정 보 보 호 학 회 지
제 34 권 제1호, 2024. 2

국내 디지털 지갑 간 상호운용을 위한 기술적·정책적 고려사항

이 강 효*, 유 주 열**, 김 경 백***

요 약

디지털 전환이 가속화되면서 다양한 형태의 디지털 지갑이 등장하고 있다. 디지털 지갑은 이용자의 신원을 보장하고 안전하게 정보를 보관하며, 온·오프라인에서 모두 활용 가능해야 한다. 특히, 블록체인, DID, 비블록체인 디지털 지갑 간 상호운용성이 중요하며, 이를 위해 정책적·제도적 준비와 기술 발전이 필요하다. 디지털 지갑의 상호운용성을 보장하기 위해 기술적 요소 외에도 정책적인 요소를 고려해야 한다. 이를 위해 다양한 분야의 전문가들과 함께 관련 연구와 기술 표준을 마련해야 한다. 본 논문에서는 디지털 지갑 간의 상호운용성을 확보하고 서비스 생태계를 활성화하기 위해 필요한 기술적, 정책적 관점의 고려사항을 살펴보고자 한다.

Ⅰ. 서 론

최근 디지털 전환이 가속화됨에 따라 기존 실물 지갑이 디지털 지갑(Digital Wallet)으로 전환됨에 따라 현금 소지, 지불·결제뿐만 아니라 각종 신분증, 결제용 카드, 필수 정보, 문서를 안전하게 보관하고 이용하는 서비스가 점차 늘어나고 있다.

특히, 디지털 지갑은 국내외에서 다양한 형태로 제공되고 있으며, 그 형태와 기능은 소비자의 다양한 요구사항에 따라 결정된다. 디지털 지갑 서비스를 구성하는 플랫폼 기술에 따라서 블록체인 지갑, DID (Decentralized ID) 지갑, 비블록체인 지갑으로 유형을 구분할 수 있다.

온·오프라인에서 모두 활용할 수 있는 디지털 지갑 서비스를 제공하기 위해서는 지갑 내에 담기는 데이터의 신뢰성과 정합성이 먼저 고려되어야 하며, 동시에 디지털 지갑을 사용하는 이용자의 신원이 보장되어야 한다. 또한, 이용자에게 편의성을 제공하기 위해서는 디지털 지갑의 유형과 관계없이 일관된 디지털 지갑 이용 경험을 제공해야 한다.

더욱이 4차 산업혁명과 함께 찾아온 온·오프라인의 경계와, 생산자와 소비자 등 모든 경계가 무너지는 빅블러 현상 속에서 데이터 자기주권의 중요성이 특히 강조되고 있다.

블록체인-비블록체인-DID 디지털 지갑 서비스 간 상호운용성을 제공하기 위해서는 국내외 정부정책 및 제도적 쟁점을 분석하고 기술의 발전 속도를 아우를 수 있는 종합적인 정책이 마련되어야 한다.

디지털 지갑 간의 상호운용성이 보장되는 경우, 효율적인 신원증명 및 데이터 활용 수단이 될 수 있다. 하지만, 디지털 지갑은 이용자 식별자 간의 호환성 부족, 디지털 지갑 상호운용성 기술표준 부재, 키 관리 및 복구방안 이슈 존재 등의 어려움을 가지고 있다.

이러한 어려움을 극복하고 기존 생태계를 파괴하지 않는 범위 내에서 디지털 지갑 생태계를 구축하고, 더 나아가 디지털 지갑 산업을 선도하기 위해서는 블록체인 관련 산·학·연 전문가들과 함께 정책적·제도적 관련 연구와 함께 기술 표준을 마련해야 한다.

본 논문의 구성은 2장에서 디지털 지갑의 정의 및 기능, 3장에서 디지털 지갑의 유형을 설명하고, 4장에서는 기술적 고려사항, 5장에서는 정책적 고려사항을 검토한 후, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 디지털 지갑의 정의 및 기능

디지털 지갑은 특정 기술이 적용된 서비스를 지칭

* 한국인터넷진흥원 블록체인정책팀, 전남대학교 정보보안협동과정 (선임연구원, kanghyo.lee@kisa.or.kr)
** 한국인터넷진흥원 블록체인정책팀 (팀장, jyyoo@kisa.or.kr)
*** 전남대학교 인공지능융합학과 (교수, 교신저자, kyungbaekkim@jnu.ac.kr)

하는 것이 아니다. 지갑 서비스 제공자가 구현하고자 하는 방식에 따라 개발한다. 이용자의 모바일 기기에 지갑 앱을 설치하는 어플리케이션 유형이나 데스크톱 또는 모바일 기기 등을 통해 원격으로 온라인 지갑 서비스에 접속하는 유형, 물리적 카드에 정보를 저장하는 스마트카드 등이 있다[1].

