THE UNIVERSITY OF BRITISH COLUMBIA

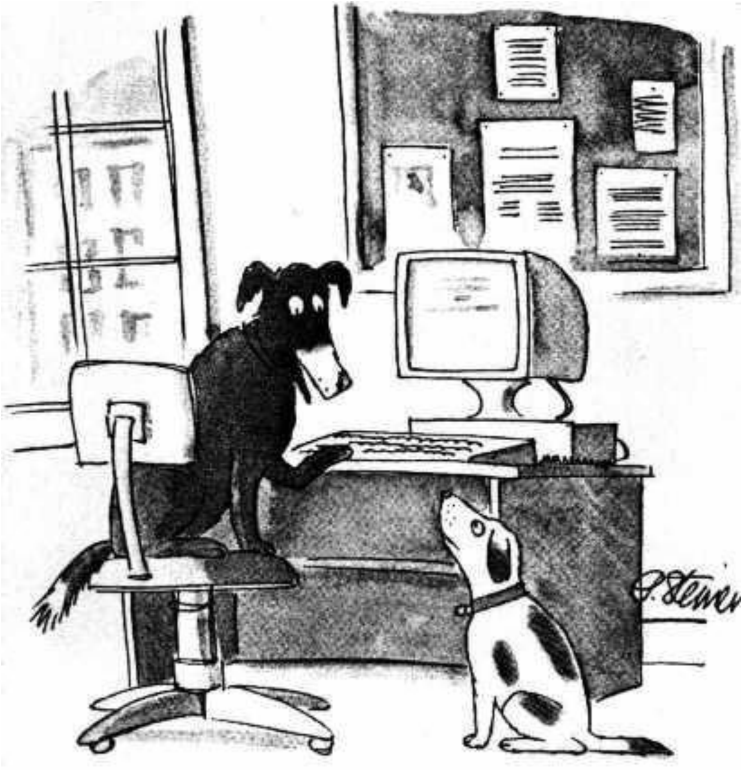
School of Information
Faculty of Arts

Decentralized Identity
Blockchain@UBC Summer Institute

JULY 14, 2025

INTRO TO DECENTRALIZED IDENTITY

Why do we need a digital Identity?



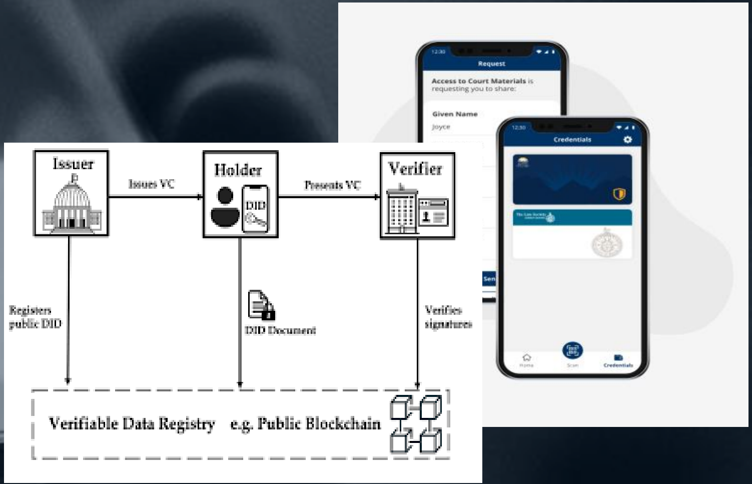
"On the Internet, nobody knows you're a dog."

The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20)only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

Physical World

VS

Digital World



Decentralized Identity offers a way to establish the authenticity of identities and attributes about them in the digital world

Identity is Multidimensional

Relationships (you don't look to the same to everyone)

- You to Bob (sister)
- You to Acme (Employer)
- You to USA (visitor)

