블록체인 기반 분산신원증명의 이해와 서비스 적용 사례

권준우*, 서승현**, 이강효***, 박소현****
*한양대학교 전자공학과
**한양대학교 ERICA 전자공학부
***한국인터넷진흥원
****한국인터넷진흥원
kjw9628@hanyang.ac.kr, seosh77@hanyang.ac.kr, kanghyo.lee@kisa.or.kr,
sohyeon@kisa.or.kr

Understanding and Applications of Blockchain-based Decentralized Identitiy

Jun-Woo Kwon*, Seung-Hyun Seo**, Kang-Hyo Lee*
*Dept. of Electrical Engineering, Han-Yang University
**Dept. of Electrical Engineering, Han-Yang University ERICA Campus
***Korea Internet & Security Agency

요 약

최근 사회는 디지털기술을 기반으로 비대면전환이 빠르게 이루어지고 있다. 이에 디지털 신분증과 디지털 신원인증에 대한 관심이 증가하고 있다. 기존 오프라인에서 사용되고 있는 플라스틱 신분증은 분실 및 위·변조의 위험성이 존재한. 또한 현재 온라인에서 널리 사용되고 잇는 신원인증 모델들을 데이터의 주권이 사용자가 아닌 서비스 제공자에게 있다는 문제점이 있다. 위와 같은 문제들을 해결하고 사용자의 신원정보를 효과적으로 관리하기 위해 분산신원증명의 필요성이 제기되었다. 본 논문에서는 분산신원증명의 구조와 서비스 적용 사례에 대해 살펴본다.

1. 서론

최근 빅블러(Big-blur)현상과 COVID-19의 확산으로 인해 디지털기술을 활용하는 서비스가 확대되고 있다. 이에 따라, 비대면 서비스를 기반으로 한 모바일과 언택트(Untact) 중심의 소비문화가 빠르게 확산되고 있다. 이러한 비대면 시대에서 신원인증은 매우 중요한 이슈이다. (그림 1)은 신원인증 모델의 변화 과정이다.

(그림 1) 신원 모델 변화 [1]

현재 널리 사용되고 있는 신원인증 모델인 개별 신원 모델(Siloed-Identities)과 연합 신원 모델(Federated - Identities)은 기업이나 기관에서 사용자의 신원 데이터를 관리하는 모델이다. 이러한 신원인증 모델들은 각 서비스 제공기관이 개별적으로 사용자의 개인정보를 관리하기 때문에 각 서비스 제공기관이 해킹대상이 된다면 사용자의 개인정보가 해킹될 수 있다는 문제점이 존재한다. 이에 사용자 본인이 직접 본인의 신원 데이터를 관리하는 방식인 자기 주권 신원 모델의 필요성이 증가하였으며, 이에 신원 모델은 기존의 개별 신원 모델과 연합 신원 모델에서 자기 주권 신원 모델(Self-sovereign-Identities)로 점차 변화하는 추세다.

분산신원증명(Decentralized Identity, DID)은 자기 주권 신원 모델과 블록체인을 기반으로 개인정보 관리와 인증을 기본적으로 개선하는 모델로, 제3의 인증기관 없이 사용자가 신원정보의 노출 범위, 사용 목적에 따라 자신의 신원정보에 주권을 행사할 수 있게 해준다. 최근 분산신원증명 기술을 이용하여 본인의 신원을 증명하고 신원 데이터를 관리할 수 있게 해주는 서비스 플랫폼들이 증가하고 있다.

본고의 2장에서는 분산신원증명을 3장에서는 분산신원증명 서비스 적용 및 연구 사례를 4장에서는 결론을 기술한다.

2. 분산신원증명(Decentralized Identity, DID)

분산신원증명은 온라인상에서 블록체인을 기반으로 사용자가 스스로 신원 등에 대한 증명관리, 신원정보 제출 범위 및 제출대상 등을 통제·수행할 수 있도록 하는 신원관리 체계이다. 전통적인 서버-클라이언트 신원관리 모델 체계와는 달리 사용자가 자신의 신원정보에 주권을 행사할 수 있으며, 분산원장의 암호학적 특성을 기반으로 한 신뢰된 ID저장소를 이용하여, 제3기관의 통제 없이 분산원장에 참여 가능한 누구나 신원정보의 위·변조 여부 검증이 가능하다.

