블록체인 기반의 디지털 신원증명 동향

이정현*, 서화정**
*한성대학교 컴퓨터공학부
**한성대학교 IT융합학부
sjeonghyeonz@gmail.com, hwajeong@hansung.ac.kr

Trends of Blockchain-based Digital Identity

Jeong-Hyeon Lee*, Hwa-Jeong Seo**
*Dept. of Computer Engineering, Hansung University
**Dept. of IT convergence Engineering, Hansung University

요 약

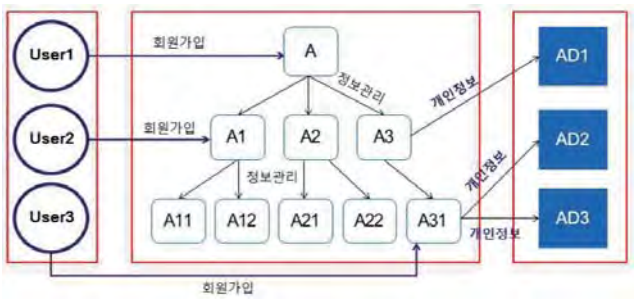
개인 정보의 유출은 유출된 당사자에게 단순 정보 유출을 넘어서 2차적인 피해를 주기 때문에 개인 정보 보호에 대한 중요성은 높아지고 있지만 오늘날까지 개인 정보 유출 사고는 끊임없이 발생하고 있다. 현재 널리 사용되고 있는 디지털 신원인 중앙 집중형 ID(Centralized Identity)는 사용자가 스스로 신원을 생성, 제어, 관리할 수 없어 개인 정보 유출 및 오남용이 쉬운 구조이다. 이러한 문제를 해결하기 위해 개인이 스스로 자신의 신원을 관리 및 통제할 수 있는 블록체인 기반의 디지털 신원의 필요성이 제기되었다. 본 논문에서는 디지털 신원(Digital Identity)의 종류와 현재 국내외에서 연구하고 있는 블록체인 기반의 신원증명 기술에 대한 동향을 살펴본다.

1. 서론

인터넷의 발전에 따라 단순히 정보를 공유하는 것을 넘어서 오늘날에는 실질적인 가치나 콘텐츠를 제작하고 공유한다. 이러한 변화를 통해 시간적, 공간적 제약이 따랐던 이전과 달리 인터넷을 통해 비교적 제약 없이 서비스 이용이 가능해졌다.

사용자는 각 서비스마다 회원가입 시 신원 정보를 입력한다. 이 때, 비밀번호는 보안을 위해 복잡한 형식으로 설정할 것을 요구한다. 대다수의 사용자는 계정 정보를 기억에 의존하기 때문에 ID와 비밀번호를 유사하게 설정한다. 그리고 서비스 이용을 위해 개인정보 수집 및 활용, 위탁 관리와 같은 필수약관에 동의한다. 이로 인해, 사용자는 원하는 서비스를 위해 특정 서비스에 가입하지만 사용자의 정보는 해당 회사의 계열사 및 위탁관리업체에 넘어가기 때문에 사용자가 서비스에 가입할수록 개인정보는 더 많은 곳에 제공된다.[1] 이러한 구조는 해킹하기 쉽게 만들고 한 사이트에서 개인 정보가 유출되면 타 사이트의 계정에도 영향을 미쳐 보안성을 저하시킨다. 유출된 개인 정보는 단순히 유출에 그치지 않고 범죄에 이용되거나 경제적 피해를 주기도 한다.[2]

또한 World bank의 데이터에 따르면 약 10억 명이 법적 신원 없이 살고 있다.[3] 자신의 신원을 증명하지 못하면 삶의 질과 기회에 있어 매우 제한적이고 최악의 경우, 기본권조차 보장받지 못한다. 국가 차원에서도 세금을 징수하거나 정책을 이행하고 범죄자를 식별하는 등 안정적인 사회 운영과 관리를 위해 신원확인은 중요하다.



