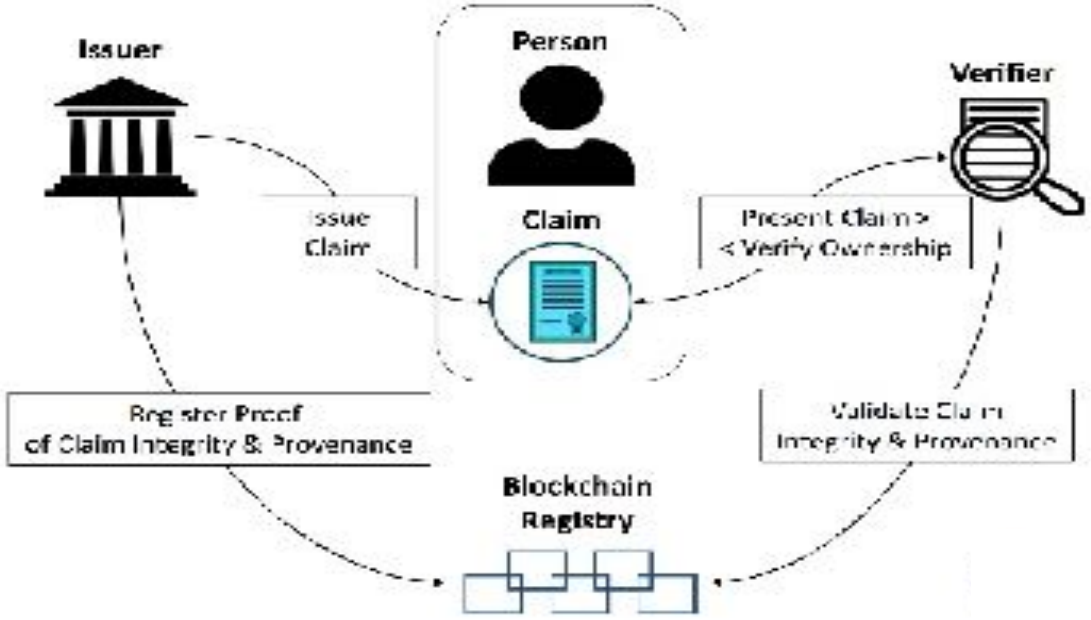
Decentralized ID & Verifiable Claims

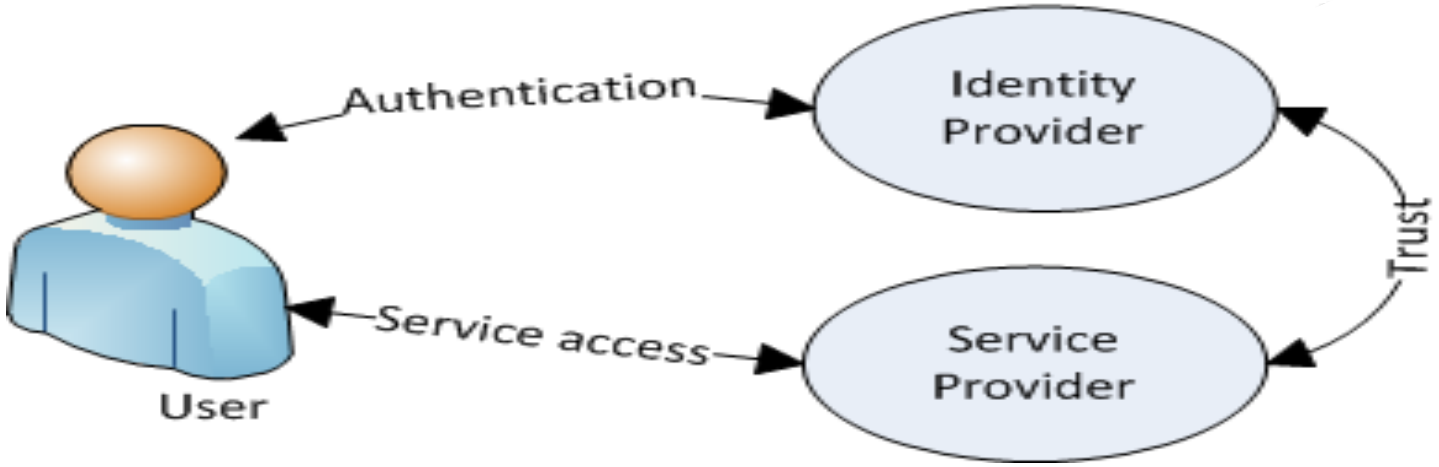
10 minutes, 10 slides, goals, tech details and why it matters



