한국정보전자통신기술학회논문지(jkiiect)'24-2, Vol.17 No.1
논문 24-17-01-47 http://dx.doi.org/10.17661/jkiiect.2024.17.1.47

하이퍼레저 패브릭 기반 탈중앙화 신원 인증 시스템 구축

고광만*

Construction of Hyperledger Fabric based Decentralized ID System

Kwang-Man Ko*

요 약 코로나 펜데믹을 거치면서 중앙정부, 지방정부, 민간사업자를 중심으로 블록체인 기반 탈중앙화 신원인증(Decentralized ID) 기술 활용 및 고도화 연구가 다양한 분야에서 활발하게 진행되고 있다. 본 논문에서는 기존 중앙 서버 기반 신원인증을 탈중앙화 기반으로 변경하기 위해 하이퍼레저 패브릭 기반으로 개발한 결과를 소개한다. 이러한 개발 결과는 상용화 목적의 신원인증 시스템에 보안성, 투명성을 강화하여 사용자 ID 발급, 조회, 폐기에 대해 안정적인 서비스를 제공할 수 있다. 또한, 탈중앙화된 신원인증 시스템은 DID 생성 262,000 rps, DID 조회 1,850 rps 성능과 DID VP 생성 200 rps, DID VP 조회 220 rps 이하의 성능 결과를 공인 인증을 통해 검증하였다.

Abstract Through the coronavirus pandemic, research on the use and advancement of blockchain-based decentralized identity authentication (Decentralized ID) technology is being actively conducted in various fields, centered on the central government, local governments, and private businesses. In this paper, we introduce the results of development based on Hyperledger Fabric to change the existing central server-based identity authentication to a decentralized one. These development results can strengthen the security and transparency of identity authentication systems for commercial purposes and provide stable services for user ID issuance, inquiry, and disposal. In addition, the decentralized identity authentication system verified performance results of DID creation of 262,000 rps and DID inquiry of 1,850 rps, DID VP creation of 200 rps, and DID VP inquiry of 220 rps or less through public authentication.

Key Words : Blockchain, Decentralized ID(DID), Hyperledger Fabric, Consensus Algorithm

Ⅰ. 서 론

블록체인은 P2P 기반 분산원장 기술을 활용하여 공인된 중개자 없이도 무결성 및 신뢰성을 보장하는 기술로서 데이터를 중앙 서버가 아닌 모든 참여자들이 동등한 위치에서 관리할 수 있기 때문에 데이터를 투명하고 신뢰성 있게 관리할 수 있다[1]. 또한, 한번 저장된 데이터는 절대로 변경이 불가능하기 때문에 저장된 데이터의 무결성을 보장할 수 있다. 이러한 블록체인 특성으로 인해서 이력 관리 플랫폼 등에서 주로 사용되고 있으며, 최근에는 기계학습 및 인공지능 분야에도 학습 데이터와 모델의 무결성 보장을 위해서 응용되고 있다.

전통적 방식에서는 사용자의 요구에 대해 3-Tier (클라이언트-AP서버-데이터베이스) 구조를 유지하면서 보안성 강화를 중점을 두었지만, 최근에는 블록체인 개념을 적용하여 데이터베이스의 일부 데이터를 블록체인에 저장하거나 일부 데이터의 해시값을 블록체인에 등록하는 방식으로 활용하고 있다[2].

블록체인이 갖는 익명성, 투명성, 무결성을 보장하

This research was supported by Sangji University Research Fund, 2021"). This work was partially supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2022-00207391, Development of Hashgraph-based Blockchain Enhancement Scheme and Implementation of Testbed for Autonomous Driving)
*Dept. of Computer Engineering, Sangji University Korea(kkman@sangji.ac.kr)
Received January 03, 2024 Revised January 10, 2024 Accepted February 04, 2024

는 기술 특성으로 인해 개인 신원 보장, 이력 관리, 공증 관련 문서의 무결성 및 보안성 제고를 위한 원장 공유 및 위·변조 방지 분야에서 활발하게 적용되고 있다[3]. 개인정보 사용 및 제공의 주체가 기업에서 개인으로 변화하고 있는 상황에서 탈중앙화 신원 인증(Decentralized ID, DID) 기술[4]을 적용하면 개인이 특정 기관과 상호작용할 때 신원 주체가 그 흐름을 통제할 수 있다. 따라서, 탈중앙화 트렌드와 맞물려 개인 신원도 탈중앙화 방식으로 관리되는 DID 도입과 활용이 더욱더 활성화될 전망이다. DID는 독자적인 서비스가 가능하지만 블록체인기반 온라인 투표, 여론조사, 모바일 신원증 등 다양한 서비스와 연계해서 활용이 가능하다. 현재 DID는 표준화(W3C DID)가 진행중이며 국내에서도 3개 이상의 얼라이언스가 서비스를 진행하고 있다[5].