디지털 지갑은 금융거래를 기본 기능으로 제공하며, 이용자의 신분을 확인하고 인증하는 기능, 필요한 문서나 자료를 안전하게 보관하고 공유하는 기능, 그리고 전자서명을 통해 서비스를 신청하는 기능 등으로 구성될 수 있다. 이러한 기능들은 디지털 지갑이 단순히 금융거래를 처리하는 도구가 아니라 이용자가 디지털 생활을 간편하게 이용할 수 있도록 지원한다.

특히, 디지털 지갑은 국내외에서 다양한 형태로 제공되고 있으며, 그 형태와 기능은 소비자의 다양한 요구사항에 따라 결정된다. 국내의 경우 디지털 지갑은 주로 간편 결제 및 송금 기능을 중심으로 제공되며, 이용자는 일상적인 금융거래를 편리하게 수행할 수 있도록 지원하고 있다. 또 다른 형태의 디지털 지갑은 디지털 인증 기능을 강화하여 이용자의 신원을 보호한다. 이 경우 이용자는 중요한 데이터는 보호하고 최소한의 정보를 노출하여 보안성을 높인다. 그 외에도 일부 디지털 지갑은 블록체인 기반 서비스를 통해 가상자산의 관리와 거래를 지원한다. 이 경우 이용자는 새로운 디지털 경제 환경에서 자산을 관리하고 거래할 수 있다.

Ⅲ. 디지털 지갑의 유형

우리는 대형 포털, 은행 등에서 제공하는 디지털 지갑 서비스를 일상에서 사용하고 있다. 디지털 지갑은 서비스 플랫폼을 구성하는 기술에 따라서 디지털 지갑의 유형을 구분할 수 있다.

3.1. 블록체인 디지털 지갑

블록체인 디지털 지갑이란 가상자산을 포함한 블록체인 상의 정보와 상호작용이 가능하도록 지원하는 인터페이스이다. 디지털 지갑에 저장되어 있는 개인키를 통해 블록체인 상의 정보에 대한 접근이 가능하다[2]. 블록체인 디지털 지갑은 현실 세계의 지갑과는 다르게 지갑 내에 가상자산을 직접 보관하는 것이 아니다. 블록체인 네트워크는 이용자의 디지털 지갑 주소와 매핑되어 관리되는 가상자산의 잔액을 관리한다. 블록체인 디지털 지갑은 지갑 주소로 가상자산의 잔액을 불러와 이용자에게 보여준다.

블록체인에서 이용자의 지갑과 연결된 자산과 정보에 접근하고 통신하기 위해서는 지갑 내의 PKI(Public Key Infrastructure) 기반 개인키가 필수적이며, 이러한 이유로 일부 기술적 관점에서는 블록체인 디지털 지갑을 개인키를 보관하기 위한 자료구조라고 정의하기도 한다.

블록체인 기반 디지털 지갑은 디지털 자산을 안전하게 보관하고 관리하는 도구로, 이용자의 개인정보와 자산을 안전하게 저장하는 서비스이다. 이러한 디지털 지갑은 이용자에게 고유한 개인 키를 제공하여 해당 자산에 액세스하는 기능을 제공한다. 이 개인키는 무결성이 보장된 형태로 암호화되어 저장되며, 블록체인 기술을 활용하여 안전하게 관리된다.

블록체인 기술을 활용하기 때문에 디지털 지갑은 높은 수준의 보안을 제공한다. 블록체인은 탈중앙화된 시스템으로, 정보를 여러 노드에 분산 저장하여 외부 공격이나 변조를 방지한다. 또한, 모든 거래 내역은 블록체인상에 공개적으로 기록되어 검증된다.

주로 가상자산을 블록체인 디지털 지갑을 통해 보관하거나 전송하지만, 디지털 자산의 종류에 따라 대체불가능토큰(NFT, Non-Fungible Token)과 같은 다양한 토큰 및 기타 자산도 관리할 수 있다[3]. 블록체인을 활용한 디지털 지갑은 메타마스크, 코인베이스 월렛 등이 있다.

3.2. DID 디지털 지갑

디지털 인증이란 디지털화된 정보를 통해 본인확인, 금융거래, 온라인쇼핑 등의 경제·사회 활동 시 이용자의 신원에 관한 주장 및 검증 과정을 뜻한다. DID 디지털 지갑은 디지털 인증에 특화된 서비스이다. 블록체인 디지털 지갑과 동일한 구조를 갖지만, 개인키만 모바일 단말에 저장하는 블록체인 디지털 지갑과 다르게 개인키 외에도 신원정보, 자격정보 등의 검증가능한 증명서(VC, Verifiable Credential)를 모바일 단말에 보관한다는 점에서 차이점을 갖는다[4].

