



# Decentralized ID 개요와 정책동향

아주대학교 사이버보안학과  
김기형

[kkim86@ajou.ac.kr](mailto:kkim86@ajou.ac.kr)

Src: <https://www.slideshare.net/JimFlynn24/overview-of-decentralized-identity>

<https://csrc.nist.gov/publications/detail/white-paper/2019/07/09/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/draft>

<https://www.w3.org/TR/did-core/>

<https://w3c-ccg.github.io/did-primer/>



# 순서

- 블록체인의 역사
- ID의 변천
- DID란?
- Verifiable Credentials
- 자기주권 ID
- DID Privacy 와 Scalability 설계
- DID 동향 및 시장
- 결론

# 블록체인의 역사

1953 Hash 알고리즘

1979 머클트리

1977  
DES  
대칭키암호화

1976  
RSA  
비대칭키 암호화

1983  
은닉서명 (Blind Signature)  
David Chaum

1985 타원곡선  
비대칭키 암호화

1989  
Zero Knowledge Proof

1989  
DigiCash 설립 (Ecash)  
David Chaum

1997  
SSI/TLS

1998  
Bit Gold  
Nick Szabo

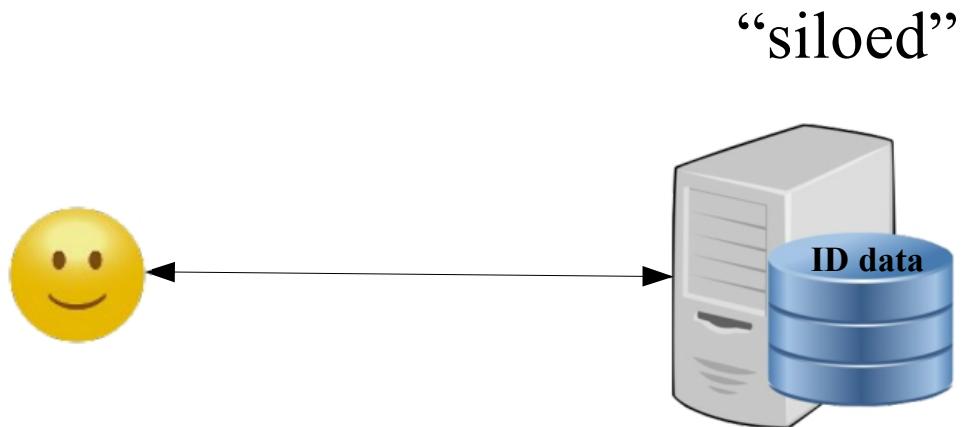
1997  
HashCash – PoW  
Adam Back

1998  
B Money  
Wei Dai

1999  
PBFT

2008  
Bitcoin  
Satoshi Nakamoto

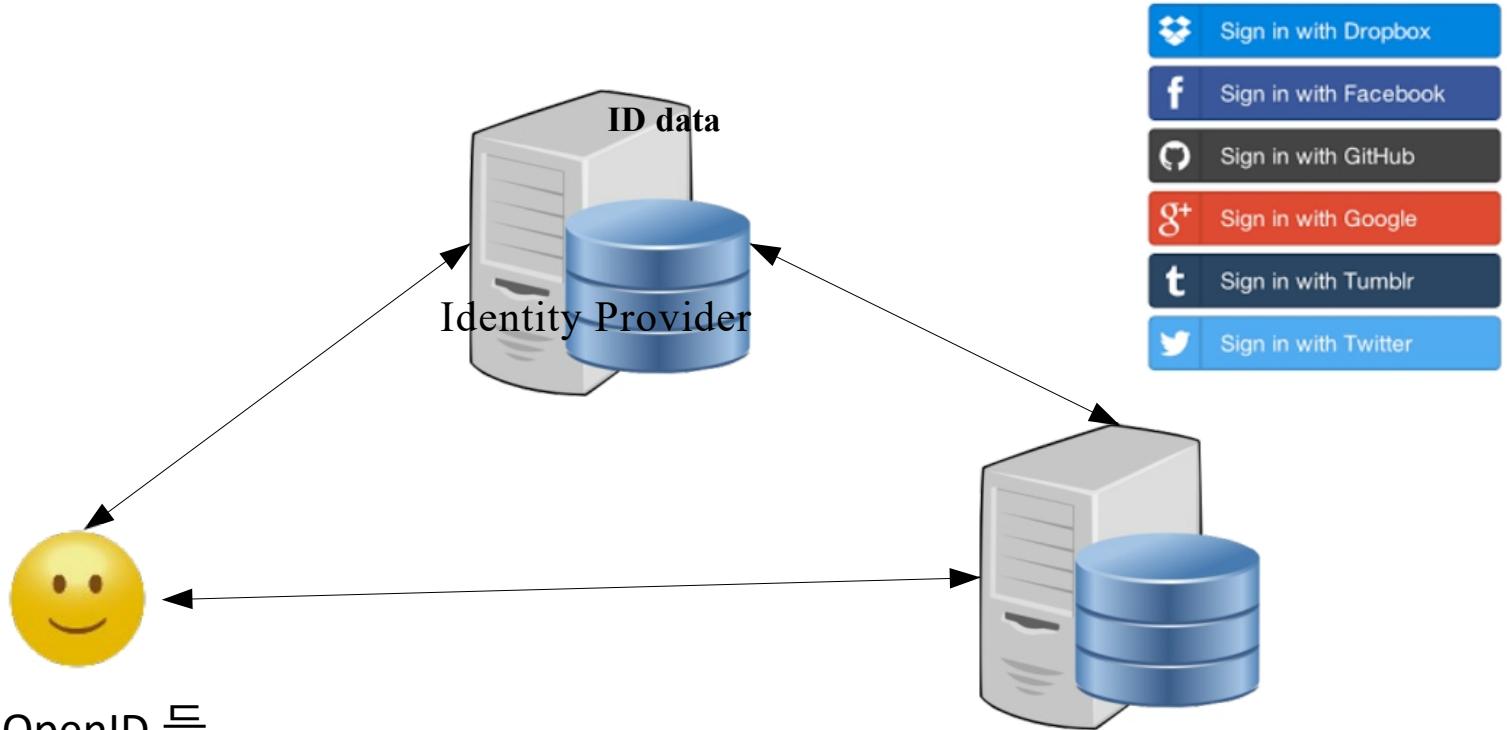
# 1세대 Siloed ID



사이트별 ID & Password

사이트별로 ID& Password 관리의 어려움, 해킹의 가능성증가

# 2세대 Federated ID



OAuth, OpenID 등

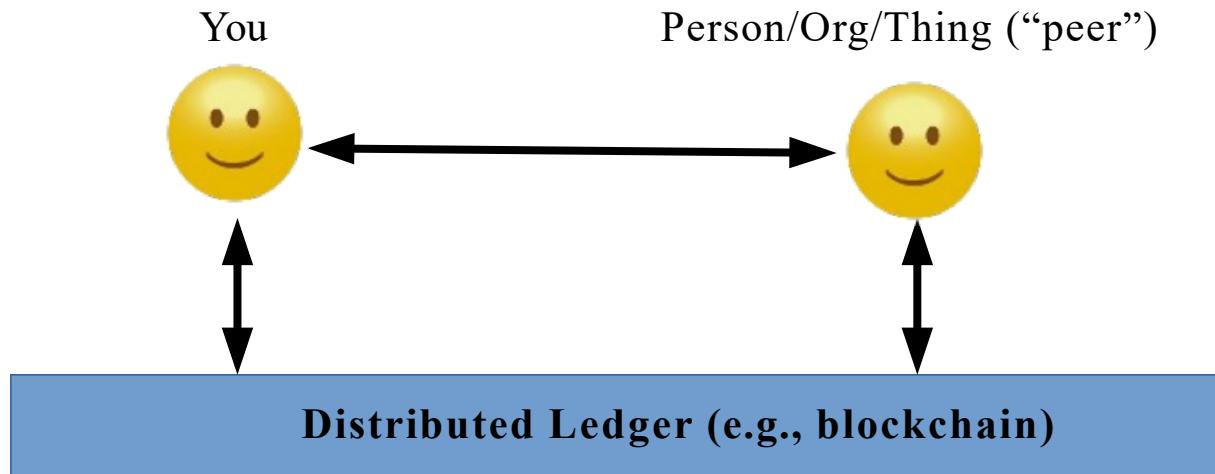
하나의 ID & Password

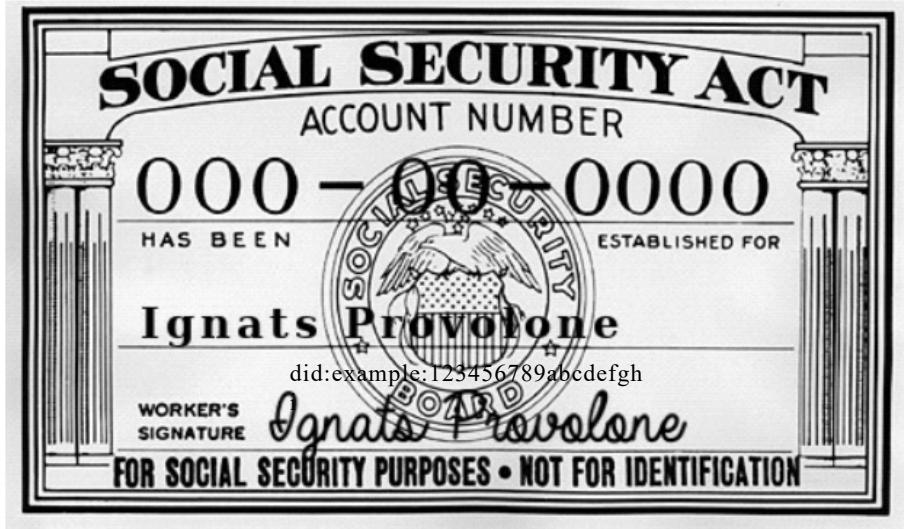
소수의 기업의 독점, 여전히 해킹의 가능성, Facebook 5천만명 개인정보유출사건

# 3세대 자기주권 분산 ID

## “Decentralized, Self-Sovereign ID (SSI)”

A Decentralized Identifier (DID) is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable





