

적합성업무와 블록체인/분산원장

(1) 블록체인/분산원장 정의

- 블록체인 및 분산원장기술(Blockchain and distributed ledger technology)은 네트워크 참여자가 거래 정보를 합의하고 기록·보관함으로써 공인된 제3자 없이도 기록의 무결성에 대한 신뢰성을 확보하게 해 주는 기술임
- 블록체인은 분산원장을 구현하는 기술 중 하나로서, 중앙 기관 없이 분산 방식으로 구현된 불변의 분산 원장 시스템이다. 이 기술은 비트코인, 이더리움, 리플 그리고 라이트코인과 같은 전자상거래 (e-commerce)의 성공을 가능하게 하였다. 이러한 이유로 블록체인은 비트코인에 종속되고 전자화폐에 국한된 것으로 인식되고 있으나, 이 기술은 다양한 응용에 이용 가능한 기술임

※ R3 Corda나 IOTA 등과 같이 블록체인이 아닌 분산원장이 존재함

- 참조 아키텍처는 인프라에 대한 템플릿이라고 볼 수 있음. 즉, 블록체인/DLT (Distributed Ledger Technology) 참조 아키텍처는 블록체인/DLT 시스템을 설계하고 구현하기 위한 기본 틀이며 참조 아키텍처 표준을 개발하고 이를 따름으로써 확장성과 상호운용성을 제공할 수 있는 블록체인/DLT 플랫폼을 빠르고 효과적으로 개발할 수 있음
- 블록체인/DLT 기반 ID 관리는 참조 아키텍처를 기반으로 제삼의 신뢰기관 없이 효율적으로 객체를 표준화된 형태로 유일하게 식별 가능하도록 하는 식별 및 인증 프로세스를 정의