모바일 단말에 중요한 정보를 보관한다는 점에서 보안적 이슈가 있을 수 있으나, [표 1] 평가보증등급(EAL, Evaluation Assurance Level)과 같은 기준을 적용하여 신원정보의 안전한 단말에만 발급하거나, 단말

〔표 1〕 평가보증등급(Evaluation Assurance Level)

구분	보증내용	평가노력(기간, 전문성, 비용)		
		범위	상세	엄격
EAL1	위협이 심각하지 않은 경우, 기초 수준의 보증	· 보안기능&보안 지원관련 인터페이스 확인	· 요구사항 분석 · 인터페이스 분석	· 기본 공격수준 취약성 조사
EAL2	개발문서가 충분하지 않은 旣 제품, 최소 보증	· TSFI 확인 · 평가자 독립시험	· 서브시스템 분석	· 설계문서 기반 취약성 분석
EAL3	개발방법론 변경 없이 기존 제품에 중간 수준의 보증	· 보안지원&비보안관련 인터페이스 행동 요약정보 확인	· 서브시스템 시험	· 설계문서 기반 취약성 분석
EAL4	개발방법론을 엄격히 적용한 제품에 높은 수준의 보증	· 인터페이스 호출오류메시지 확인 · 일부 소스코드 분석 · 보안모듈 시험	· 모듈분석 · 소스코드 분석 · 모듈 시험검증	· 강화된-기본 공격 수준 취약성 조사
EAL5	전문적인 보안공학기법 적용없이 상용 개발 방법론으로 얻을 수 있는 최대 수준의 보증	· 인터페이스 호출 이외 원인에 의한 오류 메시지 확인 · 전체모듈 시험 · 일부 모듈 복잡도 분석	· 응집도 검증 · 결합도 검증 · 코딩표준 검증	· TSFI & 서브시스템 준정형 검증 · 중간 공격수준의 취약성 조사
EAL6	전문적인 보안공학기법이 추가된 개발방법론을 적용한 제품에 높은 수준의 보증	· 전체 소스코드 분석 · 전체 모듈 복잡도 분석	· 응집도 검증 · 결합도 검증 · 코딩표준 검증	· 모듈 준정형 검증 · 높은 공격수준의 취약성 조사
EAL7	위험이 극도로 높거나 자산 가치가 높은 경우 최대 수준의 보증	· 모든 오류메시지 확인 전체 범위 평가자 독립시험	· 소스코드 시험	· 서브시스템 정형검증

또는 저장소의 안전성에 따라 저장하는 VC의 종류를 다르게 하는 등의 정책을 활용하여 보안성을 강화할 수 있다.

대표적인 사례는 행정안전부의 모바일 운전면허증이 있다[5]. 모바일 신분증으로써 실물 신분증과 동일한 법적효력을 가진다. 이용자 단말에 신분증을 보관하고 있다가 신원증명 시 필요한 정보만 골라서 제출한다. 금융결제원의 뱅크사인은 DID 기반 신원증명 플랫폼으로 전환하였으며, 기존 뱅크사인 외에 서민금융기관, 금융투자사 등 참여기관을 확대했다. 병무청은 블록체인 군인자격증명을 플랫폼에 탑재하여 군장병을 위한 금융서비스의 비대면 가입을 지원한다.

3.3. 비블록체인 디지털 지갑

민간 산업에서는 마이데이터가 화두가 되며, 하나의 앱에서 데이터를 보관하고 관리해야 하는 필요성이 부각되고 있다. 대형 포털 또는 은행에서는 플랫폼의 경쟁력을 확보하고자 디지털 지갑 형태의 비즈니스 모델을 채택하고 있다. 비블록체인 디지털 지갑에서도 본인확인, 증명서 제출을 포함하여 결제까지 다양한 서비스를 제공하고 있으나, 이용자 모바일 단말을 기반으로 중앙화된 시스템에서 발급한 사설인증서를 기본으로 설계되었다는 점에서 차이점을 보인다.

일반 디지털 지갑의 사설인증서는 휴대폰 또는 카드 본인확인, 계좌확인 등 비대면 인증 방식을 통한 신원확인 과정을 거친 후 발급된다. 또한, 타 플랫폼에서는 별도의 인증서를 발급받아야 이용할 수 있다.

비블록체인 지갑 서비스는 간편결제와 간편송금을 주요 서비스로 제공한다. 간편결제란 모바일에 신용카드, 은행 계좌 정보 등을 이용자가 미리 저장해둔 뒤, 결제 시 비밀번호 입력 혹은 단말기 접촉 등과 같은 방법으로 결제하는 방식을 뜻한다. 간편송금은 계좌이체 등의 방식으로 충전한 선불금을 전화번호, SNS 등을 활용해 송금하는 서비스를 뜻한다.

