디지털산업정보학회 논문지 제18권 제3호-2022년 9월
http://dx.doi.org/10.17662/ksdim.2022.18.3.025

블록체인 기반의 DID 문제점 분석 연구

이 광 규*

Blockchain-based DID Problem Analysis Research

Lee, Kwangkyu

〈Abstract〉

DID(Decentralized Identity Identification) is a system in which users voluntarily manage their identity, etc., and control the scope and subject of submission of identity information based on a block chain. In the era of the 4th industrial revolution, where the importance of protecting personal information is increasing day by day, DID will surely be positioned as the industrial center of the Internet and e-business. However, when managing personal information, DID is highly likely to cause a large amount of personal information leakage due to electronic infringement, such as hacking and invasion of privacy caused by the concentration of user's identity information on global service users. Therefore, there are a number of challenges to be solved before DID settles into a stable standardization. Therefore, in this paper, we try to examine what problems exist in order to positively apply the development of DID technology, and analyze the improvement plan to become a stable service in the future.

Key Words : Blockchain, DID(Decentralized Identity), Privacy, SSI(Self Sovereign Identity), ZKP(Zero Knowledge Proofs)

Ⅰ. 서론

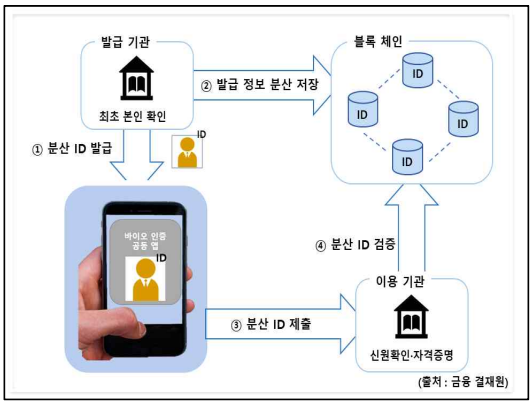
[1)]

인터넷 기술이 발달함에 따라 중립적인 정보를 공유하는 데는 유용하지만, 가치를 담고 있는 정보를 공유하는 데는 큰 제약이 생겼다. 현실에서 가장 중요한 가치를 담고 있는 정보는 바로 신원에 대한 정보인데, 개인의 신원정보를 다른 누군가가 마음대로 복제할 수 있게 된다면 인터넷 환경에서 '나'라는 존재 역시 무한대로 복제될 수 있음을 뜻한다. 이는 곧 복제본이 진본의 금융계좌를 마음대로 통제할 수 있으며, 공적인 서비스마저 서슴지 않고 이용할 수 있게 되는 결과를 낳을 수 있다. 때문에 현재의 인터넷 환경에서 신원정보를 공유할 때 반드시 신뢰할 수 있는 제3자 신뢰기관(Trust Anchor)이 보증한 인증서가 필요하다[1]. 그런데 현재 신원정보를 이용하고 관리하는 데는 상당한 번거로움과 문제점이 있다. 먼저 공인인증서의 발급과 이용상의 불편함이다. 인터넷을 통해 앱과 각종 서비스를 이용하기 위해서는 공인인증서를 통한 아이디 인증이 필수적이다. 다만 인증서

