신뢰적인 웹 3.0 생태계를 위한 탈중앙화 신원증명 기술 동향

김근형
동의대학교

요 약

최근 여러 이유로 활발하게 논의되고 있는 웹 3.0은 신뢰성, 투명성, 탈중앙화, 디지털 자산의 자기주권 보장을 특징으로 한다. 이런 특징을 기반한 웹 3.0 생태계는 사용자 중심의 데이터 경제 생태계로 진화할 것이다. 따라서 사용자가 개인정보를 직접 관리하는 탈중앙화 신원증명이 중요해졌다. 본고에서는 특정 서비스나 플랫폼에 종속되지 않고 사용자가 자신의 신원정보와 디지털 자격증명을 소유하고 신원 및 자격을 증명하는데 필요한 정보만을 제시하여 개인정보를 보호할 수 있는 탈중앙화 신원증명 기술을 살펴본다. 그리고 웹 3.0 생태계에서 신뢰적인 관계가 없는 주체가 상호 인증하고, 신뢰적인 통신 채널을 설정하는 기술과 탈중앙화 신원증명에 대해 논의하는 커뮤니티 활동을 살펴본다.

Ⅰ. 서 론

일방적인 콘텐츠의 전달과 열람이 특징인 웹 1.0 생태계와 비교하여 진보된 차세대 웹으로 등장한 웹 2.0생태계에서는 사용자가 직접 콘텐츠를 생산하고 양방향 소통이 가능한 웹 커뮤니케이션이 본격화되었다. 웹 2.0 개념은 2004년 처음으로 논의되었다. Tim O'Reilly는 웹 2.0의 특징을 플랫폼으로의 웹, 집단지성 활용, 차별화 요소로서의 데이터, 소프트웨어 배포 주기의 종말, 가벼운 프로그래밍 모델, 단일 디바이스를 넘어선 소프트웨어, 풍부한 사용자 경험의 7가지로 정의하였다[1].

웹 2.0을 표방한 기업들은 2000년 이후 사용자 정보를 중앙집중 형태로 모아 제공하는 정보 게이트웨이 역할을 시작하였다. 웹 2.0 생태계가 보편화되고 시장규모가 커짐에 따라 플랫폼 사업자는 시장 우월적 지위를 활용하여 개인 데이터의 독점과 오남용, 사용자와의 불공정 거래, 후발 기업의 시장 진입 제한 등 다양한 문제를 야기시키고 있다. 또한 개인의 신원정보와 사용자 참여로 생성된 데이터의 소유권을 플랫폼 사업자가 가지며 이를 기반으로 생성된 맞춤형 서비스 및 광고 수익을 플랫폼 사업자가 독점하는 수익배분 구조가 고착화되었다.

또한 사용자의 콘텐츠와 데이터에 대한 가치와 소유권이 정당하고 공정하게 인정되지 않았다. 이에 개인정보를 거대 플랫폼 사업자가 소유하고 활용하여 수익을 창출하는 플랫폼 경제체제에서 사용자가 중심이 되며 블록체인과 스마트 계약이 중심이 되는 프로토콜 경제체제로 전환되어야 한다.

블록체인 기반 탈중앙화 온라인 생태계인 웹 3.0생태계에서 개발된 탈중앙화 서비스는 플랫폼 사업자가 아닌 해당 서비스의 개발, 유지 및 관리에 참여하여 소유권에 대한 지분을 획득하는 사용자가 소유하게 된다. 웹 3.0 생태계가 보편화되면 "디지털 시대"라는 문구에 개방성, 신뢰성, 공정성, 탈중앙화, 자기주권 데이터라는 새로운 의미가 부여될 것이다. 즉 웹 3.0 생태계는 사용자의 데이터 및 개인정보가 플랫폼 사업자에 종속되지 않고 개인이 데이터와 개인정보를 소유하고 직접 보호하고 제어하는 탈중앙화 웹(decentralized web)의 구조를 가질 것이다.

본고에서는 탈 중앙화와 데이터의 자기주권을 보장하는 웹 3.0 생태계에서 개인의 신원정보와 개인정보를 보호하며 자격증명을 검증할 수 있는 기술 및 신원증명 기술을 활용한 신뢰할 수 있는 통신채널을 확보하는 기술과 탈중앙화 신원증명과 관련된 커뮤니티를 살펴본다.

Ⅱ. 웹 3.0 생태계

차세대 웹의 관점에서 웹 3.0이라는 용어는 1999년 팀 버너스 리가 웹의 비전으로 시맨틱 웹을 이야기하면서 언급되었다. 시맨틱 웹은 컴퓨터가 처리할 수 있는 데이터의 웹(Web of Data)의 의미를 가지며, 일상생활의 거래와 같은 사람들 간의 상호작용을 컴퓨터가 대신 해주는 지능형 에이전트의 출현을 가능하게 한다[2]. 디지털 전환으로 등장할 가상-물리-소셜 공간 〈그림 2〉에서 물리공간의 센서로 센싱된 데이터와 물리공간의 다양한 영역에서 생성된 디지털 데이터는 가상공간에 저장되고 시맨틱 웹과 인공지능 기술이 적용되어 목적에 맞게 처리된다. 이