온라인 결제 서비스의 예시는 네이버페이, 페이팔(PayPal), 구글페이 등이 있으며, 오프라인 결제 서비스의 예시는 삼성페이, 애플페이 등이 대표적이다. 간편송금의 예시는 비바리퍼블리카의 토스, 카카오페이의 카카오페이 등이 대표적이다.

Ⅳ. 디지털 지갑의 기술적 고려사항

온·오프라인에서 모두 활용할 수 있는 디지털 지갑 서비스를 제공하기 위해서는 지갑 내에 담기는 데이터의 신뢰성과 정합성이 먼저 고려되어야 하며 동시에 디지털 지갑을 사용하는 이용자의 신원이 보장되어야 한다. 또한, 이용자에게 편의성을 제공하기 위해서는 디지털 지갑의 유형과 관계없이 일관된 이용경험을 제공해야 한다.

〔표 2〕 디지털 지갑 주요 식별자

구분		식별자	형식	예시
비블록체인 지갑	공공	주민등록번호	6digit-7digit	123456-7891012
	민간	연계정보	88 Byte Hash Message	yCP3v5vRAX9GVCSmHQozi5Utjzglzq ZIC3lGRqrdzrfJz41S0M6yxB5i7eKLgo6WGXlJ5r7hWGouc1/SBajMw==
블록체인 지갑		지갑주소	0x〔40 letters and numbers〕	0x002d3f1ef827552ae1112047bd3ecf1f086ba0f1
DID 지갑		DID 식별자	〔scheme〕:〔DID method〕:〔DID Method-Specific Identifier〕	did:example:123456789abcdefghi

4.1. 호환가능한 이용자 식별자

주민등록번호(RRN, Resident Registration Number), 연계정보(CI, Connecting Information)는 사람을 식별하기 위한 목적으로 국내에서 사용되는 식별자이다. 연계정보는 주민등록번호를 기반으로 88바이트의 해시기반 메시지 인증번호이며, 사전에 공유한 SecretKey 값의 보안수준만큼의 보안성을 가진다[6]. 해당 정보는 이용자가 다른 서비스 간의 동일인임을 식별하기 위해 사용한다.

이런 기존 식별체계로는 사물인터넷, 메타버스 등 사물과 콘텐츠, 서비스를 식별하기에는 한계를 가진다. 이런 면에서 DID 식별자는 사람 이외의 사물과 컨텐츠, 서비스 등을 특정하기 위해 식별번호를 부여할 수 있다는 장점을 가진다.

식별번호를 부여하는 관점에서의 활용성을 논하자면 기존 식별체계보다 DID 식별 범위가 크다. 또한, 정부의 모바일 신분증, 백신접종증명서 등의 DID 서비스가 점차 도입되고 있다. 공공분야의 고가치의 데이터를 민간에서 활용하기 위해서는 DID 식별자를 우선적으로 연계할 수 있는 방안이 고려되어야 한다.

정부에서 발급한 DID 기반의 VC를 이용하여 디지털 지갑에 사설인증서, 졸업증명서, 자격증 정보 등의 데이터를 적재하게 된다면, 해당 정보들 또한 서비스 및 데이터의 원천이 되는 VC 수준의 신뢰성을 보장할 수 있다. 또한, 공공영역의 VC에 변동상황이 발생하는 경우 정부에서 운영하는 분산원장에 데이터의 변동 여부를 기록하게 되어있으며, 민간에서는 해당 읽기 노드 조회를 통해 이용자 데이터 변동을 확인하고, 이용자에게 이용자 정보 수정 또는 VP(Verifiable Presentation) 재제출을 요청할 수 있다.

사설인증서를 기반으로 디지털 지갑을 서비스하는 민간에서는 본인확인을 위해 카드, 휴대폰 인증 등 부가적인 인증을 활용해왔다. 사설인증서 발급을 위한 본인확인 절차를 DID 디지털 지갑 기반의 신원증명으로 전환하기 위해서 시스템의 큰 변화 없이, 정부 모바일 신분증 SDK/API 연동을 통해 사설인증서의 본인확인 절차를 대체할 수 있다. 연동방식은 플랫폼 사의 정책에 따라 달라질 수 있으나, 정부 모바일 신분증 앱과 민간 플랫폼 앱/웹 등 UX 관점에서도 손쉬운 연계 및 도입을 할 수 있다. 전환 시 시나리오를 살펴보자면, 중계기관은 공공분야 서비스 제공 전 이용자로부터 최초에 DID 식별자 정보를 전달받는다. 이 식별자는 주민등록번호와 맵핑한 후 해당 DID 식별자를 가지는 디지털 지갑에만 정부의 신분증, 증명서를 제공한다. 민간분야의 경우, 중계기관은 공공과 같은 방법으로 최초 서비스 이용시 CI와 DID 맵핑 데이터를 생성한다[7].