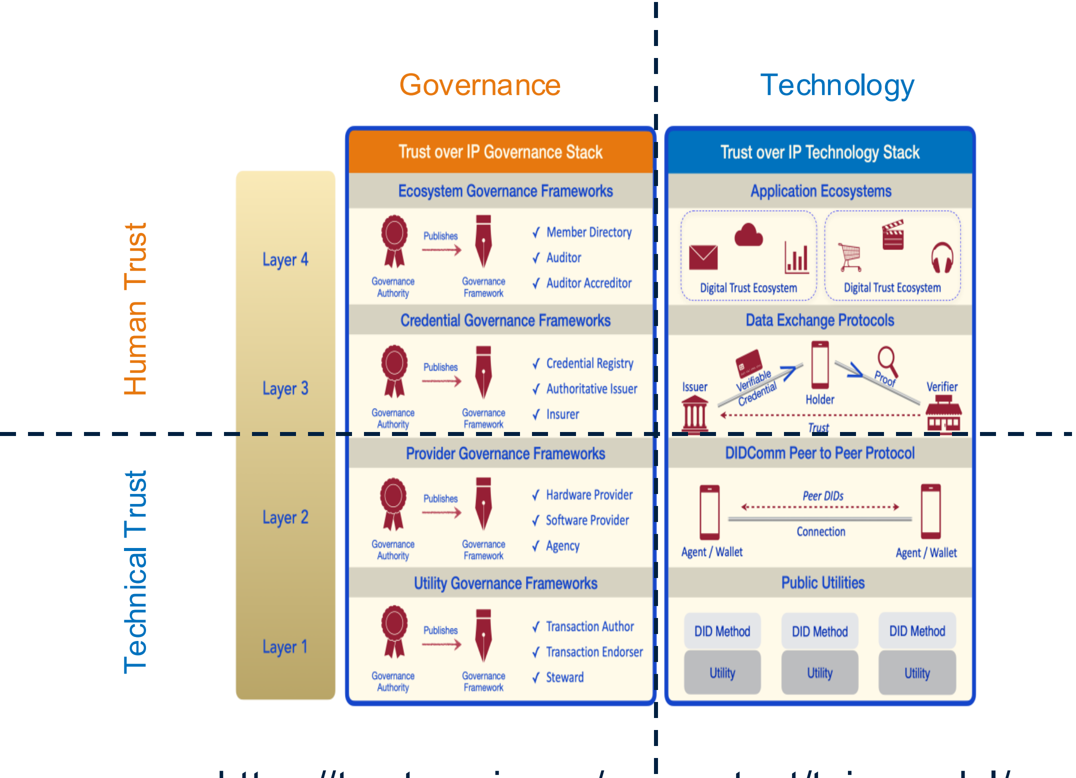
Agents (help you do things)

