넥스트 노멀,
비즈니스 변화와 도전을 위한
DID 기술 활용 방안

(주)마크애니
김 동 호

MarkAny*

Contents

Session Agenda

기업 비즈니스 혁신을 위한 DID 기술

DID개요

MarkAny

DID(Decentralized Identity) : 기존 중앙화된 신원인증방식에서 벗어나 탈중앙화 방식으로
개인 신원을 증명하고 각 개인이 자신의 정보에 대한 통제권을 가지게 하는 기술
*분산신원확인, 탈중앙화 신원확인이라고도 함

DID 관련 표준화 기관

Verifiable Credentials	W3C
DID Auth	DIF, IETF
DKMS (Decentralized Key Management System)	OASIS
DID (Decentralized Identifier)	W3C

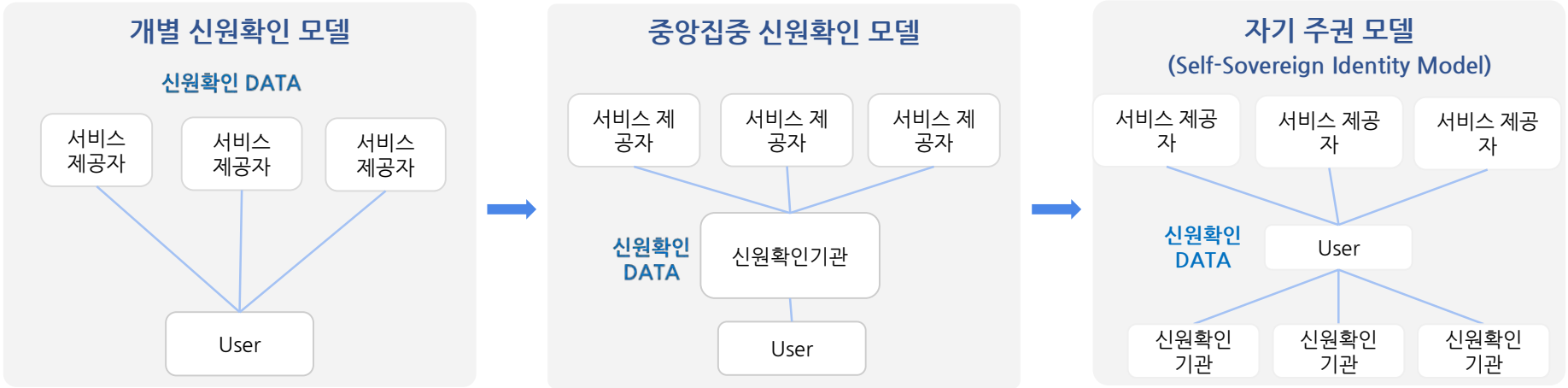
W3C(World Wide Web Consortium)가
표준화를 주도해 DID 관련 각종 표준을 제정