Terminology & Current Model

- Claim or Assertion – a claim or way of communicating what a person or thing is (in doubt until 'claims approval')
- Security token – a set of assertions
- The user requests a resource or service from the SP. The SP requests and receives an identity assertion from the IdP. This assertion allows the SP to make the access control decision to perform the service for the user.

Reference: 'The Laws of Identity' Kim Cameron (5/11/2005)

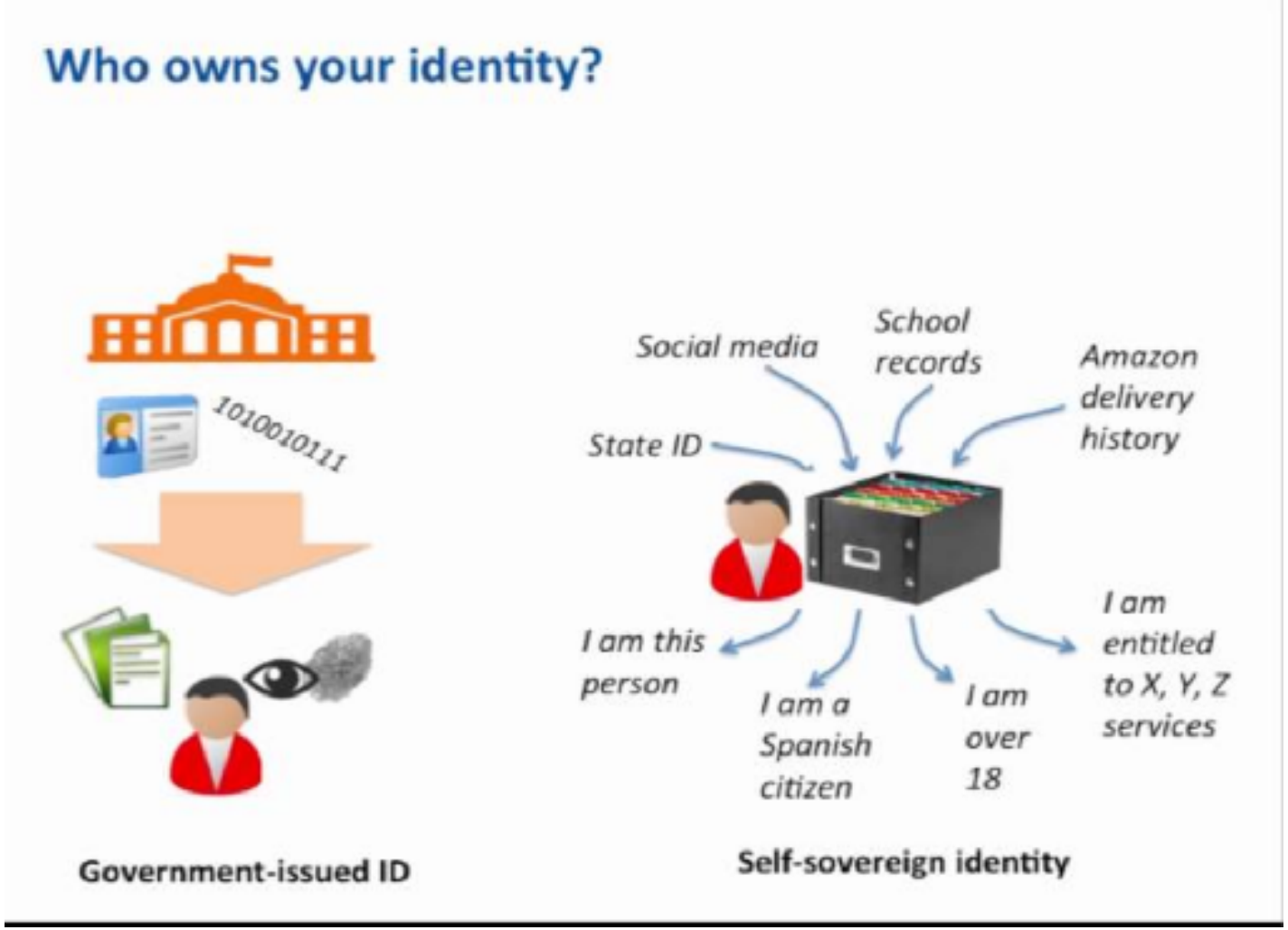


Identity provider - Trusted identity proofing entity (Google, agency, bank, etc.

Service provider – vendor, or Other agency

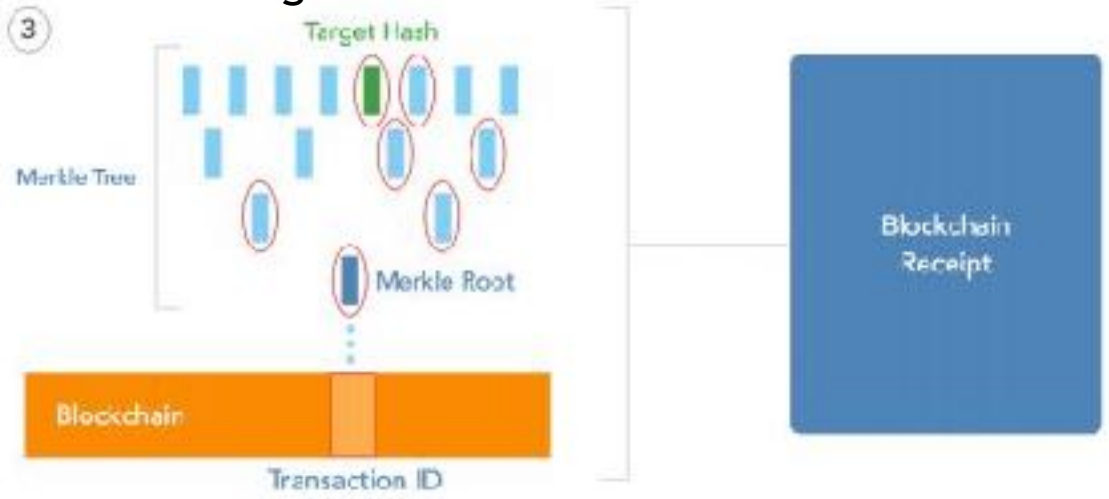
Self-Sovereign Identity – Individual as 'Identity Provider' (Much initiated 'Rebooting the Web of Trust' workshops created by Christopher Allen (one of the authors of SSL). http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html)

- User centric identity started with "the assumption that every individual ought to have the right to control his or her own online identity"
- Until recently final ownership of all identities remained with the entities that register them – which could take them away at any time!
- Self-sovereign identity is a concept, where an individual is able to control his/her identity attributes – that some credentials are NOT revocable by nations, companies, etc.
- Current 'Self-sovereign identity' systems employ both blockchain/ crypto and legal policies to support 'self-sovereignty'