- Cloud agent
- iPad/notebook
- Mobile Phone

Attributes

- DoB
- Education
- Health

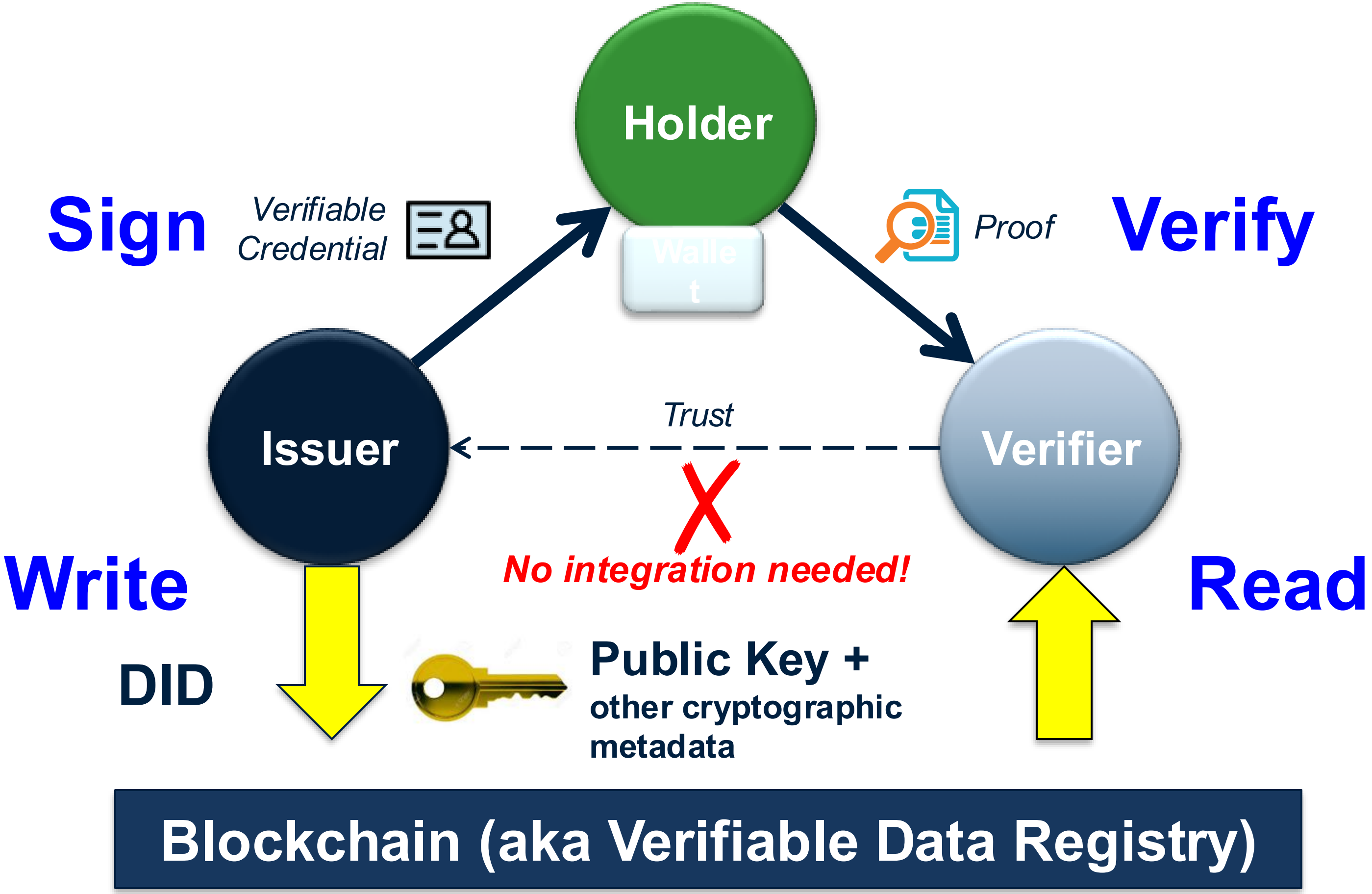
THE DECENTRALIZED IDENTITY STACK



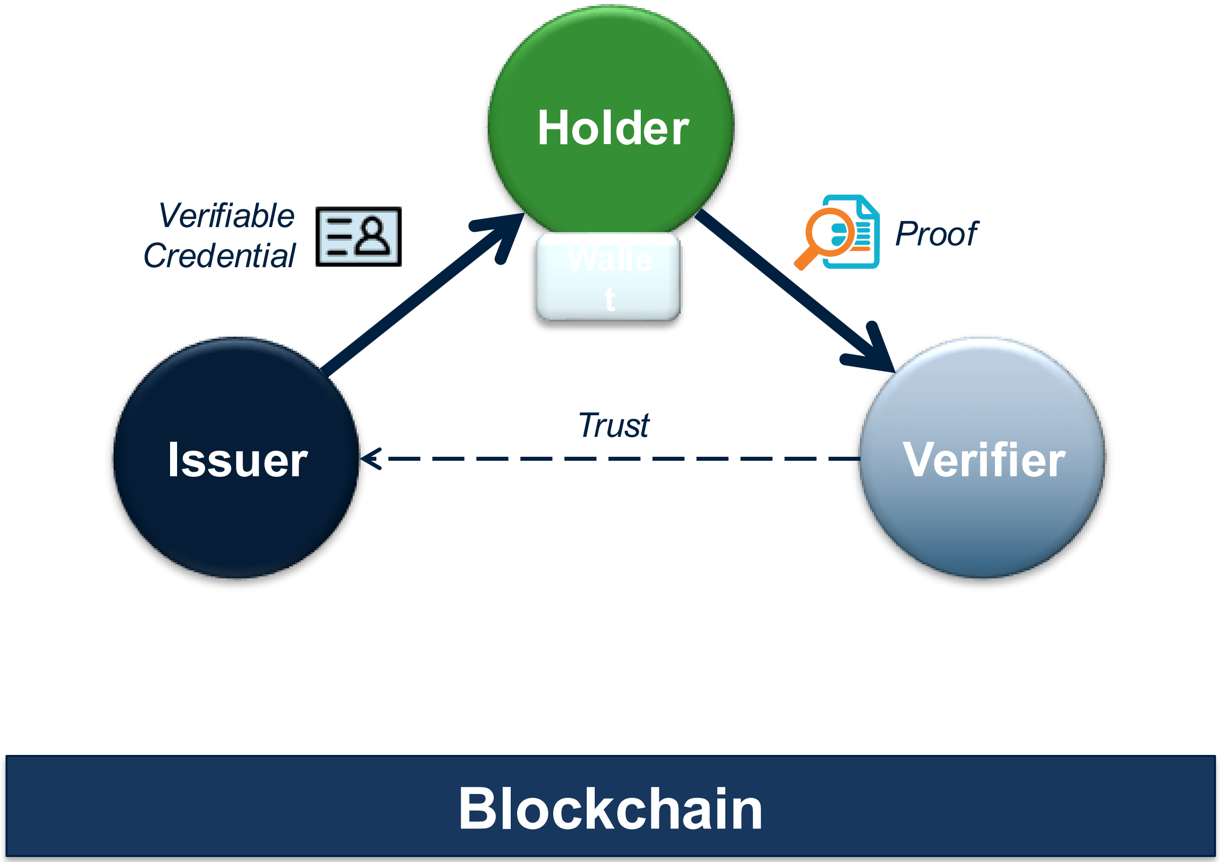
https://trustoverip.org/wp-content/toip-model/