DID Document sample

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

신원확인 모델의 변화

MarkAny



ID/PW

- 사용자는 각각 서비스 계정을 별도 생성하여 사용
- 각각 다른 ID/PW로 인하여 분실시 사용 불편
- 동일한 계정 사용시 위험 증가

OPEN ID, OAuth

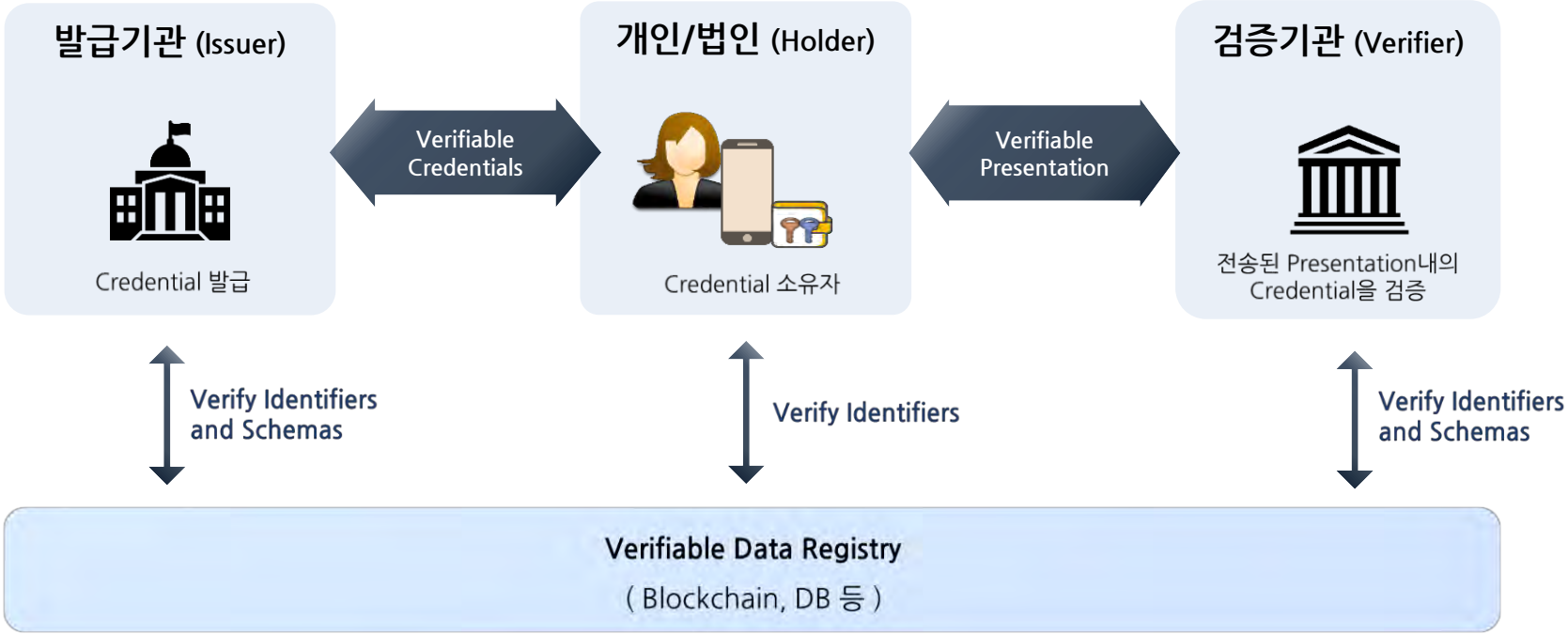
- 신원제공자 계정을 통해 연계된 서비스 로그인
- 한 개 ID/PW 발급해 통합 사용
- 소수 대기업이 사용자 정보를 독점

DID

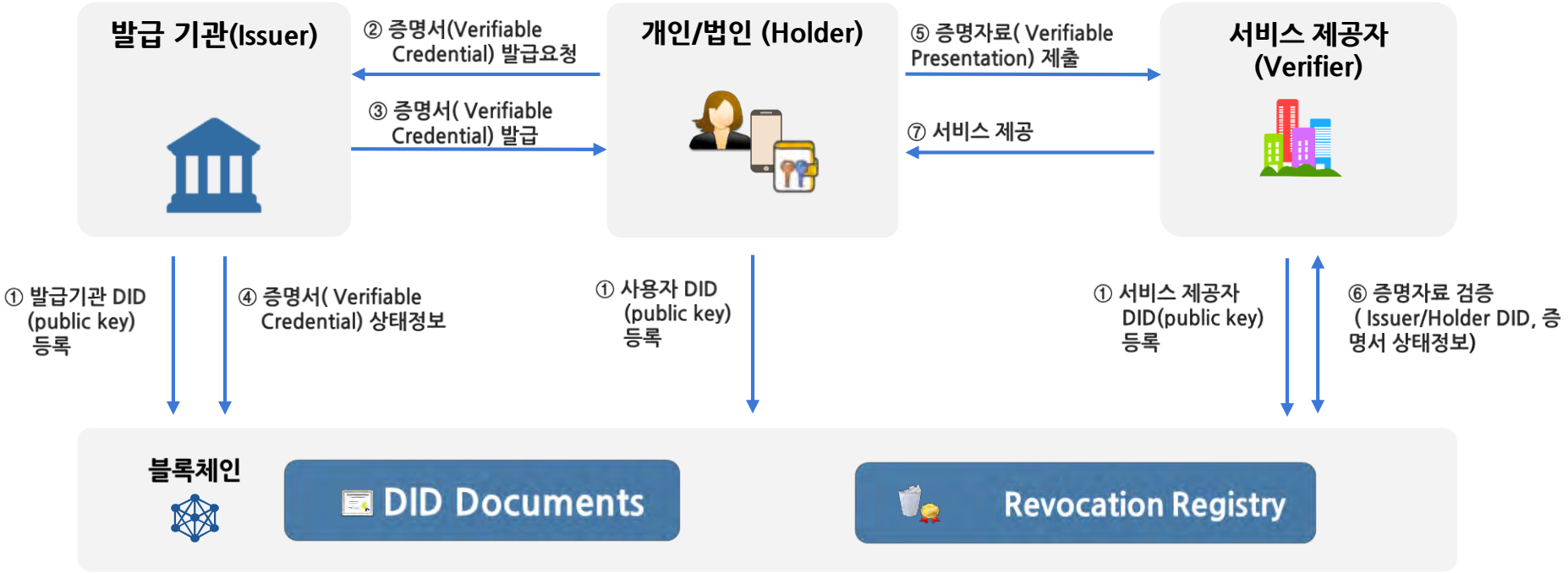
- 신원제공자에게 신원증명 정보를 발급 받은 후 사용자가 정보를 관리하면서 원하는 서비스에 로그인
- 사용자가 본인 기기에 본인 정보를 직접 관리
- 사용자 관리기기 분실 위험 존재

