BLOCKO

Blockchain Report
BLOCK-SHOT
October, 2020

DID(분산ID)와 SSI(자기주권신원), 단순 로그인을 넘어서

Copyright © 2020 BLOCKO. All rights reserved.

DID(분산ID)와 SSI(자기주권신원), 단순 로그인을 넘어서

4 디지털 신원의 발전과 분산ID

6 국내 DID 현황

7 '신원'을 구성하는 다양한 요소와 DID의 한계

Copyright © 2020 BLOCKO. All rights reserved.

유니(Uni)와 무니(Mooni), 그리고 스시(Sushi)까지. 전세계적으로 탈중앙 금융(DeFi)가 주목받을 때, 국내에선 사원증이나 면허증을 비롯해 다양한 신분증을 대체하기 위한 분산ID(DID) 사업들이 연이어 발표됐다. 지난 4월 금융보안원이 분산ID 기반 금융권 신원관리 프레임워크를 금융보안표준으로 제정한 이후, 한국인터넷 진흥원이 공공기관 최초로 분산ID 기반 모바일 사원증 도입을 발표하고 행정안전부가 모바일 공무원증과 운전면허증을 분산ID화 한다는 계획을 발표하는 등 다양한 기관과 기업이 분산ID 적용에 앞다퉈 나서고 있다. 물론, 정부 주도로 진행되고 있는 블록체인 시범사업 대다수에도 분산ID가 기본으로 들어가 있기도 하다.

하지만 분산ID의 앞날이 마냥 밝은 것 만은 아니다. 분산ID가 '단순 로그인'을 넘어 더욱 다양한 영역으로 확대되기 위해선 해결해야 될 점이 많다. 최근 전자신문을 통해 보도(공공·금융서비스 분야 'DID 단독인증' 불발…업계 "사형선고" 격앙)된 바와 같이, 한국인터넷진흥원이 공공/금융 서비스에서 분산ID 인증과 본인확인기관 2차 확인을 모두 요구하는 시행령 방침을 밝히는 등 제도적으로 풀어야 할 문제들이 아직 남아있기 때문이다.

Copyright © 2020 BLOCKO. All rights reserved.

디지털 신원의 발전과 분산ID

자세히 들어가기에 앞서 디지털 신원(Digital Identity)에 대해 알아보자. 디지털 신원이란 온라인 상의 개인이나 디바이스를 고유하게 식별할 수 있는 정보를 의미한다. 계정을 통해 증명하는 1세대, 한 기관에서 사용/발급한 인증을 다른 기관에 연동해 사용하는 2세대, 개인 정보를 본인이 직접 관리하는 3세대로 구분할 수 있다.

1) 개별 신원 모델(1세대)

여러 인터넷/서비스에 각각의 계정을 통해 인증하는 방식. 네이버, 구글 등 인터넷 포털 서비스에 회원 가입한 계정으로 본인을 증명할 수 있다. 관련 프로토콜로는 TLS(Transport Layer Security)와 SSL(Secure Socket Layer) 등이 있다.

2) 연합 신원 모델(2세대)

한 기업이나 기관에서 발급받은 인증을 다른 곳에 연동해 사용하는 방식. 개별 계정에 일일이 접속하는 번거로움을 해결하고, 한 곳의 보안 사고가 다른 곳에 영향을 미치지 않도록 하기 위해 고안됐다. 관련 프로토콜로는 SAML(Security Assertion Markup Language), OAuth, OpenID 등이 있다.

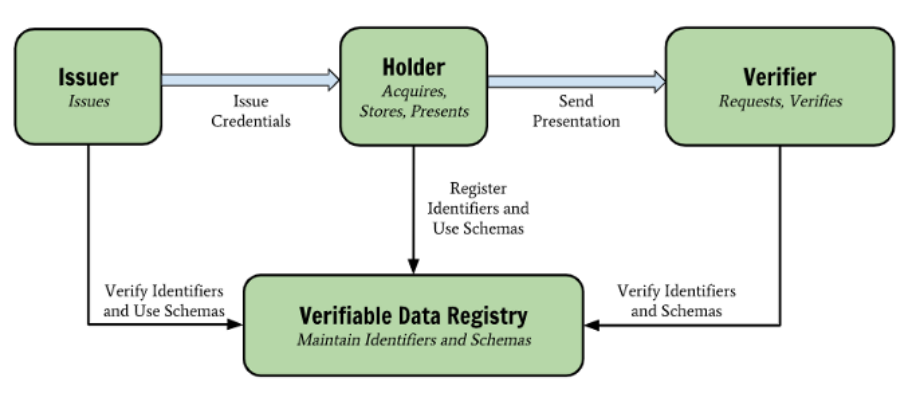
3) 자기주권 신원 모델(3세대)

개인정보를 사용자가 직접 관리하는 방식으로, 모바일 단말을 통해 증명 제출 및 서비스 사용이 가능한 방식. 현재 자기주권 신원 모델 구현 및 확산을 위해 국제 웹 표준기구 월드와이드웹컨소시엄(W3C) 주도로 분산ID 모델 관련 표준화가 진행 중이다.

Copyright © 2020 BLOCKO. All rights reserved.

