sovrin

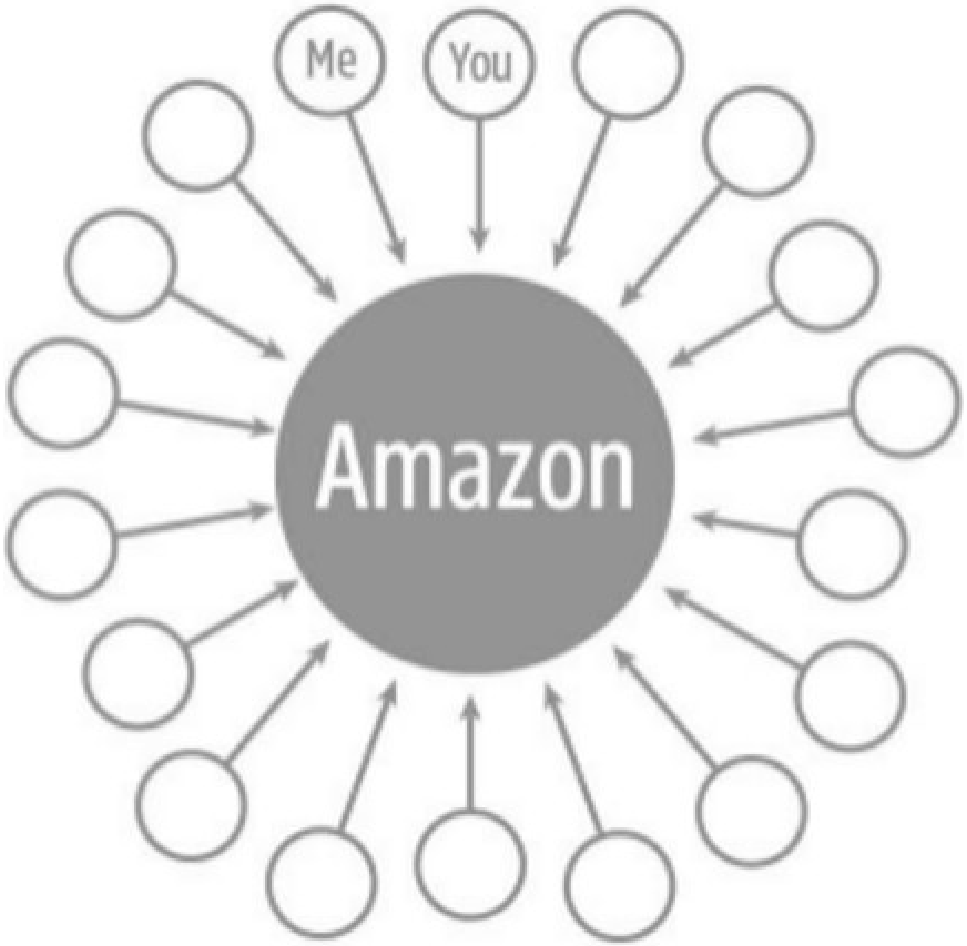
identity for all

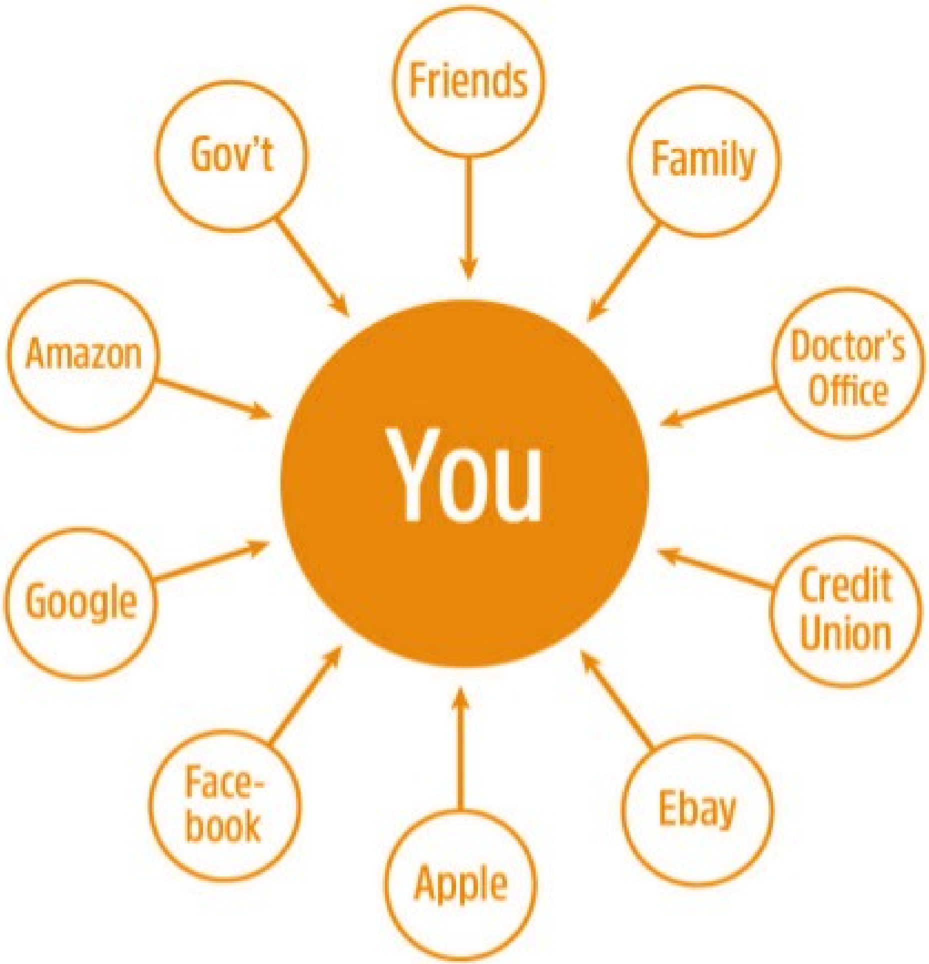
Markus Sabadello
Sovrin Foundation
Technical Governance Board

Vienna, 15th February 2018

... so home values and rents will soar due to hedonistic wage rises ...
P. Steiner

"On the Internet, nobody knows you're a dog."