공공-민간 서비스 간 공통 식별자로 DID를 활용함으로써 분야와 관계없이 신분증, 증명서를 검증할 수 있다. 식별자 맵핑 데이터는 중요데이터로 분류하여 중계기관만이 관리하며 외부에서 확인할 수 없다.

4.2. 상호운용성 기술표준

상호운용성이란 하나의 시스템이 기술적 특성으로 인한 차이에 관계없이 동일하거나 이종의 다른 시스템과 서비스의 공유 및 정보교환이 자유롭게 가능한 것을 의미한다. 블록체인 간 직접적으로 연계하여 상호운용성을 보장하기 위해서는 타 블록체인에 실제로 자산 또는 데이터가 존재한다는 것을 효과적으로 증명할 수 있어야 한다.

대표적으로는 사이드체인과 릴레이 방식을 결합하여 블록체인 A의 스마트 컨트랙트가 블록체인 B의 SPV(Simplified Payment Verification) 노드 역할을 수행하는 방식 등이 있으나, 타 검증자가 옳은 정보를

제공해야 하므로 특성이 다른 CBCP(Cross Blockchain Communication Protocol) 환경에서는 활용이 어렵다. 현존하는 블록체인 상호운용성 기술 중 소스체인의 트랜잭션을 통해 타겟체인에서 실행하는 기술들은 전부 CCCP(Cross Chain Communication Protocol)가 적용 가능한 블록체인들을 대상으로 하고 있다.

블록체인 지갑 ↔ DID 지갑, DID 지갑 ↔ DID 지갑, DID 지갑 ↔ 비블록체인 지갑 간의 상호접속 수준의 상호운용성을 보장하기 위해서는 구체적인 수준의 지갑 아키텍처, 개인 키 관리 체계, VC 저장소, 복수의 DID 간의 상호관계, 지갑 간 인터페이스 현황 등을 정리한 표준이 마련되어야 한다.

또한, 비블록체인 디지털 지갑은 블록체인과는 동떨어져 구성되어 있다. DID VC의 Claim에 속하는 데이터들 또한 문자열(String)로 관리되고 있으며, 취급하는 데이터는 사설인증서로 DID VC와는 차이점을 보인다. 간접적 상호운용성, 즉 비블록체인-DID-블록체인 상호접속 서비스를 제공하기 위해서는 디지털 지갑을 수단으로써 최소한의 데이터 및 연계 인터페이스 표준의 정립이 필요하다.

4.3. 키 관리 및 복구방안

디지털 지갑 서비스는 공공성을 위해서 이용자의 단말기에서 공개키, 개인키, DID 관련 정보, 디지털인증서 관련 정보 등을 안전한 저장 서비스 또는 보안 솔루션에 저장해야 한다. 이용자 개인키는 블록체인 내 트랜잭션을 생성하기 위해서 필수적으로 보유하고 있어야 하므로 개인키의 분실은 블록체인 서비스 사용 불가의 문제로 이어진다. 개인의 개인키 관리를 위해 디지털 지갑 서비스를 활용하여 개인키의 관리를 투명하게 하고 암호학적 설계나 불법 사용에 대한 방지 대책도 필수적으로 포함해야 한다. 이용자는 개인키를 분실하였을 때 디지털 지갑 서비스에서 제공하는 복구 기능으로 개인키를 복구할 수 있어야 한다.

블록체인 및 DID 디지털 지갑은 이용자가 개인키를 직접 관리하는 지갑으로, 블록체인 지갑의 구조적 한계로 개인키를 복구하기 어려워 분실에 대한 이슈가 존재한다. 반면, 비블록체인 지갑은 특정 기관, 기업에서 이용자의 개인키를 관리해주는 지갑으로, 이용자가 개인키 또는 개인키에 접근하기 위한 비밀번호를 분실해도 대처가 가능하다. 다만, 특정 기관/기업을 전적으로 신뢰해야 하며, 여러 사람의 개인키가 중앙형 저장소에 저장되어 있어 공격이나 내부자 유출 등의 이슈