did:sov:4e6cf0ed2d8bbf1fbbc9f2a100

# DID란?

- DID는 글로벌 Key-Value 데이터베이스 (Key = DID, Value = DID Document)
- DID Document는 JSON-LD 객체로서 6가지 컴포넌트를 포함
  - **A set of cryptographic material**, such as public keys, that can be used for authentication or
  - **interaction** with the DID subject.
  - **A set of cryptographic protocols** for interacting with the DID subject, such as authentication and capability delegation.
  - **A set of service endpoints** that describe where and how to interact with the DID subject.
  - **Timestamps** for auditing.
  - **A optional JSON-LD signature** if needed to verify the integrity of the DID document.

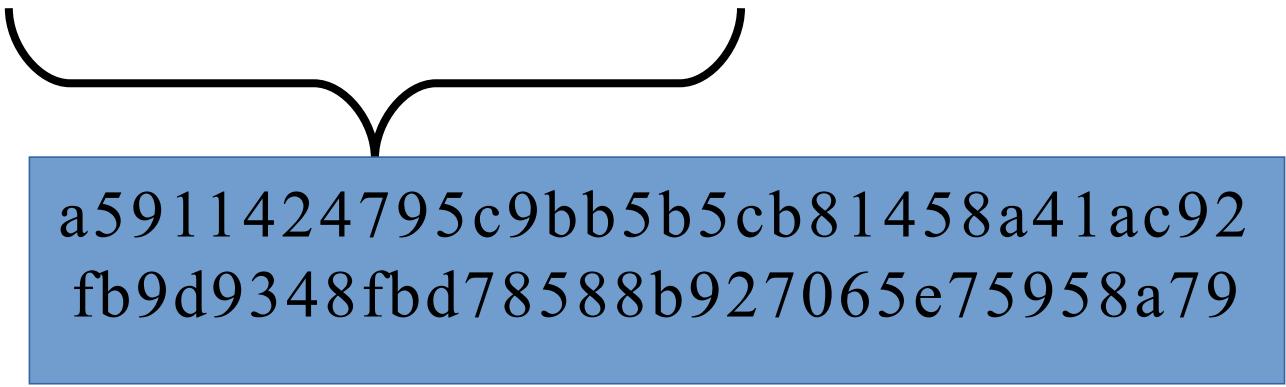
# Decentralized Identifier (DID)