출처 NIST, 'A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems'('20.01), 기반 재구성

DID의 구성요소


발급기관 (Issuer)
Credential 발급
Verifiable Credentials
개인/법인 (Holder)
Credential 소유자
Verifiable Presentation
검증기관 (Verifier)
전송된 Presentation내의 Credential을 검증
Verify Identifiers and Schemas
Verify Identifiers
Verify Identifiers and Schemas
Verifiable Data Registry
(Blockchain, DB 등)

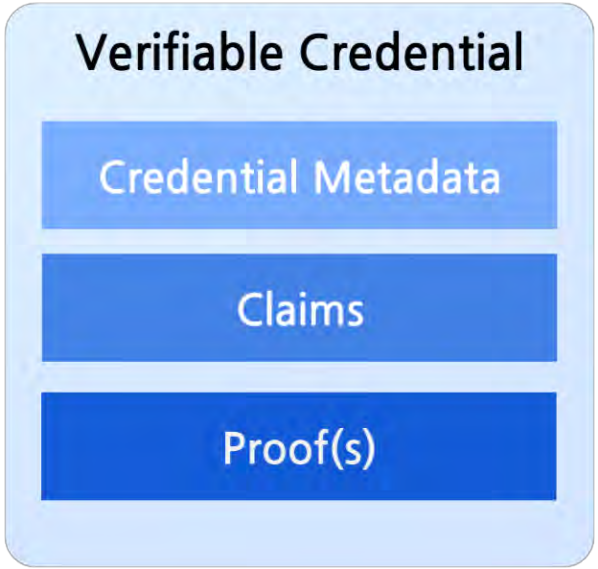
DID의 서비스 흐름


발급 기관(Issuer)
② 증명서(Verifiable Credential) 발급요청
③ 증명서(Verifiable Credential) 발급
개인/법인 (Holder)
⑤ 증명자료(Verifiable Presentation) 제출
⑦ 서비스 제공
서비스 제공자 (Verifier)
① 발급기관 DID (public key) 등록
④ 증명서(Verifiable Credential) 상태정보
① 사용자 DID (public key) 등록
① 서비스 제공자 DID(public key) 등록
⑥ 증명자료 검증 (Issuer/Holder DID, 증명서 상태정보)
블록체인
DID Documents
Revocation Registry

Verifiable Cedential

MarkAny

신원인증기관(Issuer)에서 발급돼 암호학적으로 검증 가능한 Credential (Claim의 모음)