Me
You
Amazon


Friends
Gov't
Family
Amazon
Doctor's Office
You
Google
Credit Union
Face-book
Apple
Ebay

Sovrin

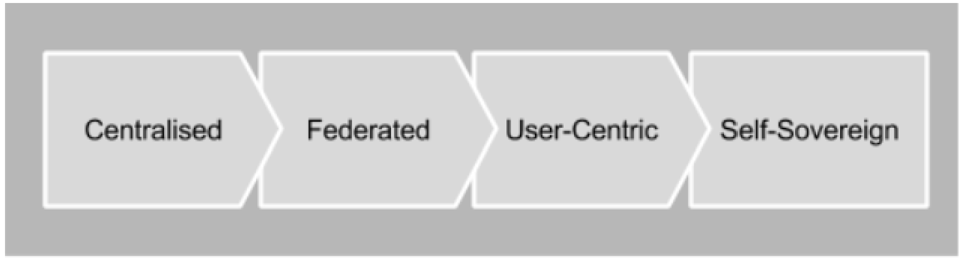
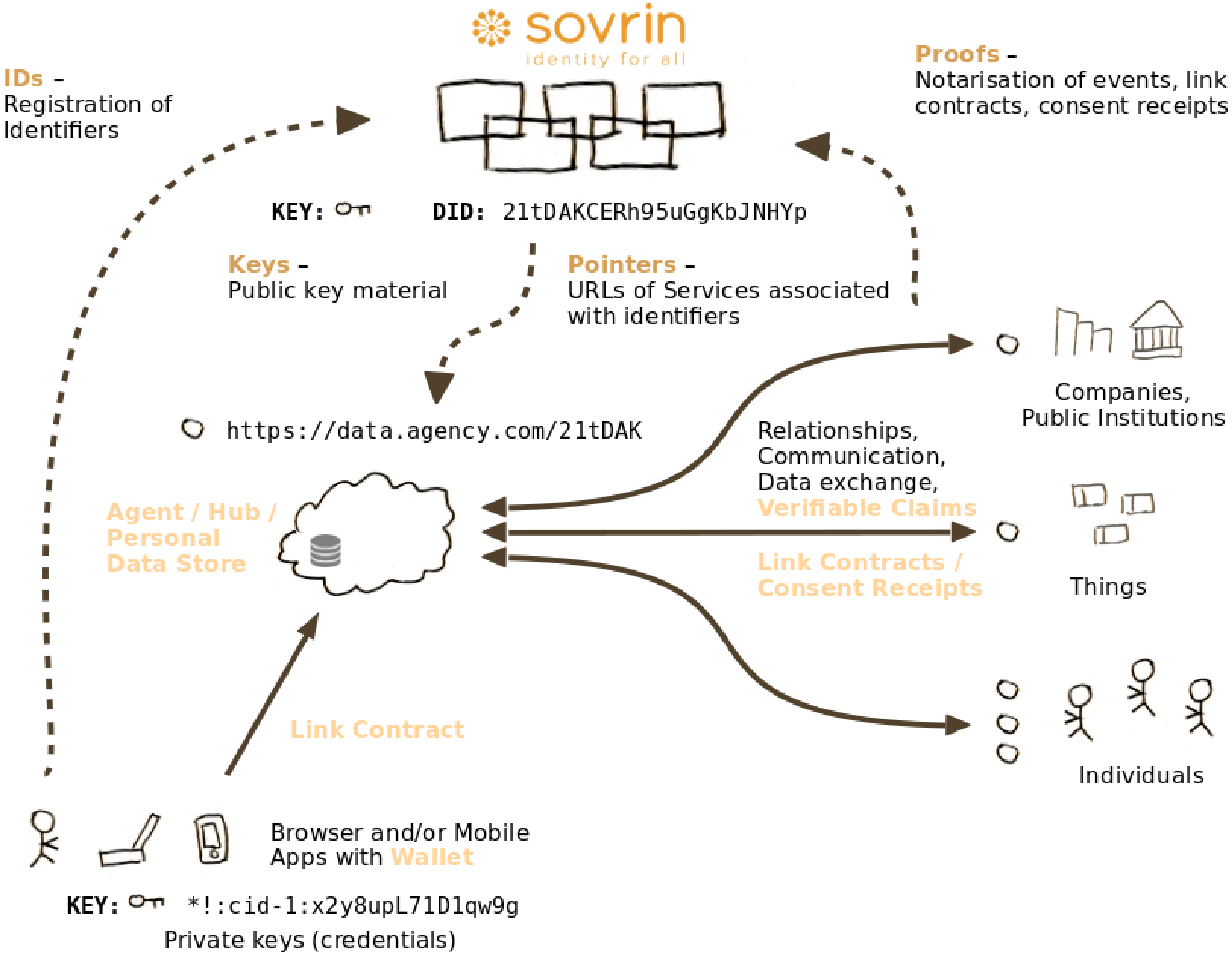


Fig 1. The evolution of online identity

- No cryptocurrency, no smart contracts.
- A distributed ledger as a registry for identifiers and keys.
- A global public utility, a digital identity backbone.
- Trust in math and protocols, instead of trust in humans.
- Digital identity for persons, organizations, things, that can only be created, used, modified, and destroyed by the identity owner.
- Decentralized Public Key Infrastructure (DPKI).

