블록체인 기반 분산ID 기술 동향

김재용*, 전문석*
*숭실대학교 컴퓨터공학과
e-mail:raient@ssu.ac.kr

Block Chaining-based distributed ID Technology Trends

Jai-Yong Kim*, Moon-Seog Jun*
*Dept. of Computer Science, Korea University

요 약

컴퓨터 환경에서 사용자의 신원을 증명하고 확인하는 기술은 기존의 중앙 집중형 시스템에서 탈피하여, 블록체인 기반의 분산 형태로 발전하고 있다. 분산ID는 4차 산업의 핵심 기술 중 하나인 블록체인을 기반으로 한 신원 증명 기술로서, 기존 중앙집중형 시스템에서 발생하는 개인 정보 침해 및 시스템 구조적 취약점등을 해결하기 위한 기술로 관심이 높다. 블록체인 기반의 신원 증명 기술은 DID(Decentralized ID)와 SSI(Self Soverin Identity) 등이 대표적이며, 다양한 환경의 수요에 맞춰 국내외에서 활발히 연구 되고 있다.

1. 서론

컴퓨팅 환경에서 사용되는 기술은 빠르고 다양하게 변화하고 있다. 특히 클라우드 및 블록체인 기술의 발전은 기존 컴퓨팅 환경의 형태와 양상을 크게 변화 시켰다. 또한 사람들의 일상생활에 제공되는 컴퓨팅 환경 기반의 다양한 서비스가 증가함에 따라 기존의 방식이 아닌 블록체인 기반의 사용자 인증 방식에 대한 연구가 활발하게 진행되고 있다.

기존의 ID/Password를 이용한 지식기반 방식부터, OTP 및 인증토큰을 이용한 소유기반의 방식과 사람의 지문, 홍체, 안면 정보등을 이용한 생체 기반 인증 방식 등이 사용되고 있다. 전통적인 컴퓨터 환경에서 중앙집중형의 형태로 정보를 처리하는 것과 달리, 블록체인은 분산처리형태로 정보를 처리하고 있다. 블록체인과 관련된 연구가 진행되면서, 다양한 환경에서 탈중앙화 시스템으로의 변화가 시작되고 있으며, 개인의 신원 정보를 증명하는 Digital ID도 그 변화와 관련된 이슈중 하나이다.

최근에 새로운 형태의 사용자 인증 방식에 대한 연구가 활발히 진행되고 있으며, DID(Distributed Indentity)와 SSI(Self-Sovereign Identity)등이 대표적이다. 또한 탈중앙화 신원정보 확인시스템 (DIDs:Decenteralized IDentifiers)은 중앙 시스템에 의해 통제받지 않고 개개인 스스로가 자신의 신원을 통제하고 확인하는 방식이다. 그와 함께 분산처리 신원증명(DID, Distributed Identity)으로 인해 구현이 가능해진 신원증명의 새로운 개념으로 최근에는 , SSI(Self-Sovereign Identity)등 새로운 형태의 사용자 인증 방식에 대한 연구가 활발히 진행되고 있으며, 다양한 분야로의 적용에 대한 시도가 이루어지고 있다. 블록체인 기반의 분산 ID 기술의 발전 동향을 알아보고자 한다.

2. 관련연구

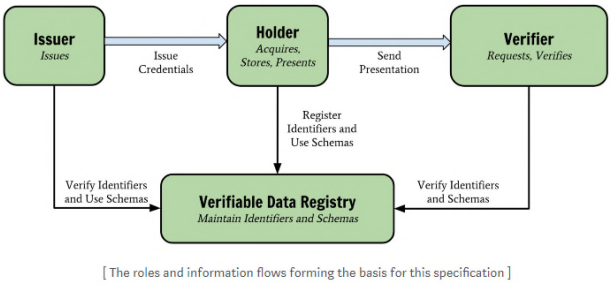
2.1 DID

블록체인 기술의 활용 분야가 확대되면서, 정보를 다루는 주체들에 대한 신원 확인 및 인증에 대한 연구도 활발히 진행되고 있다. 분산처리 신원증명 (DID : Distributed Indentity)과 탈중앙집중형 (DIDs : Decentraliezd Identifiers)가 대표적인 기술이며, 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 가질 수 있게 한다. DID의 특징은 중앙 서버에 데이터를 저장하거나, 인증 및 데이터 무결성 유지를 위한 서버의 관리를 필요로 하지 않는다는 것이다. DID는 데이터의 저장과 처리를 분산원장 시스템에 기반을 두고 있기 때문이다. 이는 기존 신원확인과는 달리, 암호화폐 사용자들이 자금을 관리하듯, 사용자가 자신의 정보를 관리할 수 있다는 특징을 갖는다.