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "id": "http://AnyBlock DID.com/credentials/1872",
  "type": ["VerifiableCredential"],
  "issuer": "https://AnyBlock DID.com/issuers/565049",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "Honggil Dong"
    "address": "10f ssanglim bldg chung-gu  seoul"
    "phone": "02-3333-4444"
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://AnyBlock DID.com/issuers/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI..."
  }
}
```

Credential ID

Issuer DID

Holder DID

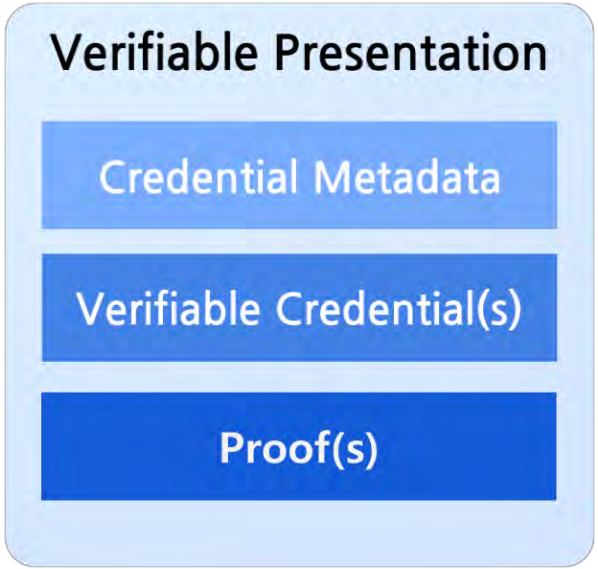
Claims(Credential Data)

Proof
(Signature form Issuer)

Verifiable Presentation

MarkAny

사용자가 소유한 증명서(Verifiable Credential)을 Verifier에게 전달하기 위한 형식



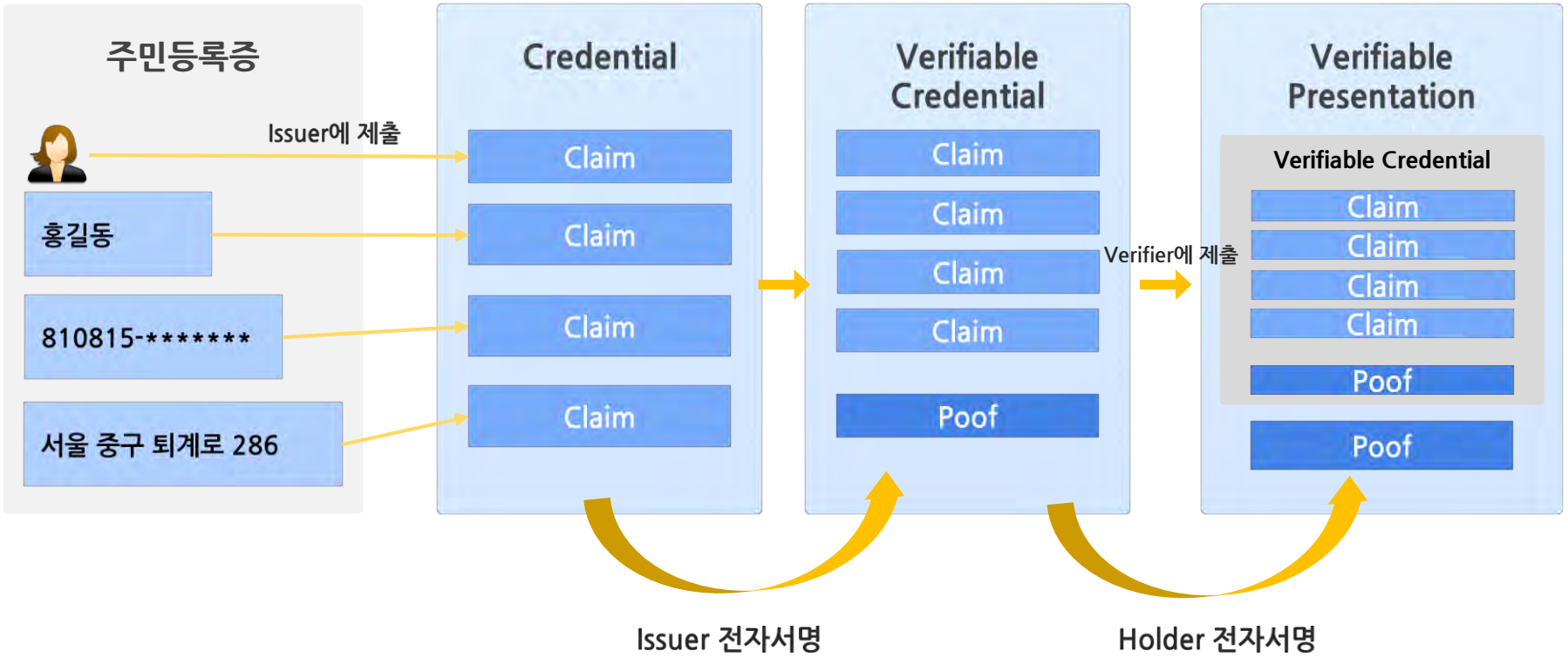