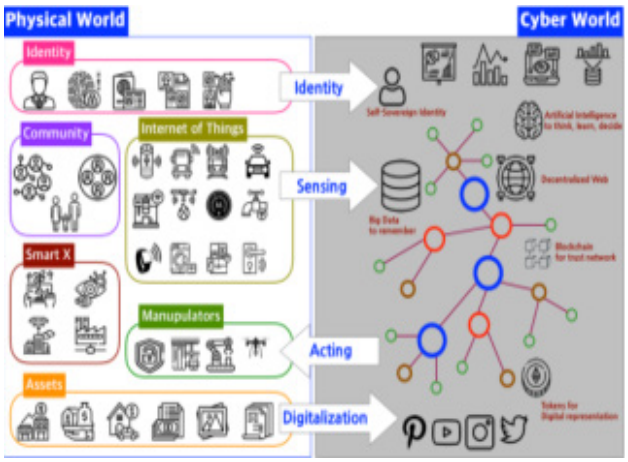

그림 1. 가상-물리-소셜 공간의 상호작용

러한 처리의 결과는 다시 물리공간의 객체를 제어하는데 활용할 수 있다.

그러므로 차세대 웹은 메타버스의 기반이 되는 가상-물리-소셜 공간의 신뢰적인 상호작용과 자동화의 기반이 되어야 한다. 예를 들면 가상공간의 내 아바타가 나를 대신하여 온라인 쇼핑몰을 찾아다니며 쇼핑몰의 아바타와 상호작용하여 원하는 조건으로 상품을 구입하게 되는 것이다.

참여와 공유가 주된 특징인 웹 2.0 생태계에서는 구글, 애플, 아마존, 메타, 트위터 등의 플랫폼 사업자가 사용자의 활동과 개인정보의 제어 및 활용을 독점하고 있어 사용자는 개인정보에 대한 제어를 할 수 없다. 이러한 폐쇄된 플랫폼 중심 웹의 문제를 해결하고자 2014년 팀 버너스 리는 WIRED와의 인터뷰에서 탈중앙화 웹(Decentralized Web)의 필요성을 언급하였다[3].

〈그림 2〉는 탈중앙화 웹의 애플리케이션 로직과 데이터가 분리된 구조로 데이터의 제어권을 사용자가 가지고 있어 데이터가 필요한 애플리케이션에 데이터를 무료로 제공하거나 판매할 수 있어 현재 중앙집중형 플랫폼의 애플리케이션이 사용자 데이터를 독점하는 문제를 해결할 수 있다.

현재 논의되고 있는 블록체인 기반 웹 3.0은 이더리움의 공동창업자인 개빈 우드가 2014년 처음 언급하였다. 개빈 우드는 웹 3.0을 블록체인 기반 탈중앙화 온라인 생태계로 정의하고 생태계를 구성하는 플랫폼과 애플리케이션을 중앙 집중형 플랫폼 사업자가 소유하지 않고 해당 애플리케이션의 개발 및 유지, 관리를 지원하고 소유권에 대한 지분을 획득한 사용자가 소유한다. 개빈 우드는 이더리움 네트워크에서 서로 신뢰관계가 없는 참여자가 상호 이익이 되도록 상호작용을 가능하게 하는 기술과 메신저 서비스를 융합하여 정보 흐름의 관리 및 권한 관리 서버를 사용하지 않고도 웹 2.0의 메신저 서비스를 구현할 수 있는 피어-투-피어 웹 환경을 웹 3.0 생태계의 기반이라 하였다[4]. 웹 3.0 생태계에서는 앞에서 살펴본 탈중앙화 웹 구조를 기반으로 사용자가 주고받는 정보, 지불하는 금액과 그 대가로 제공받는 것에 대해서 검증가능한 보증을 할 수 있도록 개인간 정보교환 및 금전 거래의 신뢰를 보장할 수 있는 프로토콜을 제공하여야 한다[5].

실리콘 밸리의 대표적 벤처 캐피탈(Venture Capital)인 a16z는 웹 2.0 생태계에서 거대 중앙 집중형 플랫폼 사업자가 플랫폼의 성장에 기여한 참여자에게 주는 보상이 공정하지 않은 문제가 있으며 이 문제의 해결책으로 웹 3.0을 제시하였다. a16z는 웹 3.0 생태계를 탈중앙화의 기반인 블록체인, 암호화 프로토콜, 디지털 자산, DeFi (Decentralized Finance), DAO (Decentralized Autonomous Organization) 등의 기술을 접목하여 만들어진 지속가능하고 신뢰적인 디지털 웹 환경으로 정의하였다[6].