- DID = Decentralized Identifiers
- DID is a unique identify – an address that someone can own
- Example: did.eth.0x34fd234ae1998bc (did . did-method . Identifier)
- •DID is controlled by a public key infrastructure
- DID can be recorded on a verifiable registry (e.g., blockchain)
- DID can be resolved to a DID Document

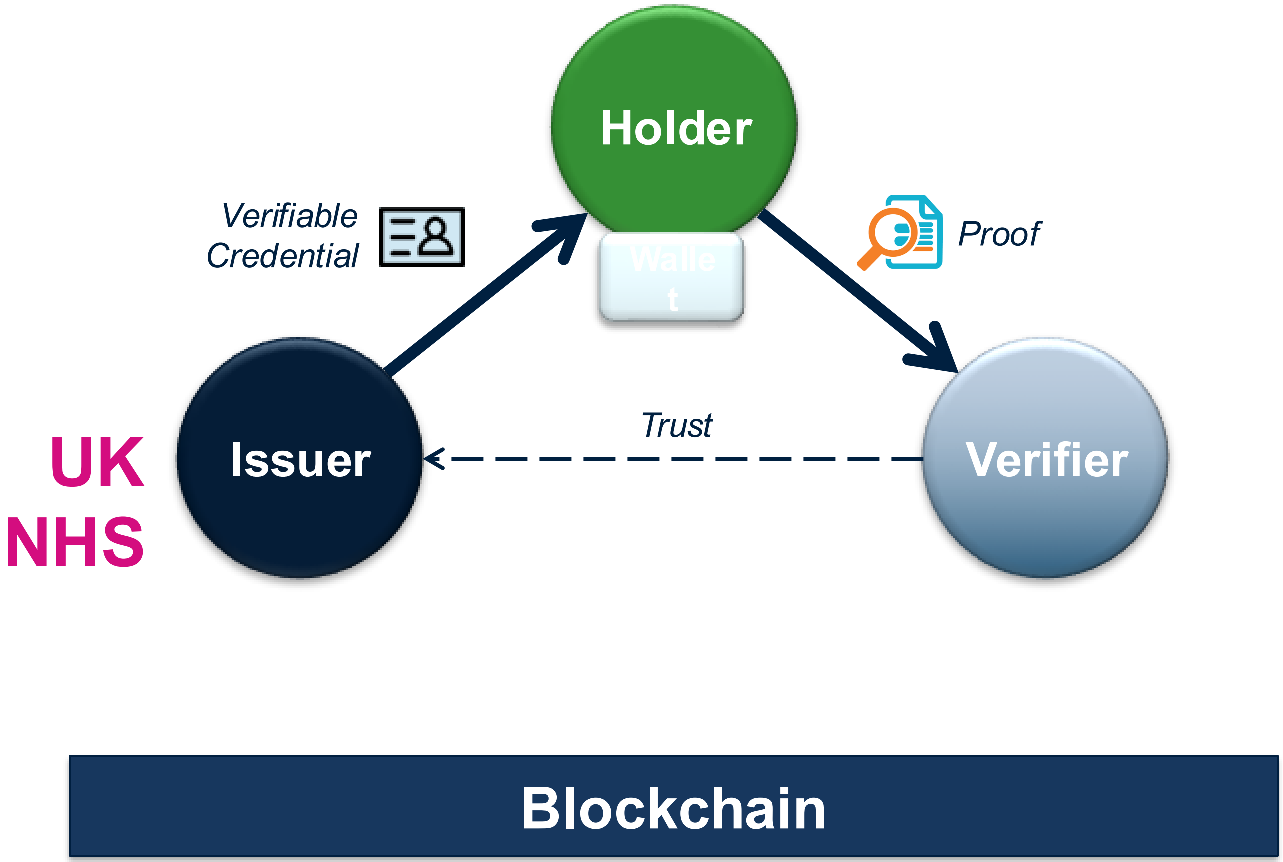
How Does Decentralized Identity Work?