```
"@context": [
  "https://www.w3.org/2018/credentials/v1"
],
"type": "VerifiablePresentation",
"verifiableCredential": [
  {
              "@context": [ "https://www.w3.org/2018/credentials/v1"  ],
              "id": "http://AnyBlock DID.com/credentials/1872",
              "type": ["VerifiableCredential"],
              "issuer": "https://AnyBlock DID.com/issuers/565049",
              "issuanceDate": "2010-01-01T19:73:24Z",
              "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "Honggil Dong"
    "address": "10f ssanglim bldg chung-gu  seoul, korea"
    "phone": "02-3333-4444"
              },
              "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://AnyBlock DID.com/issuers/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI..."
              }
  } ],
"proof": {
  "type": "AnonCredPresentationProofv1",
  "proofValue": "DgYdYMUYHURJLD7xdnWRinqWCEY5u5fK...j915Lt3hMzLHoPiPQ9sSVfRrs1D"
}
}
```

Presentation Metadata

Original Credential

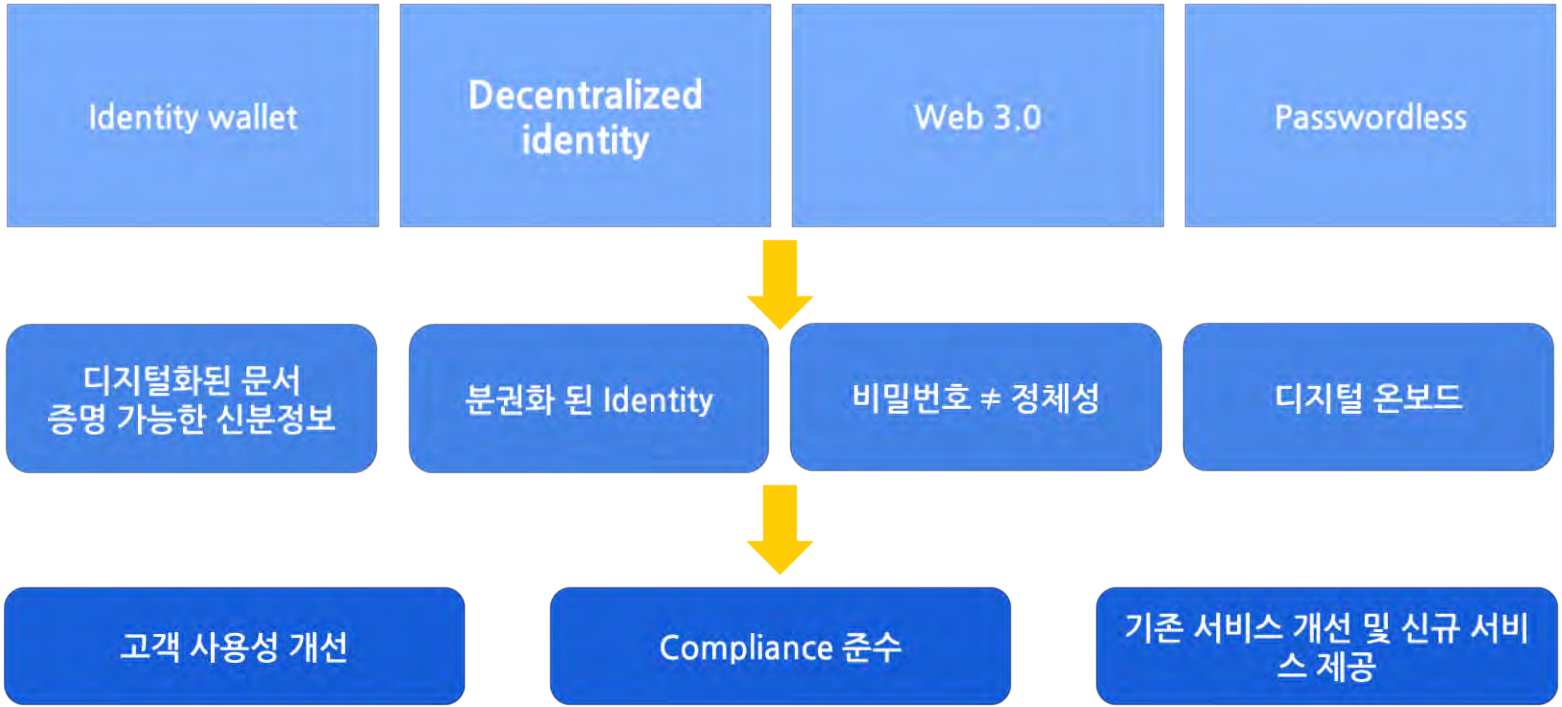
Proof (Signature from Holder)

Credential과 VC, VP 관계



DID 기술 트렌드

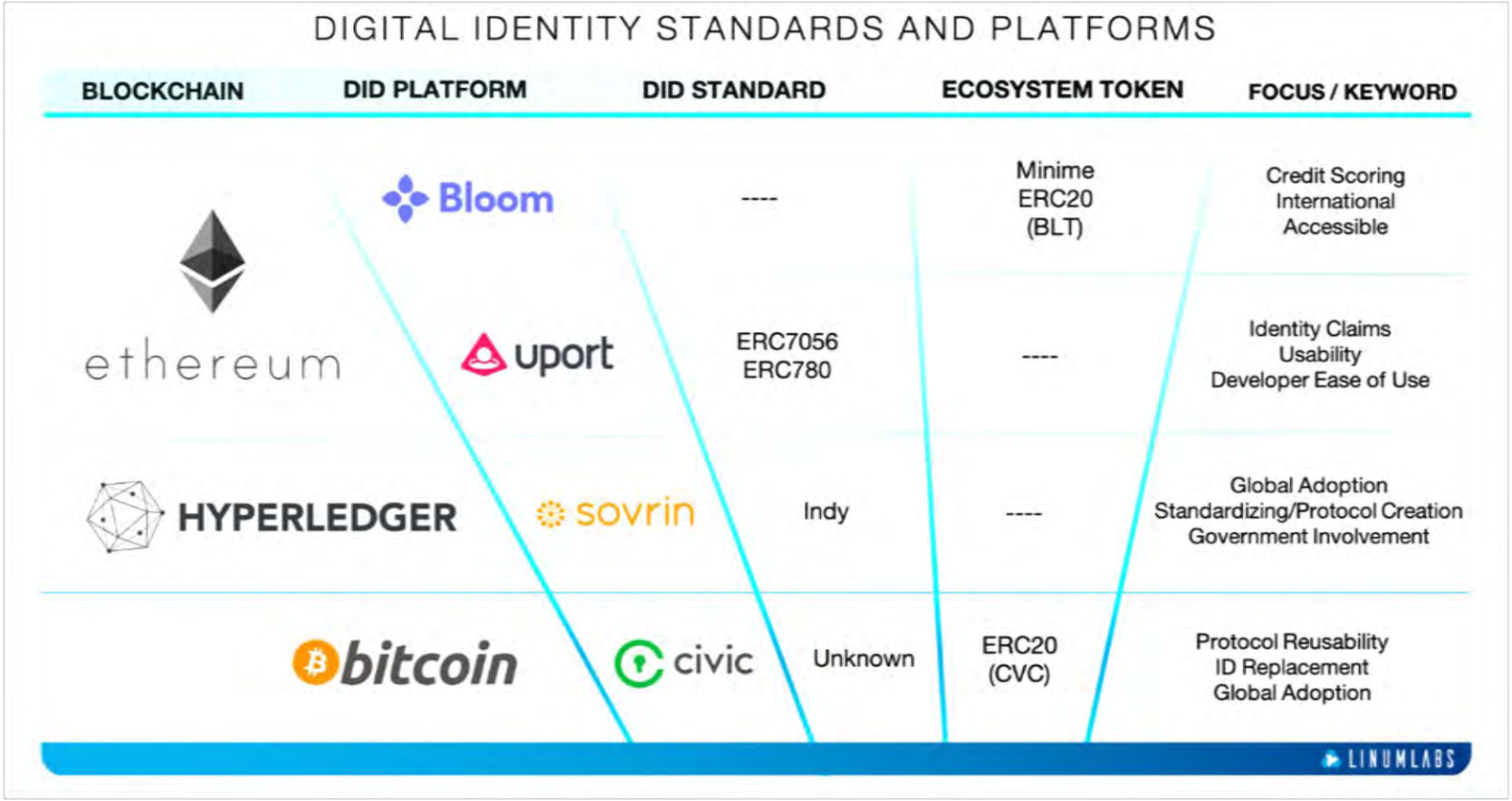
2022년 주요 트렌드



출처: 4 Digital Identity Trends and Predictions for 2022
출처: Apple, Google, and Microsoft will soon implement passwordless sign-in on all major platforms(2022.05.05)