(그림 1) 개인정보 보안 및 관리에 대한 문제점[4]

본 논문에서는 위와 같은 문제를 해결하기 위한 블록체인 기반의 디지털 신원과 연구되고 있는 ID 관리 기술에 대한 동향을 살펴보도록 한다.

2. 블록체인

블록체인(Blockchain)은 P2P(Peer-to-peer) 기술을 기반으로 중앙 기관 없이 모든 참여자가 거래 정보를 검증하여 원장에 기록하고 공유하여 데이터의 무결성과 신뢰를 보장하는 기술이다.

트랜잭션들에 해시 함수를 적용해 생성한 해시 값을 블록에 저장하고, 추가로 생성한 해시 값은 다음 블록에 저장한 후 이전 해시 값과 연결 지어 체인을 형성한다. 이를 통해 하나의 거래 정보가 변경되면 연달아 뒤에 있는 블록체인의 해시 값이 모두 변경되므로 특정 노드가 임의로 정보를 조작하는 것을 어렵게 함으로써 정보의 무결성을 유지한다. 또한 모든 노드들은 모든 트랜잭션에 대한 전체 기록을 공유하게 된다. 블록체인의 구조적인 특징으로 인해 체인이 길어질수록 임의의 참여자에 의해 데이터 위변조가 불가하며, 참여자 간 P2P 네트워크를 통해 완전히 정보가 공유되기 때문에 전체 시스템이 중단되는 단일 장애점 위험에 대비할 수 있고 데이터 보호 비용을 감소시킨다는 장점을 가진다.

3. 블록체인 기반의 디지털 신원

3.1 신원

신원(Identity)은 한 사람이 누구인지 정의하는, 다른 사람들과 구분되는, 개개인을 식별하는 이름, 직업, 주소와 같은 정보를 의미하며, 디지털 신원(Digital Identity)은 컴퓨터 시스템 상에서 개인 및 그룹 사용자들 각각을 구분하고 이에 따른 권한 부여 및 서비스를 제공하기 위해 사용되는 정보를 의미한다. 기존 신원정보를 포함하여 아이디와 패스워드 등이 디지털 신원에 해당한다.[1]

3.2 종류

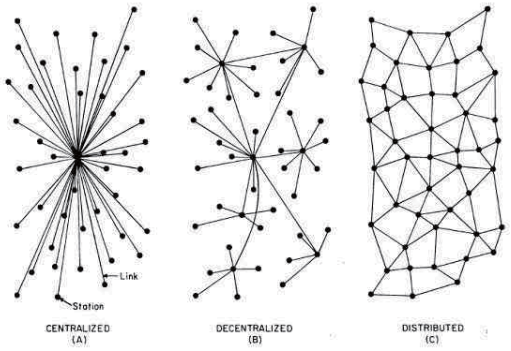
디지털 신원은 중앙 집중형 ID(Centralized Identity), 연합형 ID(Federated Identity), 사용자 중심형 ID(User-centric Identity), 자기주권형 ID(Self-sovereign Identity)로 진화하고 있다.[5]

중앙 집중형 ID는 사용자가 각 사이트에 계정을 만들 때 정보를 일일이 입력하며 이 정보를 기업이 개인 정보 제공 및 활용 동의를 받아 서버에 저장하고 관리한다. 이러한 구조에서는 사용자 스스로 개인 정보를 관리하고 통제하기 어렵고 개인 정보 유출 및 오남용 문제가 발생하기 쉽다.

연합형 ID는 OpenID, OAuth 등을 기반으로 기존 사용자의 소셜 미디어 계정으로 다른 애플리케이션이나 사이트에 로그인하는 형태이다. 계정 생성의 번거로움이 줄어들었지만 특정 대기업이나 서비스에 의존하기 때문에 개인 정보 유출 위험이 여전히 존재한다.