Blockchain Basics

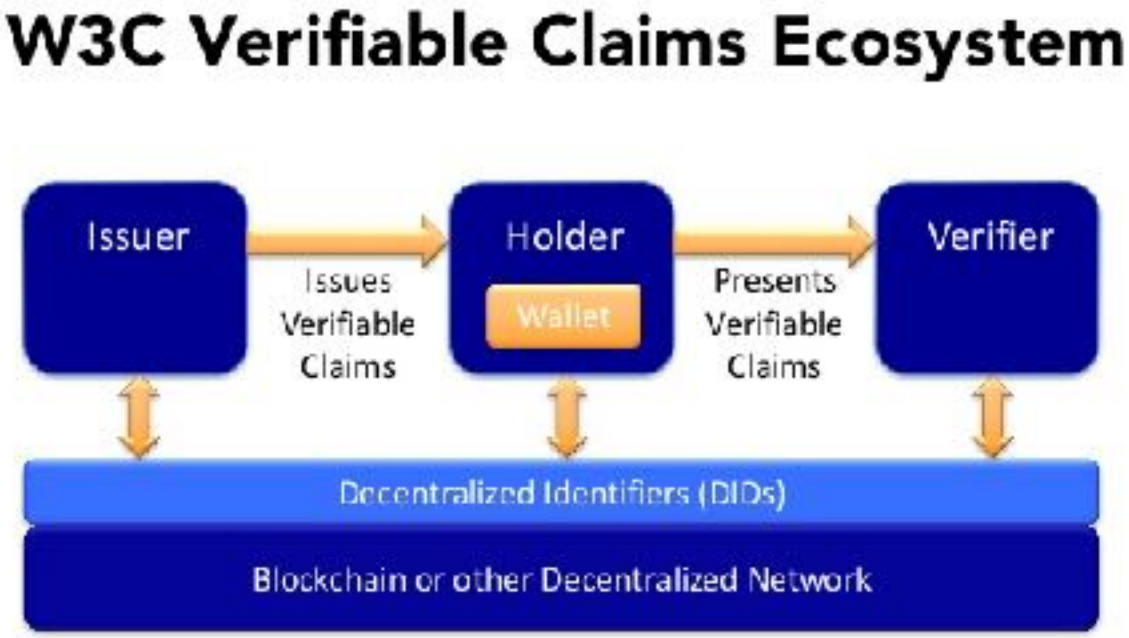
To write data to a blockchain, hash the data, assemble multiple hashes into a block,
structured as Merkle Tree. Blocks are time stamped and once the block is verified (via PoW, PoS, PoA, ..) and published it cannot be changed



A blockchain receipt provides proof that some data existed at a specific time. It contains all the information needed to prove that an individual hash was published in a transaction in a blockchain. A blockchain receipt should contain target hash, Merkle proof, Merkle root and transaction ID.