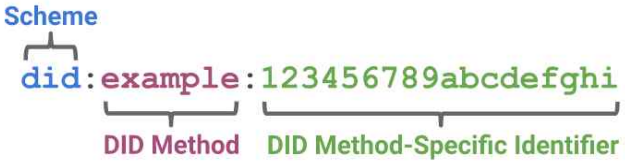
2.1 분산신원증명 특징

- 지속성: 서비스 제공자에 의해 신원정보가 관리되지 않으므로, 외부적 환경의 변화와 관계없이 사용자가 자신의 신원정보를 지속적으로 사용가능하다.
- 휴대성: 신원증명이 필요한 경우 언제든 사용자 스스로 스마트폰이나 ID카드 등으로 신원정보를 선택 후 제공이 가능하다.
- 개인정보 보호: 사용자가 스스로 신원정보를 관리하므로, 서비스 제공자는 서비스에 필요한 정보 이외의 사용자의 개인정보는 확인이 불가능하다.
- 피어(peer)기반: 신원정보의 발행 검증은 특정기관에 종속적이지 않고, 피어기반으로 독립적으로 운영하며, 누구나 필요한 신원정보를 생성하고 이용가능하다.

2.2 분산신원증명 구성요소

분산신원증명은 Key & Value 형태로 DID Identifiers와 DID document로 구성된다. 사용자는 DID Identifiers와 DID document를 함께 생성하여 DID document는 분산원장에 저장한다. 보통 분산원장으로 블록체인을 사용하며, DID Identifiers를 통하여 분산원장에 저장된 DID document를 조회할 수 있다.

- DID Identifiers: DID Identifiers는 URI 형식으로 DID document가 저장된 위치를 나타낼 수 있는 주소이다. DID Identifiers는 DID Scheme, DID Method, DID Method-Specific Identifier 3가지로 구성되어 있다. DID Scheme은 URI가 어떤 프로토콜을 통해 자원에 접근하는지를 나타낸다. 예를 들어, DID Scheme에 did가 들어간다면 did scheme이 정의한 자원 접근 방식에 따라 자원을 찾아가게 된다. DID Method는 DID document가 어떤 저장소에 저장되어 있는지를 나타낸다. 예를 들어, DID Method에 btcr이 들어간다면 비트코인 블록체인에 접근하여 DID document를 검색할 수 있다. DID Method-Specific Identifier는 DID Method가 가리키는 DID document가 저장된 정확한 위치를 검색하기 위한 주소이다.



(그림 2) DID Identifiers [3]

- DID document: DID document에는 DID의 소유권을 증명할 수 있는 인증 수단이 포함되어 있다. 검증기관은 Challenge&Response 형식으로 DID document에 포함된 공개키를 이용하여 사용자의 Response를 검증한다. DID document에는 id, publicKey, authentication, sercive 등의 구성요소들이 있다.

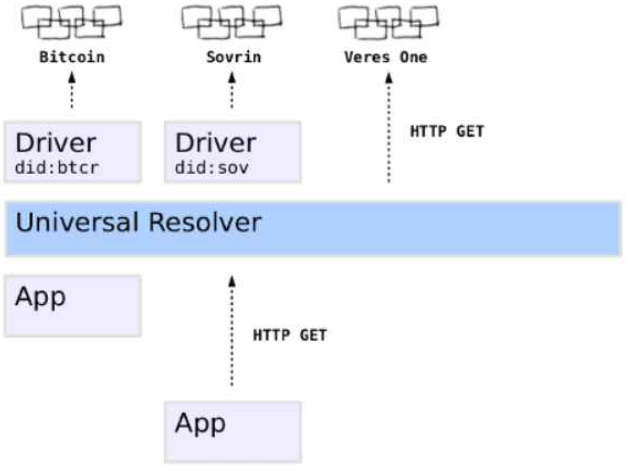
<표 1> DID document 주요 항목

구성요소	내용
id	id 항목에는 id를 통해 식별되는 객체의 DID가 들어간다. 해당 DID document가 사용자를 식별하기 위한 DID document라면 사용자의 DID가 들어가게 된다.
publicKey	publicKey 항목에는 DID소유권 인증에 필요한 다양한 종류의 데이터가 들어간다.
authentication	authentication 항목은 해당 DID document가 제공하는 소유권 인증 방식을 나타낸다.
service	serviceEndpoint라는 세부 항목을 이용해 DID를 활용한 다양한 서비스를 개발할 수 있음

- DID resolver: DID resolver는 DID Identifier를 입력값으로 받아 그에 해당하는 DID document를

출력값으로 반환하는 역할을 한다. 이러한 과정을 DID resolution이라고 하며, DID method에 따라 resolution 절차를 달리하게 된다. 이는 블록체인 플랫폼마다 DID document를 생성, 조회 갱신, 삭제하는 방법이 다르기 때문이다.

