거버넌스에 따라 탈중앙성 수준이 달라진다. DID 문서는 진위 · 무결성을 보장할 수 있는 저장소에 보관되어야 하며, 특정 중앙 운영자 API 에 의존하는 방식(예: did:genuineid)은 형식상 DID 를 따르더라도 제 3 자 신뢰에 종속되어 SSI 의 지향과 충돌할 수 있다는 지적이 있다[4]. 더 강한 탈중앙성을 위해서는 중앙식 솔루션 대신 투명성 · 불변성을 제공하고 누구나 접근 ·

검증 가능한 퍼블릭 블록체인과 같은 형태를 저장소로 채택하는 접근이 논의된다.

2.2 프라이버시 보호 기술

2.2.1 선택적 공개(Selective Disclosure)

탈중앙화 신원 프레임워크에서 신원 주체는 증명 시 프라이버시 원칙에 따라 검증에 필요한 최소 데이터만 선택적으로 제시할 수 있어야 한다. 검증가능 자격증명(VC)은 주체에 대한 클레임(claims)의 집합이며, 이 클레임은 credentialSubject 의 신원 속성이나 발급자 정보(issuer), 유효기간(issuanceDate, expirationDate), 상태정보(credentialStatus) 등 VC 내 여러 필드로 분산되어 있다. 전체를 공개하지 않고도 일부 속성만 선택적 공개하여 검증하는 기법이 제안 · 표준화되어 왔으며, 데이터 무결성(Data Integrity) 기반 BBS+ 계열이 대표적이다. 머클 트리 기반 설계의 경우 머클 루트에 커밋하고 부분 증명으로 특정 클레임만 공개하는 방식도 가능하다.

2.2.2 did 추적 방지(비연결성)

신원 주체가 매번 최소 데이터만 제시하더라도, 동일 키 쌍 · 동일 DID 로 서명된 VP 를 반복 제출하면 검증자에 의한 연결성 위험이 존재한다. 이를 완화하기 위해 매 제시마다 새로운 키 쌍을 생성하고, VP 마다 고유한 DID 문서를 등록하는 방식(일회용 DID)이 제안되었다[5]. 다만 실제 적용 측면에서 DID 문서 등록 빈도 증가로 저장 공간 부담이 커지고, 특히 블록체인에 저장할 경우 용량 · 가스비 비용이 커지는 운영상 비효율이 발생한다.

2.2.3 영지식 증명(zk-SNARK)

영지식 증명을 적용하면 DID 문서 조회 과정 없이, 사전에 정의된 증명 회로(circuit) 조건을 만족하는 단일 증명값(증명, proof)만으로 신뢰된 발급자가 발급한 신원 데이터임을 검증할 수 있다. 검증 과정에서 특정 DID 저장소에 대한 의존이 사라지므로, DID 기반 추적 위험을 고려할 필요가 줄어들며 퍼블릭 체인 기반 DID 조회 방식보다 강한 탈중앙성을 제공한다.

실무적으로는 zk-SNARK 를 사용해 스마트컨트랙트에서 온체인 검증을 수행하는 방식이 일반적이다. 회로 변경 시에는 신뢰 설정(trusted setup)을 재수행하여 증명키/검증키를 갱신한다. 증명자(Prover)는 증명키로 증명을 생성 · 제출하고, 검증자(Verifier)는 검증키로 진위를 확인한다. 이 과정에서 검증자는 조건 충족 여부만 판단하고 원본 속성 값은 알 수 없으므로, 전통적 선택적 공개보다 더 강한 프라이버시 보호가 가능하다.

또한 zk-SNARK 검증은 외부 조회 없이 온체인에서 소규모 연산으로 처리되므로 검증자 스마트컨트랙트로 구현하기 용이하다. 검증키를 보유한 컨트랙트는 트랜잭션 송신자(msg.sender)로부터 증명을 입력받아 참/거짓을 판정한다. 발급자 검증은 발급자 공개키 화이트리스트로 수행하며, 발급자 서명만으로 VC 와 그로부터 유도된 증명의 진위를 확보할 수 있으므로 소유자 서명이 추가로 필요하지는 않다. 다만 이 경우 VC 가 유출 · 양도되면 적법하지 않은 소유자도 증명 생성 자체는 가능하므로, 증명 제출자(제시자)가 VC 의 소유자와 동일한지를 확인하는 소유자 인증(Holder binding) 절차가 반드시 필요하다.

3. 제안 방식

블록체인 참여자는 지갑 주소와 개인키를 이용해 타 계정으로 자산을 전송하거나 스마트컨트랙트 함수를 호출하기 위해 트랜잭션을 생성한다. 지갑 주소는 공개키의 해시를 기반으로 파생되며, 트랜잭션 송신 주체를 나타내는 공개 식별자로 기능한다.