해외 DID 현황

MarkAny



출처: LINUMBALBS

국가별 신원·자격관리 관련 정책 동향

국가	정책 내용
EU	전자적 거래를 위한 전자적 신원확인 및 신뢰 서비스(eIDAS) 법안 시행(2014. 7.) *유럽회원국간 내 통일된 양식 한 가지 서명으로 전자적 거래가 가능하도록 법적 효력을 규정
싱가포르	디지털 신분증 (national Digital Identity: NDI) 제도 시행 계획 발표 (2017. 7. 5) * 스마트 국가 버전의 일환으로 모든 정부 서비스에 대해 전자 결제와 디지털 서명을 손쉽게 이용할 수 있도록 국민에게 디지털 신분증 제공
호주	7년 내 모든 공공 서비스 온라인화를 위한 “디지털 혁신 전략”을 발표 (2018. 11.) *디지털 신원 확인 시스템(myGovID)을 확대해 모든 공공 서비스 로그인 시스템에 활용
뉴질랜드	디지털 신원 신뢰 프레임 워크(Digital Identity Trust Framwork) (2019.3.) *디지털 신원 생태계 운영을 관리하기 위한 표준, 규칙 및 계약으로 프레임워크 구성

출처: 각국 전략발표자료 기반 재작성. 2020

주요 서비스 동향(해외)

MarkAny

서비스 모델명	개발기관	참여국가	적용분야	내용
ShoCard	스타트업 ShoCard, Inc.	미국	**모바일신원 기반 관리 플랫폼**	- 모바일 사용자 인증 애플리케이션 구현, SITA, OneLogin 등 9개 회사와 연계 - 기존 신뢰 기관을 통해 발급된 신원증명서류 (면허증 등)를 스캔해 신원정보 생성 가능
uPort	ConsenSys	유럽	**신원 및 문서 검증, 전자투표**	- 스위스 주크(Zug)시의 전자투표12) 브라질 정 보의 분산ID 기반 사용자 신원 검증 등에 적용 - 이더리움 기반으로 구현, 공개키는 별도 분산 파일시스템에 보관하여 관리 - 2021년에 uPort 프로젝트가 Serto와 Veramo로 분리
Sovrin	Sovrin 재단	여러 국가	**인터넷 자기주권신원, 투표**	- 비즈니스에 필요한 간접비용 감소 및 유동성 있는 데이터 공유 가능 - ‘Sovrin Trust Framework’를 제정하고 공개 허가형 블록체인을 기반 - IBM의 Hyperledger Indy는 Sovrin 소스 기반으로 분산ID 관련 프로젝트 진행 중
World Identity Network	유엔난민 기구 (UNHCR)	리비아 등	**이민자 신원확인**	- 아동 인신매매 문제를 해결하기 위해 이민자 신원확인 목적 - 가계도 전체에 걸쳐 신분을 표시하고 다른 가 족 구성원들이 블록체인에 디지털 서명