Sovrin Technology

Architecture



sovrin
identity for all

IDs –
Registration of
Identifiers

Proofs –
Notarisation of events, link
contracts, consent receipts

KEY: **DID:** 21tDAKCERh95uGgKbJNHYp

Keys –
Public key material

Pointers –
URLs of Services associated
with identifiers

https://data.agency.com/21tDAK

**Agent / Hub /
Personal
Data Store**

Relationships,
Communication,
Data exchange,
Verifiable Claims

**Link Contracts /
Consent Receipts**

Companies,
Public Institutions

Things

Individuals

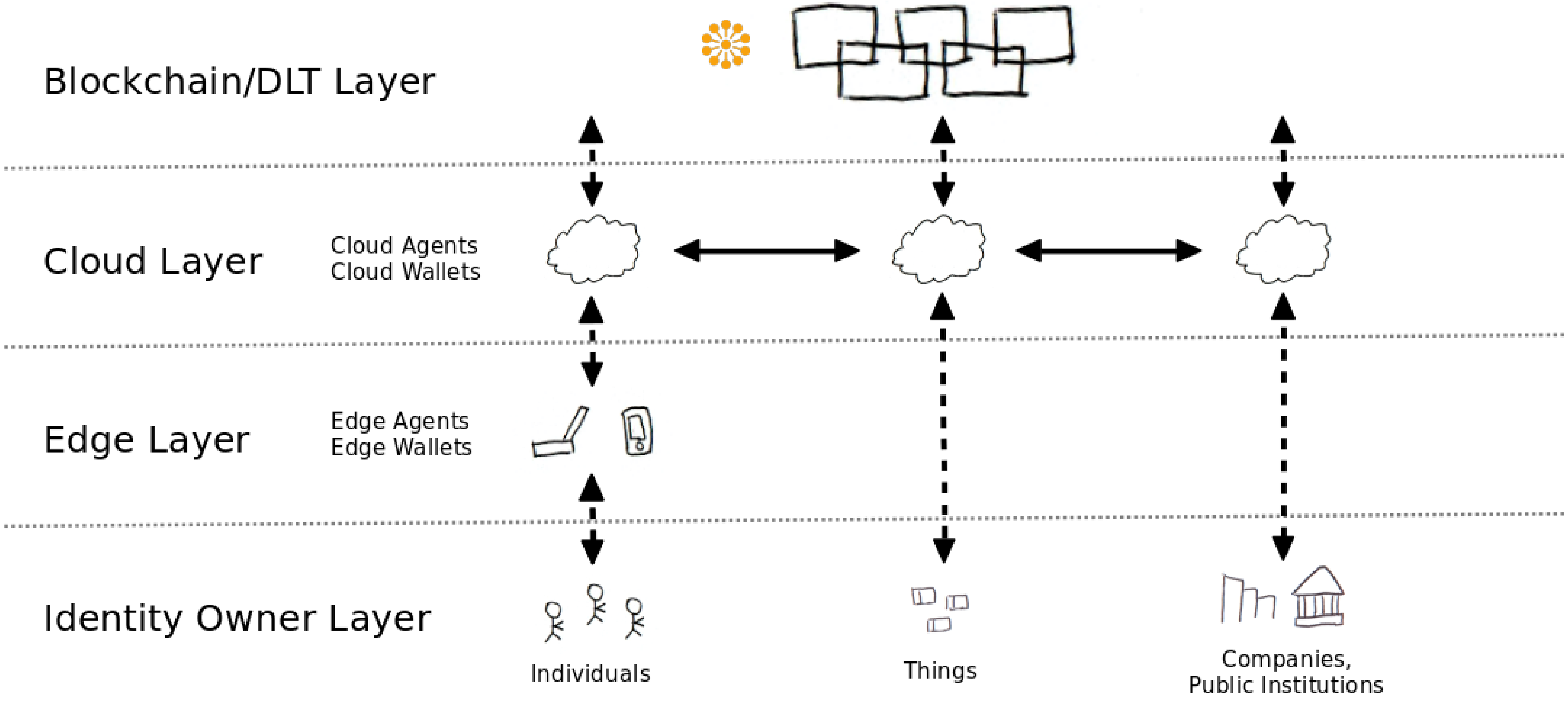
Link Contract

Browser and/or Mobile
Apps with **Wallet**

KEY: *!:cid-1:x2y8upL71D1qw9g
Private keys (credentials)

sovrin

Architecture



Blockchain/DLT Layer

Cloud Layer

Cloud Agents
Cloud Wallets

Edge Layer

Edge Agents
Edge Wallets

Identity Owner Layer

Individuals

Things

Companies,
Public Institutions

Decentralized Identifiers (DIDs)

- Decentralized IDentifiers, developed at Rebooting-the-Web-of-Trust, Internet Identity Workshop, and W3C
- Persistent, dereference-able, cryptographically verifiable identifiers
  did:sov:3k9dg356wdcj5gf2k9bw8kfg7a
- Modular specification using “methods”:
  did:sov, did:btcr, did:v1, did:uport, …
- Resolution: DID → DID Document
  - Set of public keys
  - Set of service endpoints
- Support pairwise-pseudonymous identifiers.

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

Decentralized Identifiers (DIDs)

```
{
    "@context": "https://w3id.org/did/v1",
    "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
    "publicKey": [
        {
            "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
            "type": "Ed25519VerificationKey",
            "publicKeyBase58": "lji9qTtkCydxtez_bt1zdLxVMMbz4SzWvlqgOBmURoM"
        }
    ],
    "services": [
        {
            "id": "#srv1",
            "type": "agent",
            "serviceEndpoint": "https://agent.example.com/did:sov:WRfXPg8dantKVubE3HX8pw/"
        },
        {
            "id": "#srv2",
            "type": "xdi",
            "serviceEndpoint":
                "https://xdi.example.com/did:sov:WRfXPg8dantKVubE3HX8pw/",
        }
    ]
}
```