* 신한대학교 컴퓨터공학전공 교수

를 발급하고 이용하는 과정에서 상당한 시간적인 마찰이 유발되어 내가 나임을 입증하는 일에 상당한 자원을 낭비하고 있는 느낌을 지울 수 없다. IT 업계에서 이런 시대착오적 문제점을 해결할 솔루션 하나가 나왔다. 바로 블록체인 기반의 DID이다. DID란 개인정보를 사용자의 단말기에 저장해, 개인정보 인증 시 필요한 정보만 골라서 제출하도록 해주는 전자신원 증명 기술이다[2]. DID는 중앙 기관이 아닌 개인들이 자신의 데이터를 직접 관리하는 구조다. 따라서 기존 방식과 달리 서비스 이용 과정에서 모든 개인정보를 제공하지 않아도 된다. 각각의 사용자가 인증을 위해 꼭 필요한 정보만을 선택해 제출할 수 있기 때문이다. 예컨대 편의점에서 술을 구매할 때 직원에게 보여주는 주민등록증에는 나이뿐 아니라 주소, 이름, 주민번호 등 모든 개인정보가 노출된다. 하지만 DID 기반 신원지갑을 사용하면 '20세 이상 성인'처럼 필요한 사실만 확인시켜줄 수 있다. 온라인 플랫폼을 사용할 때는 편의성도 개선될 것으로 보인다. DID를 이용하면 매번 별도로 인증할 필요 없이 이전에 인증했던 데이터를 불러오면 된다. 즉, 개인정보를 반복적으로 입력하거나 일일이 신분증 사진을 올리지 않아도 된다. <그림 1>처럼 DID 기술은 인증 정보를 각 사용자의 디바이스에 분산된 형태로 저장하는 안전한 인증 시스템을 구축하여 기존의 중앙화된 인증 시스템의 문제점을 해결하고자 한다. 태생적으로 분산 시스템이고, 암호학적으로 안전하게 설계된 블록체인 네트워크를 이용하면 탈중앙화와 안전이라는 목적을 쉽게 달성할 수 있기 때문에 DID 인증 시스템에서는 블록체인 네트워크를 인증 시스템의 하부 인프라로 주목하고 있으며, 통합 로그인과 같이 사용자 편의성은 증대된 상태 그대로 유지할 수 있는 방안을 제시하고 있다[3].

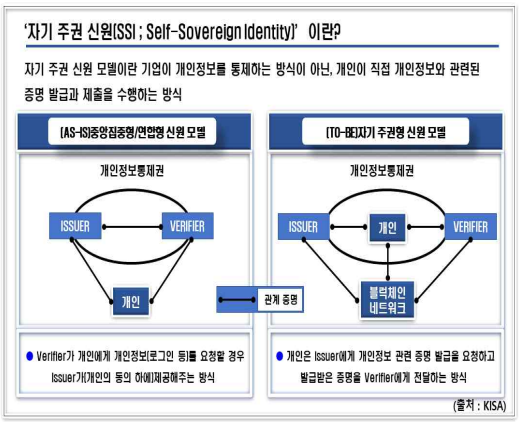
DID 모바일 신분증의 핵심은 스마트폰과 분산 네트워크 기술로, 각종 신분증과 증명서를 개인 스마트폰에 보관할 수 있게 함으로써 사용 편리성을 강화하



<그림 1> DID(탈중앙화 신원증명)구현 방식

고, 이때 발생할 수 있는 위·변조 문제는 블록체인과 같은 분산 네트워크 기술을 이용해 해결한다. 여기에 더해 영지식 증명(ZKP:Zero-Knowledge Proofs) 기술을 활용함으로써, 신원 증명 시 모바일 신분증상에 기록된 개인정보 중 필요 최소한의 정보만 노출되도록 하고 이때 노출된 정보는 다른 곳에는 활용할 수 없게 해 개인정보 자기주권신원(SSI:Self Sovereign Identity)을 강화한다. 자기주권신원이란 <그림 2>처럼 기업이나 신뢰기관이 개인정보를 통제하는 방식이 아닌, 개인이 직접 개인정보와 관련된 내용을 증명하는 방식이다. 결국 개인의 데이터의 주권을 개인이 관리하고 운영하게 되는 것이다[4]. 이런 세상이 도래하면 더 이상 기업이 개인의 데이터를 기반으로 과대하게 이익을 창출하는 일을 방지 할 수 있다. 또한 다양한 측면에서 활용되어지고 사회가 발전할 수 있는 토대를 마련할 수 있다. 그 중심이 이 DID이다. 하지만 DID가 개인이 생성하는 디지털 족적이나 축적된 속성을 신원정보로 인정할 수 있는가에 대한 논의, 제3자 신뢰기관의 근간으로 개인과 국가에 대한 패러다임 전환, 디바이스 혹은 지갑 클라이언트가 인터넷에 연결되어 있으면서도 개인정보의 원본에 접근할 수 없는 보안 알고리즘이나 하드웨어 등 해결해야 하는 문제가 있다[5]. 이러한 배경에서 본 연구는

DID가 안정적인 서비스로 정착하기 위한 개선방안을 제시함으로써 DID 기술 발전의 전략적 방향을 제고하고자 한다.