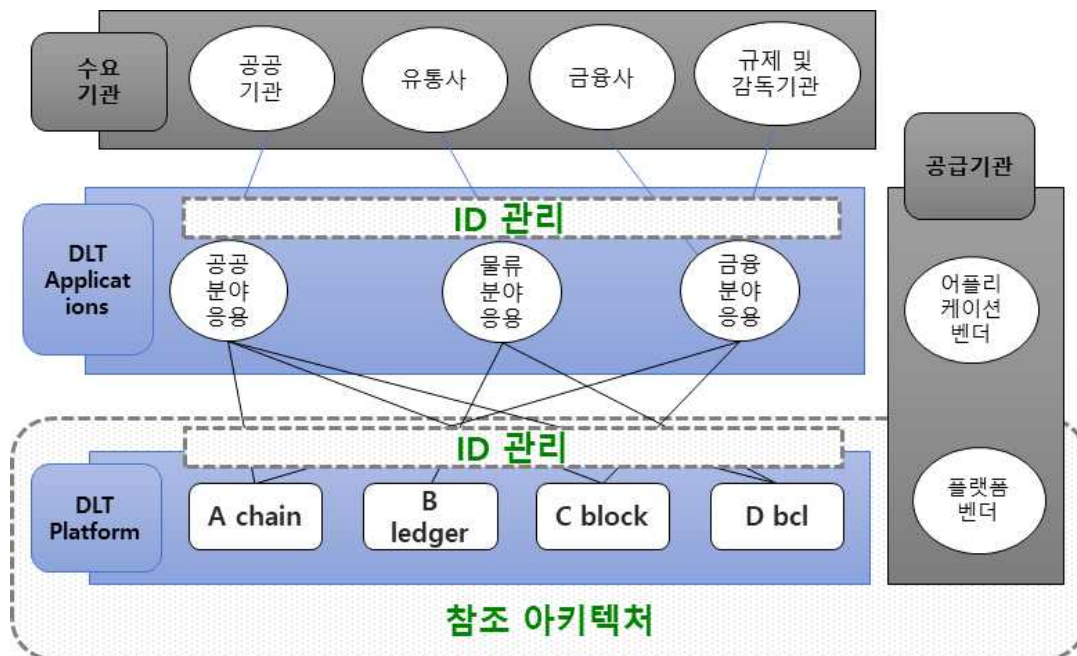


그림 1. 블록체인/DLT 생태계 내에서 참조 아키텍처와 ID 관리

(2) 필요성

- 블록체인/DLT 기술은 거래 기록의 변경불가능성과 중앙집권화된 통제 없이 참가자들의 합의에 대한 신뢰를 제공함으로써 기존의 비즈니스 프로세스를 바꾸어 낼 새로운 패러다임으로 부상
 - . 2016년 초 세계경제포럼(World Economic Forum, WEF)에서 제4차 산업혁명 시대를 이끌 핵심기술 중 하나로 선정
 - . 2016년 가트너(Gartner) 하이프사이클에서 향후 5~10년간 주류를 이룰 기술로 선정, 딜로이트 역시 중요한 emerging technology로 선정
 - . (Gartner) IAM(Identity and Access Management)을 위한 블록체인 기술은 태동기(Innovation Trigger) 단계로, 금융기관, 정부, 산업체에서 적극적으로 지원하고 있어 빠른 속도로 개발 중
 - * Hype Cycle for Identity and Access Management Technologies(Gartner, 2018)
 - . (IDC) 세계 IAM 시장이 '21년 8,202백만\$에 이를 것으로 전망, 특히 IAM 전체 시장의 연평균 성장률 7.5%에 비해, B2C 신원관리 시장은 17.3%로 고속 성장 중
 - * Worldwide Identity and Access Management Forecast, 2017-2021(IDC, 2017)
- 암호화폐로 인해 널리 알려졌으나 다양한 응용가능성으로 거의 모든 분야에 적용 가능하며 전 세계적인 관심사가 되고 있음
 - . 블록체인/DLT는 비용절감 가능성으로 인해 금융 분야에서 가장 먼저 본격적으로 응용되고 있음
 - . 조건에 따른 자동 실행을 보장하는 스마트 계약 기능은 디지털 정보의 보관, 디지털 인증, 디지털 자산의 거래, 디지털 지갑을 이용한 암호 화폐 거래 등 다양한 분야에서 새로운 신뢰 모델을 제공하는 응용을 개발할 수 있게 함
 - . 이론적으로는 모든 종류의 자산의 등록, 보관, 거래에 블록체인/DLT가 적용 가능하며, 이에 따라 블록체인/DLT 기술은 금융 분야뿐만 아니라 물류·유통, 나아가 정부 공공·행정 서비스에도 적용되고 확산될 것으로 전망되고 있음
 - . 미국 서유럽 등의 선진국 뿐만 아니라 중국, 동유럽, 라틴 아메리카, 아프리카 등의 국가들도 이 단순하고 강력한 기술을 자신들의 필요에 따라 적용하기 위해 동시 다발적인 노력을 기울이고 있음
- 블록체인/DLT 기술이 제공할 수 있는 가치 실현을 지원하고 상호운용성과 안전에 대한 적절한 지침을 제공하기 위한 표준화 요구 제기
 - . 현재의 분산원장 기술은 서로 다른 사설 및 오픈소스 프로젝트가 동시에 구현되고 있어 상호운용, 연동 및 확산의 장애로 작용
 - . 현재와 같이 유사하지만 서로 다른 방식으로 구현되는 분산원장기술 플랫폼을 확장, 연동 및 상호운용이 가능하도록 기본 개념, 용어 및 공통 참조 아키텍처의 수립이 필수적이며, 국제 표준화를 통하여 블록체인/DLT 관련 서비스의 상호 운용성, 구현 및 이용을 가능하게 함
 - . 참조 아키텍처는 이에 포함되는 보안 기능을 정의함으로써 블록체인/DLT에 기반한 공공 및 사회적 서비스를 더 안전하게 제공

※ 금융분야에서 국제 법규에 따라 필수적으로 요구되는 KYC(know your customer, 고객알기제도) 준수를 위한 부담을 표준화를 통해 크게 감소

