하이퍼레저 패브릭 블록체인 기반 간단검증 탈중앙 신원 증명 시스템

조욱*, 김도훈**, 김호원†

*, ** 부산대학교 (대학원생), † 부산대학교 (교수)

Lightweight Verification Decentralized Identifier System based Hyperledger Fabric Blockchain

Uk Jo*, Dohun Kim**and Howon Kim†,

*, ** Pusan National University (Graduate student)

† Pusan National University (Professor)

요 약

탈중앙 신원 증명 시스템(Decentralized Identifier, DID)은 사용자 신원 증명을 중앙 시스템에서 사용자 중심으로 변화시켰다. 탈중앙 신원 증명 시스템은 사용자의 신원 증명시 개인정보 및 제공을 사용자가 직접 관리할 수 있다. 현재 DID 증명은 발급기관이 발급한 VC(Verifiable Credential)를 사용자가 VP(Verifiable Presentation)로 가공하여 서명한 후 검증기관에 제출하고 검증기관은 두 번의 서명을 검증하여 신원 증명을 완료한다. 본 논문에서는 두 번의 서명검증 단계를 VP ID 등록 검증과 VP검증 단계로 성능을 높임을 보였다. VP ID 등록 검증을 통해 불필요한 서명검증 단계의 계산 시간을 줄이는 효과를 보였다.

I. 서론

정보의 디지털화가 가속화되며 인터넷을 통해 유통되는 개인정보는 급속도로 증가하고 있다. 무분별한 개인정보 제공으로 발생하는 개인정보의 유출을 방지하기 위해 개인은 자신의 개인정보에 대해 주체적으로 정보를 소유하며 통제할 수 있는 방법이 필요하다.

블록체인은 4차 산업혁명의 발전과 함께 다양한 도메인(금융, 물류, 부동산)과 융합되어 이용되고 연구되고 있다.[1] 특히 탈중앙 신원 증명 시스템은 블록체인으로 자기 주권 신원(Self-Soverign Identity, SSI)를 구현한 시스템[2]으로 기존의 중앙 시스템이 사용자의 개인정보를 보관하고 관리하는 방식에서 벗어나 사용자가 자신의 개인정보를 전적으로 소유하고 관리한다.[3]

본 논문에서는 블록체인 기반의 탈중앙 신원 증명 시스템의 성능을 높이는 것을 목표로 한다. 특히 검증단계에서 검증기관이 사용자가 제출한 VP의 두 번의 서명을 검증하는 과정을 query transaction으로 확인하는 VP ID 등록 검증과 VP 검증 단계로 나눔으로써 성능을 높이는 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 하이퍼레저 패프릭과 탈중앙 신원 증명 시스템을 설명한다. 3장에서 하이퍼레저 패브릭 기반 간단검증 탈중앙 신원 증명 시스템을 제안하고 간단자격검증 단계를 소개하여 성능 향상됨을 보인다. 4장에서 결론을 맺는다.

II. 배경지식

2.1 하이퍼레저 패브릭(Hyperledger Fabric)

리눅스 재단에서 진행중인 오픈소스 기반 블록체인 프로젝트인 Hyperledger의 Fabric은 기존의 누구나 참여 가능한 비허가형 블록체인(비트코인, 이더리움)이 아닌, 시스템 관리자가 허

가한 참여자만 참여 가능한 허가형 블록체인 네트워크 구조를 가지고 있다.[4]

탈중앙화, 데이터의 무결성과 같은 블록체인의 장점을 활용하기 위해 다양한 블록체인 플랫폼이 연구·개발되고 있지만, 네트워크의 참여자와 트랜잭션 처리가 증가하며 처리속도에 대한 효율성 문제가 발생하고 있다. 이러한 문제점을 해결하기 위해 기존 블록체인의 장점을 가지며 필요한 참가자만 사용 가능한 허가형 블록체인인 Hyperledger Fabric이 개발되었다.

2.2 탈중앙 신원 증명

기존의 중앙기관 중심의 신원인증 방식이 아닌 정보 주체가 신원인증에 필요한 정보를 직접 소유하며 블록체인 플랫폼에 저장된 인증정보를 통해 사용자의 신원을 검증한다.[5] 탈중앙 신원 증명을 통해 발급받은 유일한 식별자를 통해 사용자를 구분하며 불필요한 추가 개인정보 노출의 위험없이 필수정보만을 제출하여 사용할 수 있다.