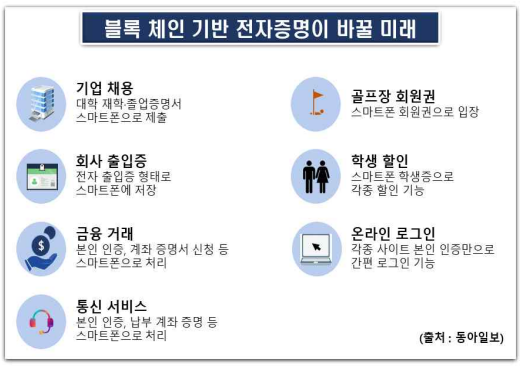


<그림 2> 자기주권신원 모델 개요

본 논문 구성은 다음과 같다. 먼저 2장에서 DID의 관련 연구를 살펴본다. 3장에서는 DID의 한계와 문제점을 살펴보고, 4장에서 DID의 장점은 개인정보를 사용자가 인증을 위해 꼭 필요한 정보만을 선택해 제출하는 것인데, 이와 같은 장점에도 불구하고 DID의 전반적인 문제점에 대한 분석을 기술하고, 결론 및 향후 연구 방향은 5장에서 언급한다.

Ⅱ. 관련 연구

블록체인을 암호화폐로만 여기는 사람이 대부분이다. 이는 블록체인 적용으로 주목받은 분야가 암호화폐 말고 없기 때문일 것이다. 그러나 2023년에는 이러한 인식이 조금씩 바뀔 전망이다. <그림 3>처럼 블록체인은 다양한 분야의 상용 서비스가 출시될 전망이기 때문이다. 그중 하나가 블록체인을 기반으로 신원을 증명하는 시스템인 DID이다[6]. DID의 특징은 중앙기관이나 기업이 통제해왔던 신원정보를 사용자 스스로가 생성 및 관리할 수 있다는 데에 있다. 이는 개인에게 신원정보관리 시스템을 구현하고 사용할 수 있는 길을 만들어 주며 사용자 데이터 정보의 보안, 결정권 및 수익에 대한 정당한 보상을 가능하게 한다. 이러한 특징은 P2P 기반으로 운영되며 위·변조가 불가능한 블록체인의 암호학적 특성을 기반으로 제 3의 중앙 기관을 거치지 않고도 사용자가 신원정보의 위·변조 여부를 검증하도록 함으로써 구현되었다[7]. 핵심은 데이터 주권이 중앙기관·기업에서 개인에게로 온다는 사실이다. 소수의 서비스 제공자가 운영하는 중앙 시스템에 방대한 양의 개인정보가 몰리는 것은 상당히 위험한 현상이다. 서비스 제공자들은 처리해야 하는 데이터양이 기하급수적으로 증가하며 관리에 어려움을 느끼고 있다. 그럼에도 불구하고IT 공룡들과 정부 기관들은 개인이 생성하는 데이터를 통해 막대한 가치를 만들어 내고 있다. 즉, 각각의 개인들에게는 본인이 만든 데이터에 대한 주권이 없는 상황이다. 이토록 난해한 데이터 주권 문제, DID가 해답을 제시할 수 있다. 블록체인이라는 기술을 통해 만들어지는 보안성과 신뢰성 높은 디지털 환경 속에서 개인은 자기 데이터의 주권을 회복할 수 있고, 더 나아가서는 거대 서비스 제공자들에게 우리가 생성한 데이터를 이용하는 행위에 대한 합리적 보상도 요구할 수 있을 것이다.