※ 블록체인/DLT 기술을 이용한 국제 간 송금의 실시간 전송은 개발 도상국의 이용자들에게 금융에 대한 접근성을 높이고 더 큰 이익을 제공

- 전 세계적으로 블록체인/DLT에 대한 관심이 높아지는 가운데 기술 활용을 위한 국제적 협력이 증가하는 추세이며, 글로벌 금융기관들은 플랫폼 생태계 구축과 서비스 표준화를 위해 세계최대의 글로벌 블록체인 컨소시엄인 R3CEV와 IBM 주도의 하이퍼레저(Hyperledger) 프로젝트 등 다양한 기술개발 시도를 하고 있으며, 국내 금융권 내에서도 블록체인/DLT 기술의 상용화를 위해 2016년 12월 “금융권 공동 블록체인 컨소시엄”이 구성되어 현재 금융위원회 주관하에 운영 중에 있다.
- 블록체인/DLT 기술은 금융 분야뿐만 아니라 물류·유통, 나아가 정부 공공·행정 서비스에도 적용이 예상되며, 이론적으로는 모든 종류의 자산의 등록, 보관, 거래에 블록체인/DLT 기술이 적용 가능하며, 전 세계적으로 블록체인/DLT을 기반으로 국가 차원의 시스템 개발이 활발하게 진행되고 있다.
- 향후 디지털 정보의 보관, 디지털 인증, 디지털 자산의 거래, 디지털 지갑을 이용한 암호화폐, 스마트컨트랙트등 다양한 분야에 적용을 위하여 참조 아키텍처와 “동전이 없는 사회”를 지향하는 실명 거래를 위하여 신원정보관리 표준 개발이 시급하다.

(3) 대상기술 및 사업의 범위

① 블록체인 기반의 탈중앙 신원정보관리 지침 국제표준 개발 (ISO/TC307)

- 제삼의 신뢰기관이 없는 탈중앙, 분산환경에서 객체를 식별 및 인증을 위한 신원정보관리
 - . 신원정보관리의 위기를 초래하는 중앙제어 시스템을 탈피하는 구조 정의
 - . 블록체인/DLT 기반의 시장에 적용하는 상업적, 특히 금융권의 핀테크(FinTech)에 적용을 포함하는 신원정보관리 지침
 - . 식별자를 개인, 법적 객체, 사물(Things: IoT & objects)과 프로세스로 확대하여 향후 IoT 및 스마트시티와 같은 분야에 적용
 - . 신원정보관리 시스템의 진화에 따른 개인정보보호를 위한 자가-통제(Self-sovereign) 신원정보관리 시스템을 위한 기술
- ※ 신원정보관리 시스템 진화 단계 : 독립(Isolated Identity) 모델 - 중앙제어(Central Identity) 모델 - 유저중심(User-centric Identity) 모델 - 연방(Federated Identity) 모델 - 자가통제(Self-sovereign) 모델
- 또한 블록체인 기반 탈중앙 신원정보관리 기술은 은행권을 중심으로 상용화를 진행하고 있으며, 향후 e-Commerce, 핀테크, 식당, 의료, 공항, 여행, 교통, 전자시민증, 전자투표 등으로 확대가 진행되고 있으며, 이러한 제품과 서비스의 안정적 제공을 위하여 적합성평가에 활용하기에 최적의 기술 중의 하나이다.