본 논문의 구성은 2장에서 블록체인 기반 탈중앙화 신원 인증 시스템 개발의 기반 연구와 연구의 기여 내용을 소개한다. 3장에서는 본 논문에서 제안하고 시도하는 하이퍼레저 패브릭 기반 탈중앙와 신원 인증 시스템에 대한 개발 내용과 결과를 제시한다. 마지막으로 4장에서는 본 연구의 결론과 본 연구가 갖는 한계점 및 향후 연구에 대해 기술한다.

II. 연구배경 및 관련연구

2.1 탈중앙화 신원 인증(DID)

신원 정보 저장과 관리는 ID/PW 기반의 중앙집중형으로 출발하여 PKI 기반의 공인인증서와 최근에는 블록체인 기반 DID 형태로 발전해 가고 있다. DID 기술은 공개키를 중앙 집중 관리 대신 블록체인 플랫폼에 분산 저장시켜 자기 주권 신원(Self-Sovereign ID, SSI) 개념으로 확대하여 서비스 제공하고 있다. DID는 아직 표준화가 제정되지 않은 상황이며 DID를 통해 구현하고자 하는 서비스 목적, 신원정보 저장 위치, 구현하고자 하는 플랫폼 유형에 따라 다양한 서비스가 등장하고 있다[6].

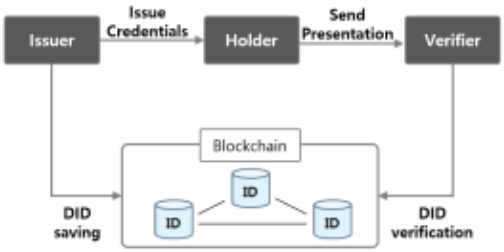


그림 1. 블록체인 탈중앙화 신원 인증 시스템
Fig. 1. Blockchain based DID System

사용자(holder)는 SDK를 통해 신원 정보를 DID 발행기관(issuer)에게 등록 요청(claim)을 생성하거나 검증기관(verifier)에게 등록 요청 정보를 제시(presentation)하여 조회를 요청한다. 발행기관에서는 등록 요청을 검증한 후 발행기관의 개인키와 공개키를 생성한다. 발행기관 개인키는 인증 내용과 결합하여 사용자에게 정상적인 인증서(credential)를 반환한다. 발행기관 공개키는 DID 문서에 추가하여 분산저장한 후 검증 과정에서 활용한다. 정상적인 인증서는 사용자의 SDK에서 사용자의 개인키와 공개키를 생성해서 개인키는 인증서와 결합하여 검증에 이용하며, 공개키는 검증을 위해 DID에 추가된다. 검증기관(verifier)은 개인 서비스 신원 증명 필요시에 사용자와 발행기관의 공개키로 검증한다. 블록체인 DID는 발행기관과 사용자의 공개키를 분산저장 및 관리한다. 개인의 신원 정보는 설계에 따라 개인 스마트폰에 보관, 인증기관에서 보관, 블록체인에 등록하는 방법으로 구분된다. 이 과정에서 신원 정보 확인에 필요한 개인키는 반드시 개인이 보관하고 공개키는 블록체인 DID에 등록되어야 한다. DID 수행 절차는 PKI 기반 공인 인증서 수행 절차와 비슷하지만 공개키를 중앙 서버에서 관리하는 대신에 블록체인에 분산 저장시켜서 DID 개념을 자기 주권 신원 개념으로 확대하여 서비스를 진행한다.

표 1. 탈중앙화 신원 인증 시스템 비교
Table 1. Comparison of Decentalized ID

	Sovrin[8]	uPort[9]	SecureKey[10]
Foundation	SovrinFoundation	Consensys	SecureKeyTechnologies
Goal	DID Eco-system	DID on Mobile System	DID Eco-system
Character	Anonymous DID	Public Key, IPFS	Chtagories DID
Info. location	Mobile (ID) Blockchain (public key)	Mobile (ID) Blockchain (Hash value)	Issuer (ID) Blockchain (public key)
Network	Permitted ID validation value	Node consensus	Validation ID value generation
DID Type	Private	Public	Consortium
Blockchain	SovrinLedger (Sovrin source + HyperledgerIndy)	Ethereum	HyperledgerFabric
DID service	ID exchange platform	ID creation/validation	Digital asset management
Use case	immigrated labor ID	ZugID - Voting, Citized ID (Swiss)	Canada : Cyber renewal