Doctor’s Passport Example



Doctor’s Passport Example



Holder

Walle
t

Verifiable Credential

Proof

UK
NHS

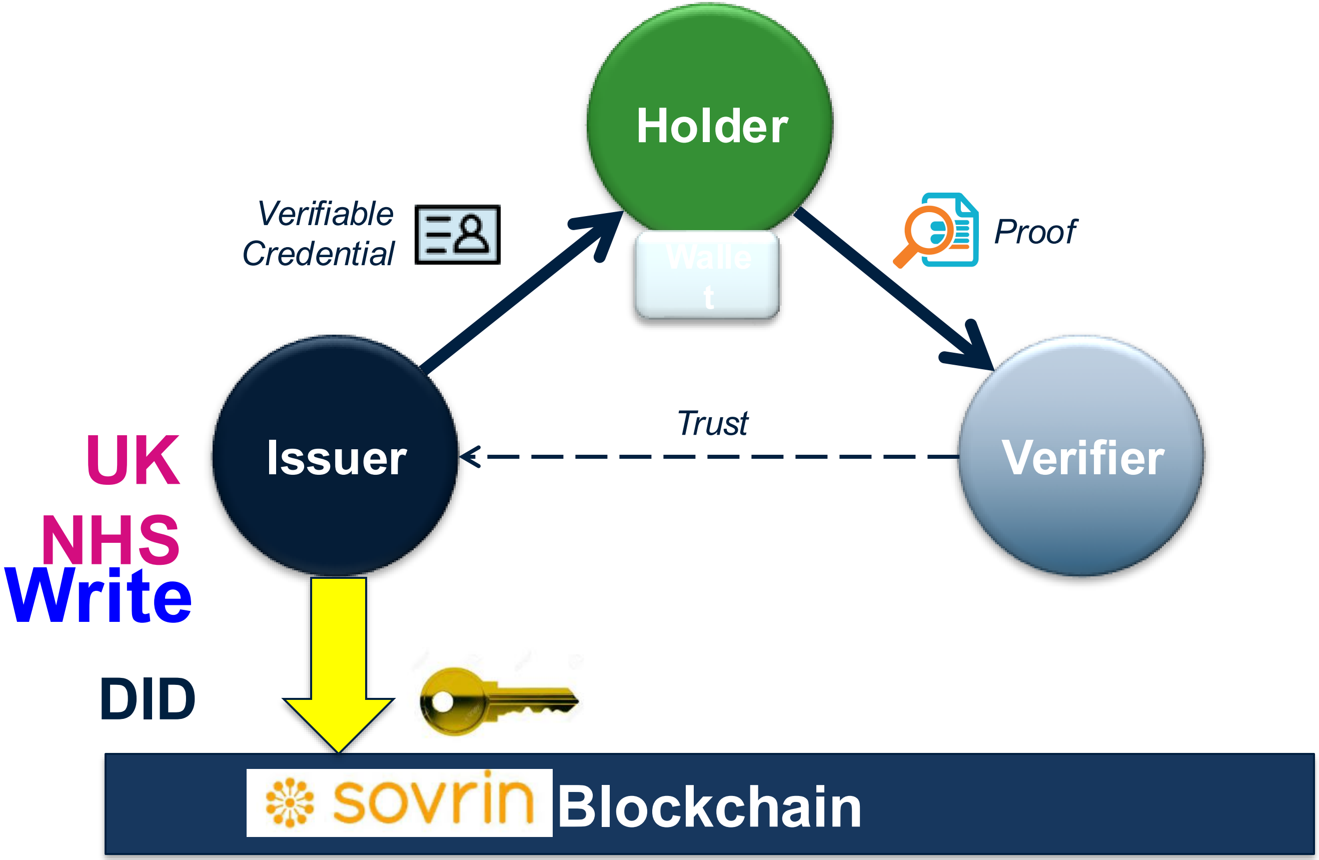
Issuer

Trust