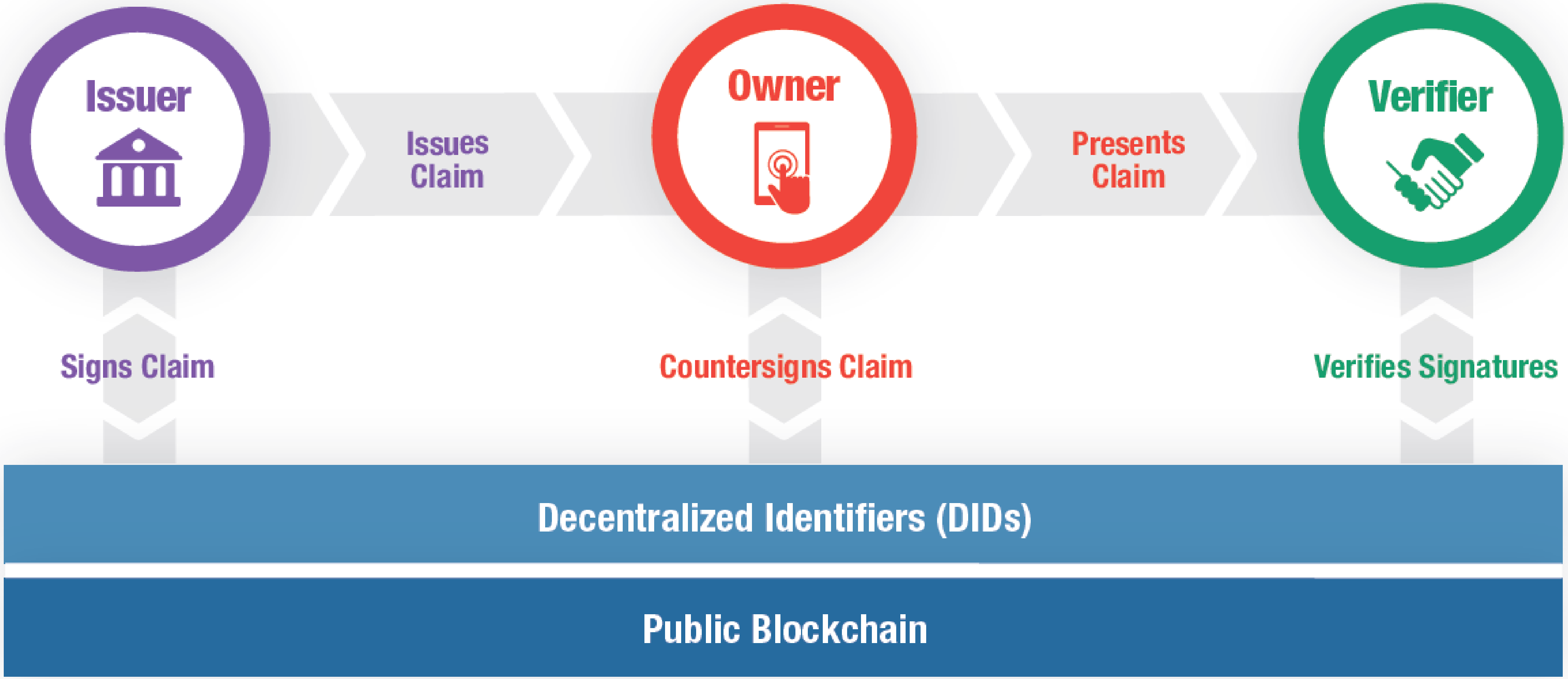
Verifiable Claims

- Semantic data that is “attested” instead of “self-asserted”.
- Cryptographically verifiable statements of an entity (“Issuer”) about another entity (“Subject”), e.g.:
  - Post office says: “Ms. Stern has an address in 1010 Vienna.”
  - University says: “Mr. Sabadello has a Master’s degree.”
- Based on RDF data model and JSON-LD format.
- Support selective disclosure using zero-knowledge proofs.

Verifiable Claims

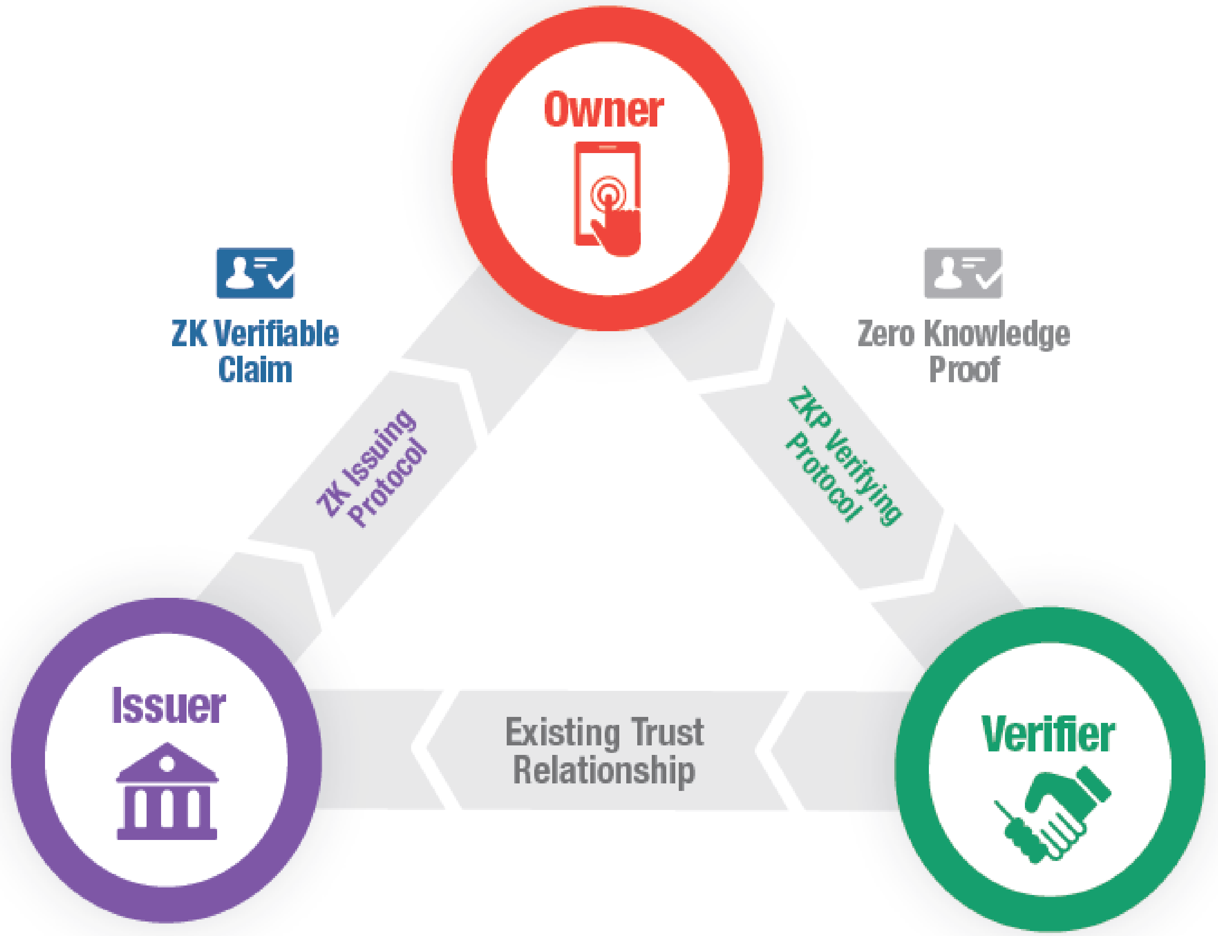
```
{
  "@context": "https://w3id.org/security/v1",
  "type": ["Credential", "AddressCredential"],
  "issuer": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "issued": "2017-01-01",
  "claim": {
    "id": "did:sov:Bda9VcXbnUGFaDZSHdbEhn",
    "street": "Wallnerstraße 8",
    "postalCode": "1010",
    "city": "Vienna",
    "country": "Austria"
  },
  "signature": {
    "type": "LinkedDataSignature2017",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4..."
  }
}
```

Verifiable Claims



Verifiable Claims

- Support pairwise-pseudonymous identifiers.
- Support selective disclosure using zero-knowledge proofs.