사용자 중심형 ID는 신원 입증을 요구하는 자와 신원을 입증하고자 하는 두 당사자 사이에 신분증, 여권과 같은 기존의 신뢰할 수 있는 신원증명 제공자가 신원증명을 수행하고, 추후 제3의 기관에 의한 유효성을 검증하기 위해 입증 내용을 분산 원장에 기록하는 방식이다. 탈중앙형 네트워크의 모형과 유사한 구조로 연합형 ID와 비슷하지만 특정 기업이나 서비스가 아닌 기존의 신원증명 방식을 사용하기 때문에 일반적으로 오프라인에서의 신원 확인을 병행한다.

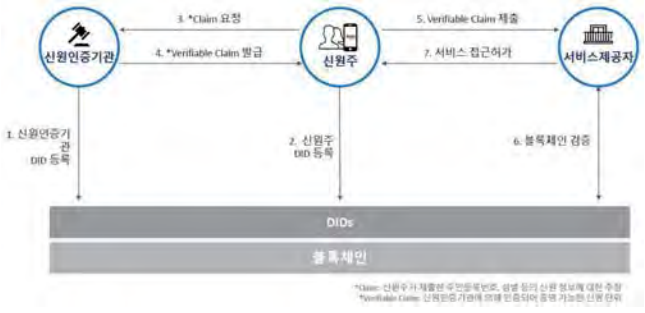
자기 주권형 ID는 사용자 스스로 자신의 정보를 저장하고 소유하기 때문에 중앙기관이 필요 없으며, 스스로 통제하기 때문에 유출 가능성이 없는 신원이다. 분산 네트워크의 모형과 유사한 구조를 가지며 신원은 분산 ID 공개키, 신원 소유자가 공개하고자 하는 기타 모든 공개 자격 증명 및 상호작용을 위한 네트워크 주소를 포함하는 분산 ID 문서와 함께 블록체인에 저장된다.



(그림 2) 디지털 신원의 종류에 따른 모형[6]

3.3 신원증명 시스템

국내외로 블록체인을 기반으로 한 신원 증명 서비스를 제공하기 위해 연합체를 형성하고 많은 기업들이 파트너로써 참여하고 있다. 다양한 시스템과 연합들이 존재하지만 대표적인 서비스 위주로 살펴보고자 한다.



(그림 3) DID 서비스 흐름[7]

3.3.1 해외

3.3.1.1 ShoCard

ShoCard는 사용자가 신원을 주민등록증, 여권, 운전면허증 같은 기존의 신뢰할 수 있는 자격 증명으로 생성하여 데이터를 단말기에 저장하게 한다. 사용자는 직접 생성한 신원의 공개 범위를 제어할 수 있으며 초대를 받은 관련 당사자에게만 신원을 공개한다. 많은 데이터 중 공유할 데이터 일부를 선택함으로써 검증할 데이터를 최소화한다. 개인 식별 정보의 해킹을 방지하기 위해 ShoCard 시스템은 개인 식별 정보는 블록체인이 아닌 단말기에 저장하고 검증 정보만 블록체인에 저장함으로써 이동성을 가진다. 또한, ShoCard 알고리즘은 다양한 블록체인에 독립적으로 존재해 투명성을 확보하였으며 다른 블록체인에서도 동작하기 때문에 일부 블록체인이 동작하지 않더라도 신원은 유효하게 남는 지속성을 가진다.[8][9]

3.2.1.2 Sovrin

Sovrin은 허가된 분산 원장을 기반으로 구축된 분산 신원 네트워크다. 공개 표준과 오픈 소스인 Hyperledger Indy 프로젝트를 기반으로 하여 공개적인 네트워크지만 크리덴셜(Credential)이라 불리는 은행, 대학, 정부 등과 같은 신뢰할 수 있는 기관들만이 보안성과 확장성에 초점을 둔 분산 합의 프로토콜에 참여하는 노드를 실행함으로써 원장이 허가된다. 사용자는 어떤 신원을 사용할지 선택할 수 있고, 속성에는 사용자가 지정한 사람이나 사용자에게 위임을 받은 대리인만 접근하며, 영지식 증명을 기반으로 전체 속성 중 공개하고 싶은 속성을 선택함으로써 데이터를 최소화한다. 모든 상황이나 관계에 대해 별도의 신원을 부여하는 양방향 식별자를 지원하기 때문에 제3자가 사용자의 신원에 접근하여 유출시키더라도 다른 곳에서 해당 신원을 사용할 수 없게 되고, 사용자는 문제 상황을 감지해 신원을 변경할 수 있다. 처음부터 이 관계에서만 유효한 신원을 당사자 간에 공유했기 때문에 변경한 신원은 다른 관계에는 영향을 미치지 않는다. ShoCard와 달리 신원들은 제3자인 재단이 소유하기 때문에 이동성은 없다.[8][10]