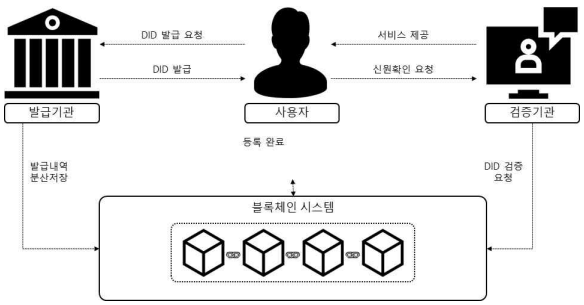

그림 1. DID 기반 신원인증 절차

III. 본론

하이퍼레저 패브릭 기반 간단검증 탈중앙 신원 증명 시스템 아키텍처는 그림1에서 보이듯이 발급기관, 검증기관, 사용자, 리졸버, 블록체인 시스템으로 구성된다. 블록체인 시스템은 전체 참여자 공개키와 발급기관이 VP ID를 등록하는 채널로 나뉜다. 발급기관와 검증기관 그리고 사용자는 리졸버를 통해 블록체인 시스템과 통신한다. 사용자는 발급기관를 통해 자격을 검증받고, 사용자가 검증기관의 서비스를 이용하고자 할 때 발급기관을 통해 받은 자격을 통해 이용할 수 있다. 시스템의 과정은 자격 발급 단계, 자격 검증 단계로 나뉜다.

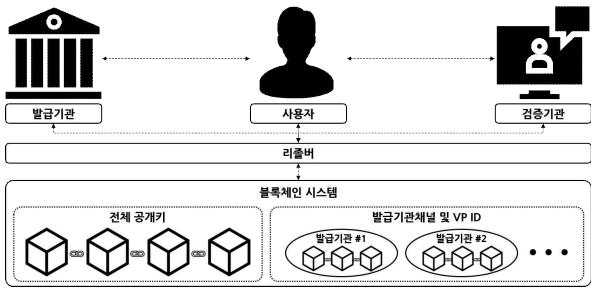

그림 2. 탈중앙 아이디 시스템 아키텍처

그림2는 자격발급단계의 전체 흐름을 보여준다. 자격발급단계 전에 모든 참가자는 자신의 공개키를 블록체인 시스템에 저장한다. 자격발급단계는 발급기관과 사용자 사이에서 일어난다. 사용자가 발급기관에게 자격 발급 요청을 하면 발급기관은 사용자의 자격을 자체적으로 검증하고 검증이 완료되면 VC를 사용자에게 전달하고 리졸버에게 블록체인 시스템에 VC ID 등록 요청을 한다. 리졸버는 발급기관의 해당 채널에 사용자의 VC ID를 등록한다.

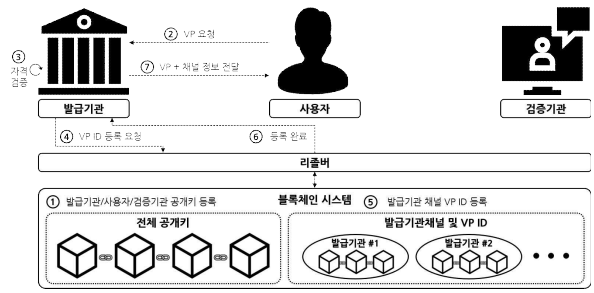

그림 3. 자격 발급 단계

그림3의 자격검증단계는 검증기관와 사용자 사이에서 발생한다. 제안된 검증 단계는 2단계로 나뉘며, 전체자격검증과 간단자격검증으로 구성된다. 전체자격검증은 기존 DID 검증 단계와 같이 VP를 사용자 서명과 발급기관 서명을 각각 검증한다. 간단자격검증은 검증기관이 리졸버에게 VP ID와 검증기관 채널을 리졸버에게 전달하고 해당 채널에 VC ID가 등록되어있는지 검증 요청한다. 리졸버는 해당 채널에 사용자 공개키가 있는지 확인하고 등록되어 있는 경우 발급자 결과와 발급자 공개키를 전달하고 등록되어 있지 않은 경우 검증 실패 결과를 전달한다. 검증기관은 VP의 발급자 서명을 검증

함으로써 사용자 VP의 자격 검증을 완료한다.