2.2 탈중앙화 신원 인증 사례

하이퍼레저 패브릭은 리눅스 재단에서 개발한 프라이빗 블록체인 플랫폼으로서 5개의 프레임워크(Fabric, Sawtooth, IROHA, INDY, Burrow)와 5개의 도구(Caliper, Cello, Composer, Explorer, Quilt)로 구성되어 있으며 비즈니스 목적에 적합한 블록체인 플랫폼을 구축하는 것을 목표로 하고 있다. 특히, MSP 인증관리 시스템 (참여/접근 제한)과 Channel · Private Data Collection 개념을 도입하여 블록체인 참여자들 간의 프라이버시 보호를 위한 기밀성을 보호하는 특징을 가지고 있다[7].

Sovrin[7]은 ID, PW 체계를 서비스별로 구축하여 어디에서든지 접근 및 서비스가 가능하도록 하는 보안성, 익명성의 특징을 가지고 있다. UPort[8]는 모바일 기기에서 사용자의 신원을 생성하고 관리할 수 있는 오픈 신원 인증 시스템으로서 이더리움 기반으로 개발되었다. SecureKey[9]는 사용자의 패스워드 관리 목적으로 개발된 신원 인증 플랫폼으로서 디지털 자산 관리 분야에서 적극적으로 활용되고 있다.

본 연구에서 개발한 하이퍼레저 패브릭 기반 신원 인증 시스템은 첫째, 기존 중앙 집중형 서버 방식으로 운영되고 있는 사용자 ID 생성, 조회, 폐기 동작과 API를 통해 연동 및 운영되고 있다. 따라서, 중앙 집중형 서버의 변경없이 쉽게 연동이 가능하다. 둘째, 탈중앙화 및 보안성을 인정받고 있는 하이퍼레저 패브릭 기반으로 개발하였다. 블록체인에서 합의된 트랜잭션을 분산 저장하는 성질로 인해 합의에 참여한 노드에 대해 51% 이상의 보안 공격(위협)이 불가능하므로 보안 안정성을 유지하고 있다. 또한, 합의 과정에서 불필요한 내용을 제거하고 Kafka 합의 알고리즘을 경량화하여 읽기, 쓰기 TPS 성능이 기존 하이퍼레저 패브릭보다 우수함을 확인할 수 있다.

Ⅲ. 하이퍼레저 패브릭 기반 탈중앙화 신원 인증 시스템

3.1 전체 시스템 구성

본 논문에서는 중앙 서버 기반 사용자 신원 인증(ID Verification Server)을 하이퍼레저 패브릭 기반으로 탈중앙화된 신원 인증을 위해 그림 2와 같이 개인키를 소유한 사용자가 신원 인증 웹서버 등록, 조회, 폐기를 요청한다. 이 과정은 W3C DID 표준에 따라 신원 인증 요청 및 결과값이 전송된다. 신원 인증 서버에서는 요청한 사용자의 개인키를 이용하여 사용자를 웹서버에서 조회한 후 정상적으로 조회되는 사용자에 대해 킷값과 개인정보를 PIKEY 해쉬값으로 생성하여 하이퍼레저 기반 DID 시스템으로 전송한다.

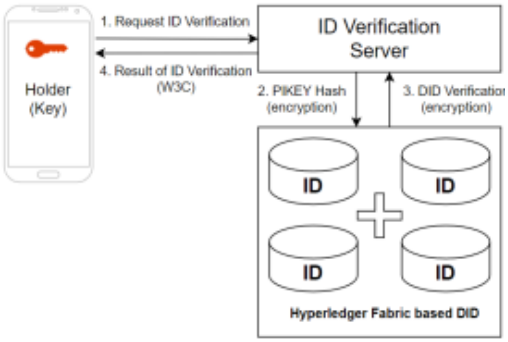


그림 2. 하이퍼레저 패브릭 기반 DID 시스템
Fig. 2. Hyperledger Fabric based based DID System

3.2 사용자 ID 생성(등록)

사용자는 DID에 최초 등록을 위해 그림 3과 같은 과정으로 회원 개인정보와 DID 발급에 필요한 내용을 ID 검증 서버에 제공한다(claim 생성). ID 검증 서버는 DID 인증에 적합한 정보에 대한 확인 절차를 수행하면 실질적인 탈중앙화 분산 인증은 그림 3의 단계 5에서 VC(사용자 DID+PIKEY+해시값)를 생성하여 DID를 등록(공개키, DID 문서)하며 개인키는 사용자가 소유한다.