- Universal Resolver: 현재의 분산신원증명 프로젝트들은 각각 개별적인 생태계를 구축하고 있다. 따라서 분산신원증명 확산 관점에서 DID 상호이용이 대두되고 있다. Universal Resolver는 다양한 DID Method의 상호 연동을 지원하고, 서로 다른 블록체인 내의 DID document를 찾을 수 있도록 해준다.



(그림 3) Universal Resolver 구조 [4]

3. 분산신원증명 서비스 적용 및 연구 사례

분산신원증명은 블록체인을 이용하여 데이터의 무결성을 보장하고, 데이터의 주권이 사용자에게 있다는 이점을 가지고 있다. 따라서 현재 국내외에서 분산신원증명을 활용한 서비스 적용 사례들이 증가하고 있다. 여러 기업들이 분산신원증명을 실제 신원증명 및 증명서 발급 서비스에 접목하고 있다., 나아가 건축물, IoT디바이스, 차량 등 사물에도 분산신원증명을 적용시키려는 움직임이 활발하다.

SKT는 '시티랩스 컨소시엄'의 '블록체인 기반 위험구조물 안전진단 플랫폼' 사업에 자사의 DID 서비스인 'initial'을 지원한다. 이는 국내 최초의 블록체인 기술과 IoT 기술을 융합한 DID 서비스이다. 건축물의 고유식별자는 LoRa(Long Range, 장거리 데이터 전송이 가능한 무선 통신 방식)기반 IoT센서로 확인할 수 있다. 또한 기울기, 분열 등의 데이터를 블록체인에 저장하여 위험구조물 안전진단을 실시할 예정이다. 이를 통해 기존 건축물 안전진단 수행에 소요되었던 시간을 단축하고, 위·변조의 위험성을 없애 신뢰도 문제를 해결할 수 있다. [5]

ReapCahin은 기존 DID 기술을 Reap SDK의 독자적인 암호화 기술을 통해 각 사물에 적용하여 새로운 사물 인증체계인 PID(Private ID)를 구현하고 데이터의 보안성을 확보하고 있다. 또한 2020년 6월 쿠노소프트와 협약하여 블록체인 기반 IoT플랫폼 서비스 생태계 확보 및 사업화를 진행할 예정이다.

세종시와 '라온시큐어'는 '자율주행 상용화를 위한 블록체인 기반 자율주행자동차 신뢰 플랫폼 구축 사업'을 진행중이다. 본 사업은 자율주행차의 안전한 운행을 위해 자율주행차량을 비롯해 자율주행 환경을 구성하는 사물에 DID를 부여하고, 차량-차량, 차량-관제센터, 차량간 서비스 간 송수신되는 정보의 보안을 강화할 예정이다. DID를 활용한 자율주행차 인증을 통해 장애 없는 안정적인 서비스 운영은 물론 인증서 발급에 따른 제반 비용도 절감할 것으로 기대하고 있다. [6]

질병관리청과 '블록체인랩스'는 블록체인 기반 분산신원증명 기술을 활용하여 사용자의 개인정보를 저장하고, QR코드를 이용해 스캔하는 방식의 백신 여권 앱 'COOV'를 개발하였다. [7]

행정안전부와 '라온시큐어'는 모바일 신분증을 통해 온·오프라인에서 디지털 신원증명 기능을 제공한다. 신분증 소유자는 자신의 신분증(신원정보)를 본인 스마트폰에 발급받고, 본인의 판단에 따라 신원정보 제공 여부를 결정한다. 또한 신분증 사용 이력은 본인만 확인할 수 있고, 중앙서버에는 저장되지 않는다. [8]

'드림시큐리티', '삼성SDS', '시스젠'은 '블록체인 기반 비대면 국민연금 수급권 확인 시스템 구축 시범사업'을 통해 분산신원증명을 기반으로 한 국민연금 수급권 확인서류 제출 시 종이 서류 없이 편리하게 제출할 수 있는 서비스를 제공 예정이다. [9]