Trust Framework

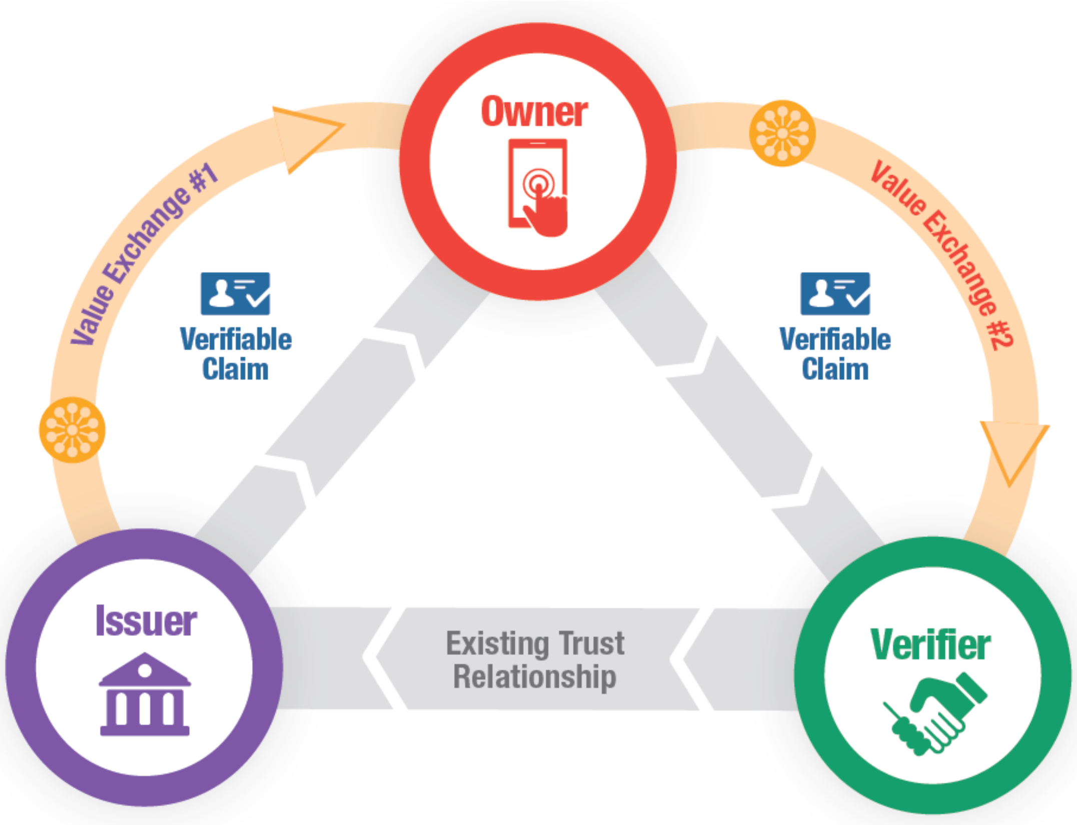
Sovrin Trust Framework

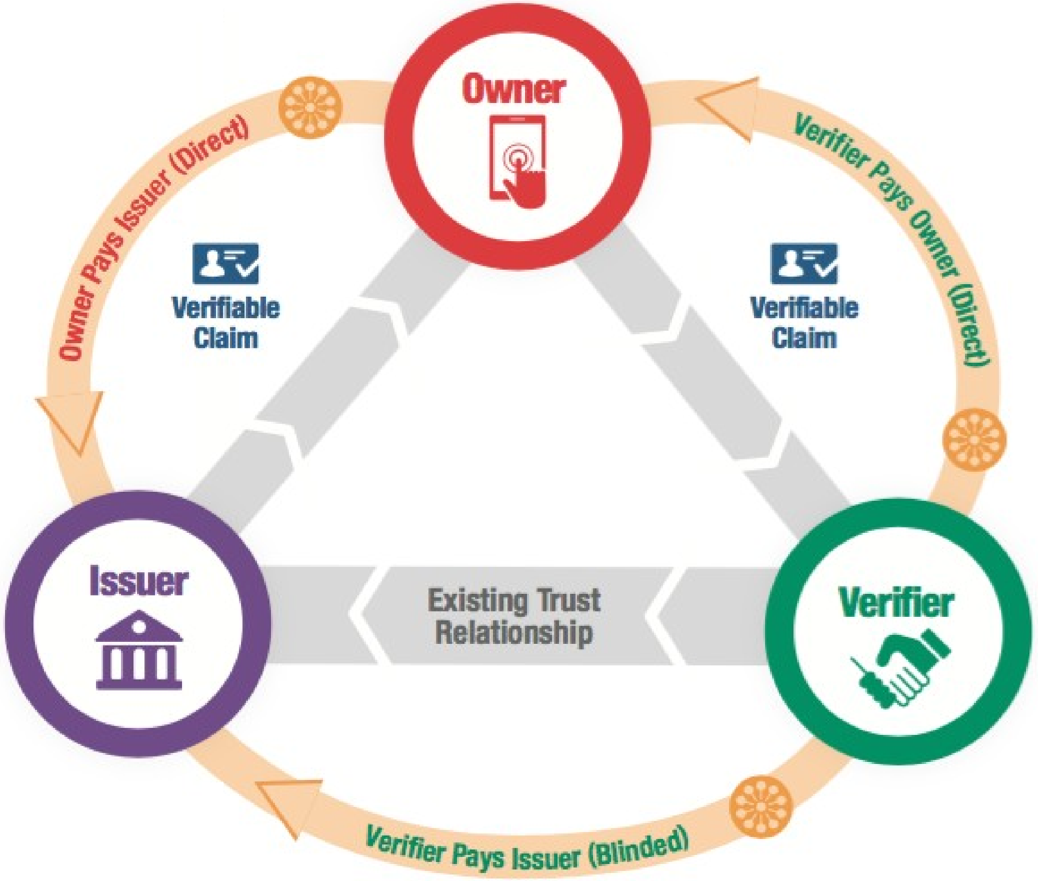
- Question:
  - How does a verifier determine whether they can trust the issuer of the claim?
  - Without a single “root of trust”?
- Answer:
  - Anyone can be a “root of trust”.
  - Communities define Trust Frameworks with business and legal rules.
- Sovrin Web of Trust Alliance:
  - Law firms help their clients develop “Sovrin Powered Trust Frameworks”

Sovrin Token

token

There is value in exchange of trusted, verifiable claims in digital relationships and transactions.




