분산ID 기술 및 정책 동향

오석환, 김경백*

*전남대학교 정보보안협동과정

Trends of Decentralized Identifier Technology and Policy

Seok-Hwan Oh, Kyungbaek Kim*

*Interdisciplinary Program of Informaton Security, Chonnam National University

요 약

인터넷 기술이 발전함에 따라 공공, 금융 등 다양한 영역에서 온라인상으로 개인의 신원을 증명해야 할 상황이 증가하고 있다. 최근, 기존 중앙집중형 신원확인 체계에서 발생할 수 있는 개인정보 유출사고의 문제점을 해결하고, 사용자의 자기주권신원증명 모델의 확립을 위한 분산 신원증명 기술이 연구되고 있다. 이 논문에서는 블록체인 기반의 탈중앙화된 신원증명 서비스를 제공하는 분산ID의 기술과 정책 동향에 대하여 살펴본다.

I. 서론

2020년 5월 전자서명법 개정안이 국회 본회의를 통과하면서 공인인증서의 독점적 지위가 폐지되었다. 이로 인해 새로운 전자서명 기술이 등장하고 있으며, 특히, 온라인 환경에서 사용자가 스스로 신원정보를 관리·통제할 수 있도록 하는 새로운 인증체계인 블록체인 기반의 탈중앙화 신원증명(DID, Decentralized Identifier)이 주목받게 되었다.

기존 대부분의 신원확인 서비스는 서비스제공 기업이 사용자 인증정보와 개인정보를 중앙화된 시스템에서 관리한다. 하지만 인증 서비스가 중앙 시스템에서 관리될 경우 개인정보 유출 사고, 프라이버시 침해 등에 대한 문제점이 존재한다.

이에, 사용자의 프라이버시를 보호하고 각 서비스제공 기관마다 사용자 인증정보 및 개인정보를 관리함에 따른 문제를 해결하기 위해사용자가 자신의 신원정보를 직접 관리하고, 노출 범위를 선택할 수 있는 자기주권 신원증명(SSI, Self-Sovereign Identity) 모델이 등장하였다. DID는 이를 기반으로 오프라인에서 신원인증을 하는 것처럼 온라인에서 자신의 신원정보를 관리·통제할 수 있다. 비대면 서비스의 수요가 확대됨에 따라 DID는 이를 활성화하는 중요한 기반이 될 수 있다.

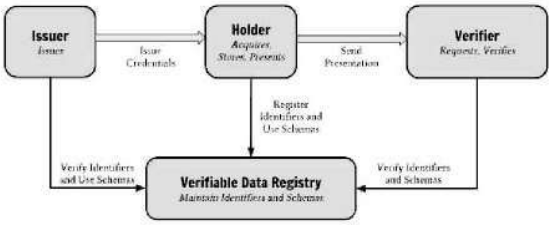
II. 블록체인 기반 분산ID

2.1 SSI(Self-Sovereign Identity)

자기 주권 신원(SSI)은 스스로 권한을 부여한 신원으로 정의될 수 있으며, 이것은 신원 증명의 패러다임이 중앙집중형 신원 증명 방식에서 개인이 주권을 가지고 자신의 신원을 관리 및 활용할 수 있는 체제로의 변화를 의미한다.

자기 주권 신원은 블록체인을 사용하므로 중앙 디렉토리 없이도 분산식별자를 조회할 수 있다. 누구나 블록체인을 사용하여 분산 식별자

〔그림 1〕 DID example (출처 : W3C)



〔그림 2〕 SSI 시스템 도식화 (출처 : W3C)

를 조회하고 연결된 공개키를 확인할 수 있다. 또한 어떠한 크리덴셜도 자유롭게 보관할 수 있으며 어떤 크리덴셜을 신뢰할지를 선택할 수 있기 때문에 많은 분야에서 자기 주권 신원확인 체계를 이용할 수 있다.

2.2 DID

분산ID는 중앙기관 없이 온라인상에서 분산원장을 기반으로 사용자가 스스로 신원 등에 대한 증명 관리, 신원정보 제출 범위 및 제출대상 통제 등을 수행할 수 있도록 하는 신원관리 체계이다. 기존에 디지털 정보의 경우 생성, 흐름, 보관 등의 과정에서 위변조의 가능성이 높았다. 하지만 블록체인의 특징 중 하나인 불변성을 통해 이러한 문제를 해결할 수 있다. 결국 블록체인과 디지털ID의 결합을 통해 SSI가 가능하게 되었다.