출처: [2021년 KISA Report 9월호_4] 디지털전환 사회를 위한 생애주기형 분산신원증명 모델

주요 서비스 동향(국내)

MarkAny

플랫폼, 표준화, 서비스

구분	DID 어소시에이션	마이아이디 얼라이언스	DID 얼라이언스 코리아
주요 파트너사	통신 3사, 코스콤, KEB하나은행, 우리은행, 신한은행, NH농협은행, 삼성전자, BC카드, 현대카드 등 10여개사	아이콘루프, 증권사, 이커머스, 제조사 등 20여개사	금융결제원 한국전자서명포럼, 한국파이도산업포럼, 신한은행, NH농협은행, 라온시큐어 등 20여개사
혁신 금융 서비스	-혁신금융서비스 (코스콤, 비상장기업 주주명부 및 거래 플랫폼) -과기부 민간과제(SKT 컨소시엄)	-혁신 금융서비스 (아이콘루프, 비대면 계좌개설 서비스)	-혁신금융서비스 (파운트, RA용 비대면 계좌개설 서비스) - 과기부 공공과제 (병무청, 라온 시큐어)
주요 기반 기술	SK텔레콤 블록체인(패브릭)	아이콘루프 블록체인 (루프체인)	라온시큐어 블록체인 (옴니원)
특징	성적증명, 졸업증명, 모바일 전자증명 등	금융권 중심 디지털 신분증 개발	DID 기술 표준화
출범 시기	올해 내 예정	11월 5일 출범	10월 22일 출범

출처: [2021년 KISA Report 9월호_4] 디지털전환 사회를 위한 생애주기형 분산신원증명 모델

DID 기술 활용을 통한 비즈니스 혁신 사례

DID Use Case

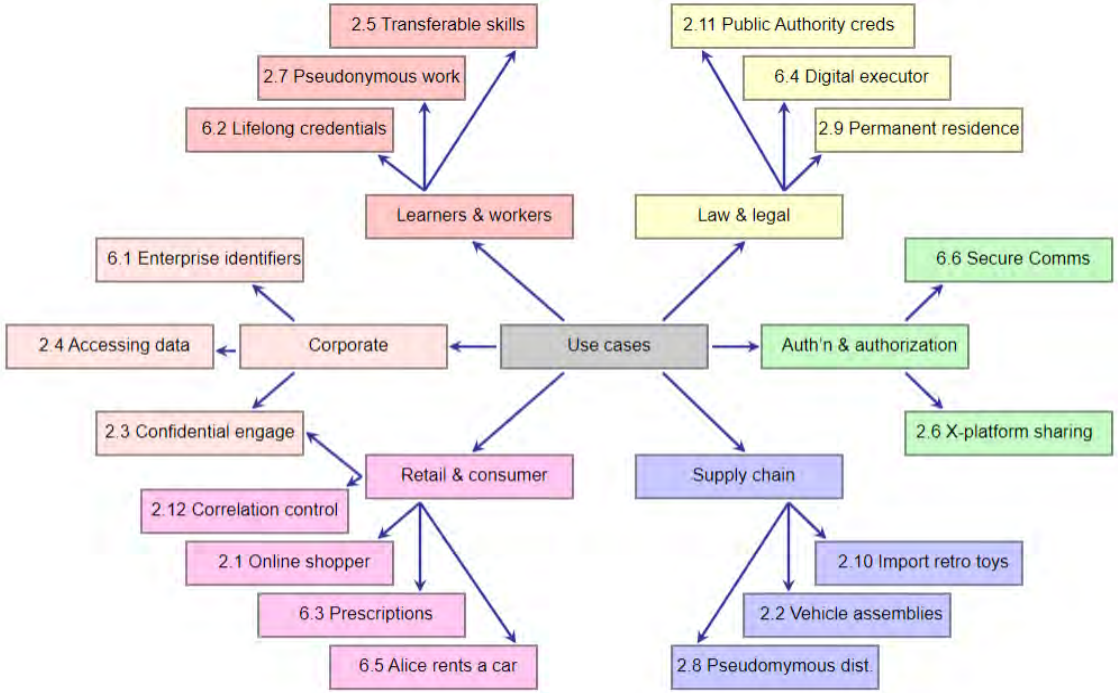


Figure 1 Each use case is assigned to one of six broad domains

출처: Use Cases and Requirements for Decentralized Identifiers,2021

DID가 바꿀 미래

MarkAny

기업채용
대학 재학, 졸업증명서
스마트폰으로 제출

온라인 로그인
각종 사이트 본인 인증만으로
간편 로그인 가능

회사 출입증
전자 출입증 형태로
스마트폰에 저장

통신 서비스
본인 인증 계좌 증명서 신청 등
스마트폰으로 처리

금융 거래
본인 인증, 계좌 증명서 신청 등
스마트폰으로 처리

학생 할인
스마트폰 학생증으로
각종 할인 가능

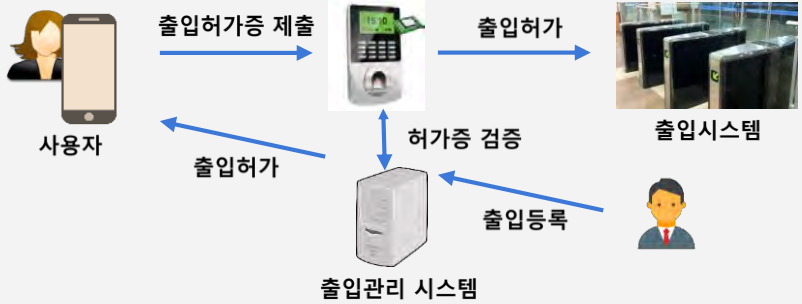
출처: "탈중앙화 신원증명(DID), 데이터의 주권은 '개인'에게 있다!". 동아일보, 201-11-15

용도별 사용 사례

MarkAny

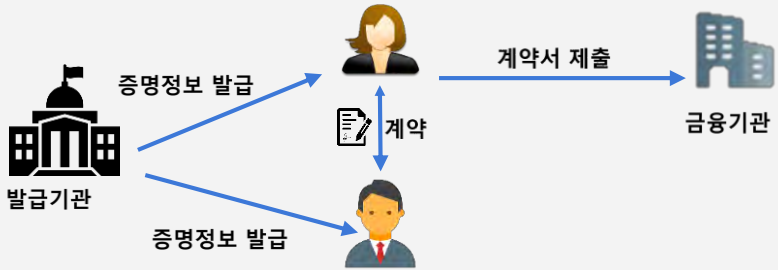
증명서 제출

출입문 통제



디지털 신분증

출입문 통제



대표적 활용 사례 - 증명서(발급)