Owner
Owner Pays Issuer (Direct)
Verifier Pays Owner (Direct)
Verifiable Claim
Verifiable Claim
Issuer
Existing Trust Relationship
Verifier
Verifier Pays Issuer (Blinded)

“Premium Claims”

sovrin

identity for all

Sovrin Governance

Governance

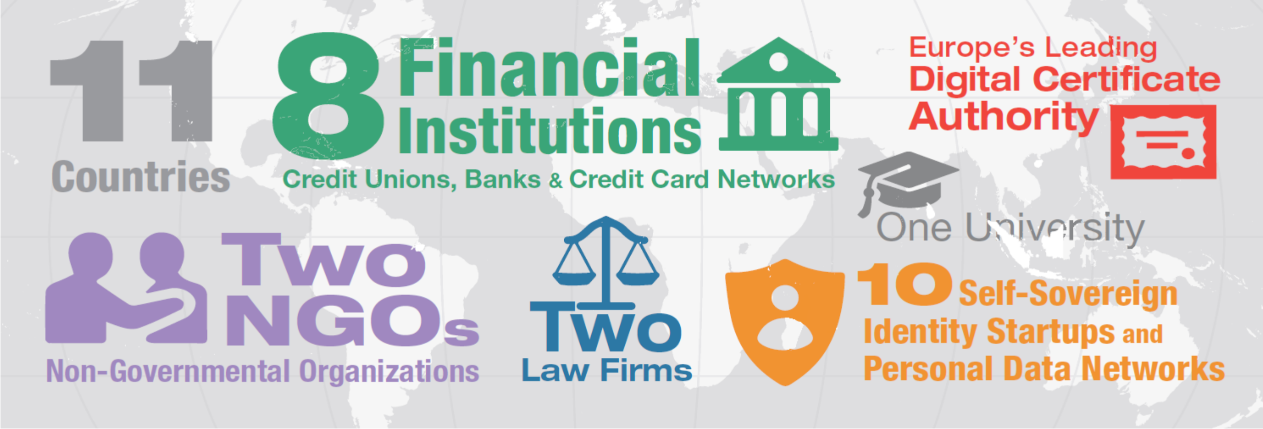
Who can operate a node?

Who can use the nodes?

	Permissionless	Permissioned
Public	Bitcoin Ethereum Veres One IOTA	Sovrin IPDB
Private	Hyperledger Sawtooth* * in permissionless mode	Hyperledger (Fabric, Sawtooth, Iroha) R3 Corda CU Ledger

Governance

- Sovrin Foundation
  - Board of Trustees
  - Technical Governance Board
  - Various Working Groups
- Sovrin Trust Framework
- Over 30 stewards, and growing…
- Principle of “Diffuse Trust”