**Format:** “did:” + <method> + “:” <method-specific identifier>

**Example:** did:sov:4e6cf0ed2d8bbf1fb9c9f2a100 **address on a ledger**



**private key in a digital wallet**



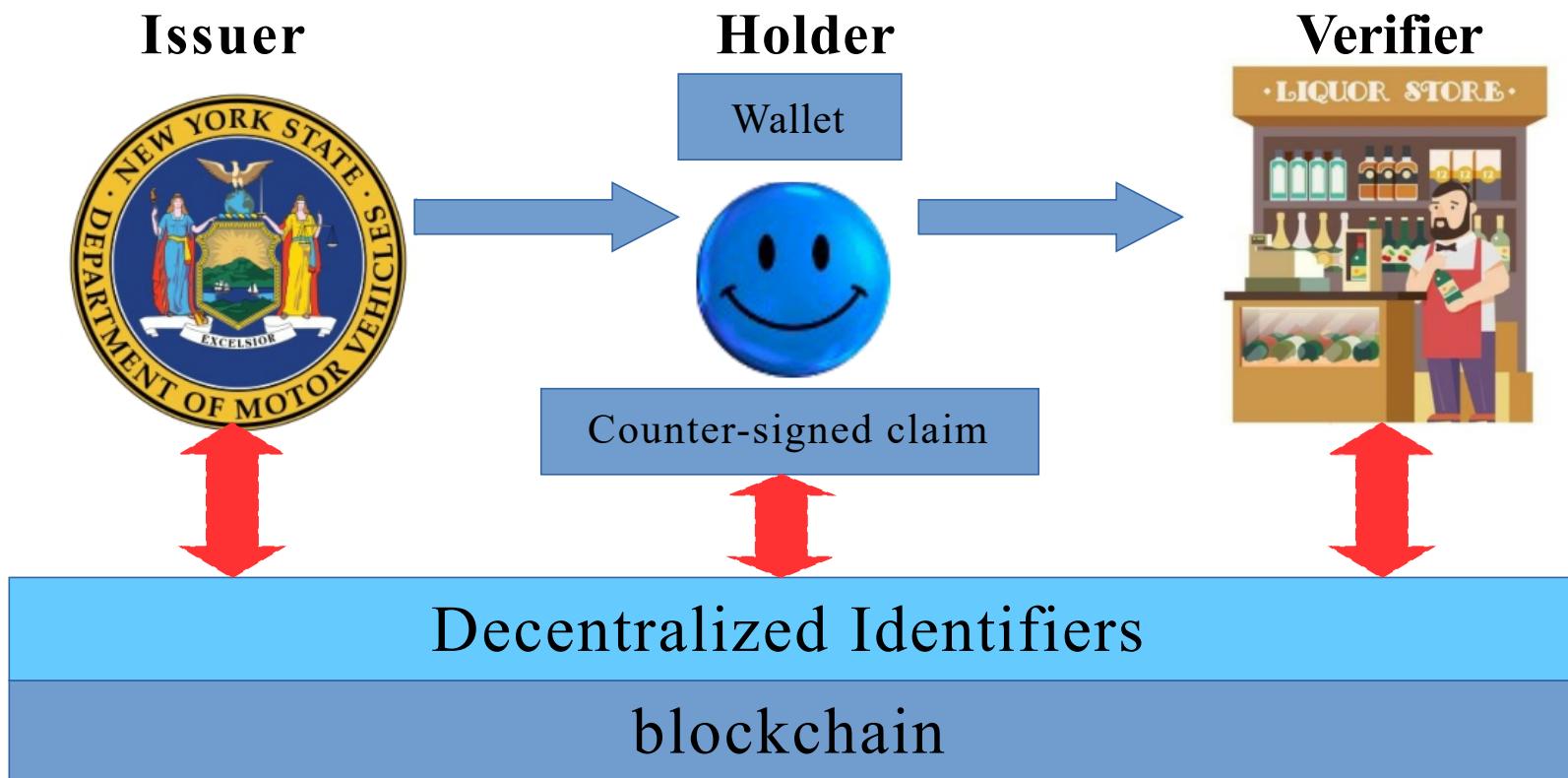
Method	DID Prefix
Sovrin	did:sov:
Bitcoin	did:btcr:
uPort	did:uport:
VeresOne	did:v1:
IPFS	did:ipid:
IPDB	did:ipdb:
Blockstack	did:stack