W3C Decentralized Identifiers (DIDs) v0.7

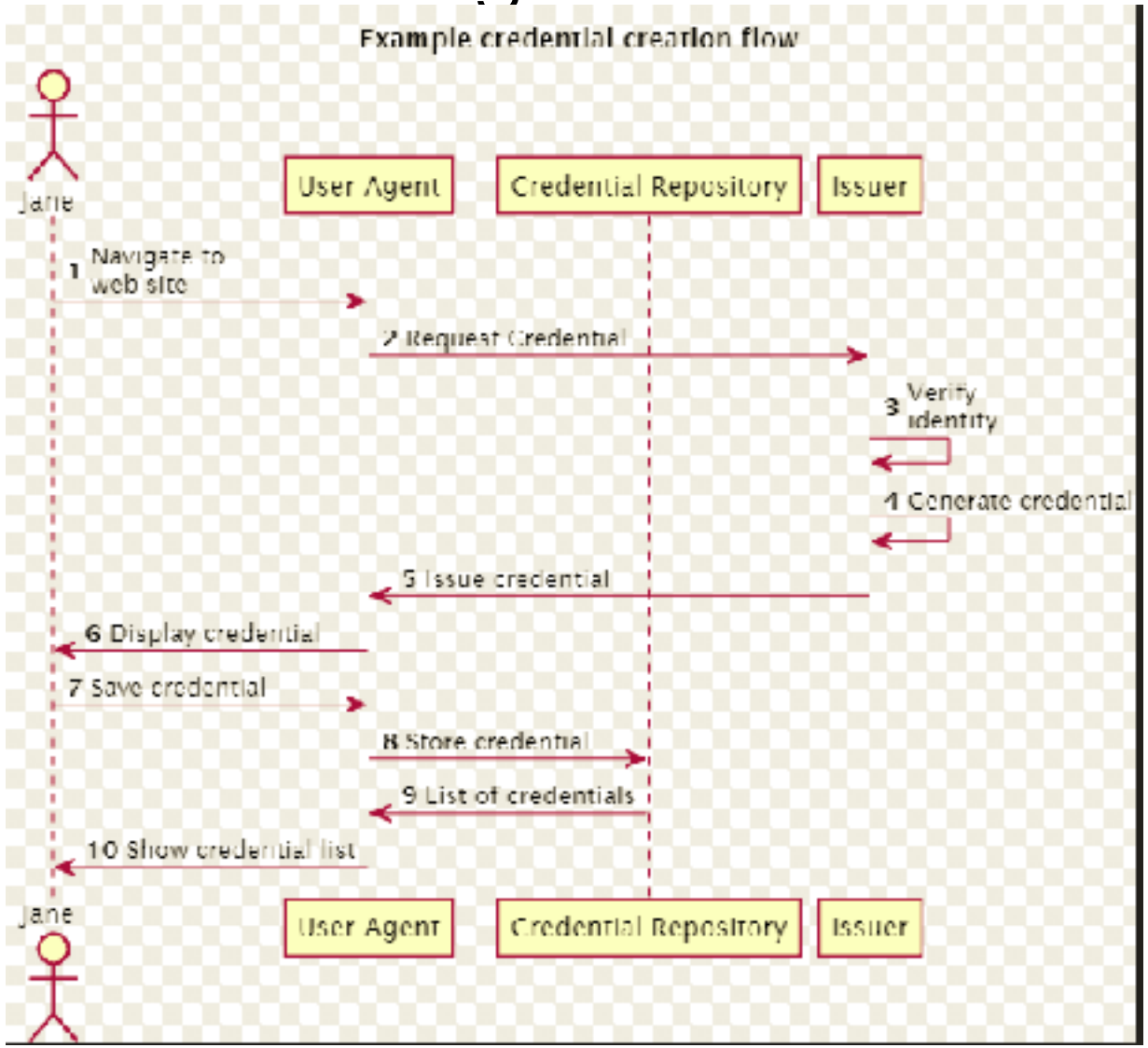
- Decentralized Identifiers (DIDs) are a new type of identifier for verifiable "self-sovereign" digital identity.
- DIDs are fully under the control of the DID owner/user/'subject' - the are URIs, but don't have to be findable through DNS or IP addresse
- Specified by DID documents which specify:
  - cryptographic capabilities including authentication, and
  - service endpoints which define 'trusted' interactions.



Can think of a DID document as a class, and a DID an
Object that can provide various ID related

Verifiable Claims Data Model and Representations W3C First Public Working Draft 03 August 2017

- Driver's licenses are used to claim that we are capable of operating a motor vehicle,
- University degrees can be used to claim our education status, and
- Government-issued passports enable holders to travel between countries.
- Verifiable claims are statements made by an entity about a ‘subject’ whose authorship can be cryptographically verified and dated
- Ideally - cryptographically secure, privacy respecting, and automatically verifiable.



DID Formats

- Typically ‘JSON-LD’ (Linked Data) and may contain:
  - Exactly one top-level context statement
  - Primary ID
  - Authentication credential
  - Authorization capability
  - Credential repository service
- DID operations – at a minimum CRUD
- DID resolvers accept requests for DID lookups and execute the corresponding DID method