III. 분산ID 기술 동향

3.1 DIF(Decentralized Identity Foundation)

DIF는 전 세계의 모든 사람 및 회사에 분산 ID 생태계의 생성을 통한 사용자 지원, 체인 및 서비스 공급자에서 실행되는 분산ID 프로토콜, 사양 및 새로운 표준을 개발하는데 목표를 두고 있다.

3.2 uPort

uPort는 이더리움 블록체인에 기반한 자기주권 디지털 신원 플랫폼이다. 사용자가 자신의 ID 정보와 개인정보를 제어할 수 있는 자기주권 신원이 가능한 최초의 ID 관리 시스템으로, 해당 플랫폼을 통해 중앙 집중형 방식으로 서버 없이 메시지 송신자를 신뢰할 수 있도록 한다. 스마트 컨트랙트의 특성을 이용하여 영구 ID를 생성하여 개인키 분실로 인한 신원 인증의 문제점을 보완하였다.

3.3 Sovrin

Sovrin은 프라이빗 블록체인으로 운용되는 오픈소스 분산ID 네트워크로, 이용자와 관계된 모든 사이트에 대해 서로 다른 DID를 가질 수 있도록 지원한다. Sovrin은 uPort와 달리 이용자의 요청에 대한 증명 및 검증이 가능하며, 영지식 증명을 지원하고, 개인정보 최소 공개의 원칙을 준수할 수 있도록 설계되었다. [1]

3.4 MyID Alliance

아이콘루프의 자체 분산아이디 기술로 구현한 블록체인 기반 모바일 신분증 서비스인 MyID를 중심으로 한 협력체이다. 비대면 계좌 개설의 실명확인증표 사본 확인과 기존 개설 계좌 거래 절차를 MyID 플랫폼을 통해 정보제출로 대체하는 규제 특례를 획득하였다.

3.5 Initial DID Association

SK텔레콤이 주도하고 과학기술정보통신부와 한국인터넷진흥원이 추진하는 2019 블록체인 민간주도 국민 프로젝트로 선정돼 결성된 연합체로 컨소시엄형 블록체인 네트워크이다. 국내 통신 3사가 참여하고 있어, 빠른 대중화를 이루기에 유리한 입지에 있다.

이니셜(Initial)은 국내 통신 3사와 은행 등이 연합하여 만든 블록체인 기반의 분산아이디 서비스이다. 이를 활용하면, 모바일 전자 증명 앱에서 발급 및 제출을 원하는 기관의 증명서를 선택해 원하는 작업을 할 수 있다. 이를 위해

각 기관 웹 페이지에 제공된 QR코드를 이니셜 애플리케이션으로 인식해 증명서를 발급 및 제출할 수 있는 기능을 갖출 계획에 있다.

3.6 DID Alliance Korea

DID Alliance Korea는 라온시큐어가 개발한 분산ID 플랫폼인 옴니원에 기반하고 있다. 이오스(EOS) 플랫폼을 DID에 최적하해 개발한 옴니원은 병무청 민원서비스 블록체인 플랫폼에 적용되었다. DID Alliance Korea는 특정 기업 주도로 DID 서비스를 제공하는 것이 아닌 분산ID의 표준화되고 상호호환 가능한 프레임워크의 개발을 목표로 하고 있다.

IV. 분산ID 정책 동향

4.1 국내 동향

DID는 비대면 환경에서 신원증명을 제공하고 개인정보를 직접 관리할 수 있는 비대면 경제의 맞춤형 기술로서 집중육성이 필요하다고 보고 전략 추진중에 있다.

정부에서 발표한 첫 번째 전략은 범부처 통합 공공플랫폼 구축이다. 공공부문 DID 서비스 이용 시 국민이 여러 앱을 설치해야 하는 불편함이 없도록 국민의 신원·자격증명을 정부가 발행하고, 증명정보를 민간이 검증할 수 있도록 범정부 차원의 통합 공공플랫폼 지원체계를 마련하여 공공플랫폼이 민간의 DID 플랫폼과 연계될 수 있도록 추진한다.