W3C에서 정의하는 자기주권 신원 모델의 구조와 역할은 다음과 같다.

[그림 1] 자기주권 신원모델의 구조와 역할



(출처-Verifiable Credentials Data Model 1.0, W3C)

1) Holder (사용자)

자신의 신원 정보(Verifiable Credentials)을 보유한 주체로, 해당 신원 정보 기반의 제공 데이터(Verifiable Presentations)을 생성한다. 학생, 직원, 고객 등 일반 사용자가 여기 해당된다.

2) Issuer (발급자)

사용자의 신원 정보를 발급하는 주체이다. 제출된 정보(Claim)을 바탕으로 신원 정보(VC)를 발급한다.

3) Verifier (검증자/서비스 제공사)

사용자가 제공한 VP에 포함된 VC를 통해 신원을 검증하려는 주체이다.

4) Verifiable Data Registry (검증가능한 데이터 저장소)

VC를 활용하기 위해 필요한 각종 검증키나 식별자가 저장된다. 보안 데이터베이스, 분산 장부 등 다양한 방식의 저장소가 활용될 수 있다.

Copyright © 2020 BLOCKO. All rights reserved.

국내 DID 현황

국내는 다양한 방식의 신원 모델이 혼용되고 있으며, 공인인증서를 대체하기 위한 DID 컨소시엄들이 출범해 다양한 사업을 진행하고 있다. SK텔레콤·KT·LG U+ 등 통신3사가 이끄는 '이니셜 DID 어소시에이션'을 비롯해, 'DID얼라이언스 코리아', '마이아이디 얼라이언스', '마이키핀얼라이언스' 등 4개 컨소시엄이 활동 중이다.

	이니셜 DID 어소시에이션	DID 얼라이언스	마이아이디 얼라이언스	마이키핀 얼라이언스
주요 참여사	통신 3사, 코스콤, KEB하나은행, 삼성전자 등	라온시큐어, BC카드, 삼성SDS 등	아이콘루프, 신한은행, IBK기업은행 등	코인플러그, 매직에코, PSI컨설팅 등
특징	정부24 연계 공공제증명 서비스 예정	DID네트워크 간 기술 및 서비스 모델의 상호 호환성 마련	금융권 중심 전자증명	국내외 게임, 미디어, 정부·비정부 조직 등

이렇듯 다양한 기업 및 기관이 DID 서비스를 앞다퉈 출시하고 있지만, 구축 사례 대부분은 일반 사용자들이 활용하는 신원 정보(VC) 중 극히 일부문만을 활용하는 데에 머물고 있다.

Copyright © 2020 BLOCKO. All rights reserved.

‘신원’을 구성하는 다양한 요소와 DID의 한계

신원(Identity)은 하나의 고정된 개념이 아니다. 세계경제포럼(WEF)에서는 신원정보의 속성을 3가지로 구분한다. 나이, 생일, 지문을 비롯한 태생적 속성(Inherent Attributes), 건강기록, 신용정보 등의 축적된 속성(Accumulated Attributes), 그리고 주민/여권번호 등의 부여된 속성(Assigned Attributes)가 그것이다.

하지만 DID를 포함한 현재의 신원인증 개념은 태생적 속성과 부여된 속성에만 집중하고 있다. 그러다보니 ‘공인인증서 대체’가 DID의 가장 큰 목표가 돼버렸고, 공인인증서를 기준으로 쓰여진 금융실명법 등의 현행법과 계속 충돌하고 있다. 반면, 훨씬 다양한 영역(그리고 실생활에 가까운 영역)에 쓰일 수 있는 신원 정보가 포함된 ‘축적된 속성’은 큰 의미를 부여받지 못하고 있다.

물론, DID를 수단으로 하는 SSI의 핵심 가치는 검증되는 데이터의 종류가 아니라 데이터의 주권이 특정 기관이나 기업에서 개인으로 이동하는데에 있다. 하지만, 한정된 개인 정보만을 가지고, 특별한 차이점 없이 ‘로그인 방식 중 하나’인 식으로 접근하는 현 방식은 오히려 불편함을 가중시키고 보안 책임만을 떠넘기는 것과 다름이 없다.

DID를 위시한 SSI가 확대되기 위해선 더 가볍고, 실생활에 가까운 개인 정보/신분 인증을 활용할 수 있는 방법에 대한 고민이 필요한 시점이다.

Copyright © 2020 BLOCKO. All rights reserved.

블로코(BLOCKO) 소개

블로코는 2014년 설립된 블록체인 기술 전문 기업입니다. 블록체인 생태계 확장을 위해 한국은행, 한국전자통신연구원, 금융보안원, 금융결제원 등 다양한 국가 기관 및 기업체와 협력하고 있으며, 한국거래소와 신한금융그룹, 현대자동차그룹, 롯데카드, 경기도를 비롯해 국내외 대기업과 금융권, 공공 기관에 블록체인 기반 서비스를 구축한 국내 최대 블록체인 인프라 공급 기업입니다.

Copyright © 2020 BLOCKO. All rights reserved.

BLOCKO

Blockchain Report
BLOCK-SHOT
October, 2020

www.blocko.io
info@blocko.io
82 31 8016 6253

Copyright © 2020 BLOCKO. All rights reserved.