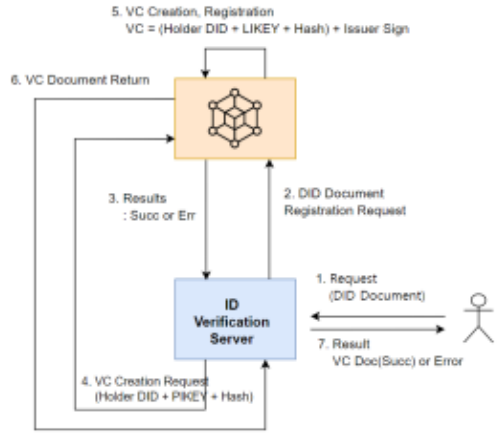


그림 3. DID 시스템 사용자 ID 생성 및 등록
Fig. 3. Holder ID Creation and Registration on DID System

DID 요청에 대해서 그림 4와 같이 DID 문서 생성, 발행기관 서명, 개인키, 공개키를 확인할 수 있으며 정상적인 DID 생성 및 등록의 결과(StatusCode: 200)를 확인할 수 있다.

그림 4. 사용자 ID 생성 및 등록 결과
Fig. 4. Result of Holder ID Creation and Registration

3.3 사용자 ID 조회(검증)

사용자 조회는 DID 시스템에 등록 여부를 확인하기 위해 VP 생성(그림 5, 좌)과 생성된 VP 검증(그림 5, 우) 과정을 수행해서 생성(등록)된 DID 문서의 유효성 검사를 수행한다. 사용자 조회시에 핵심 정보가 되는 VP는 "VC+사용자 개인키"로 구성되어 있다. 특히, 단계 4에서 VP와 VC에 대한 검증을 위해 사용자와 이슈어에 대한 서명을 확인하는 중요한 절차를 수행한다. 생성된 VP는 암호화된 ID 형태로 DID 상에서 검증(단계8-단계 12) 과정을 거친다.

3.4 성능평가

DID 생성(등록), DID 조회(검증), VP 생성, VP 조회에 대한 성능평가는 온-프레미스 환경 실험하고 평가하기 Intel Core i5-13500 (2.5GHz), 우분투 운영체제, 하이퍼레저 페브릭(HyperLedgerFabric estNe)에서 수행하였다. DID 생성(등록), DID 조회(검증), VP 생성, VP 조회에 대한 성능평가 결과는 표 2와 같다. 사용자 신원을 중앙 서버에서 생성, 조회, 폐기하는 중앙 집중형 시스템을 하이퍼레저 패브릭 기반으로 DID 기술을 개발하여 현장에서 활용되고 있는 개발 내용을 소개한다. 실제로 개발된 내용은 상용화 목적의 신분 인증 시스템에 보안성, 투명성 강화 목적으로 적용하여 사용자 ID 발급, 조회, 폐기에 대한 안정적인 서비스를 제공하고 있으며, D 생성 262,000 rps, DID 조회 1,850