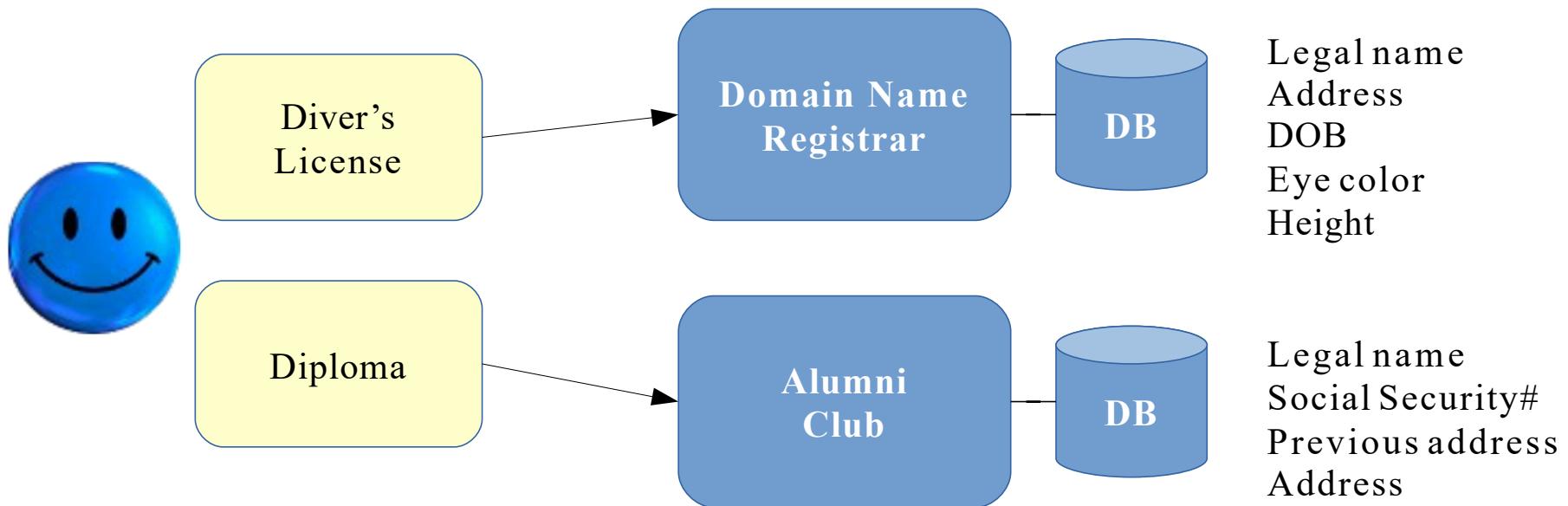
# DID Document Example

```
{  
  "@context": "https://w3id.org/did/v1",  
  "id": "did:example:123456789abcdefghi",  
  "publicKey": [ {  
      "id": "did:example:123456789abcdefghi#keys-1",  
      "type": "RsaVerificationKey2018",  
      "owner": "did:example:123456789abcdefghi",  
      "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----  
      \r\n    },  
    "authentication": [ {  
        // this key can be used to authenticate as DID ...9938  
        "type": "RsaSignatureAuthentication2018",  
        "publicKey": "did:example:123456789abcdefghi#keys-1"  
      }],  
    "service": [ {  
        "type": "ExampleService",  
        "serviceEndpoint": "https://example.com/endpoint/8377464"  
      }]  
}
```

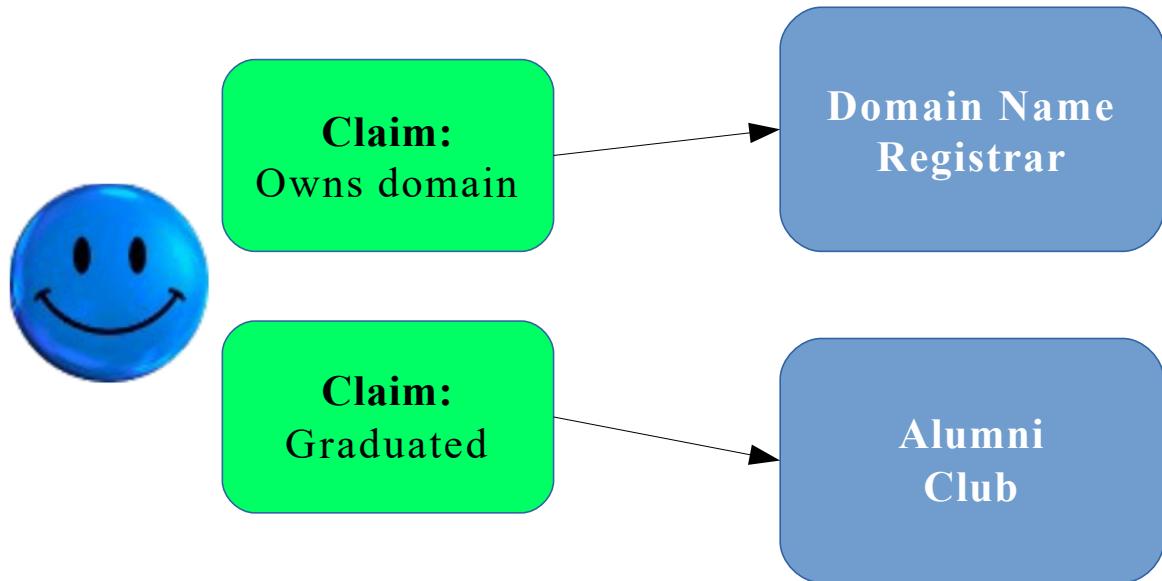
# Verifiable Claim: Are you 21?