시큐어키는 분산신원증명 플랫폼을 제공하는 캐나다 기업이다. 시큐어키는 캐나다 주요 은행, 공공기관 등과 함께 분산신원증명 서비스 베리파이드미(Verified.Me)를 활용한 사용자 간편인증 방안을 준비 중이다. [10]]

표2는 현재 분산신원증명을 활용하여 진행중인 사업이나 서비스들에 대해 비교하고 있다. 표에서 볼 수 있듯이 분산신원증명은 사용자 신원인증, 신분증, 건축물 등 다양한 분야에서 활용되고 있다. 행

정안전부, 질병관리청 등 국가기관에서는 여러 기업들과 협력하여 분산신원증명을 사람에게 적용하여 관련 증명서를 발급받을 수 있는 서비스를 진행하고 있다. 나아가 분산신원증명은 사용자의 신원증명에 국한되는 것이 아니라, IoT기기, 건축물 등 사물에 분산식별자를 부여하여 활용하는 서비스와 연구가 진행되고 있다. 최근 사례들로 살펴볼 때, 분산신원증명은 여러 자율주행차량, IoT기기 등에 확장되어 사용될 것으로 보인다.

<표 2> 분산신원증명 서비스 적용 및 연구 사례

	참여기업 및 기관	적용대상
블록체인 기반 위험 구조물 안전진단 플랫폼	시티랩스컨소시엄 SKT	건축물
PID(Private ID)	ReapChain	IoT디바이스
자율주행 상용화를 위한 블록체인 기반 자율주행자동차 신뢰 플랫폼 구축	세종시 라온시큐어	자율주행차량
COOV	질병관리청 블록체인랩스	예방접종증명서
모바일 공무원증	행정안전부 라온시큐어	공무원증
블록체인 기반 비대면 국민연금 수급권 확인 시스템 구축	드림시큐리티 삼성SDS, 시스젠	국민연금 수급권
시큐어키 (securekey)	캐나다 공공기관 캐나다 주요은행 시큐어키	사용자 간편인증

4. 결론

앞서 분산신원증명 기술의 기본적인 구성요소와 서비스 적용 및 연구 사례에 대해 살펴보았다. 분산신원증명은 자기주권신원(Self-Sorvereign Identity, SSI)과 디지털 신원인증에 있어 꼭 필요한 기술이다. 또한 분산신원증명 기술은 신원 데이터의 주권을 서비스 제공자에서 사용자 자신에게로 가져오고, 디지털 신분증과 접목하여 기존 오프라인 신분증의 분실 및 위·변조 문제를 해결하는 역할을 하고 있다. 위와 같은 이점 때문에 현재 통신사, 금융사 등 여러 기업들이 연합체를 구성하여 분산신원증명을 활용한 서비스를 진행하고 있으며, 정부기관 역시 분산신원증명을 모바일 공무원증, 백신 접종증명, 모바일 운전면허증 등에 활용하고 있다. 타 플랫폼간의 상호연동 문제와 표준화 이슈 등을 해결한다면 분산신원증명 서비스의 빠른 확산에 도움이 될 것이다.

분산신원증명은 현재까지 사용자의 신원증명에 초점이 맞추어져 있었다. 하지만 그 활용도가 높아 분산신원인증을 여러 사물에 적용한 서비스들이 개발될 것이라고 기대된다.

Acknowledgement

“이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국인터넷진흥원의 지원을 받아 수행된 연구임(KISA-2021-145)”

참고문헌

[1] 금융보안원, “전자금융과 금융보안” 제16호, 2019

[2] Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2017

[3] W3C, “Decentralized Identifiers (DIDs)” v1.0, 2021

[4] Markus Sabadello, https://danubetch.com/ , 2019

[5] SKT telecom PR실, SKT ‘이니셜’, 사물 DID 시대 열었다! (https://news.sktelecom.com/132449), 2021

[6] 라온시큐어, 자율주행자동차 플랫폼구축, https://www.raonsecure.com/ko/solution/omnioneenterprise, 2020

[7] 질병관리청, 코로나19전자예방접종증명 COOV소개(https://ncv.kdca.go.kr/menu.es?mid=a12501000000), 2021

[8] 행정안전부 디지털안전정책과, 모바일 신분증 시대를 열기 위해 모바일 공무원증 우선 도입 (https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=82228), 2021

[9] 과학기술정보통신부, 보도자료, 우리 생활에 블록체인을 접목한다!, 2021

[10] 시큐어키, http://securekey.com , 2020