〔표 3〕 모바일 단말 제조사 별 보안 솔루션 기술현황

구분	Android OS(삼성전자)			iOS(애플)
	TEE(Trust Zone)	eSE(Secure Element)	Strong Box	SEP(Secure Enclave Processor)
개요	일반 저장소와 논리적으로 구분된 보안영역 제공	일반 저장소와 물리적으로 구분된 보안영역 제공		일반 저장소와 논리적으로 구분된 보안영역 제공
지원단말	Knox가 탑재 모든 단말	S21, S20 및 중저가모델(A시리즈)	S20 이후 플래그쉽 모델	iOS 8 이상 탑재 단말
저장위치	보안영역 內 TA 저장소에 저장	보안영역 內 TA 저장소에 저장	별도 Chip 內 저장	App에 할당된 저장소에 저장
저장방법	TZ 內 암호화 처리 및 저장	eSE Key로 암호화 처리 후 TZ에 저장	StrongBox 內 암호화 처리 및 저장	SEP 內 암호화 처리 및 저장
Crypto Lib. support	Android Keystore, 자체구현 알고리즘	자체구현 알고리즘	Android Keystore Only	SEP Keychain, 자체구현 알고리즘
	Android Keystore, iOS Keychain에서 블록체인에서 사용되는 알고리즘을 지원하지 않음			
HW 분리여부 및 방법	X	O	O	O
	-	별도 Chip 사용 Processor, Memory 동일	별도 Chip 사용 Processor, Memory 분리	동일 Chip 사용 Processor 분리
보안등급	EAL 2+	EAL 5	EAL4+(S20), EAL5+(S21)	FIPS 140-1,2
적용모델	삼성페이, KB국민은행 간편인증 서비스, 카카오 간편인증서	-	-	애플페이

가 존재한다.

블록체인 디지털 지갑은 키 관리에 대한 이슈가 지속적으로 제기되어 왔으며, DID 디지털 지갑의 경우 모바일 단말에 VC를 보관하는 만큼 보안 또한 중요하다. [표 3]과 같이 신뢰실행환경(TEE, Trusted Execution Environment), Strong Box, SEP(Secure Enclave Processor) 등 다양한 저장소가 존재하지만 이용자가 단말 또는 개인키 접근 패스워드를 분실하는 경우 복구가 불가능하다.

상호운용이 가능한 지갑의 설계 시, 비밀 분산, MPC(Multi-Party Computation) 등 다양한 방안을 활용하여 키 분실, 단말 분실에 대한 복구 방안을 제공해야 하며, 분실 시 별도 신고를 통해 발행된 VC 활용이 중지될 수 있는 절차를 마련해야 한다.

DID 디지털 지갑의 상호운용성을 보장하기 위해서는 디지털 지갑 내에 신원정보를 비롯하여 다양한 이용자들의 개인정보를 모바일 단말에 보관하고 있어야 한다. 또한, 디지털 지갑의 경우 간접적 상호운용성, 즉 상호접속 서비스의 핵심이므로 다양한 공격의 매개가 될 수 있으며, 이를 선제적으로 고려하여 데이터의 중요도에 따라 저장소를 구분하는 등 보안 이슈에 대한 충분한 고려가 필요하다.

Ⅴ. 디지털 지갑의 정책적 고려사항

4차 산업혁명과 함께 찾아온 온오프라인의 경계와 생산자와 소비자 등 모든 것의 경계가 무너지는 빅블러 현상 속에서 자기주권과 DID의 중요성이 강조되고 있으며, 블록체인-DID-비블록체인 디지털 지갑 서비스 간 상호운용성 제공을 위해서는 무엇보다도 정책 및 제도적 쟁점을 분석하고 이를 통한 기술의 발전 속도를 아우를 수 있는 제도적 준비가 필요하다.

5.1. 디지털 지갑 서비스 간 사업영역 침해

디지털 지갑의 상호운용성을 제공하기 위해서는 신원증명이 필수적으로 요구된다. 정부에서 발급하는 모바일 운전면허증은 온라인에서의 신분증 역할을 수행할 수 있어, 지금까지 온라인에서 신분증을 대체해온 본인확인시장을 침해할 수 있다는 우려도 존재한다. 이는 기존 신분증을 제출해야 하는 높은 수준의 실지명의를 요구하는 서비스에 한해서 디지털 지갑 서비스를 제공해야 한다. 더욱이 우리나라는 ‘20년 12월 기준으로 공인전자서명제도 폐지와 함께 시행된 전자서명법 개정안으로 인해 사설인증 시장이 빠르게 성장하고 있으며, ’24년 2월 기준으로 22개 전자서명인증사업자가 있으며, 해당 사업자들의 서비스 모델, 이용규모에 따라 보호하거나 연계하는 조치가 필요하다.

공공영역에서는 정부 발급 신분증을 이용한 신원증명 의무화를 적용할 수 있으나, 최소한 민간시장에서 정부의 신원증명 증명서를 활용한 사설인증서를 발급하게 하고, 사설인증서의 LDAP(Lightweight Directory Access Protocol)으로 DID 신분증의 분산원장을 활용하게 하는 등 상생을 위한 정책적 수단이 마련되어야 한다.