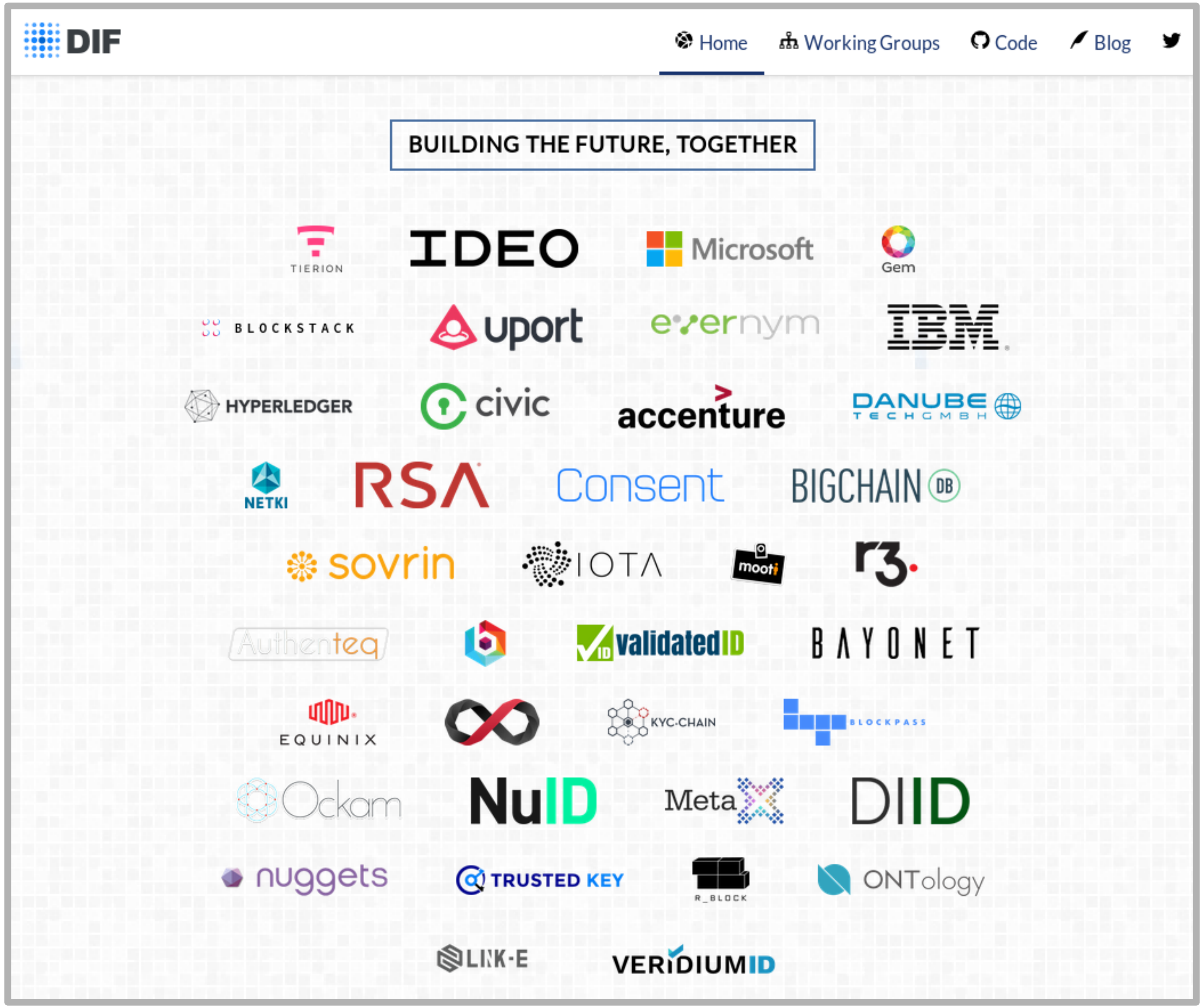

11 Countries
8 Financial Institutions
Credit Unions, Banks & Credit Card Networks
Europe’s Leading Digital Certificate Authority
One University
Two NGOs
Non-Governmental Organizations
Two Law Firms
10 Self-Sovereign Identity Startups and Personal Data Networks

Sovrin Community

Community

- Decentralized Identity Foundation:

  Interoperable open-source code for decentralized identity



Community

- Hyperledger Indy:

  Open-source code behind Sovrin

THE LINUX FOUNDATION

HYPERLEDGER

Community

- World Wide Web Consortium (W3C):

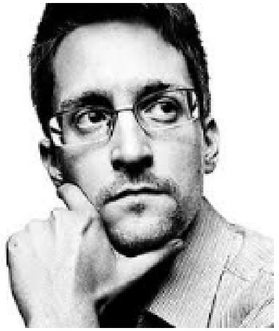
  Standardization of DIDs, Verifiable Claims

Current Activities

Current Activities

- PoCs around the world with financial institutions, NGOs, governments…
- CULedger network of credit unions
- Partnership with R3
- United Kingdom: Doctor’s Link
- Province of British Columbia: Digital corporate register
- Illinois Blockchain Task Force: Birth certificates
- TrustNet: Research project in Finland
- iRespond: Refugee project in Thailand (see ID2020 initiative)
- Gartner: Report on Decentralized Identity
- WEF: Known Traveler Digital Identity Concept

"The central problem of the future is, how do we return control of our identities to the people themselves?"
- Edward Snowden

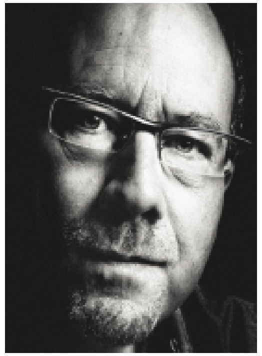


UBS

"...we think self-sovereign [identity] solutions are likely to be the standard against which other platforms will need to be held."

PERKINS COIE
COUNSEL TO GREAT COMPANIES

"DLT is generally well-suited to serve as the underlying technology for SSI because it offers a way to create a single source of identity that can be trusted by everyone, that is completely portable, but that no one entity owns or controls."



Craig Newmark
Founder, CraigsList

"I'd like to use [blockchain] for verifiable identity."