최근 웹 3.0 생태계와 관련하여 여러 관점에서 다양한 용어(특성)가 논의되고 있다. 〈그림 3〉은 최근 웹 3.0을 정의할 때 논의

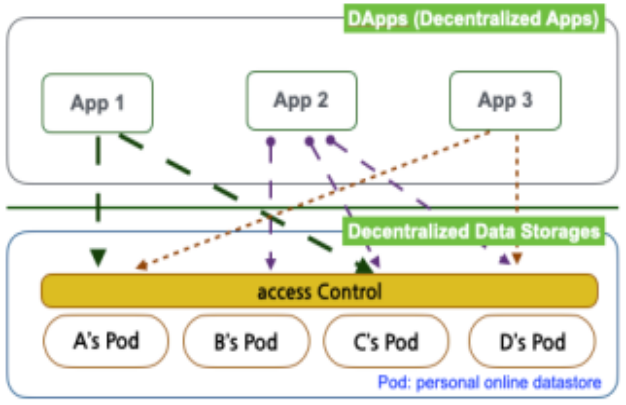

그림 2. 탈중앙화 웹 앱과 데이터의 분리 모습.

그림 3. 웹 3.0 생태계 관련 용어(특성)

되고 있는 핵심 용어들이다. 웹 3.0 생태계의 서비스 제공구조는 개인의 자율성과 소유권을 보장하고 개인 간 신뢰적인 거래를 보장할 수 있도록 진화할 것이다. 이는 물리공간의 많은 데이터가 디지털 전환되어 디지털 자산화가 이루어져서 온라인 (가상공간)에서 디지털 자산의 소유권의 거래가 활발하게 이루어질 것이기 때문이다. 디지털 자산의 공정한 거래를 위해서는 웹 2.0의 중앙집중형 플랫폼 경제의 사업모델과 다르게 사용자의 디지털 자산에 대한 소유권을 보장하고 거래 당사자간 신뢰적인 통신과 거래를 위한 기술이 요구된다.

이러한 기술을 기반으로 구축되는 웹 3.0 생태계는 새로운 글로벌 디지털 경제를 활성화하고 새로운 사업모델과 시장을 창출하고 중앙집중형 플랫폼 사업자가 독점한 데이터에 대한 불법적인 조사 및 검열과 같은 개인 정보에 대한 공격을 어렵게 할 것이다.

Ⅲ. Decentralized Identity

1. Decentralized Identifiers(DIDs)

DID는 웹의 모든 사용자의 개인정보 보호를 고려한 글로벌하고 유일한 온라인 식별자로 합의 기반의 데이터 공유를 가능하게 하는 도구[7]로 다음의 네 개의 요구사항을 만족한다.

- 탈중앙화(decentralization): 중앙의 발급 또는 등록 기관이 없이 식별자 생성 가능
- 지속성(persistent): 식별자를 영구적으로 사용할 수 있다.
- 암호로 검증가능(cryptographically verifiable): 암호로 식별자의 소유권을 증명할 수 있다.
- 해석 가능(resolvable): 식별자와 관련한 메타데이터를 검색할 수 있다.

글로벌하고 유일한 식별자 체계로 대표적인 것은 인터넷 도메인 이름체계, 디지털 환경에서 객체를 식별하는 DOI(Digital Object Identifier) 시스템, 바코드에서 사용되는 GTIN(Global Trade, Item Numbers)이 있다. 그러나 이들은 모두 중앙 기관이 식별자를 발급 또는 등록 및 관리하는 글로벌 식별자[8]로 탈중앙화의 요구사항을 만족하지 못한다.

중앙의 등록기관이 없는 글로벌하고 유일한 식별자로는 UUID(Universal Unique Identifier)[9]가 표준화되었다. UUID는 글로벌하고 유일하지만 해석이 가능하지 않다. 지속성이 있는 식별자로 URN(Uniform Resource Name)[9]이 표준화되었으나 글로벌하게 해석이 되기 위해서는 중앙의 등록기관이 요구된다. 그리고 UUID와 URN은 식별자의 소유권을 암호로 검정하는 기능이 없다.

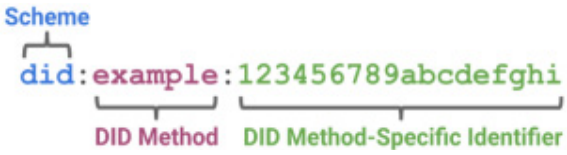

그림 4. DID (Decentralized Identifier) 형식과 예[12]

DID의 형식은 〈그림 4〉와 같이 URN형식의 기본 패턴을 따르며 여러 블록체인에서 동작될 수 있도록 제안되었다. 체계(scheme)요소에는 urn 대신 did로 지정되고 urn의 이름공간(namespace) 요소에는 DID가 어느 블록체인에서 작동하는지를 정의하는 DID 메소드를 명시한다. DID 메소드 명세는 메소드 별 식별자(DID Method Specific Identifier)의 형식과 해당 DID 문서를 읽고 쓰는 방법을 정의하며 메소드 별 식별자는 〈그림 4〉의 DID 메소드 별 식별자 영역에 표현되고 해당 DID 메소드 이름공간 내에서 유일해야 한다[11].

DID는 탈중앙화 구조의 블록체인과 결합된 URN 형식을 따르고 있어 글로벌하고 유일한 식별자로 발급 및 등록의 탈중앙화에 대한 요구사항을 만족한다. 그리고 DID는 사용자가 만들고 소유할 수 있어 지속성 요구사항도 만족한다.