<그림 3> 블록체인 기반의 DID 응용 분야

이런 시점에 필요한 것이 바로 DID다. 해외에서는 이미 서비스 개발을 시작했다[8]. 일례로, 마이크로소프트는 비트코인 블록체인 기반의 탈중앙화 신원증명 프로젝트 아이온(Identity Overlay Network, ION)의 프리뷰 버전을 오픈소스로 공개한 바 있다. 페이스북은 리브라 백서에 디지털 아이덴티티(Digital ID)를 탈중앙화된 방향으로 혁신하겠다는 의견을 제시했다. 물론 구체적인 방향을 정하지는 않았다. IBM은 이미 블록체인 프로젝트를 위한 탈중앙화 네트워크 옐로페이지(Yellow Pages)에 가입해 DID 서비스 개발을 시작했다. 이미 전 세계적으로 DID 시장은 주목받고 있다. 자이온(Zion), 포춘 비즈니스 인사이트 등 글로벌 리서치기관에 따르면 글로벌 DID 인증 시장은 2023년 101억 달러에서 2025년 252억 달러 규모로 성장할 것으로 전망된다[9]. 이미 글로벌 IT 기업인 IBM을 비롯해 요티(YOTI), 시큐어키(SecureKey), 블록스택(BlockStack) 등 여러 스타트업들의 도전도 활발히 이어지고 있다. 하지만 문제는 국내 DID 모바일 신분증 사업의 추진 방향이 글로벌과는 다소 거리가 있다는 점이다. 해외의 경우 블록체인 외에도 다양한 분산 네트워크 기술을 활용해 DID를 구축하고 있다.

DID 시장은 분명 성장 가능성이 높은 시장이지만 기술 구현을 위한 구체적인 체계가 잡혀있지 않다. 시스템의 한 부분으로만 생각할 뿐 생태계적 관점에서는 충분한 고민이 없는 상태다. 무엇보다 표준 정립이 시급하다. 전 세계 시스템을 하나로 통일하는 건 어렵겠지만, 적어도 핵심적인 기능들에 대한 표준화 작업은 필요하다. 특히 2022년은 DID 개발 그룹의 형태가 구체화되고 관련 서비스 개발 및 연계가 시작됐다는 소식도 다수 전해지고 있고, 정부 역시 국민이 체감할 수 있는 실용적인 블록체인 개발을 정책 슬로건으로 내세우고 있는 만큼, DID 활용 사례 발굴에 지대한 관심을 가질 필요가 있다[10].

Ⅲ. DID의 문제점

DID의 가장 큰 장점으로는 탈중앙 구조에 따른 제3 중앙 기관의 필요성 제거와 이에 따른 개인 사용자의 온전한 정보 소유 및 통제가 꼽힌다. 그러나 블록체인이 모든 문제를 해결하는 만능키라는 태도를 지양해야 하듯이 DID의 탈중앙 구조가 모든 문제를 한 번에 해결해주는 만능키 역할을 할 것이란 무조건적인 기대 역시 한 번쯤 되짚어 볼 만하다. 이를 위해 먼저 어떤 면에서 DID의 기술 구현 방식의 문제점과 한계점을 살펴본다[11].