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authorizationCapability": [{
    // this entity is a delegate and may update any field in this
    // DID Document using any authentication mechanism understood
    // by the ledger
    "permission": "UpdateDidDocument",
    "entity": "did:example:zxyvwtrkpn987654321"
  }],
  "credentialRepositoryService": "https://vc.example.com/abcdef",
  "authenticationCredential": [{
    // this biometric can be used to authenticate as DID ...fghi
    "id": "did:example:123456789abcdefghi/biometric/1",
    "type": "PseudonymousBiometricTemplate2017",
    "owner": "did:example:123456789abcdefghi",
    "biometricService": "https://example.com/authenticate"
    "biometricTemplateShard": "Mjk4MzQyO...5Mzg0MDI5Mwo="
  }]
}
```

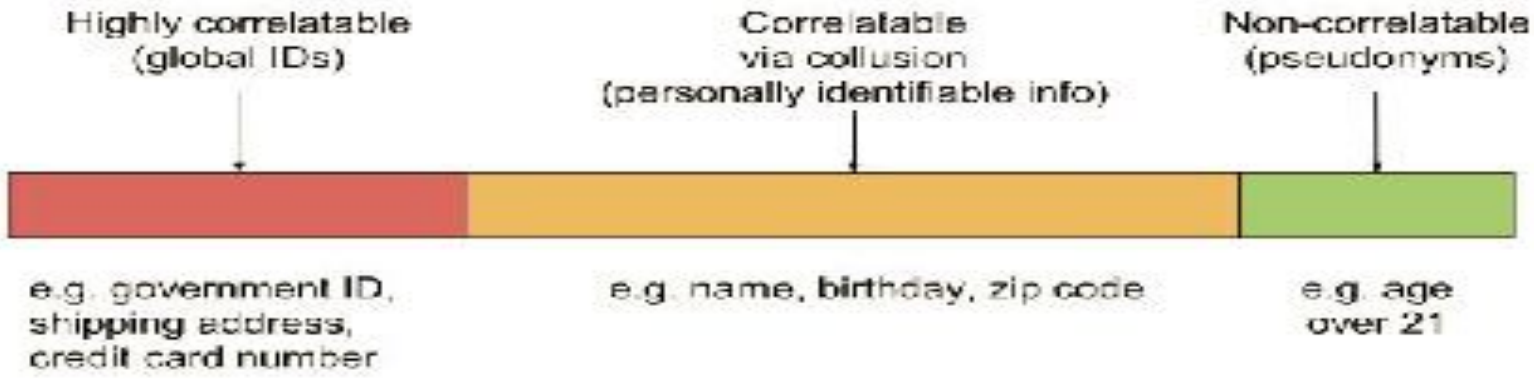
Verifiable Claims Forma

- Typically JSON or JSON-LD
- IDs for both entities issuing claims, and subjects of those claims are URI representing them. May be long-lived but not required.
- Entities have id, type and signature
- Claims – Contain subject ID at least one custom property and is signed by the issuer


```
{
  "@context": "https://w3id.org/security/v1",
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": [
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  ],
  "revocation": {
    "id": "http://example.gov/revocations/738",
    "type": "SimpleRevocationList2017"
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:10:18Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/
    MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
    [illegible]
    +k3JT24="
  }
}
```

Various issues

- Some of the standard PKI applies to DPKI – proving ownership of a public keys, non-repudiation, timestamps, key and signature expiration, revocation and recovery
- Different - Proving ownership of DIDs and verifying claims, keeping the right information on and off chain (e.g. PII typically off ledger)
- DID correlation and pseudonymous DIDs
- Hashing private information and putting the hash on a timestamped public ledger
- Zero knowledge proof (ZPF) technology



Real world initiatives?

- Various DID formats are defined and in use (sovrin, bitcoin, uport, Consent, Veres One)
- Sovrin Trust Framework - International, non-profit Sovrin Foundation is governed by a constitutional Trust Framework that ensures its independence from government or industry influence and codifies its dedication to providing self-sovereign digital identity for all.
- Technology & Utilities - Decentralized identity foundation (IDF) is working on universal resolver for DIDs, identity hubs, protocols (chainpoint)
- Refugees/Document-less ‘citizens’ and UN ID2020:
  - Blockchain for Social Impact Coalition (BSIC)
  - World Food Program (WFP) Building Blocks Program
  - Project Amply - early childhood development in Africa
  - Kora project & Everex – for those underserved by current financial system
- Pilot projects for Canada, Illinois, and various refugee projects