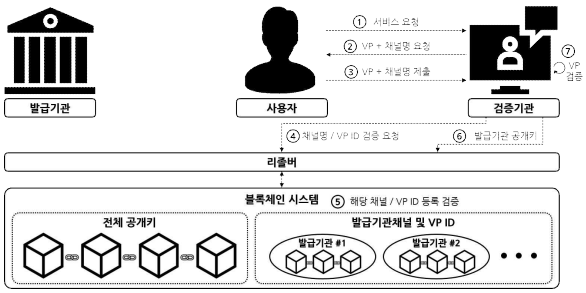

그림 4. 간단 자격 검증

제안한 간단검증단계는 사용자가 제출한 VP의 서명을 검증하기 전 VP의 등록 여부를 확인함으로써 불필요한 검증 과정을 생략할 수 있다. 하이퍼레저 패브릭 블록체인은 state db를 사용하여 가장 최신의 key/value 값을 query transaction으로 간단하게 확인가능하다. 보증(endorsment)-오더링(ordering)-검증(validation) 단계를 거치는 invoke-trasaction 과는 다르게 그림4와 같이 피어내에서 체인코드 시뮬레이션만을 통해 해당 값의 존재 여부만을 간단하게 확인가능하다. 등록 여부가 확인되면 발급기관의 공개키로 VP 서명을 검증한다. 기존의 검증단계가 ECDSA(Elliptic Curve Digital Signature Algorithm)을 두 번 계산하는 것에 반해 간단검증단계는 한 번의 query transation 호출과 ECDSA 한 번 계산하는 것으로 가능함을 보임으로 성능 개선이 가능함을 보였다.

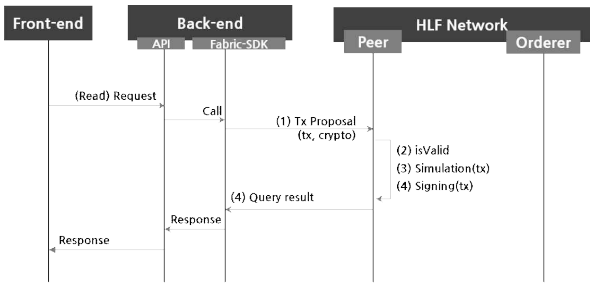

그림 5. query-transaction flow

IV. 결론

본 논문에서는 하이퍼레저 패브릭 블록체인을 기반 간단검증 탈중앙 신원 증명 시스템에 대해서 제안했다. 특히 검증단계에서 발급기관 서명만을 검증하는 간단검증단계를 제안했다. 간단검증단계는 query transaction을 통해 블록체인내에 블록을 생성하지 않고도 피어내 시뮬레이션만을 통해 간단하게 등록여부를 확인할 수 있으며 등록 여부가 확인 되었을 경우에만 VP 서명을 검증한다. 기존 VP의 두 번의 ECDSA 계산 서명검증 방식을 한 번의 query transaction 호출과 한 번의 ECDSA 계산 방식으로 가능함을 보였다. 향후 제안한 인증 방식에 대한 구현을 통해 기존 방식들과의 성능차이에 대해서 분석하고자 한다.

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2019-0-01343,융합보안핵심인재양성사업)

[참고문헌]

[1] Mohamed, N., & Al-Jaroodi, J. (2019, January). Applying blockchain in industry 4.0 applications. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0852-0858). IEEE.

[2] Zbinden, F., & Kondova, G. (2019). Economic development in Mexico and the role of blockchain. Advances in Economics and Business, 7(1), 55-64.

[3] EU Blockchain Observatory and Forum, “Blockchain and Digital Identity,” 2019. https://www.eublockchainforum.eu/reports

[4] Hyperledger Fabric: Read-the-Docs, https://hyperledger-fabric.readthedocs.io/en/latest,

[5] World Wide Web Consortium (W3C), “Decentralized Identifiers (DIDs) v1.0: Core Data Model and Syntaxes,” 2021. https://w3c.github.io/did-core/#did-document