[그림 1] DID examle (출처 : w3c)

2.2 SSI

자기주권 신원증명(SSI : Self-Sovereign Identity)은 개인 혹은 조직이 실제 생활하는 세계, 즉 오프라인에서 자신을 제외한 그 누구도 침해 할수 없고, 각 상황에 맞는 신원정보를 가지고 있다는 개념에서 출발한다. 예를 들어 한 개인은 국외를 방문할 때 사용하는 여권이나, 자동차를 운전할 수 있는 자격을 나타내는 운전면허증, 특정 학교의 학생임을 증명하는 학생증 등의 한 개인의 고유한 신원을 증명하는 다양한 ID를 가지고 있다는 것이다. 또한 각 개인과 조직은 그 정보를 소유자의 허락 없이 다른 제 3자가 사용하거나, 변조하는 등의 행위를 나쁜 행위로 인식하고 있으며, 나아가 법이나 제도를 통해 엄격히 금지하고 있는 환경에서 살고 있다. 또한 앞서 설명한 예와 같이 개인이 소유하고 그 개인을 타나내는 정보지만, 그 소유자가 아닌 제 3자를 통해 발급되고, 증명되는 신원 관련 문서의 형태로 표시되는 정보들이 많이 있으며, 이런 정보들은 누군가의 개입으로 유지되거나 취소가 될 수도 있다.



[그림 2] DID examle (출처 : w3c)

3. 본론

3.1 분산ID 국내 동향

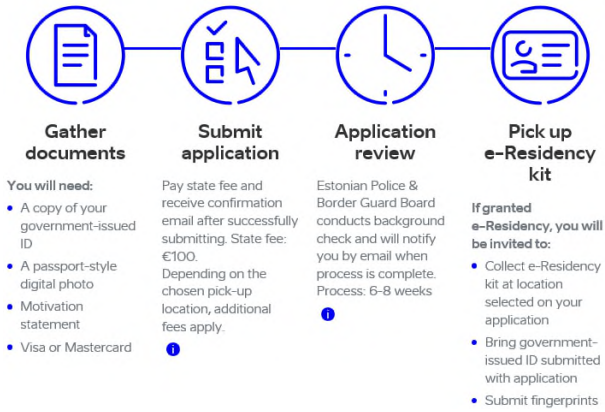
국내 정부부처와 산업계는 블록체인에 대한 높은 관심을 바탕으로 다양한 분야에서 적용 가능한 기술들을 연구 개발 하고 있다. 분산ID는 금융 산업계를 중심으로 다양한 형태의 움직임을 보이고 있으며, 연합체를 조직하여 자체적인 연구개발을 진행 하고 있다. 대표적인 연합체로 아이콘루프를 주축으로한 마이아이디 얼라이언스가 있으며, 비대면 계좌 개설의 "실명확인증표 사본 확인"과 "기존 개설 계좌" 거래 절차를 마이아이디 플랫폼을 통한 정보제출로 대체하는 규제 특례 획득 하였다. 마이아이디 얼라이언스는 은행이 인증한 신원정보를 바탕으로, 다양한 산업군에 서비스 확장을 예정하고 있다.

SK텔레콤이 주도로 한 통신 3사 및 주요 금융사 등 대기업 중심으로 형성한 "이니셜 컨소시엄"은 제증명서 서비스를 국책 과제로 수행한 경험을 바탕으로 은행, 카드, 증권, 보험 연계 금융 서비스와 국가기관과 학교기관, 교육기업과 연계한 증명서 서비스, ICT 보안 연계 출입통제 서비스 등으로 확장 하고 있다.

"DID 얼라이언스 코리아" 는 병무청 민원서비스 플랫폼을 개발한 라온시큐어의 옴니원 기반이며, 앞의 두 연합체의 목표가 특정 기업 주도로 DID 서비스를 제공하는 것과 달리 디지털 신원증명과 같은 상위 개념이나 DID 표준화 제정 논의를 주도 하고 있다.

3.2 분산ID 국외 동향

에스토니아는 블록체인 기술 활용에 가장 적극적인 국가 중 하나이며, 국가 차원에서 디지털 아이덴티티 기술을 활용하고 있다. 에스토니아는 2013년부터 블록체인을 기반으로 한 신원 증명 기술을 사용였으며, 다양한 방면에서 공공사업을 진행 중에 있다. 전자거주권(e-Residency) 프로그램을 통해 전 국민의 98%에게 온라인 시민권으로 사용 할 수 있는 ID Card를 발급했으며, 인-구의 2/3이상이 적극적으로 활용하고 있다. 에스토니아는 온라인으로 디지털 ID 형태의 신원증명서 발급을 위한 인프라를 구축하여 EU 및 에스토니아 정부가 제공하는 행정 서비스 이용에 활용 하고 있다.