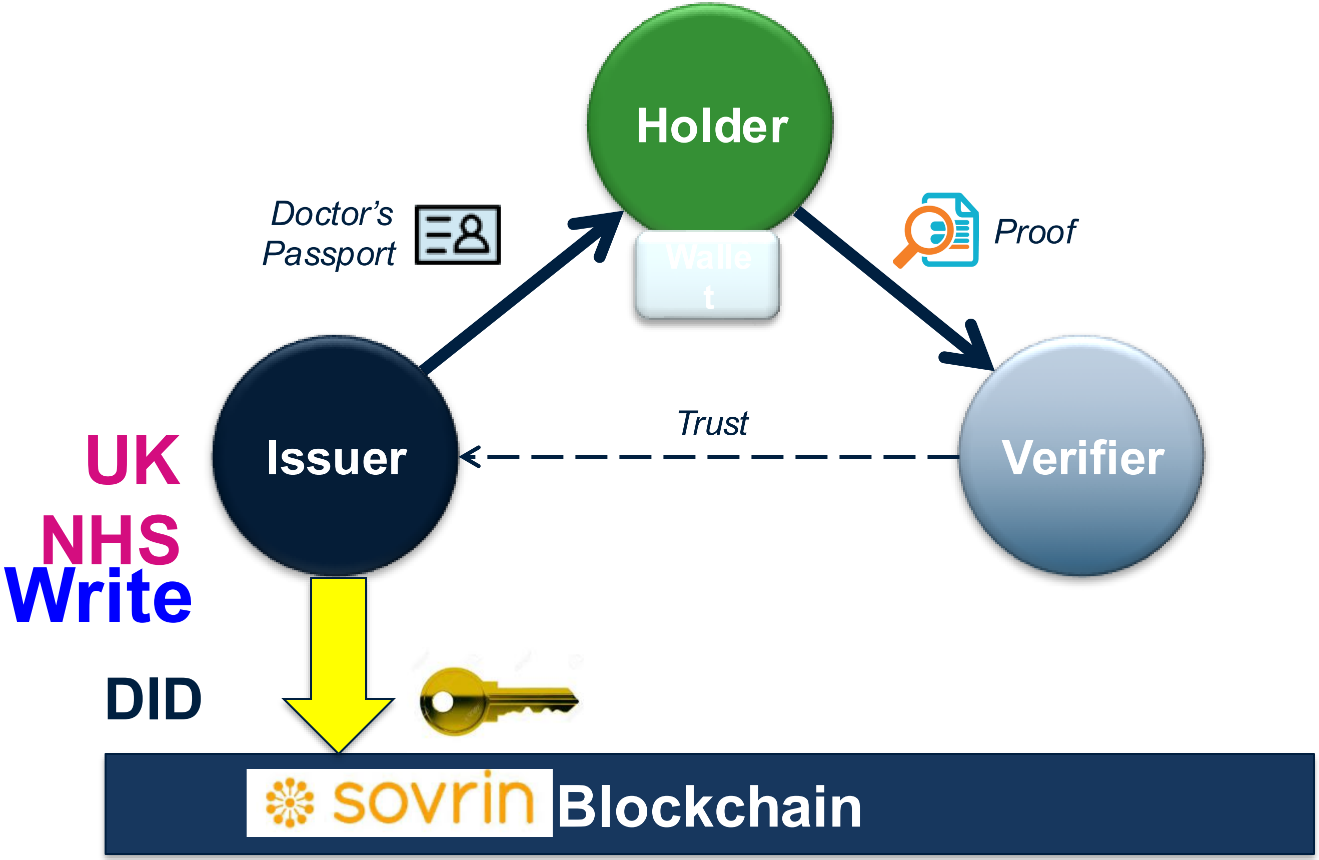
Verifier

Blockchain

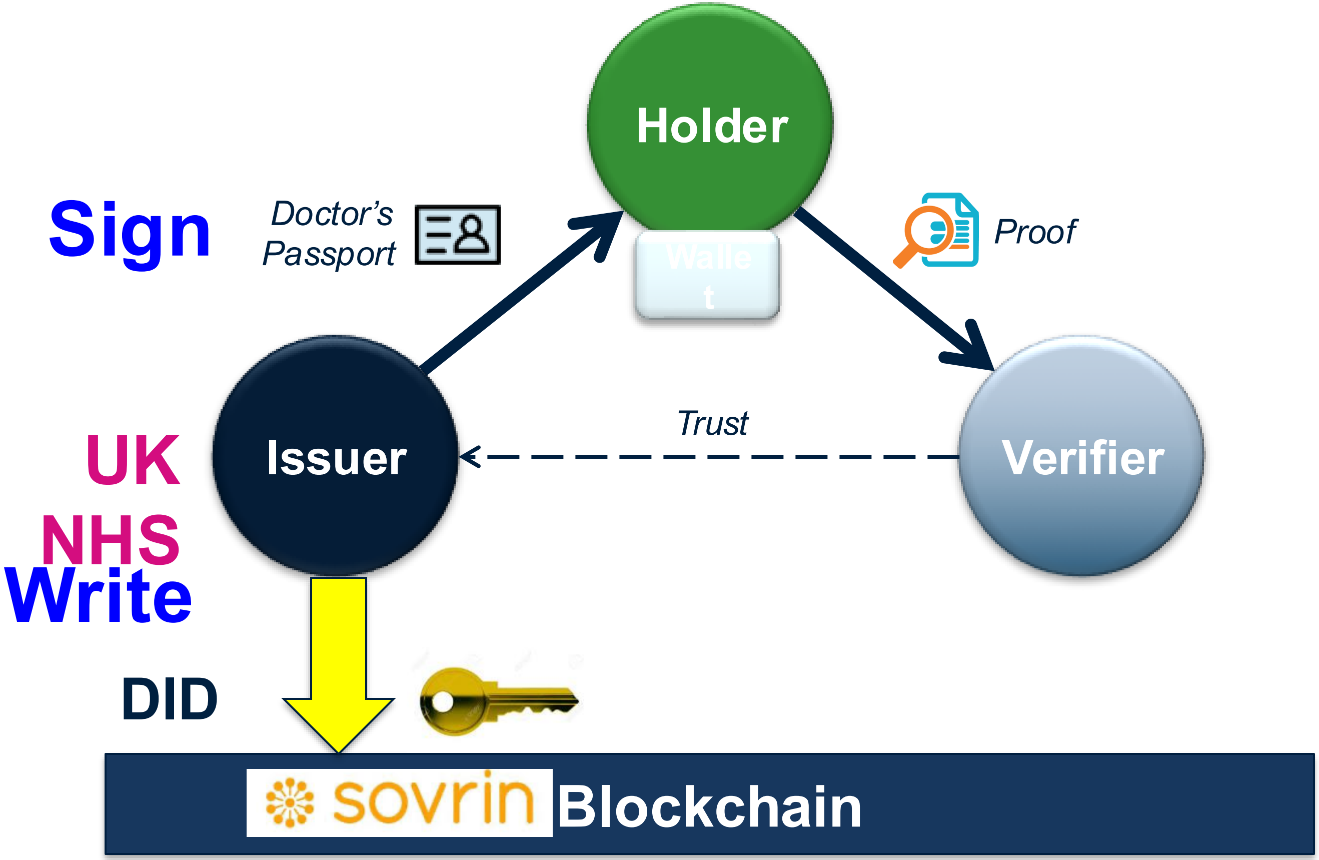
Doctor’s Passport Example



Doctor's Passport Example