① 데이터 주권

현재 DID는 공인인증 대체로 주목받을 뿐만 아니라, 신원증명으로 확장해 주목받고 있다. 병적 증명서를 DID로 신원 증명하듯이, 학력 증명, 출생 신고, 거주지 등에 관한 인증을 DID로 증명받을 수 있다. 자기주권신원은 본인이 원할 시 전자서명을 통해 신원을 증명할 수 있는 기술을 뜻한다. DID 인증 시스템을 이용할 때 필요한 실제 인증 정보뿐만 아니라 누가 누구에게 인증을 요청했는지 등의 부가 데이터도 역시 중요한 데이터이다[12]. DID 인증 시스템에서는 이러한 인증 관련한 데이터의 관리를 사용자에게 맡김으로써 데이터 주권을 사용자에게 돌려준다. 사용자는 잘 만들어진 DID 애플리케이션을 통해 자신의 인증 데이터가 어떤 모습으로 어디로 전달되는지 투명하게 볼 수 있고, 데이터 제공을 승인/거절하거나 개인적으로 데이터에 이용약관 등을 추가하여 기업에게 해당 데이터의 이용을 제한할 수도 있다. 물론 이 자체만으로도 좋다고 생각할 수도 있다. 하지만 다른 각도로 보았을 때, 사용자가 직접 인증 데이터를 관리하는 것이 정말 사용자에게 좋기만 한지 고민을 해봐야 한다.

② 기밀성과 무결성

블록체인 기반 분산형 자기주권신원 정보관리는

비교적 새로운 개념이며 빠른 변화가 일어나는 중이다. 현재 실생활에서 사용자가 주민등록증 등 신원증명을 관리하는 것처럼, 온라인에서도 개별 서비스 제공기관이 아닌 사용자 스스로 자신의 신원정보를 생성·관리하고 정보의 선택적 공개를 통해 개인정보 보호가 가능한 분산형 자기주권 신원정보 기술은 소브린(Sovrin), 유포트(uPort), 쇼카드(ShoCard) 등 다양한 형태로 존재하며 개발 진척 단계도 제각기 다르다. 향후 다양한 분야에서의 실증 및 표준화 작업을 통한 상용화 준비 기간이 필요하지만, 도입 검토 시 이 시스템이 개인정보 또는 사용하는 사람들의 자유를 위협하지 않으면서 자연스러운 인간의 활동을 지원하기 위해 사용자의 편리성과 더불어 신원이 안전하게 관리될 수 있도록 기밀성 및 무결성 보장을 위한 보안 대책 마련이 필요하다[13].

③ 개인정보 과실

기존에는 개인신원을 증명할 때 기관이나 기업에 우리의 정보를 제공해 주고 최종 신원에 대한 인증을 기업과 기관에게 의탁하는 방식을 가지고 있다. 현재의 모든 사회시스템은 이 기반에 작동한다. 그런데, DID는 이 방식을 바꾼다. 그건 개인 스스로가 자신의 신원을 인증하게 한다. 이 방식이 적용이 되면 더 이상 개인정보에 대한 탈취나 개인정보를 조작하거나 변경하는 등의 위법 행위들이 발생하지 않게 된다. 물론 세부적으로, 기술적으로 해결해야 할 문제들이 있지만, 개인은 기본적으로 힘이 약한 존재다. 갑자기 사고를 당할 수도 있고, 관리했던 위치를 잃어버릴 수도 있다. 그리고 이미 우리는 대부분의 관리를 위탁하고 있기 때문에 이러한 편리성에서 탈피하기 위한 사회적 인식의 변화는 더 오랜 시간이 소요된다. 보안이 강화되었고, 개인에게 데이터의 주권을 돌려주자는 주장은 멋지지만, 그것을 현실에 적용했을 때 발생할 수 있는 문제들에 대한 대책은 여전히 마련되어 있지 않다. 결국 개인의 데이터의 주권을 개인이 관리하고 운영하게 되는 것이다. 그런데 이 DID가 반드시 해결해야 하는 문제는 비트코인 및 암호화폐 거래에도 지속적으로 발생하는 문제인데, 개인이 직접 개인 키(개인 인증을 위한 암호화키)를 관리하기 때문에 개인이 발생하는 실수에 대한 해결방안이 없다는 것이다[14].