[그림 3] 에스토니아 전자거주권 발급 절차
(출처 : https://e-resident.gov.ee/become-an-e-resident/)

에스토니아 외에도 다양한 국가에서 Sovin, uPort, ShoCard 등 비영리 업체와 스타트업이 중심으로 분산 ID 플

랫폼을 출시 하고 있다. Sorvin은 동명의 비영리 재단이 주관하는 플랫폼으로 사용자의 주권을 보장하는 디지털 신원정보의 개념으로3 출시되었다. 자주적 디지털 신원을 실현하기 위한 방침, 법적 동의, 기술 등에 대해 명세한 “Sovrin Trust Framework”를 제정하고, 이를 바탕으로 사용자에게 디지털 신원정보 플랫폼을 제공한다. Sorvin은 이주 노동자를 대상으로 신원 및 자격을 증명하는 이키가이(Ikigai) 프로젝트에 분산ID 기술을 적용하였다.

3.3 분산ID 표준화 동향

국제 웹 표준기구 W3C는 분산처리 신원증명을 위한 DID 및 DIDs 뿐 아니라 SSI 구현과 확산을 위한 표준화를 주도하고 있다. W3C는 2016년부터 블록체인 커뮤니티그룹을 결성하여, 블록체인 유스케이스, 블록체인 메시지 형식 및 저장 사용 지침 등의 표준을 개발하고 있다. W3C가 DID 표준화와 모델 관련하여 발표한 문서는 다음과 같다.

분산 식별자(Decentralized Identifiers)에 대한 데이터 모델과 신텍스 관련 문서 “Decentralized Identifiers(DIDs) v0.13 Data Model and Syntaxes”와 “증명가능 주장(Verifiable claims) 유스케이스를 기술 보고서(2017.6)”를 발행하였으며, 정식 WG 문서로 “증명가능 주장 데이터 모델과 표기법(Verifiable Claims Data Model and Representations 1.0)”을 2020년 5월 8일 개정하였다.

4. 결론

블록체인과 연계된 DID와 SSI를 활용한 신원정보 증명시스템은 기존의 신원관리 유형에 비해 신원정보의 대량유출을 방지하고, 보다 안전하게 이용자의 신원정보를 관리하며, 이용자의 편의성 또한 증진시킬 수 있어 향후 금융권의 주요 보안인증 수단으로서 활용 할 수 있다. 단 상용화 단계에서 서비스를 제공하기 전에, 사용자의 신원이 안전하게 관리될 수 있도록 기밀성 및 무결성을 보장하는 확실한 보안대책의 마련이 필요하다. 또한 이용자 단말에서 고객 단말에서의 신원 유출 및 위·변조를 방지하기 위해 암호화 및 신뢰실행환경(TEE: Trusted Execution Environment) 등의 기술을 활용하여 정보를 저장하고, 신원정보에 접근하는 고객에 대한 충분한 인증절차 마련도 필요하다. peer to peer 기반의 DID 네트워크 플랫폼은 공격자가 증명 관리 시스템에 등록된 고객의 증명확인 정보 에 접근하지 못하도록 활용목적과 확장성 및 보안성을 고려하여 네트워크를 구성하고, 접근통제를 실시해야 한다.

블록체인으로부터 시작된, 다양한 컴퓨팅 환경의 탈중앙화 움직임은 굉장히 빠른 속도로 진행이 되고 있으며, 점차 영향을 받는 영역을 크게 늘어 날 것으로 예측 된다. 현재 블록체인과 연계된 DID와 SSI를 활용한 신원정보 증명시스템은 미완성 단계이나 멀지 않은 기안내로 기술의 완성과 서비스의 상용화가 이루어질 것으로 예상한다. 블록체인과 디지털 ID의 결합을 통해 자기주권 신원증명(SSI: Self-Sovereign Identity)의 적용이 가능하게 되었고, 향후 DID는 프라이버시, 보안, 효율성 등이 요구되는 다양한 분야에서 활용 가능한 좋은 신원정보 증명기술이 될 것이다.

참고문헌

[1] 금융보안원 보안연구부, “신원정보 관리유형의 변화와 특징 비교”, 2017.07

[2] 기주희, “인증 기술의 과거와 현재”, 정보통신기술 진흥 센터 주간 기술동향, 2017.09

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (https://bitcoin.org/bitcoin.pdf)

[4] Sorvin Foundation, Sorvrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, (https://sovrin.org/wpcontent/ uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf)

[5] DIDs: Decentralized Identifiers(DIDs) v.0.11, (https://w3c-ccg.github.io/did-spec/)

[6] A. Simons, “Decentralized digital identities and blockchain:The future as we see it,” Microsoft, Feb. 2018. Available at https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital- identities-and-blockchain-the-future-as-we-see-it/

[7] H. Farahmand, “Blockchain: EvolvingDecentralized Identity Design,” Dec. 2017. Available at https://www.gartner.com/doc/3834863

[8] N. George, “Self-Sovereign Identity 101-An introductionto Multi-sourced Identity and the core open standard for Self-Sovereign Identity,” sovrin foundation, eic2018