Blockchain's Relationship with Sovrin for Digital Self-Sovereign Identities

Daan Weller & Raoul Dijksman
Our Project

- TNO
- Sovrin identity network
- Self-Sovereign Identity
- Blockchain technology
To what extent does the Sovrin network require blockchain for self-sovereign identity?
Research Questions

- What is Self-Sovereign Identity?
- How does Sovrin implement self-sovereign identity?
- Which functions are supported by blockchain technology?
What is Self-Sovereign Identity?
Self-Sovereign Identity (SSI)

User-centric:
- Independent existence, persistence
- Control over credentials, portability, consent of presentation
- Interoperability
- Protection of user rights

The individual is able to control the credentials and use them in a privacy-preserving manner whenever and wherever they want.
Decentralized Identifiers (DID)

- Created and controlled by the DID subject
- Ownership can be cryptographically proven
- Has corresponding DID document
- URI format:

```
Scheme
did:example:123456789abcdefghijkl
```

Image: https://github.com/WebOfTrustInfo/rwot6-santabarbara
DID Document

- JSON object
- Key/Value - DID/DID Document
- Everything necessary to setup cryptographically-verifiable interactions with the DID subject
  e.g. public keys, authentication protocols, and service endpoints

```json
{
    "@context": "https://w3id.org/did/v1",
    "id": "did:example:123456789abcdefg01",
    "publicKey": [{
        "id": "did:example:123456789abcdefg01#keys-1",
        "type": "RsaVerificationKey2018",
        "owner": "did:example:123456789abcdefg01",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...
        "authentication": [{
            "type": "RsaSignatureAuthentication2018",
            "publicKey": "did:example:123456789abcdefg01#keys-1"
        }],
    "service": [{
        "type": "ExampleService",
        "serviceEndpoint": "https://example.com/endpoint/8377464"
    }]
}
```
Identity and claims

- Identity consists of attributes
- A claim is an assertion about a attribute of the subject
- Validity of claims
Verifiable Credentials

- Work in progress by the W3C
- A set of claims made by an issuer
- A verifiable credential is a tamper-evident credential that can be cryptographically verified.
Verifiable Credentials

Issuer -> Issue Credentials -> Holder

Holder -> Send Presentation -> Verifier

Issuer -> Verify Identifiers & Use Credential Schema

Verifiable data registry

Verifier -> Verify Identifiers & Credential Schema
Blockchains

- *Distributed Ledger Technology* (DLT)
- Immutable datastore
- Peer-to-peer network with a consensus algorithms to ensure replication across nodes
- Validators of new blocks may be unknown
  requires proof: e.g. *proof of work* or *proof of stake*
- Permissioned blockchains: validators are invited to take part in the network
Decentralised Key Management System (DKMS)

- Enables the creation of secure private channels
- No centralised authorities
- Alternative to centralised PKI with CAs
- *Trust* is gained from exchanged verifiable credential
DKMS Trust Relationship

Issuer -> Issue’s Credentials -> Holder

Holder -> Present Credentials -> Verifier

Issuer <-> Verifier: Existing Trust Relationship
Web of Trust

- *Trust* is the certainty of a public key actually belonging to the person in question
- Trust may be assigned individually or derived from others, i.e. key signing
- *Trust anchors* may provide trust on greater scale
- *Key servers* are special servers that provide keys and *trust signatures*
Trust model in PGP

"Trust" comes from Bob's Key Pair

Bob's Key Pair

Owens
Trust model in DKMS

- Alice
- Alice's Computer
- Bob's Computer
- Bob

Bob's Key Pair:
- Credential #1
- Credential #2
- ... (N)

Issuer #1
Issuer #2
Issuer #N

"Trust" comes from

Satifies Issuer requirements

Owns

Issues
DLT in Sovrin

- Public DID's
- Credential Schema's & Definitions
- Agent Policies
- Revocations
Sovrin’s DLT contributes to:

- Key management problem
- Secure user’s privacy
- Ensure technical decentralisation - No centralised *root of trust*
Future Work

- Implications of the introduction of the Sovrin Token
- Alternative implementation of Verifiable Credentials with out DLT
Questions?