# From Who to What



# From Who to What



# Verifiable Credentials

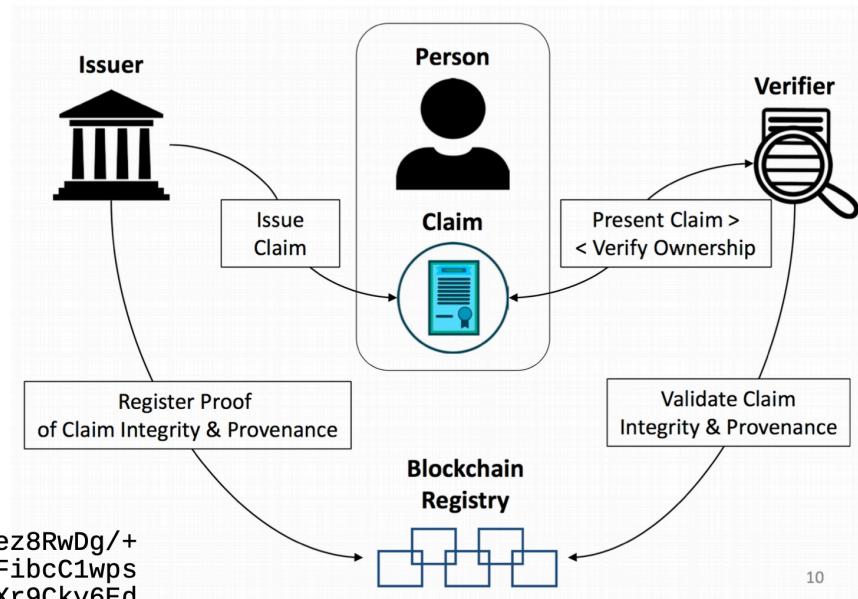
## ■ Example:

```
{
  "@context": "https://w3id.org/security/v1",
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2017-01-01",
  "claim": {
    "id": "did:sov:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavEl10/I1zpYw8XNi1bgVg/sCne04Jugez8RwDg/+  

      MCRVpjOboDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps  

      PRdW+gGsutPTLzvueMwmFhwYmfIFpbBu95t501+rSLHIEuuujM/+PXr9Cky6Ed  

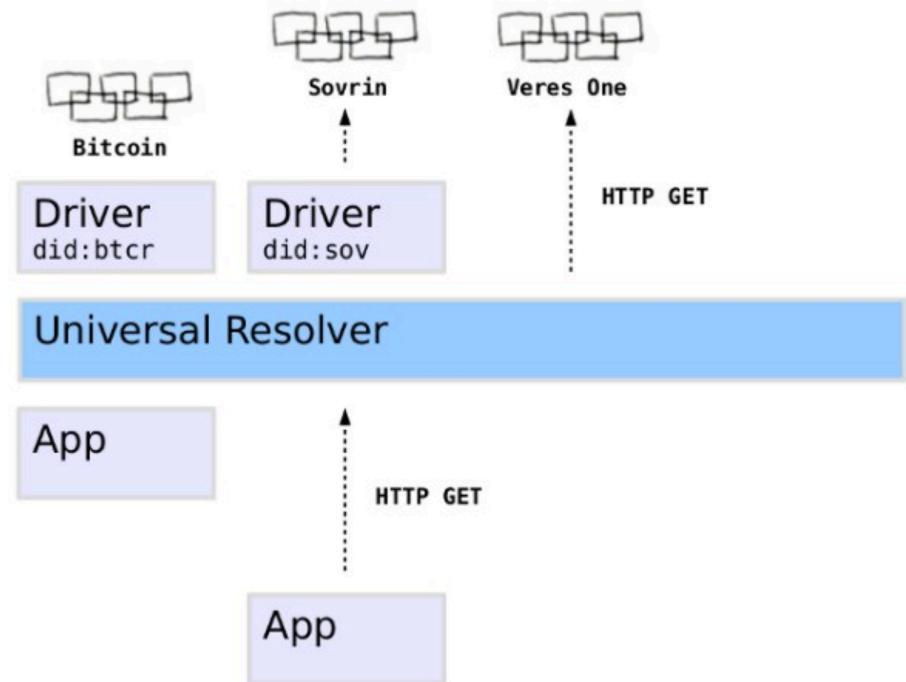
      +W3JT24="
  }
}
```