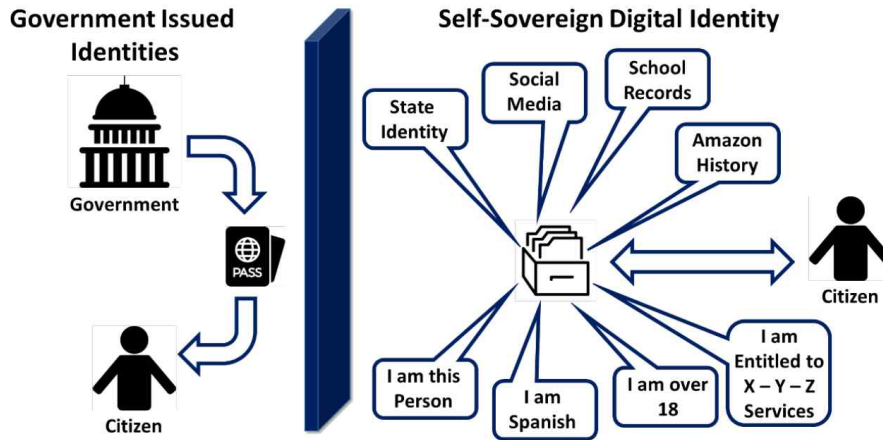


그림 2. 탈중앙/자가통제(self-sovereign) 신원정보관리 개념도

② 적합성평가 시스템 신뢰성 제고를 위하여 탈중앙 O2O기술 활용

- 적합성평가 시스템의 안정적 운영을 위해서, 기록보관 및 시험성적서의 진위 파악이 용이하도록 평가자, 수검자, 시스템 운영자 및 전산시스템이 투명하고 신뢰성 있게 운영이 되도록 전산시스템을 중심으로 온라인의 문서와 오프라인의 시험성적서의 진본성과 무결성 제고에 탈중앙 환경의 O2O 기술의 도입이 필요
- 부실시험, 시험데이터 조작 등의 부정행위 방지를 위하여 시험, 검사, 인증업무 전반에 대해 신뢰성 확보가 요구됨
- 시험의 수행 및 결과 등의 기록을 서버에 저장하여, 인적오류를 방지하고, 시험데이터 조작, 위조 등을 방지
- 시험성적서의 위변조를 예방하기 위하여 시험성적서의 무결성 강화
- 자체적인 감사조직을 운영함에 있어서, 업무를 간소화하여 효율적이고 유효한 감사활동을 지원하는 체제를 위하여 시스템에 접근인원에 대한 신원확인 강화
- 시험결과의 검증 및 재시험을 효율적으로 운영하기 위하여 기록의 추적성 강화

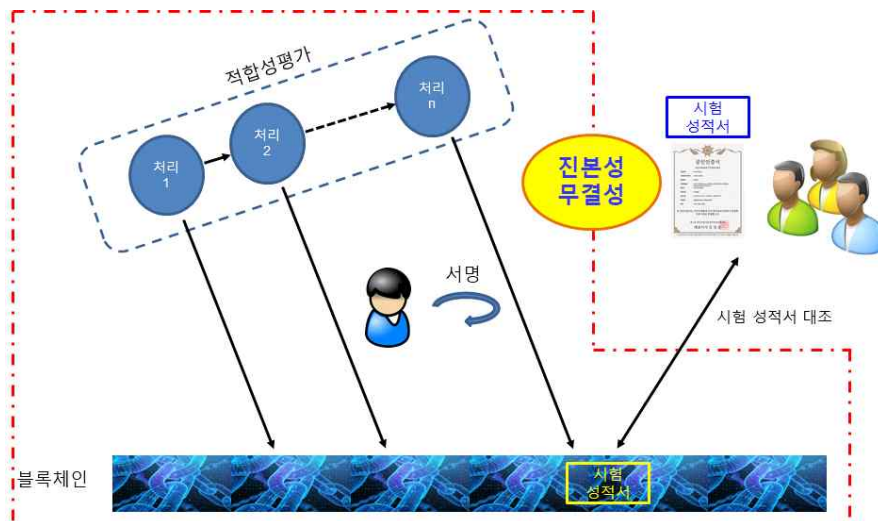


그림 3. 시험성적서 위변조 방지를 위한 블록체인 기반의 O2O기술의 적합성평가 업무에 적용예

본 연구는 2020년도 산업자원통신부의 재원으로 국가표준기술력향상사업의 일환으로 수행 중.

[20005255, 블록체인 기술을 활용한 적합성업무 관리 참조모델 운영 및 표준화 전략], 한국전자통신연구원 정보보호연구본부