④ 기술 표준화

DID는 사용자 신원증명정보를 본인이 직접 발급해 관리하는 서비스다. 기존 중앙집권형 디지털 체제는 해커가 특정 시스템을 공격할 경우 손쉽게 개인정보 탈취가 가능했다. DID 데이터는 네트워크에 연결된 여러 컴퓨터에 분산 저장돼 보다 안전하게 개인정보를 보호한다. DID가 공인인증서를 대체하는 새로운 방식의 모바일 신분증으로 자리 잡을 수 있다고 기대를 모으는 이유다. 하지만 문제는 국내 DID 모바일 신분증 사업의 추진 방향이 글로벌과는 다소 거리가 있다는 점이다. 해외의 경우 블록체인 외에도 다양한 분산 네트워크 기술을 활용해 DID를 구축하고 있다. 그러나 국내 시범 사업의 경우 블록체인 기반의 DID 일변도이기에 표준화 시 기술 중립성 확보에 어려움이 있을 수 있다. 더욱 큰 문제는 국내 DID 사업의 경우 특정 기업들에 지나치게 의존적이며, 대부분 허가형(permissioned) 블록체인에 기반하고 있어 폐쇄적이라는 점이다[15].

Ⅳ. DID의 문제점 분석 연구

DID는 개인정보를 사용자의 단말기에 저장해, 개인정보 인증 시 필요한 정보만 골라서 제출하도록 해주는 전자신원증명 기술이다. 즉, 중앙 기관이 아닌 개인들이 자신의 데이터를 직접 관리하는 구조다. 따라서 기존 방식과 달리 서비스 이용 과정에서 모든 개인정보를 제공하지 않아도 되며, 각각의 사용자가

인증을 위해 꼭 필요한 정보만을 선택해 제출할 수 있는 장점이 있다. 이 장에서는 이와 같은 장점에도 불구하고 3장에서 제시한 DID의 전반적인 문제점에 대한 개선방안을 분석한다.

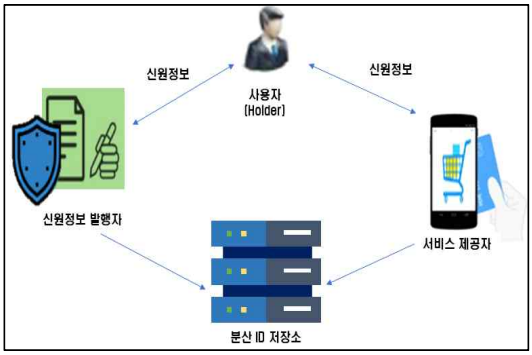
① 데이터 주권 한계

분산 네트워크 사용에 따른 탈중앙 구조와 신원정보에 대한 주권 및 프라이버시 강화에서 기대되는 데이터 주권이 현실에서 구현되기까지는 아직 넘어야 할 한계가 존재한다. 현실적으로 이 문제를 해결하기는 어렵기 때문에 DID 모델은 <그림 4>처럼 신뢰할 수 있는 제3의 중앙화된 신뢰기관으로 처리한다.

- 사용자가 서비스 제공자로부터 개인정보에 대한 인증 요청을 받으면 해당 내용을 인증할 수 있는 발행자에게 신원 확인 발행을 요청
- 발행자는 사용자가 적법한 권한을 가지고 있는지 확인 후 사용자에게 신원 확인을 발행하고, 발행과 관련된 사항을 분산 ID 저장소에 등록 및 서명
- 사용자는 신원 확인을 취득하고 발행자가 서명한 내용에 대해 Counter-sign을 수행함으로써 DID 키 생성
- 사용자는 서비스 제공자가 요구하는 수준의 정보를 정의한 Presentation을 생성하여 서비스 제공자에게 전달
- 서비스 제공자는 DID 키를 통해 분산 ID 저장소에서 해당 내용을 확인하고, 내용에 문제가 없을 경우 검증을 완료

② 기밀성과 무결성

블록체인 기반 DID는 특정 노드가 임의로 정보를 조작하는 것을 불가능하게 함으로써 정보 무결성을 유지하고 P2P 네트워크를 통한 완전한 정보 공유로 특정 노드에 대한 외부로부터의 해킹 시도를 무력화



<그림 4> 자기주권신원 흐름도

시킴으로써, 아래 <표 1>과 같이 5가지 사항에 대한 기밀성 및 무결성을 확보하는 기술이다.