3.2.1.3 uPort

uPort는 모든 사람들에게 분산 신원을 제공하는 것이 목표인 오픈소스 분산 신원 프레임워크로, 이더리움 분산 원장에 차세대 DApp과 이메일, 은행과 같은 기존의 중앙 집중식 애플리케이션용 신원 관리에 사용된다.

uPort는 모바일 애플리케이션, 개발자 라이브러리, 스마트 컨트랙트로 구성된다. 모바일 애플리케이션에는 신원 관련 데이터와 사용자의 키를 보관하여 사용자가 중앙기관 없이 스스로 신원을 생성, 제어 및 접근하고 다른 사람이 정보를 사용하기 전에 동의 여부를 확인한다. 개발자 라이브러리는 타사의 개발자가 uPort에 대한 지원을 자신의 앱에 통합하는 방법을 지원한다. 스마트 컨트랙트에는 컨트롤러와 프록시가 있다. 컨트롤러는 신원 형성의 주요 부분을 담당하며, 친구나 가족 같은 개인이나 은행, 신용조합 같은 기관이 복구 대리인 명단에 등록되어 있다가 사용자가 모바일 기기를 분실했을 경우 복구 대리인들이 투표해 정족수가 넘으면 사용자 신원을 복구하는 로직을 관리한다. 오직 다른 uPort 신원만 입증할 수 있기 때문에 이동성이 부족하다.

속성 데이터 구조 내 특정 속성은 개별적으로 암호화되지만, 신원 제공자, 이용자와의 관계나 특정 속성에 대한 메타 데이터가 유출될 수 있는 전체 JSON 데이터 구조가 표시되기 때문에 레지스트리에 과도하게 의존하면 정보가 유출될 수 있다. 또한 스마트 컨트랙트에 대량의 데이터를 저장하는 것은 비효율적이므로 JSON 속성 구조의 해시만 레지스트리에 저장하고 데이터 자체는 오픈 분산 원장 데이터 저장소인 IPFS에 저장하여 레지스트리로 저장된 데이터를 참조한다.[8][11]

3.2.2 국내

3.2.1 MyID

마이아이디(MyID)는 개인정보를 자신의 단말기에 저장하고, 인증할 때 필요한 정보만 골라 제출할 수 있게 하는 블록체인 기반 전자 신원증명 플랫폼이다. 통합된 ID 플랫폼을 사용함으로써 신원증명절차를 간소화하여 하나의 신원으로 다양한 곳에서 증명할 수 있게 되었고, 신원 정보는 생체인증을 통해 활성화함으로써 보안성을 강화하였다.

금융위원회 샌드박스를 통해 독점적 라이선스를 획득함에 따라 금융 서비스에 특화된, 국내에서 유일하게 금융실명법과 전자금융법에서 요구하는 금융권 실명 신원 확인이 가능한 분산 ID이다. 또한 국내 최초로 분산 ID 관련 W3C Method Registry를 등록하고 실 서비스를 오픈함으로써 검증된 안정적 기술력을 가졌다.[12]

3.2.2 Initial

국내 주요 통신사들을 중심으로 한 컨소시엄형 블록체인 네트워크로 각종 증명서 등을 담을 수 있는 지갑 형태의 앱을 개발하여 출시 예정에 있다. 규모는 다른 두 연합체보다 제일 작지만, 중소기업이 중심인 타 연합체와는 달리 대기업이 주도하고 파트너사도 대기업들이기 때문에 빠른 대중화가 용이하다.