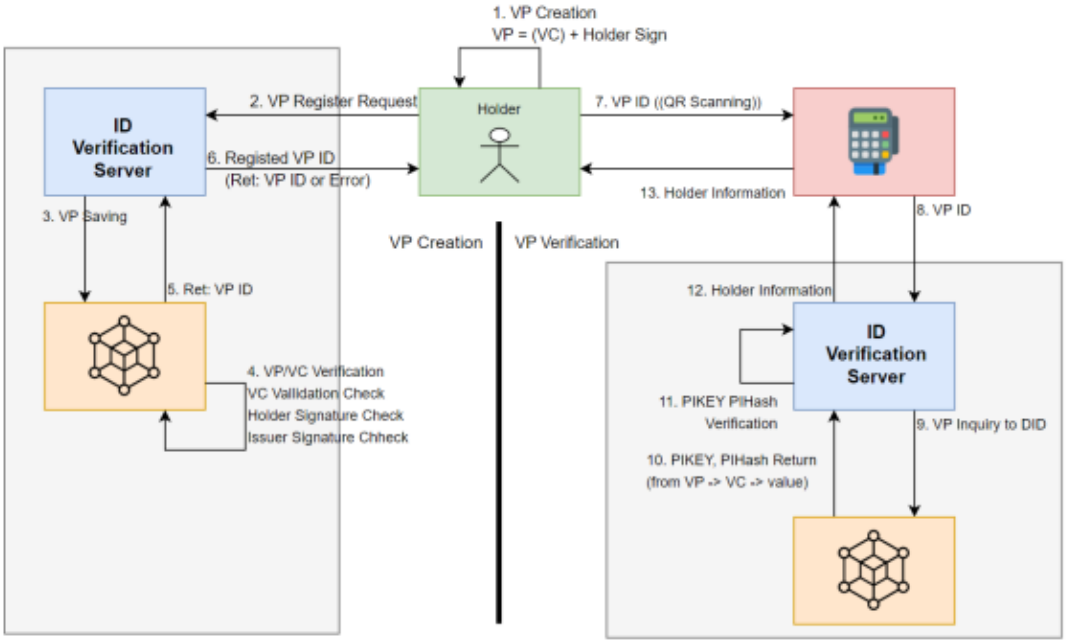


그림 5. DID 상에서 사용자 ID 조회 및 검증 결과
Fig. 5. Result of Holder ID Inquiry and Verification on DID

rps, VP 생성 200 rps, VP 조회 220 rps 이하의 성능 결과를 공인 인증을 통해 검증하였다.

표 2. 성능 평가 결과
Table 2. Performance Evaluation Results

Performance Evaluation Index	Results(rps)
DID Document Creation	262,000
DID Verification	1,850
VP Creation	200
VP Verification	220

이 실험 결과는 생성 및 조회가 성공한 경우에 한정하여 공인기관 평가를 마친 결과이다. 본 연구의 실험은 온프레미스 환경에서 실행한 결과로서 DID 문서 생성 및 조회, VP 생성 및 조회의 기능에 초점을 맞추고 있으며, 향후에 클라우드의 다수의 접속자 환경에서 추가 실험을 진행할 예정이다.

Ⅳ. 결론 및 향후 과제

DID 기술은 공개키를 중앙 집중 관리 대신 블록체인 플랫폼에 분산 저장시켜 자기 주권 신원(Self-Sovereign ID, SSI) 개념으로 확대하여 서비스 제공하고 있다. 논문에서는 사용자 신원을 중앙 서버에서 생성, 조회, 폐기하는 중앙 집중형 시스템을 하이퍼레저 패브릭 DID 개발 내용과 결과(기능 및 성능) 소개하였다. 블록체인 신원인증 기술은 온라인 투표, 여론조사, 기부 시스템 영역에서 용자의 신원을 확인하고 중복참여을 방지하기 위해 활용되고 있다. 본 연구는 기존 중앙 서버 중심에서 이용되는 신원 인증을 탈중앙화 방식으로 전환을 목적으로 하는 연구 개발에 활용될 수 있다.

향후, 클라우드 환경에서 5000명 이상의 동시 접속자에 대해 합의 알고리즘을 개선하여 서비스 반응 속도의 성능을 지속적으로 개선할 예정이다.

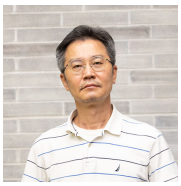
그림 6. DID 상에서 사용자 ID 조회 및 검증 결과
Fig. 6. Result of Holder ID Inquiry and Verification on DID

REFERENCES

[1] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System (August 21, 2008). https://ssrn.com/abstract=3440802
[2] Konstantions Christidis, Michaek Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE ACCESS, Volume 4, 2016.
[3] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," IEEE Internet Things J., vol. 6, no. 5, pp. 8114-154, 2019.
[4] MORTEZA ALIZADEH, KARL ANDERSSON, OLOV SCHELÉN, "Comparative Analysis of Decentralized Identity Approaches," IEEE Access, Vol. 10, Page(s): 92273-92283. 2022.
[5] Honggi Cha et. al, "International Standardization on Blocjchain," Journal of ETRI Trend Analysis, Vol. 34, No. 2, 2019
[6] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," ACM Computing Surveys, Volume 54, Issue 8, 2021.
[7] Hyperledger Fabric White Paper: https://www.hyperledger.org/learn/whitepapers
[8] Sovrin : https://sovrin.org/
[9] uPort : https://www.uport.me/
[10] SecureKey : https://securekeygroup.com/

저자약력

고 광 만 (Kwang-Man Ko)



- 1991년 2월 : 원광대학교 컴퓨터공학과(공학사)
- 1993년 2월 : 동국대학교 컴퓨터공학과(공학석사)
- 1998년 2월 : 동국대학교 컴퓨터공학과(공학박사)
- 1998년 3월~2001년 8월 : 광주여자대학교 컴퓨터과학과 교수
- 2001년 9월~현재 : 상지대학교 컴퓨터공학과 교수

〈관심분야〉 컴파일러, 블록체인, 소프트웨어 보안