<표 1> 기밀성과 무결성 개선방안

문제점	개선방안
기밀성과 무결성	▪ 지속성 확보:외부적 요인으로 인한 서비스 운영 중지에도 유효성 유지가 필요 ▪ 독립성 확보:특정기관이 아닌 피어(peer) 기반으로 독립성 확보 ▪ 휴대성 확보:필요 시 언제든 사용자의 스마트폰을 이용하여 신원정보를 선택하여 서비스 제공자에게 제공하는 휴대성 확보 ▪ 개인정보 보호:개인정보가 포함된 신원정보는 암호화 등의 조치를 수행하거나 분산 원장 밖에서 저장 가능 ▪ 확장성 확보:금융권 이외의 디지털 신원 확인을 위해 표준에 근거한 확장성 확보

③ 개인정보 과실

하드웨어 보안 모듈 (HSM : Hardware Security Module)이 DID에서 발생할 수 있는 개인 키에 대한 분실, 도난 등에 대한 유일한 해결책이며, <표 2>의 HSM은 암호의 핵심인 암호키에 관련된 두 가지 기능을 제공하는 전용 H/W 장비다.

HSM 장비는 강력한 암호키를 생성하고, 암호키를 안전하게 보관하는 전용 장비다. 또한, 신원 및 거래의 신뢰성을 보장함으로써 신원도용, 사기, 문서위조를 방지하고 있다. 이러한 변화에 있어서 DID 기술

<표 2> 단말기(개인 키) 분실을 위한 HSM 해결방안

문제점	해결방안
개인정보 과실	▪ 보안 모듈(HSM)을 이용한 도난, 분실 예방 ▪ 노이즈를 소스로 하여 난수를 발생하는 기능 ▪ 탈취를 위한 아래와 같은 2가지 공격에 대한 방어 기능을 지원 네트워크를 통한 사이버 공격을 방어하기 위해 전용 OS와 전용 SW를 사용-공격 시도 시 보관 중인 암호키를 스스로 파기하는 기능

발전이 긍정적으로 잘 적용되고, 블록체인의 가장 큰 개인정보의 보안 이슈를 HSM 기술이 해결할 수 있다.

④ 기술 표준화

DID 시장은 분명 성장 가능성이 높은 시장이지만 기술 구현을 위한 구체적인 체계가 잡혀있지 않다. 시스템의 한 부분으로만 생각할 뿐 생태계적 관점에서는 충분한 고민이 없는 상태다. 특히 각 서비스별로 모바일 신분증을 제각각 발급하는 해프닝이 벌어질 수 있다. 외국의 경우에는 비트코인 철학과도 일치하는, 오픈소스(open source), 개방형(public), 비허가형(permissionless)의 설계 원칙하에 개발되고 있어, 어떤 중앙화된 주체나 신뢰할 수 있는 중개인 없이도 독립적으로 운영될 수 있으며 무한한 글로벌 확장성을 제공하고 있다. 하지만 아직까지 국내 표준화 작업이 이뤄지지 않고, 해외 표준에 의존하기 때문에 기술 표준 확립, 제도 마련, 생태계 구축, 편리한 사용성 등이 미흡한 실정이다. 데이터의 안전한 활용이 강조되는 4차 산업혁명 시대에 DID나 블록체인에 대한 정부나 기업의 관심은 환영할 만한 일이다. 그러나 그렇다고 해서 특정 기술이나 기업에 지나치게 의존한다거나 정부가 과도하게 관여하는 것은 곤란하다. 디지털 시대의 중심은 데이터다. 그리고 데이터의 중심이 기관에서 개인으로 이동하고 있다. 서비스 제공자 중심으로 만들어진 기존의 비즈니스 모델은 개별 사용자 중심으로 개편될 것이다. 사회의 패러다임이 전환되고 있는 것인데, 이런 큰 변화 속에는 반드시 기회가 존재한다. 전 세계 시스템을 하나로 통일하는 건 어렵겠지만, 따라서 <그림 5>처럼 핵심적인 기능들에 대한 표준화 작업은 필요하다.