본 연구의 핵심은 온체인 검증자(스마트컨트랙트)에게 zk-SNARK 증명을 제출할 때 제출자의 지갑 주소는 개인키 보유자만 생성 가능한 불변 식별자라는 점에 착안하여 소유자 인증(Holder binding)을 달성하는 것이다. 구체적으로, VC 발급 단계에서 소유자가 제어하는 지갑 주소를 VC 에 바인딩하고, 제시 단계에서 증명자는 선택한 단일 주소를 공개 입력(public input)으로 포함한 증명을 온체인 검증자에 제출한다. 검증 단계에서 검증자는 증명의 참 · 거짓을 검증키로 확인하고, 공개 입력에 포함된 지갑 주소와 트랜잭션 송신자 주소의 일치를 확인한다. 이 두 조건이 모두 충족되는 경우에만 제시자가 곧 VC 의 소유자임을 인정함으로써, DID 문서 조회 없이도 VC 또는 증명이 적법한 소유자에 의해 생성 · 제출되었음을 보장한다.

다중 체인 환경을 고려해 여러 지갑 주소를 하나의 VC 에 바인딩할 수 있으며, 필요 시 머클 트리로 주소 집합을 커밋하여 제시 시 단일 주소만 선택적으로 공개하도록 구성한다.

4. 적용 방안

4.1 고려 사항

zk-SNARK 는 비대화형 영지식 신원증명 프로토콜로, 검증 연산의 크기가 작아 블록체인 상의 검증자 스마트컨트랙트 구현에 적합하다. 증명자는 사전에 공개된 증명키로 단일 증명을 생성하여 검증자에게 한 번 제출하면 되고, 검증자는 검증키만으로 검증을

수행한다.

다만 검증 컨트랙트가 검증 조건을 변경·추가할 필요가 있을 때는, 분산된 제 3 자 참여로 신뢰 설정(trusted setup)을 재수행하여 새로운 증명키/검증키 쌍을 생성하고, 해당 검증키를 사용하도록 컨트랙트를 배포·업데이트해야 한다.

이때 지갑 주소 일치 여부를 회로의 검증 조건에 직접 포함하면 다음의 제약이 발생한다.

1) 비대화형성 저하 및 탈중앙성 문제: 최초 요청 이전에는 검증자가 증명자의 지갑 주소를 알 수 없으므로, 실제 제출에 앞서 별도 절차로 주소를 통지해야 하고, 이는 비대화형 프로토콜의 이점을 훼손한다. 또한 회로 컴파일은 오프체인에서 수행되어 온체인으로 반영되므로 오라클/거버넌스 문제가 생길 수 있다.

2) 신뢰 설정·배포 오버헤드: 개별 제출자 주소에 맞춰 회로를 고정하면 매번 신뢰 설정(예: Power of Tau)을 반복해야 하며, 한 번 배포한 스마트컨트랙트의 재사용성이 떨어져 대기시간·가스비가 증가한다.

따라서 본 연구는 지갑 주소 일치 검증을 회로가 아닌 검증 컨트랙트 로직으로 분리하여, 비대화형 특성을 유지하고 운영 오버헤드를 최소화하는 방식을 채택한다.

4.2 검증 회로

zk-SNARK 는 공개 입력(public input)과 비밀 입력(비밀 증명값, witness)을 분리한다. 원본 신원 데이터는 비밀 입력으로 연산하여 조건 충족만 드러내고, 제출에 사용할 지갑 주소는 다른 신원 속성과 달리 숨길 필요가 없는 공개 값으로 취급한다. 이에 따라 프라이버시 보호 수준을 유지하면서도 비대화형 흐름을 깨지 않기 위해, 지갑 주소 일치 검증은 회로에 포함하지 않고, 회로는 신원 속성의 조건 충족만 책임지도록 한다.

4.2 검증 컨트랙트

검증 컨트랙트는 증명의 참·거짓을 검증키로 확인함과 동시에, 증명에 포함된 공개 입력의 지갑 주소를 추출하여 트랜잭션 송신자(msg.sender)와 직접 비교한다. 일치할 때에만 검증을 최종 성공 처리함으로써, 제시자=VC 소유자(Holder) 동일성을 보장한다.

```
function verifyVC(
    uint[2] calldata a,
    uint[2][2] calldata b,
    uint[2] calldata c,
    uint[] calldata publicSignals
) external view returns (bool) {
    require(
        verifier.verifyProof(a, b, c, publicSignals),
        "Invalid ZK proof"
    );
    address selected = address(uint160(publicSignals[0]));
    require(msg.sender == selected, "Wallet mismatch");
    return true;
}
```

(그림 1) 스마트 컨트랙트 검증 함수

4.3 VC 발급

발급자는 소유자의 요청에 따라 하나 이상의 지갑 주소를 VC 에 바인딩한다. 예시로, 이더리움 계열 주소를 DID 래핑 표기로 나타낼 수 있으며(예: did:ethr:0x…), 특정 체인만 허용하려면 체인 ID 를 함께 명시해 제어 지갑 주소 리스트를 구성한다.