디지털 지갑의 상호운용성을 제공하기 위해서는 블록체인 사업자, 디지털 지갑 사업자, 전자서명인증사업자, 본인확인기관 등 다양한 이해관계자 간의 사회적 합의가 필요하다. 각 시스템 별로 상이한 기술 규격을 조정하고, 지갑 서비스의 보안 수준에 따라 사용분야와 역할을 구분해야한다. 정부는 사업자들의 공감대를 형성하고 합의를 확보하기 위한 정책 마련 및 표준 규격 지원 등의 노력이 필요하다.

5.2. 디지털 지갑 최소기능요건

디지털 지갑은 블록체인 서비스에서는 가장 핵심이 되는 기술이며, 블록체인 네트워크 확장성 관련된 기술의 성숙도가 높아지고 있는 지금 시점에서 가장 집중해야 할 기술 중 하나이다.

민간시장에서도 대부분의 플랫폼 사업자들이 모노호밍(Mono Homing)을 강화하고, 플랫폼 서비스의 영역을 확장하기 위해 디지털 지갑 형태의 사업 구조를 채택하고, 다양한 서비스를 연계 중이다.

블록체인 디지털 지갑과 비블록체인 디지털 지갑은 기술 규격이 상이하나 이용자의 신원정보, 개인정보를 기반으로 다양한 서비스를 제공한다는 점에서 유사하다. 또한, 블록체인, DID 서비스, 비블록체인 디지털 지갑은 디지털 지갑을 사용한다는 공통분모를 보유하고 있으므로 [표 4]와 같이 디지털 지갑의 유형과 관계없이 최소한의 기능 호환성을 제공하기 위해서 공통된 규격을 마련해야 한다.

〔표 4〕 디지털 지갑 최소기능요건

기능	기능 설명
지갑 생성	새로운 지갑을 생성하는 기능으로 이는 내부적으로 공개키, 개인키, 니모닉에 대한 생성을 의미한다. 다수의 지갑을 생성할 수 있도록 허용한다.
지갑 복구	개인키 혹은 니모닉을 통해 지갑을 복구한다.
개인키 커스터디	지갑에 대한 암호키(개인키, 니모닉) 관련 정보를 대신 보관해주는 기능이다.
지갑 활성화	사용하고자 하는 지갑을 활성화하기 위해서 지갑의 주소 또는 식별자를 사용가능하도록 허용한다.
지갑 비활성화	활성화된 지갑을 비활성화하여 네트워크 내 블록체인의 기능을 관련 지갑으로 사용하지 못하도록 한다.
암호화	지갑과 관련한 해시 함수, 암호화, 서명 등의 암호학적 도구 기능을 제공한다.

5.3. 국내·외 디지털 지갑 정책방안

유럽연합의 경우, EBSI(European Blockchain Service Infrastructure), eIDAS(Electronic IDentification, Authentication and trust Services) 등에서 디지털 지갑과 관련된 표준을 다루고 있고, 일부 디지털 지갑과 관련하여 구현 적합성 준수 여부를 점검하고 있다[8]. 이는 EBSI에서 구현한 블록체인 생태계와의 상호운용성을 점검하는 수준에 이른다. 또한, EU 집행위원회는 2030년까지 EU 시민의 80%가 디지털 지갑을 통해 공공서비스 접속, 증명서 발급 등 일상에서 사용할 수 있도록 디지털전환 정부 전략을 추진 중이다. 이는 공공-공공, 공공-민간, 온라인-오프라인 간 디지털 신분증과 증명서를 자유롭게 주고받는 생태계를 사전에 확보할 의도이다.

국내는 2018년부터 과학기술정보통신부를 통해 블록체인과 관련하여 다양한 시범사업과 기술검증 지원사업을 추진하는 등 전문기업 육성을 위해 노력해왔다. 하지만, 지원 예산의 규모와 사업의 숫자에 비해 지속해서 서비스 중인 사업의 절대적인 수는 부족하며, 개별적으로 구축되고 있다. 블록체인 플랫폼 또는 네트워크 구성의 차이점으로 상호운용성 제공이 어려운 상황이다. 현재 사일로(silo) 형태로 구축된 블록체인 및 DID 서비스의 상호운용성을 확보를 위해서는 디지털 지갑을 상호운용의 수단으로 활용할 수 있도록 장기적이고 체계적인 지원사업과 함께 정책, 연구 개발이 추진되어야 한다.