해석 가능성과 암호로 검증되어야 한다는 요구사항 때문에 DID 문서가 정의되었다. DID와 DID 문서로 구성되는 DID 아키텍처는 키(key)가 DID이고 값(value)이 DID 문서인 가상 데이터베이스를 중심으로 한다. DID 문서에는 DID로 식별되는 엔티티들이 서로 암호로 검증가능한 상호작용을 스스로 시작하기 위해 필요한 공개키, 인증 프로토콜 및 서비스 종단점 등이 기술된다. DID문서의 구성 항목으로는 DID문서에서 사용되는 @context, DID 문서가 설명하는 객체의 DID를 표현하는 id, DID 주체와 상호작용 또는 인증에 필요한 데이터를 포함하는 publicKey와 authentication, DID주체와 상호작용하는 서비

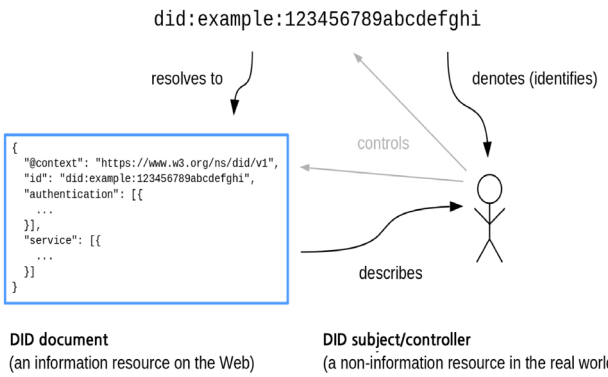

그림 5. DID, DID 컨트롤러, DID문서 간 관계[13]

스의 위치와 방법을 기술하는 서비스 종단점을 포함하는service 항목이 있다.

〈그림 5〉는 물리공간의 객체를 식별하는 DID와 가상공간에서 물리공간의 객체를 설명하는 DID 문서와의 관계를 나타낸다. DID와 DID문서에 대한 제어권은 DID 컨트롤러가 가진다. 앞에서 살펴본 DID문서에 정의된 항목의 기능들을 활용하면 다양한 행태의 인증 서비스를 제공할 수 있다.

2. Verifiable Credentials

우리는 일상생활에서 자신의 신분 및 자격의 증명을 수시로 요구 받는다. 예들 들면 자동차 운전 자격을 증명하는 운전 면허증, 교육수준을 증명하는 학위증, 기업의 직원임을 증명하는 사원증, 국가 간 여행을 위한 여권 등이 있다. 물리공간에서 이루어지는 자격증명에 기반한 활동을 가상공간으로 확장하기 위해서는 가상공간에서 믿을 수 있게 자격증명을 표현하고 검증하는 방법이 필요하다. 즉, 물리 공간의 물리적 자격증명이 제공하는 것과 동일하게 가상공간에서 인정을 받을 수 있도록 디지털 자격증명을 표현하여야 한다.

물리적 자격증명의 이미지 파일 또는 PDF 형식의 디지털 자격증명을 사용할 경우, 검증에 요구되는 정보 외에 다른 정보들이 공개될 수 있으며 문서의 출처와 진위여부를 확인하는 것이 복잡하다. 문서의 출처와 진위 여부를 확인하기 위해서는 발급기관이 해당 자격증명을 발급할 권한이 있는지, 자격증명이 정상적으로 발급되었는지, 자격증명을 제출하는 사람이 자격증명의 정당한 소유자인지, 제출된 자격증명의 유효한지 등의 확인이 필요하다.

검증가능한 자격증명 (VC: Verifiable Credential)은 가상공간에서 물리공간의 자격증명을 개인정보가 보호되며 컴퓨터가 해석할 수 있도록 표현하는 메커니즘을 제공한다. 디지털 자격증명의 한 형태인 VC는 〈그림 6〉과 같이 물리적 자격증명인 운전면허증에서 동일한 정보를 표현하는 VC로 매핑이 가능하다. 디지털 자격증명인 VC는 디지털 서명기술과 결합하여 물리적 자격증명보다 신뢰할 수 있고 위조의 검증이 가능해서 검증가능한 자격증명이라고 한다.

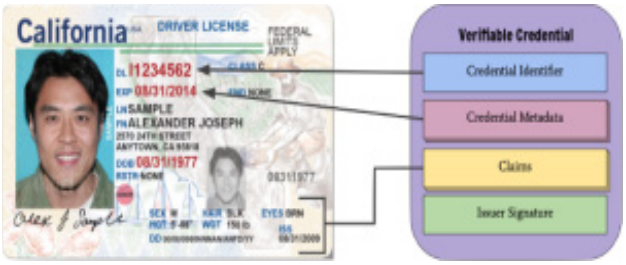

그림 6. 물리적 자격증명과 VC의 관계[14]

물리적 자격증명은 자격증명 주체의 식별정보, 발급기관 정보, 자격증명 유형, 자격증명 주체에 대해 발급기관이 주장하는 특정 속성과 관련 정보, 자격증명이 파생된 방법과 관련 증거, 자격증명의 제약조건 관련 정보로 구성되며 VC는 물리적 자격증명과 동일한 모든 정보를 가진다.