10

# Universal Resolver

- Looks up (“resolves”) DID to its DID document.
- Provides a universal API that works with all DID methods.
- Uses a set of configurable “drivers” that know how to connect to the target system.
- Can return metadata about the resolution process.
- <https://uniresolver.io/>



# Self Sovereign ID의 10가지 원칙

- SSI 10대 원칙 by Christopher Allen
  - Existence – 사용자는 독립적 존재이어야 한다
  - Control – 사용자는 그들의 개인정보에 대한 통제권을 가져야 한다
  - Access – 사용자는 그들의 개인데이터에 접근 가능해야 한다
  - Transparency – 시스템과 알고리즘은 투명해야 한다
  - Persistence – 개인정보는 장기간 보관되어야 한다
  - Portability – 개인정보와 서비스는 이동 가능해야 한다
  - Interoperability – 개인정보는 호환이 가능해야 한다
  - Consent – 사용자는 그들의 개인정보 사용에 대해 동의하여야 한다
  - Minimize – Claim 의 사용은 최소화 되어야 한다
  - Protection – 사용자의 권리는 보호되어야 한다

# DID와 Privacy by Design

- 1. Pairwise Pseudonymous IDs
  - 휴대전화번호같이 개인당 한개의 ID가 아닌 각 관계마다 Pseudonymous DID
- 2. 개인정보는 오프체인에 저장
- 3. 선택적 공개
  - DPKI?
  - Zero Knowledge Proof?
  - 잊힐 권리?

# DID와 Scalability by Design

- Scalability

- 10억명 (+alpha) 의 신원정보를 넣을수 있는 블록체인?
- SideChain?
- Sidetree by Microsoft?
- IPFS?

- Interoperability

- 서로 다른 Decentralized Identity Platform간의 호환성?

# 신용정보법 드디어 국회 첫발

| 데이터 경제 3법

자료: 각부처

법률명	소관부처	규제완화 주요내용
개인정보보호법	행정안전부	- 가명정보를 상업적 목적으로 활용 가능 - 개인정보 관리 개인정보보호위원회로 일원화
신용정보법	금융위원회	- 가명정보 금융분야 빅데이터 분석 및 이용 가능 - 가명정보 주체 동의 없이 이용 및 제공 허용
정보통신망법	과학기술정보통신부 방송통신위원회	- 온라인상 개인정보보호 규제 감독 권한 개인정보보호 위원회로 변경



금융위원회는 2019년 11월 28일 보도 참고 자료를 내고 신용정보법 개정안이 정무위원회 소위를 통과했다고 밝혔다. 신용정보법 개정안은 빅데이터 분석·이용의 법적 근거 마련을 위해 개인을 알아볼 수 없도록 조치한 가명정보 도입 등을 골자로 한다.

가명정보의 경우 상업적 목적을 포함한 통계작성과 연구, 공익적 기준보존 목적 등으로 동의 없이 활용할 수 있게 됐다.

출처 : 대한금융신문(<http://www.kbanker.co.kr>)

Src: <https://www.kbanker.co.kr/news/articleView.html?idxno=87723>



# DID 신원관리 시장규모

- 2023년 19억달러 예측 (Market Research Future)
- 2024년 34억달러 예측 (Zion Market Research)

# 요약

- Pairwise pseudonymous
  - One for each relationship
- Permanent
- Resolvable
- Cryptographically verifiable
- Decentralized