Ⅵ. 결 론

디지털 지갑은 블록체인 지갑, DID 지갑, 비블록체인 지갑 간의 상호운용성이 보장되는 경우, 강력한 온·오프라인에서의 신원증명 수단이 될 수 있다. 현재 금융권에서 사용되는 마이데이터 뿐만 아니라 이용자의 의료정보를 비롯한 모든 마이데이터가 DID 기반 디지털 지갑에 보관되어 정보의 자기주권강화 실현에 한발 다가설 수 있다. 또한, 디지털 지갑은 가상자산 커스터디 서비스, NFT, 분산자율조직(DAO, Decentralized Autonomous Organization) 등 블록체인 서비스와 연계되어 생태계 전반적으로 중심적인 역할을 수행할 수 있다. 사설인증서 발급을 위한 본인확인 절차로도 사용될 수 있으며, 민간의 비블록체인 지갑에는 이용자가 직접 발행자(Issuer)가 되어 정부로부터 발급받은 VC 내의 Claim 정보를 이용자 디지털 지갑에서 재발급하는 것도 가능할 것이다.

이처럼 디지털 지갑은 높은 활용도와 넓은 확장성을 보유하고 있는 빅블러 시대에 적합한 기술 중 하나이지만 본인확인 시장을 비롯하여 증명서 발급, 금융권 마이데이터 사업 등 기존에 구축되고 유지되고 있는 시장과 역할을 구분해야한다. 기존 생태계를 파괴하지 않는 범위 내에서 건전한 디지털 지갑 생태계를 구축하고, 디지털 지갑 산업을 선도하기 위해서는 블록체인 관련 산·학·연 전문가들과 함께 정책적·제도적 관련 연구와 함께 기술 표준을 마련해야 한다.

참 고 문 헌

[1] 이재성, 우성도, “디지털 지갑의 사이버보안 위협 및 보안 요구사항 분석”, *KISA Insight*, Dec. 2022.

[2] 윤태연, 문종섭, “블록체인 기반 서비스 환경에서의 개인키 백업 및 복원 프레임워크”, *디지털콘텐츠학회논문지*, 20(12), pp.2485-2493 Dec. 2019.

[3] 권혁준, 임민수, 김협, “NFT의 거래 가능성 및 확장성에 대한 고찰 -대체거래소 연계를 중심으로-”, *한국지급결제학회지*, 13(1), pp. 257-272, Jan. 2021.

[4] 임승주, 김기형, “자기주권신원에 기반한 검증 가능

한 자격증명의 안전한 위임 기법", *한국통신학회논문지*, 47(4), pp.656-662. Apr. 2022.

[5] 양희선, 이강효, 이종혁, "블록체인 모바일 운전면허증 표준 소개", *대한전자공학회지*, 49(1), pp. 35-51, Jan. 2022.

[6] 이강효, 윤여준, 이중엽, 민경식, "분산ID(DID) 확산을 저해하는 문제점에 관한 연구", *한국통신학회 학술대회논문지*, pp.96-97, Feb. 2020.

[7] 이강효, 박소현, 김현준, 하태균, 유주열, 김경백, "분산신원증명(DID)과 공개 키 기반(PKI) 간 상호운용가능한 신뢰연결 프레임워크 기본모델 제안", *한국통신학회논문지*, 47(10), Oct. 2022.

[8] 김근형, "탈중앙 메타버스에서 자기주권 신원확인을 위한 OpenID Connect와 eIDAS 2.0 기술 동향", *한국통신학회지*, 41(1), Dec. 2023.

〈저 자 소 개〉

이 강 효 (Kanghyo Lee)

정회원

2014년 2월 : 한양대학교 ERICA 컴퓨터공학과 졸업
2016년 8월 : 한양대학교 일반대학원 컴퓨터공학과 석사
2021년 3월~현재 : 전남대학교 정보보안협동과정 박사과정
2017년 4월~현재 : 한국인터넷진흥원 근무
<관심분야> 블록체인, 클라우드, 정보보안

유 주 열 (Yoo Joo Yeol)

2005년 2월 : 세종대학교 정보통신공학과 졸업
2015년 8월 : 아주대학교 정보통신공학과 석사
2018년 2월 : 숭실대학교 IT정책경영학과 박사
2006년 12월~현재 : 한국인터넷진흥원 근무
<관심분야> 블록체인, 네트워크, 개인정보

김 경 백 (Kyungbaek Kim)

종신회원

1999년 2월 : 한국과학기술원 전기 및 전자공학과 졸업
2001년 2월 : 한국과학기술원 전기 및 전자공학과 석사
2007년 2월 : 한국과학기술원 전기 및 전자공학과 박사
2007년~2011년 : University of California Irvine, 박사 후 연구원
2012년~현재 : 전남대학교 소프트웨어공학과 교수
2021년~현재 : 전남대학교 인공지능융합학과 교수
<관심분야> 분산시스템, 소프트웨어 정의 인프라스트럭쳐, 빅데이터 플랫폼, AI기반 CPS, 재난대응시스템, 정보보안, 블록체인