물리공간의 객체를 식별 및 자격증명이 이루어지는 디지털 생태계는 발급자 (issuer), 보유자 (holder), 검증자 (verifier), 분산원장 (distributed ledger), 디지털 지갑(wallet)으로 구성된다 〈그림 7〉.

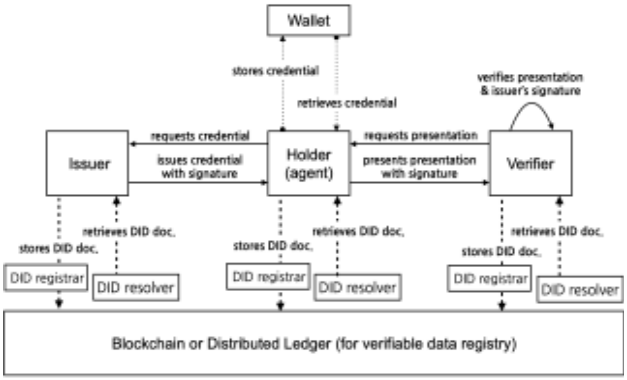

그림 7. 탈중앙화 신원증명 생태계 구성요소

발급자는 디지털 생태계에서 주체에 관한 주장인 클레임(예, 철수는 대학생이다.)으로 VC를 만들어 보유자에게 전송한다. 여기서 발급자는 개인 또는 기관(정부, 기업 등)이 될 수 있다. 보유자는 발급자에게 VC 발급 요청을 한 후 발급된 VC를 자산의 디지털 지갑에 보관한다. 그 후 보유자는 검증자에게 자신의 신원을 증명하기 위해서 보유한 VC의 속성 중 필요한 속성만을 추출하여 하나의 검증가능한 표현(VP: Verifiable Presentation)을 만든 후 자신의 서명을 추가하여 검증자에게 제출한다.

분산원장은 탈중앙화 디지털 신원증명을 위해 생태계 참여자들의 공개키, VC 스키마, VC 폐기 레지스트리와 같은 정보를 서로 공유 및 확인하는데 사용된다. 분산원장을 통해 공유가 되기 때문에 관련 정보의 투명성과 불변성을 보장할 수 있다.

발급자가 사용자의 신원과 자격을 증명할 수 있도록 발급되는 VC는 자격증명 메타데이터(Credential metadata), 클레임, 증명(proof)으로 구성된다. 사용자가 검증자에게 제출하는 VP는 표현 메타데이터(Presentation metadata), VC, 증명(proof)으로 구성된다.

VC의 자격증명 메타데이터 영역에는 VC발급자, 자격증명 대

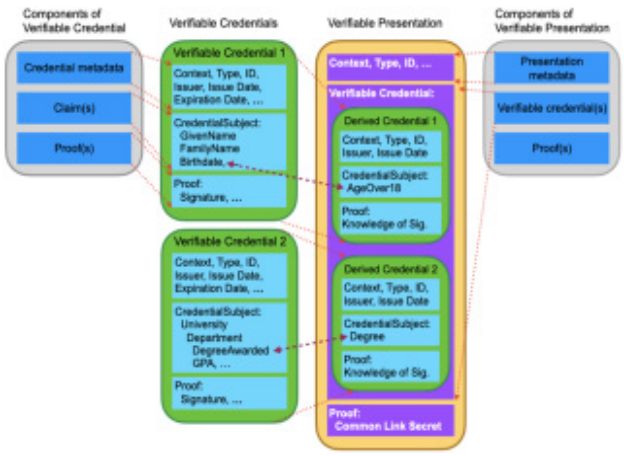

그림 8. VC/VP 구성요소와 VC와 VP 상관관계

상, VC 발급일자, 만료일자, 폐기방법 등이 정의된다. 클레임 영역에는 주체의 자격을 증명하는데 필요한 자격증명 속성이 포함되며 credentialSubject항목 내에 기술된다. 증명(proof) 영역은 VC 발급 시 필수적인 것으로 VC의 무결성 보장 및 검증을 위해 VC 발급자의 서명이 추가된다.

VP의 표현 메타데이터 영역에는 VP와 관련한 이용약관, evidence 등 VP 검증에 참고할 수 있는 데이터가 포함되며 VC 영역에는 발급자가 발급한 VC의 클레임 중 검증자가 요구하는 속성에 해당하는 클레임과 증명 항목이 포함된다. 마지막으로 증명 영역에는 해당 VP가 검증하려는 사용자가 제출한 것인지 확인을 위해 사용자의 서명이 포함된다.

〈그림 8〉은 신원증명 VC1과 학위 자격증명 VC2 중 나이와 학위만으로 구성된 VC를 포함하는 VP를 생성하였을 때 각 구성요소 간의 상관 관계를 보인다.