두 번째 전략은 DID 간 연동 지원 및 타 인증수단 연계다. DID 서비스와 관계없이 신원증명 검증을 쉽게 하도록 지원하는 DID 통합 해석기 연구개발 및 적용 확산할 예정이다.

세 번째 전략은 사람의 자격증명을 넘어서 전자계약, 사물(IoT), 제어 등 혁신적 DID 서비스를 발굴하기 위한 시범사업으로 내용은 다음 표와 같다.

마지막 전략은 DID 생태계 활성화를 위한 거버넌스 구축이다. 공공·민간 DID 생태계 활성화를 위해 관계부처·전문기관·기업이 참여하는 민관 합동 DID 협의체를 구성하고 운영할 계획이다. 위 협의체에는 과기정통부를 중심으로 행안부, 병무청 등 DID 사용기관 및 KISA, ETRI, TTA 등 전문기관 및 민간 DID 얼라이언스 등이 참여한다. [2]

4.2 해외 동향

캐나다에서는 2017년부터 금융기관을 중심으로 블록체인 기반 신원인증 시스템인 Verified.ME 시범사업을 운영하고 있다. Verified.ME앱은 IBM 블록체인 상에 구축되어 Hyperledger Fabric v1.2을 기반으로 B2B 사업을 주력으로하는 DID 프로젝트 기반의 프로토콜을 개발, 활용 중이다.

스위스는 2017년부터 Zug시에 크립토 밸리를 조성하였으며 블록체인 기반의 신원인증 사업을 운영하고 있다. Zug시 시민을 대상으로 블록체인 기반 신분증을 발급하는 파일럿을 운영 중이며 등록된 사용자의 공개키 관련 정보(계정 주소)와 사용자 본인을 확인하는 정보를 Zug시 ID 발급기관에 제공해 신분증을 발급한다. 해당 신분증은 블록체인 시스템에서 신분증 내부에 저장되어있는 개인정보가 노출되는 것을 막기 위하여 분산원장 밖에 저장되는 Off-Chain 방식으로 제공된다. [3]

V. 결론

본 논문에서는 블록체인 기반 DID의 기술과 정책 동향에 대해 살펴보았다.

블록체인은 데이터를 중앙 관리자가 아닌 데이터를 제공하는 주체들이 직접 관리하는 기술이기 때문에 데이터 주권 확보를 위한 다양한 모델 구현에 대한 시도가 가능하지만, 블록체인 속성상 수정·삭제가 힘든 문제, 관리 책임 귀속의 어려움 등 현재의 개인정보보호법 체계와 상충되는 점이 많기 때문에 아직 해결해나가야 할 문제가 많다.

블록체인은 코로나-19로 인한 초연결·비대면으로 대표되는 뉴노멀 사회에 대응하여 사회적 신뢰를 구축할 수 있는 기술로서 무한한 잠재력을 가지고 있기 때문에 4차 산업혁명 시대의 데이터 보호의 문제점을 해결할 수 있도록 연구와 투자르 지속할 필요가 있다.

ACKNOWLEGEMENTS

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

[참고문헌]

[1] 권한영, "데이터 주권 시대의 블록체인 기술 활용 가능성과 개발 현황", 정보통신기획평가원, 2020. 7

[2] 대통령직속 4차산업혁명위원회, [16차전체회의] 안건2 : 블록체인 기술 확산 전략, 2020.06

[3] Paul Kohlhaas, "Zug ID: Exploring the First Publicly Verified Blockchain Identity," Dec. 2017. (https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702)

[4] Verifiable Credentials Data Model 1.0, W3C,(https://w3c.github.io/vc-data-model/#ecosystem-overview)

[5] 김석현, 조영섭, 김수형 "블록체인 기반의 ID 관리 기술 동향," OSIA Standards & Technology review, 32:1, 16-22

[6] 김경환, 김지영, 이동선, 이남용 "클라우드 기반 시스템을 위한 분산 ID(DID) 적용 방안 연구," 한국IT정책경영학회 논문지 2020, vol.12, no.4, pp.1933-1938

[7] 권동승, 이현, 박종대 "디지털 신뢰 사회 실현을 위한 디지털 아이덴티티 동향," 전자통신동향분석, 제34권 제3호 ,2019. 6, pp.114-124