3.2.3 DID Alliance Korea(DAK)

분산형 ID 서비스를 표준화된 한 체계 안에서 만들어야 한다는 필요성이 제기됨에 따라 2019년, 미국과 한국이 공동 주도하여 DID Alliance를 출범시키면서 국내에서 진행되는 활동을 담당하기 위한 DID Alliance Korea도 생겼다. 앞서 살펴본 두 협의체는 특정 기업이 주도하여 분산 ID 서비스를 제공한다면, DAK는 상위 개념인 디지털 신원증명이나 분산 ID 표준화 제정과 운영체계 구축 등을 논의한다.

4. 결론

본 논문에서는 디지털 신원의 진화 과정을 살펴보고 기존의 중앙 집중식 신원관리 시스템의 문제점을 해결하기 위해 연구되고 있는 블록체인 기반의 디지털 신원과 시스템에 대해 살펴보았다.

분산 ID를 사용하면 신원증명 절차 간소화로 간편함을 제공하고 인증과 관련한 시간적, 물질적 비용을 절감함과 동시에 기업에서도 개인 정보 관리에 대한 부담과 비용을 줄일 수 있다는 경제적인 효과와 동시에 스스로 신원을 관리해 개인 정보 유출 및 오남용과 그에 따른 2차적 피해를 줄일 수 있다.

이러한 장점 때문에 현재 다양한 디지털 신원 중 사용자가 중앙기관의 개입 없이 신원을 생성 및 제어할 수 있는 자기 주권형 ID가 세계적으로 활발하게 연구 및 개발되고 있다. 해외에서는 이미 실생활에 분산 ID를 적용한 사례가 있지만[13], 국내에서는 지난 2020년 3월 31일에 분산 ID의 금융보안표준이 제정되었으며, 현재 서비스를 앞두고 있거나 서비스는 출시되었지만 사용처 확보가 미흡한 상황이다. 대한민국의 잘 갖춰진 신원확인 시스템을 바탕으로 분산 ID에서도 금융권을 비롯한 다양한 산업과 해외 서비스와의 상호운용성이 확보된다면 글로벌 분산 ID 시장을 선점할 수 있을 것이다.

참고문헌

[1] Han-Jae Jeong. “Design and Implementation of Blockchain Based Digital Identity Management System”, Soongsil University, Dec. 2017.

[2] “개인정보 유출 뭐가 문제죠?”, JoongAng Ilbo, 2014.03.26. https://news.joins.com/article/14259415 (2020.01.23.)

[3] “ID4D Data: Global Identification Challenge by the Numbers”, World bank, June, 2018. https://id4d.worldbank.org/global-dataset (2020.01.23.)

[4] Kwang-Hee Jang. “Design of Personal Information Security and Utilization System Structure Using Blockchain Technology”, Hanyang University, Aug, 2019.

[5] Jae-Hoon Na. “Blockchain Identity Management and Privacy Standard Trend”, Journal of the Korean Telecommunications Society, vol. 36, no. 7, pp.20-25 Jun, 2019.

[6] Paul Baran. “Centralized, Decentralized and Distributes Systems”, Rand Corporation, Sep, 1962.

[7] Sun-Kyu Park, “Digital Signature-Based Digital Identification System Implementation and Use Cases”, IconLoop, Aug, 2019.

[8] van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. “Self-sovereign identity solutions: The necessity of blockchain technology”, arXiv preprint arXiv:1904.12816., Apr, 2019.

[9] ShoCard Whitepaper, "Identity Management Verified Using the Blockchain", Jan. 2018.

[10] Sovrin Whitepaper, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust", Jan. 2018.

[11] uPort Whitepaper, "A Platform for Self-Sovereign Identity", Oct. 2016.

[12] MyID Alliance Intorduction, “MyID Alliance Introduction”, Apr, 2020.

[13] “英서는 DID로 담배 구매… "한국도 표준화 작업 서둘러야"”, The Block Post, 2019.12.18., https://www.fnnews.com/news/201912181715015337 (2020.01.23.)