Doctor’s Passport Example



Sign

Doctor’s Passport

Holder

Walle
t

Proof

UK NHS

Issuer

Trust

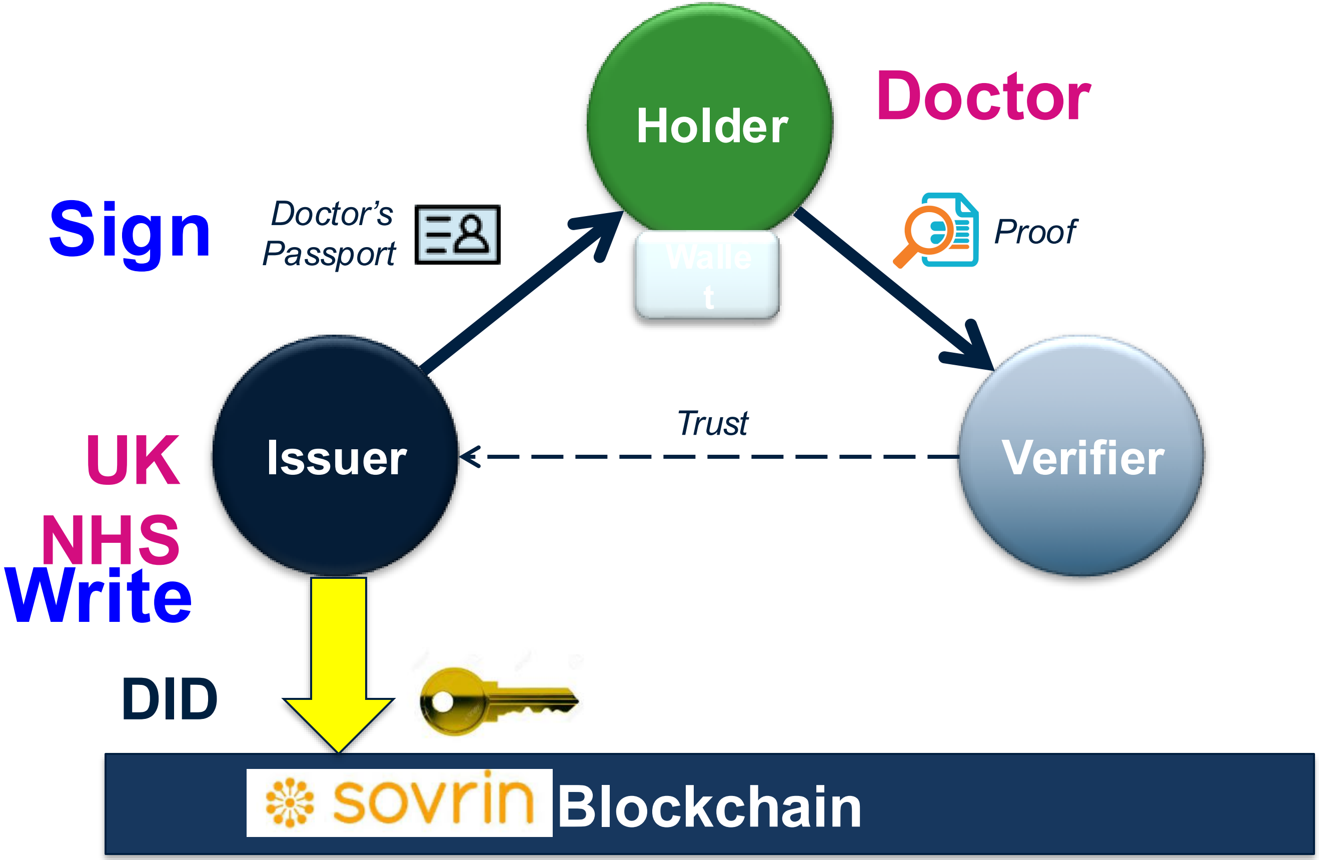
Verifier

Write

DID

sovrin Blockchain