3. 탈중앙화 디지털 생태계와 개인정보 보호

개인정보 보호는 웹 3.0 생태계에서 자기주권 신원정보 관리의 필수적인 구성 요소로서 퍼블릭 블록체인을 활용한 글로벌 신원정보 시스템에서 특히 중요하다. DID와 VC가 기반이 되는 탈중앙화 디지털 생태계에서 개인정보 보호는 다음의 내용을 고려할 수 있다.

- VC 암호화: DPKI(Decentralized Public Key Infrastructure)를 사용하여 자격증명을 암호화하여 전송하여 개인정보를 보호한다.
- 관계 별 익명 DID: 공개 식별자인 DID가 아닌 일상생활의 관계별로 발급된 개인 식별자로 DID를 사용한다.
- 오프체인 개인 데이터: 누구나 언제든지 접근이 가능한 퍼블릭 블록체인에는 암호화된 데이터라도 개인정보를 저장하지 않고 오프체인에 저장하고 암호화된 피어-투-피어 연결을 통해서만 개인정보를 교환하여 개인정보를 보호한다.
- 선택적 공개(Selective disclosure): VC의 클레임 중 검증자가 요구하는 속성만을 공개하고 검증자가 요구하지 않는 개인정보는 공개하지 않아 보호한다.
- 영 지식 증명(Zero knowledge proof): 보유자가 자격증명에 대한 진술이 사실이라는 것만 공개하고 다른 실제 정보를 공개하지 않아 개인정보를 보호한다.

IV. 상호인증 및 신뢰적인 채널 확보 기술

본 장에서는 DID를 사용한 디지털 생태계에서 참여자 간 신뢰적인 통신채널 확보 및 상호인증 기술에 대해서 살펴본다.

1. DID Auth

DID Auth[15]는 RWOT(Reboot of the Web of Trust)[15]에서 진행 중인 작업으로 신원 소유자가 상호작용을 할 대상에게 본인이 해당 DID의 제어권을 가지고 있음을 증명하는 방법으로 서로를 인증하는데 사용된다. DID Auth는 DID 문서의 authentication 항목으로 지정된 메커니즘을 사용하여 DID를 제어할 수 있음을 보인다. DID Auth는 상호 인증된 통신채널을 설정하고 웹 사이트 및 애플리케이션에 인증하는 기능을 포함한다. DID Auth는 〈그림 9〉와 같이 Challenge-Response 인증 방식을 사용한다.

검증자는 DID 컨트롤러의 DID를 얻은 후 분산원장에서 해당 DID에 대한 DID 문서를 열람한 후 DID 문서에 포함된 인증관련 데이터에 포함된 컨트롤러의 공개키를 사용하여 Challenge를 생성한 후 컨트롤러에게 전송한다. Challenge를 받는 사용자는 자신의 DID 문서에 명시된 공개키와 인증방식 정보를 사용

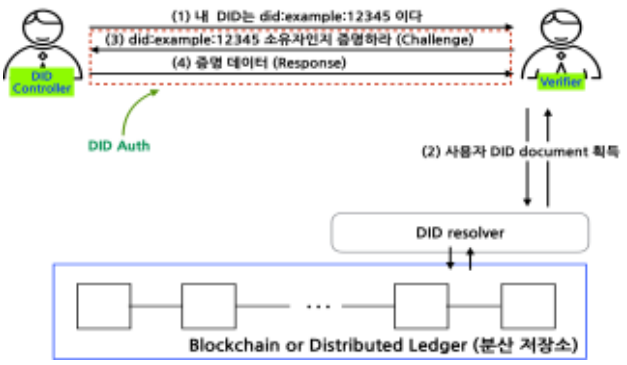

그림 9. DID Auth 절차

하여 Response를 생성한 후 검증자에게 전송하여 컨트롤러의 DID 제어권을 증명한다.

2. DIDComm

DIDComm은 DID의 탈중앙화 설계를 기반으로 구축된 안전하고 보안된 통신방법의 제공이 목적이다[17]. DIDComm은 DPKI에 기반하여 사람, 사물, 또는 조직에 의해 제어되는 소프트웨어 에이전트 간 안전한 통신채널을 생성한다.

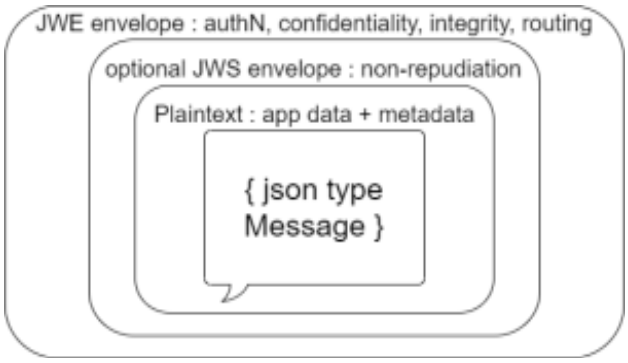

그림 10. DIDComm 메시지 유형

DIDComm은 〈그림 10〉과 같이 기본적으로 세가지 메시지 유형을 정의한다. 첫 번째 유형은 암호화하지 않는 일반적인 텍스트 메시지, 두 번째 유형은 서명된 메시지, 세 번째 유형은 암호화된 메시지이다. 서명과 암호화는 본인의 개인키와 상대방의 공개키를 사용하여 이루어진다. 실제로는 세 가지 메시지 유형뿐만 아니라 메시지 무결성 확인을 위한 암호화와 서명을 혼합하여 사용하는 것도 가능하다.