<그림 5> DID 기술 표준화

Ⅴ. 결론 및 향후 연구방향

DID가 탈중앙 신원증명으로 개인이 스스로 신원정보를 생성 및 관리할 수 있다는 장점이 있지만, 아직까지 서비스가 안정화되기에는 풀어야 할 과제들이 있다. 즉, 공인인증서의 고질적인 문제였던 공급자 중심 구성으로 인한 사용자의 불편함을 획기적으로 개선해야 하는 편의성과 범용성 확보와 DID가 사용자에게 신원정보에 대한 자기 통제권 및 데이터 주권을 확실히 돌려준다는 사용자 인식 개선이 필요하다는 것이다. 본 연구에서는 최근 핫이슈가 되고 있는 DID의 문제점을 분석하고 그에 대응하는 연구를 진행하였다. 본 연구에서 제언한 DID 분석이 개인의 신원관리시스템을 구현하고, 탈중앙 신원증명의 가이드라인을 제시함으로써 DID 기술 활성화에 실질적인 도움을 줄 수 있을 것으로 기대한다. 향후 연구로는 DID가 블록체인 기반이기 때문에 탈중앙성, 투명성, 불변성, 가용성의 기술적 특성을 제공한다. 그렇기에

블록체인 기반 DID의 경우, 신분증의 위조 방지에는 강점을 보이는 반면, 신분증 상에 기록된 개인정보의 노출에는 취약하다. 이러한 문제를 해결하고 필요한 최소한의 개인정보만을 노출 조건을 충족시키기 위해, 블록체인 기반 DID 이외에도 영지식을 추가하는 기법을 제안할 계획이다.

참고문헌

[1] H.S KIM, “Blockchain-based distributed identification technology trend,” KIICE, JUN. 2019.

[2] Luniverse, The sovereignty of my data is to me, Jul. 2020.

[3] Blockchain Research, Blockchain-based DID security and limitations, Jan. 2019.

[4] Coscom, Decentralized identification (DID), data sovereignty rests with individuals, Nov. 2019.

[5] Asiae, What’s wrong with the domestic DID mobile ID business?, Sep. 2020.

[6] The Science Times, DID emerges as a future identification technology, Feb. 2020.

[7] 전은아, “블록체인 기술 및 보안 위협 분석”, 디지털산업정보학회 논문지, 제14권, 제4호, 2018년, pp.47~56.

[8] Identity (ID) concept and overseas technology development trend, FSI, Apr. 2019.

[9] Digital Identity, Easy Guide to Distributed ID, Jul. 2019.

[10] Blotter, DID as a blockchain relief pitcher, Sep. 2020.

[11] 최희식·조양현, “블록체인 안전성 확보를 위한 거래 검토,” 디지털산업정보학회, 제15권, 제1호, 2019년, pp.77~86.

[12] KEM, Homework DID needs to solve, Jul. 2020.

[13] Hs-itl, Decentralized identification (DID), features and problems to solve?, Aug. 2020.

[14] Hankyung, DID (decentralized identification) homework, Jul. 2020.

[15] IT-Chosun, DID commercialization, a long way to go...The MSIT puts hands on technology standardization, Feb. 2020.

■ 저자소개 ■

이 광 규
(Lee, Kwangkyu)

1996년 3월~현재 신한대학교 컴퓨터공학전공 교수
2002년 8월 충북대학교 컴퓨터과학과 (이학박사)
1991년 2월 동국대학교 수학과(이학석사)
1985년 2월 동국대학교 수학과(이학사)

관심분야 : 인공지능, 빅데이터, 블록체인, 정보보안
E-mail : kklee@shinhan.ac.kr:

논문접수일 : 2022년 7월 28일
수 정 일 : 2022년 8월 18일
게재확정일 : 2022년 9월 4일