MarkAny

CASE 1) APP에서 직접 발급

① 발급요청 → ② 발급기관선택 → ③ 증명서선택

ⓐ 추가정보입력 → ⓑ 본인확인 → ⓒ 증명서 발급 → ⓓ 증명서 발급확인

CASE 2) PC를 통한 발급

① 증명서 선택 → ② QR코드 → ③ QR코드 촬영

대표적 활용 사례 - 증명서(제출)

MarkAny

CASE1) QR코드 제출

①가입페이지접속

②입력정보QR코드

③QR코드촬영

④VC에서 정보읽은 후 전송정보 선택

⑤사용자 재확인

⑥회원가입완료

CASE2) App to App 방식

①사용 페이지접속

②DID App을 호출 하여 정보 전송요청

③VC에서 정보읽은 후 전송정보 선택

④ 사용자 재확인

⑤ 회원가입완료

참고자료

- Decentralized Identifiers (DIDs) v1.0 : https://www.w3.org/TR/did-core
- DID Specification Registries : https://w3c.github.io/did-spec-registries/#did-methods
- DID Auth : https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md
- A Primer for Decentralized Identifiers : https://w3c-ccg.github.io/did-primer
- Verifiable Credentials Data Model 1.0 : https://www.w3.org/TR/vc-data-model
- Verifiable Credentials Use Cases : https://www.w3.org/TR/vc-use-cases
- [2021년 KISA Report 9월호_4] 디지털전환 사회를 위한 생애주기형 분산신원증명 모델
- Apple, Google, and Microsoft will soon implement passwordless sign-in on all major platforms(2022.05.05): https://www.theverge.com/2022/5/5/23057646/apple-google-microsoft-passwordless-sign-in-fido
- 4 Digital Identity Trends and Predictions for 2022: https://www.signicat.com/blog/2022-trends-and-predictions

감사합니다.

QnA

도입 및 기술지원 센터
02-2262-5278
상담시간 : 평일 09:00~18:00 (점심시간 12:00~13:00제외)

MarkAny