DIDComm을 이용한 통신은 중앙 서버를 필요로 하지 않고 통신 참여자의 소프트웨어 에이전트가 메시지 암호화, 복호화 기능을 가지면 상대방과 신뢰할 수 있는 통신이 가능하다. 즉 중앙 서버의 개입이 없는 탈중앙화 디지털 생태계에서 참여자 간 신뢰할 수 있는 피어-투-피어 통신채널을 확보할 수 있다.

V. 탈중앙화 디지털 생태계를 위한 커뮤니티

1. DIF(Decentralized Identity Foundation)

DIF[18]는 DID를 위한 개방형 생태계를 구축하고 참여자 간 상호 운용성을 보장하기 위한 기본 요소 개발을 위한 조직이다. 〈그림 11〉은 DIF 조직 내에서 활동 중인 워킹 그룹이다.

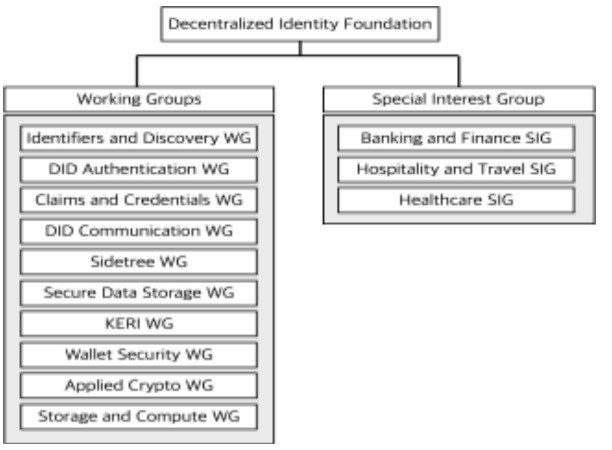

그림 11. DIF 조직 내 WG과 SIG

DIF 조직 내의 워킹 그룹은 DID를 이용하여 사람, 조직, 사물을 식별하고 검색하는 방법, 암호화 프로토콜을 활용한 인증 및 권한 부여 프로토콜, 클레임을 애플리케이션과 서비스에 결합하는 방법, DIDComm, 보안 데이터 구문, 저장, 전송, 지갑 아키텍처, 지갑에 적용할 보안 아키텍처, 실제적인 암호화 알고리즘 개발 등 DID를 기반한 탈중앙화 디지털 생태계 구축에 필요한 대부분의 기술에 대해서 논의가 이루어지고 있다.

2. \3C(World Wide Web Consortium)

W3C는 웹과 관련한 사실 표준을 제정하는 조직으로 탈중앙화 신원증명과 관련한 표준 개발은 DID WG, VC WG, CCG(Credential Community Group)에서 이루어지고 데이터와 애플리케이션의 분리와 관련한 표준 개발은 Solid CG에서 이루어지고 있다.

W3C DID WG에서는 앞에서 살펴보았던 DID에 관한 표준(DID v1.0)이 2022년 7월에 제정되었다. DID 표준은 DID 구문, 공통데이터 모델, 핵심적인 속성, 직렬화된 표현, DID 메소드, DID 생성 및 제거 등의 프로세스를 포함한다. W3C DID WG의 산출물은 DID Use Cases and Requirements, DID Specification Registries, DID Core Implementation Report가 있다. 2022년 9월 기준으로 DID Specification Registries에 등록된 DID 메소드는 약 125개 정도이다. DID WG의 표준화는 DID v1.0이 완성된 후 새로운 작업으로 대표적인.DID 메소드(did:web, did:key등)와 DID resolver에 대한 표준화를 진행할 계획이다.

검증가능한 자격증명과 관련하여 W3C VC WG은 2022년 3월 Verifiable Credential Data model v1.1을 개정하였다. VC WG의 결과물로는 Verifiable Credentials Use Cases v1.0과

Verifiable Credentials Implementation Guideline 1.0 이 있다. 향후 표준화 과제로 Verifiable Credential in Data Model v2.0 표준 개발을 논의 중이다.

W3C Solid CG는 탈중앙화 웹을 위한 표준을 개발하는 Solid 프로젝트[19]의 결과에 대해 논의를 하는 그룹으로 웹 애플리케이션에서 데이터 소유권 및 개인정보 보호 문제 등을 개선하는 것을 목적으로 한다.

W3C CCG[20]에서 VC를 교환 및 검증을 위한 웹 API (Application Programming Interface)를 표준화 중이다. 이 API는 DID와 VC를 구성된 탈중앙화 신원증명 생태계에서 사용하는 데이터를 생성, 확인, 제시, 관리를 위한 데이터 생명주기 모델 및 HTTP 프로토콜을 규정한다. 또한 CCG내 VC-EDU TF에서 온라인 교육의 자격증명을 VC로 기술하는 것에 대한 논의를 하고 있으며 2022년 10월에 상호운용성 검증을 하였다.