증명 회로는 VC 의 임의 속성에 조건을 지정할 수 있지만, 오프체인 VP 를 사용하는 경우에는 제시와 무관한 지갑 주소를 모두 포함하는 것이 바람직하지 않다. 본 연구의 설계는 온체인/오프체인 겸용을 고려하므로, 선택적 공개가 가능하도록 credentialSubject 의 지갑 주소 필드를 머클 트리 커밋 또는 선택적 공개 가능한 서명 방식으로 구성하여, 제시 시 필요한 단일 주소만 공개할 수 있게 한다.

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://chungnam.ac.kr/credentials/9999",
  "type": ["VerifiableCredential", "ControlledAddressesCredential"],
  "issuer": "http://chungnam.ac.kr/issuers/1",
  "issuanceDate": "2025-09-30T23:00:00Z",
  "controlledAddresses": [
    "did:ethr:0xAAAaaaAAAaaaAAAaaaAAAaaaAAAaaaAAAaaaAAA1",
    "did:ethr:0xBBBbbbBBBbbbBBBbbbBBBbbbBBBbbbBBBbbbBBB2"
  ],
  "credentialSubject": {
    "id": "did:example:holder123456",
    "name": "Alice Kim",
    "studentNumber": "202500000",
    "email": "alice@example.com",
    "phone": "010-1234-5678"
  },
  "proof": {
    "type": "DataIntegrityProof",
    "cryptosuite": "bbs-2023",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:key:zExampleKey123456",
    "created": "2025-09-30T23:00:00Z",
    "proofValue": "u2VcVhQk...exampleProofValue"
  }
}
```

(그림 2) VC 내 지갑 주소 바인딩 예

4.4 소유자 지갑 동작

제출자(소유자)는 제출에 사용할 지갑 주소가 VC에 바인딩되어 있는지 확인하고, 해당 주소를 공개 입력에 포함하여 증명을 생성·제출한다. 이때 불필요한 주소 노출을 피하기 위해 제시 목적에 필요한 단일 주소만 선택해야 하며, 일치 여부 판단은 검증 컨트랙트의 msg.sender 비교로 수행된다.

5. 결론

본 연구는 zk-SNARK 기반 온체인 VC 검증 체계에서 지갑 주소 바인딩을 활용해 소유자 인증(Holder binding)을 달성하는 기법을 제안하고, 비대화형 흐름과 온체인 효율성을 유지하면서 프라이버시 보호를 강화한다. 또한 다중 주소 바인딩과 선택적 공개 설계를 통해 필요 이상의 메타데이터 노출을 줄이면서 온체인 적용성을 높였다.

향후에는 VC 발급 시점의 주소 소유 검증 절차(예: 메시지 서명, 소액 전송 챌린지 등)를 표준화하여 홀더가 자신의 제어 주소를 정확히 바인딩했음을 강하게 보장하는 방안을 추가 검토할 예정이다. 이를 통해 제안 기법의 보안성·현장 적용성·상호운용성을 한층 강화하고자 한다.

사사의 글

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (NO.2023R1A2C1006936)

참고문헌

[1] C. Allen, “The Path to Self-Sovereign Identity,” Life With Alacrity blog, Apr. 25, 2016. https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/.

[2] Q. Stokkink and J. Pouwelse, “Deployment of a Blockchain-Based Self-Sovereign Identity,” Technical Report, Delft University of Technology, 2018.

[3] D. Schumm, K. O. E. Müller, and B. Stiller, “Are We There Yet? A Study of Decentralized Identity Applications,” arXiv preprint arXiv:2503.15964, 2025.

[4] C. Allen, “Musings of a Trust Architect: When Technical Standards Meet Geopolitical Reality,” Life With Alacrity blog, Jul. 15, 2025. https://www.lifewithalacrity.com/article/musings-gdc25/.

[5] 김태훈, 김수현, 이임영, “DID 에서 사용자 비연결성을 제공하기 위한 일회용 DID 에 관한 연구,” ACK 2023 학술발표대회 논문집(30 권 2 호), 2023, pp. 210‑ 211.