Thank You

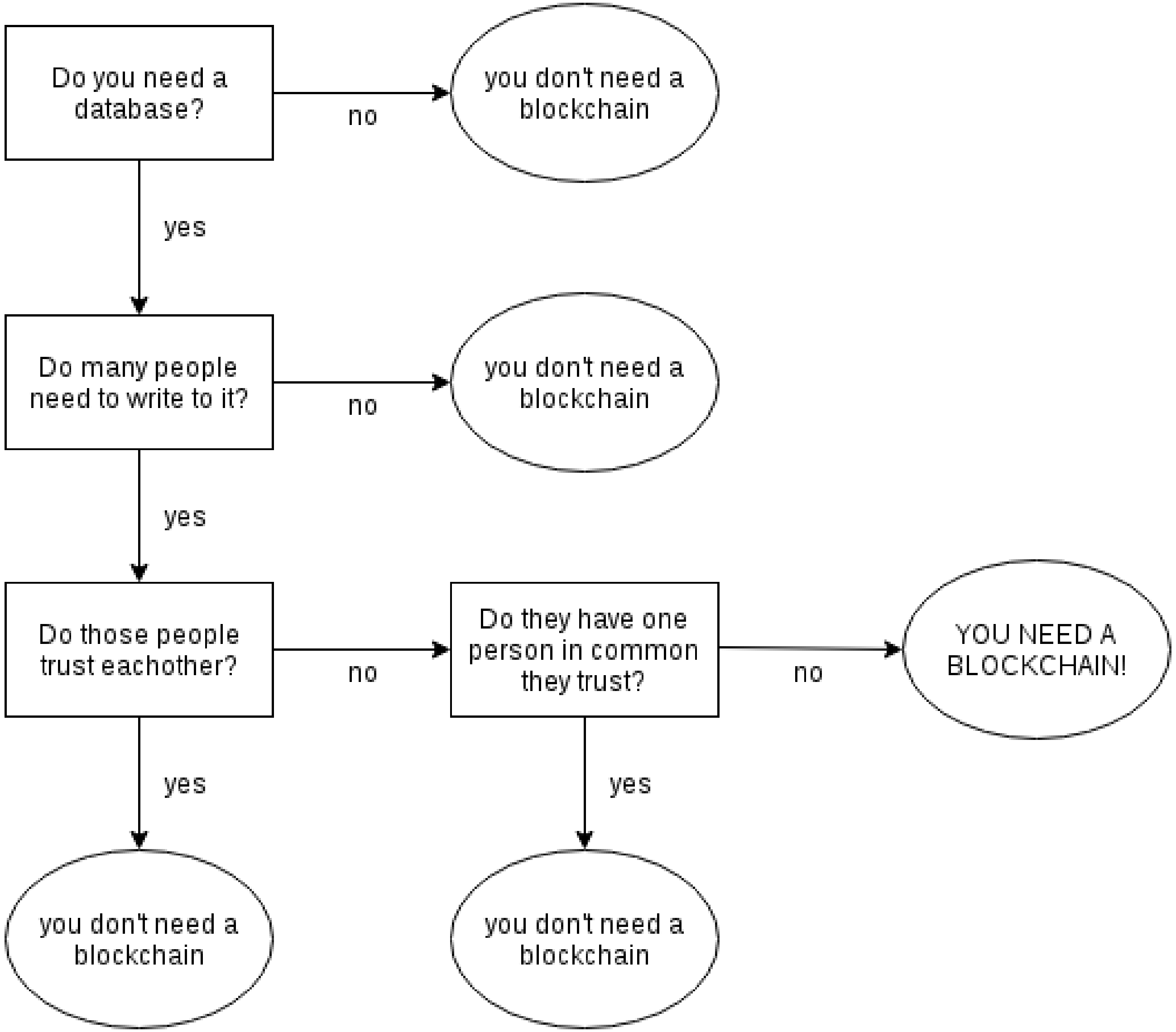
Thank You

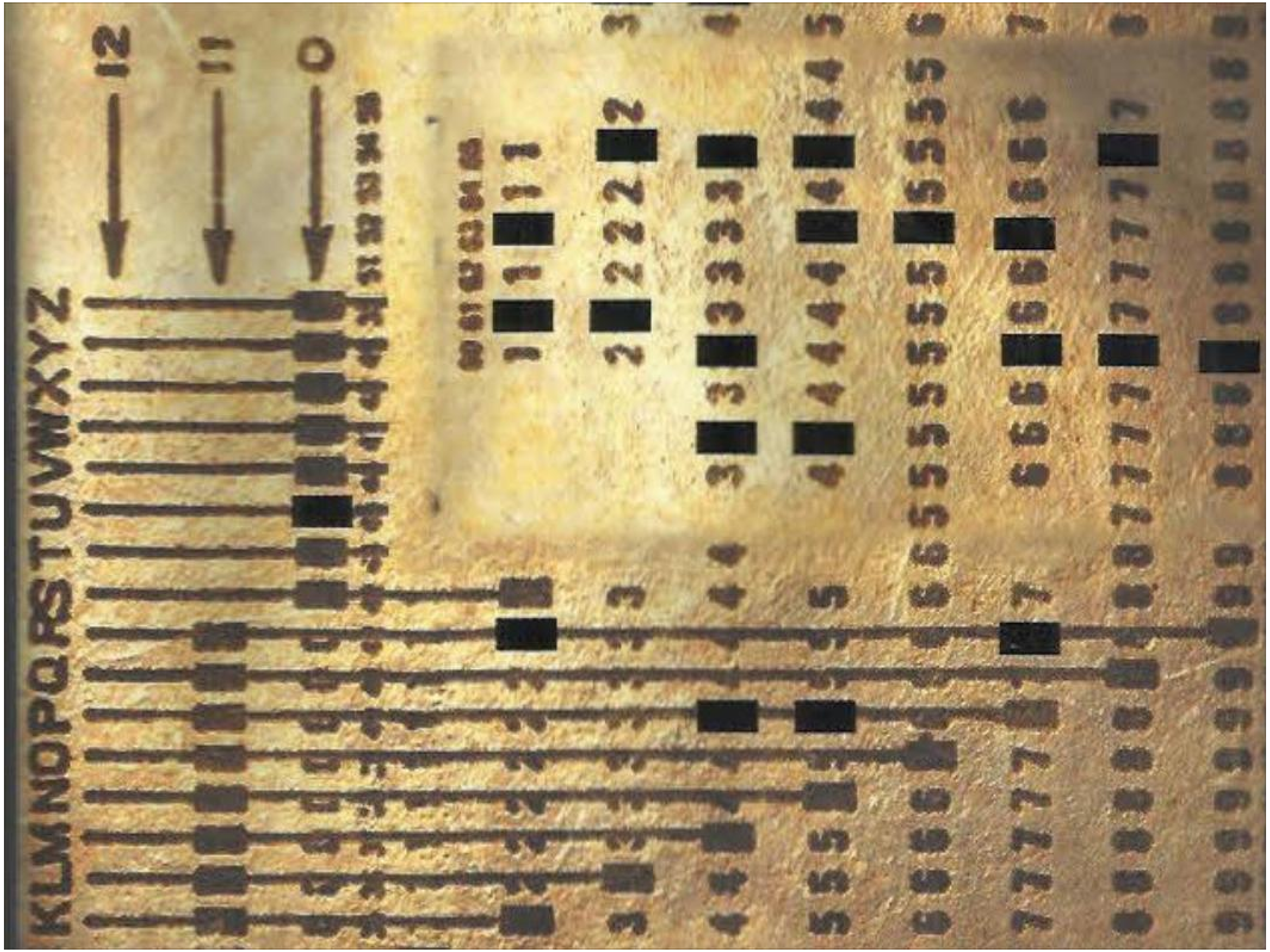
- Markus Sabadello
- Sovrin Foundation – https://sovrin.org/
  Technical Governance Board
- Danube Tech GmbH – https://danubetech.com/
  Founder, CEO
- markus@danubetech.com

Extra Slides

Evolution of Digital Identity

- Username+Password
- Centralized: MS Passport/365, Login with Facebook, Google, Twitter
- Enterprise/Government Identity Federation: SAML
- User-Centric Identity: Eclipse Higgins, OpenID, Cardspace, OAuth, UMA
- Federated Social Web: Diaspora, OStatus, IndieWeb
- Personal Data Stores: Personal.com, MyDex, Azigo
- Personal Clouds/PIMS: Meeco, CozyCloud, Digi.Me, Respect Network
- Decentralization: Unhosted, Webfinger, WebID/Solid, XDI, FreedomBox
- First-Party Terms, Consent Receipts, Link Contracts, DNT
- Blockchain Identity: Namecoin, Blockstack, uPort, Sovrin, Jolocom, DIDs

Do you need a database?
no
you don't need a blockchain
yes
Do many people need to write to it?
no
you don't need a blockchain
yes
Do those people trust eachother?
no
Do they have one person in common they trust?
no
YOU NEED A BLOCKCHAIN!
yes
you don't need a blockchain
yes
you don't need a blockchain


12
11
0
KLMNOPQRSTUVWXYZ