3. RWOT와 IIW

RWOT(Rebooting the Web of Trust)는 온라인에서 개인의 디지털 자산 및 계정을 통제할 수 있도록 신원 및 정보의 탈중앙화 모델을 생성하는 커뮤니티를 지원하는 것을 목표로 하는 워크숍 조직으로 지난 7년 동안 50개 이상의 백서, 기술 명세, 코드 저장소를 발표하였다. 워크숍은 기술 모델, 평판 시스템, 스마트 계약 등, 탈중앙화 신원증명에 대해서 논의를 한다. 사용자로부터 실제 사용 사례 및 애플리케이션에 대한 의견을 수집하고 엔지니어에게 기술 명세와 코드를 개발하도록 운영된다. 현재 이 워크숍의 결과물은 웹 3.0 생태계의 신원증명 기술로 활용이 가능하다.

IIW(Internet Identity Workshop)[21]은 2005년부터 년 2회 신원증명과 관련한 문제를 논의하기 위해 캘리포니아의 컴퓨터 역사 박물관에서 이루어지는 워크숍으로 사용자 중심의 신원증명과 관련한 주제를 논의하고 있다. 최근에는 자기주권 신원증명(SSI: Self-Sovereign Identity), 블록체인 기반 신원증명과 관련한 시스템에 대해서 논의 중이다. 그리고 IIW는 OAuth(Open Authorization), OpenID Connect, FIDO(Fast Identity Online)와 같이 웹에서 새로운 인증을 가능하게 하는 시스템과 프로토콜 개발을 위한 포럼의 역할을 하고 있다.

VI. 결 론

본고에서는 신뢰성, 탈중앙화, 디지털 자산의 자기주권이 특징인 웹 3.0 생태계에서 활용할 수 있는 신원증명 기술에 대해서 살펴보았다. 살펴본 신원증명 기술은 디지털 전환으로 증가할 디지털 자산의 소유권과 소유자의 신원정보를 탈중앙화하고 사용자가 자신의 신원정보와 디지털 자산의 관리 및 유통에 직접 참여하여 개인정보를 보호하고 정보 및 데이터에 대한 주권을 확보하여 궁극적으로 신뢰성 있는 웹 3.0 생태계를 구축하는 기반이 될 것이다.

Acknowledgement

본 연구는 2022년 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행됨 (No. NRF-2021R1F1A1047573)

참 고 문 헌

[1] Tim O'Reilly, "What is Web 2.0: Design Pattern and Business Models for the Next Generation of Software," Communication & Strategies, No. 1, pp. 17, First Quarter 2007.

[2] Berners-Lee, Tim, Fischetti, Mark, "Weaving the Web," HarperSanFrancisco, chapter 12, ISBN 9780-06-251587-2.

[3] WIRED UK Article, "Tim Berners-Lee: We need to-decentralise the Web," June 2014.

[4] Gavin Wood, "Why We Need Web 3.0," https://uri.ki/v8go6.

[5] The WIRED Article, "The Father of Web3 Want You to Trust Less," https://wired.com/story/web3-gavin-wood-interview.

[6] Digital Insight 2022, "Web 3.0, 디지털 공간 속 공정함과 새로움을 논하다." 한국지능정보사회진흥원.

[7] W3C DID Working Group, https://w3.org/2019/did-wg/

[8] W3C Editor's Draft 25, "Use Cases and Requirements for Decentralized Identifiers," March 2021.

[9] IETF RFC 4122, "A Universally Unique Identifier(UUID) URN Namespace," July, 2005.

[10] IETF RFC 8141, "Uniform Resource Names(URNs),"April, 2017.

[11] W3C Community Group Draft Report, "A Primer for

Decentralized Identifier," Nov. 2021.
[12] W3C Recommendation, "Decentralized Identifiers (DIDs) v1.0 Core architecture, data mode, and representations," July, 2022.
[13] A Preukschat, D. Reed, "Self-Sovereign Identity," Manning 2021.
[14] W3C Recommendation, "Verifiable Credential Data Model v1.1," March, 2022.
[15] S. Appeicline, "Introduction to DID Auth," July, 2018.
[16] Rebooting the Web of Trust, https://weboftrust.info
[17] S. Curren, T. Looker, O. Terbu, "DIDComm Messaging v 2.0," http://url.kr/cr7o4z.
[18] DIF homepage, https://url.kr/61vkpe.
[19] Solid Project homepage, https://solidproject.org.
[20] W3C Credentials Community Group, https://w3c-ccg.github.io.
[21] Internet Identity Workshop, https://internetidentityworkshop.com.

약 력

김 근 형

1986년 서강대학교 공학사
1988년 서강대학교 공학석사
2005년 포항공과대학교 공학박사
1988년~1990년 LS 산전 연구원
1990년~1993년 삼성종합기술원 선임연구원
1993년~2007년 KT BcN본부 수석연구원
2007년~현재 동의대학교 게임공학전공 교수
2019년~현재 동의대학교 블록체인기술연구소장
관심분야: 탈중앙 웹, 웹 3.0, 블록체인, 자기주권 데이터