Doctor’s Passport Example



Holder

Walle
t

Doctor

Sign

Doctor’s Passport

Proof

UK
NHS

Issuer

Trust

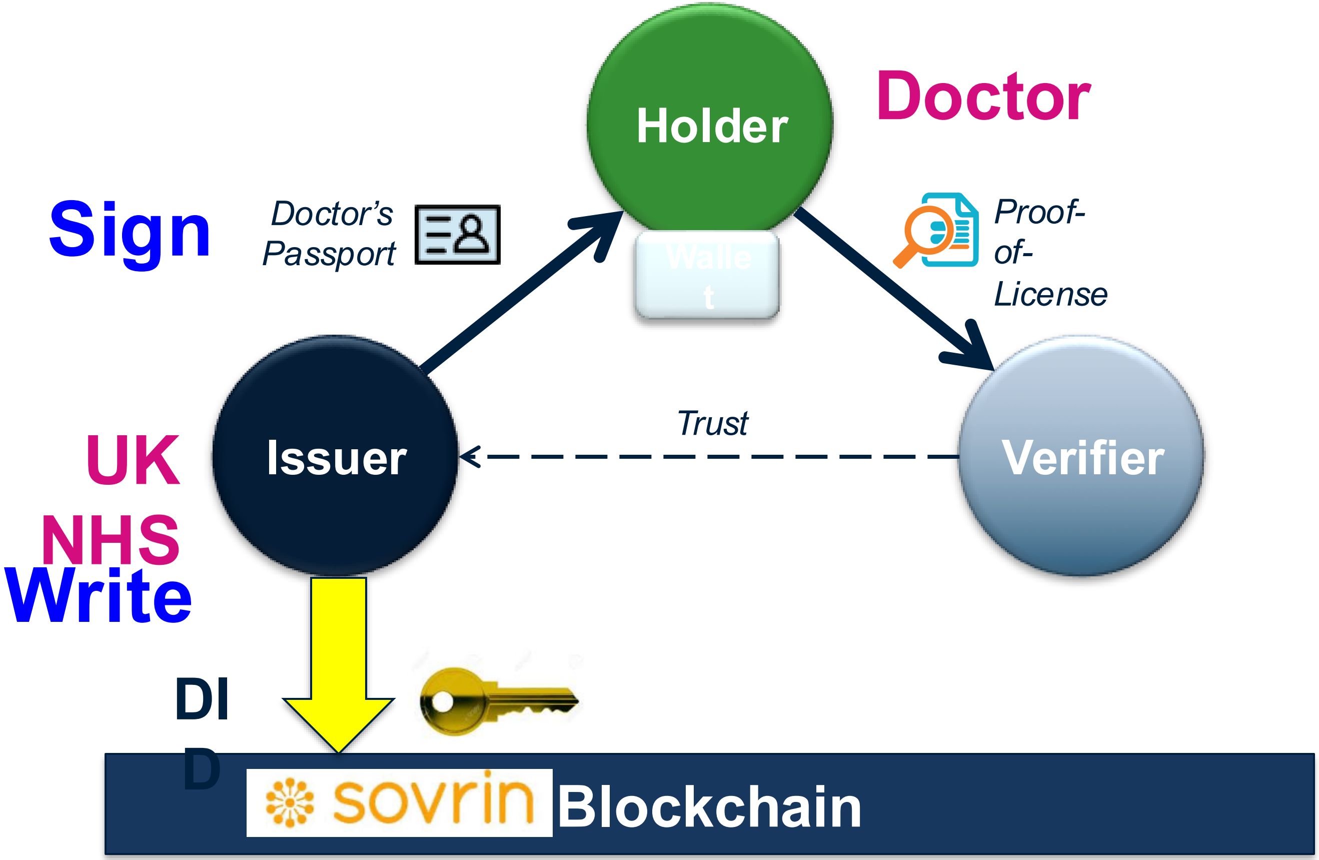
Verifier

Write

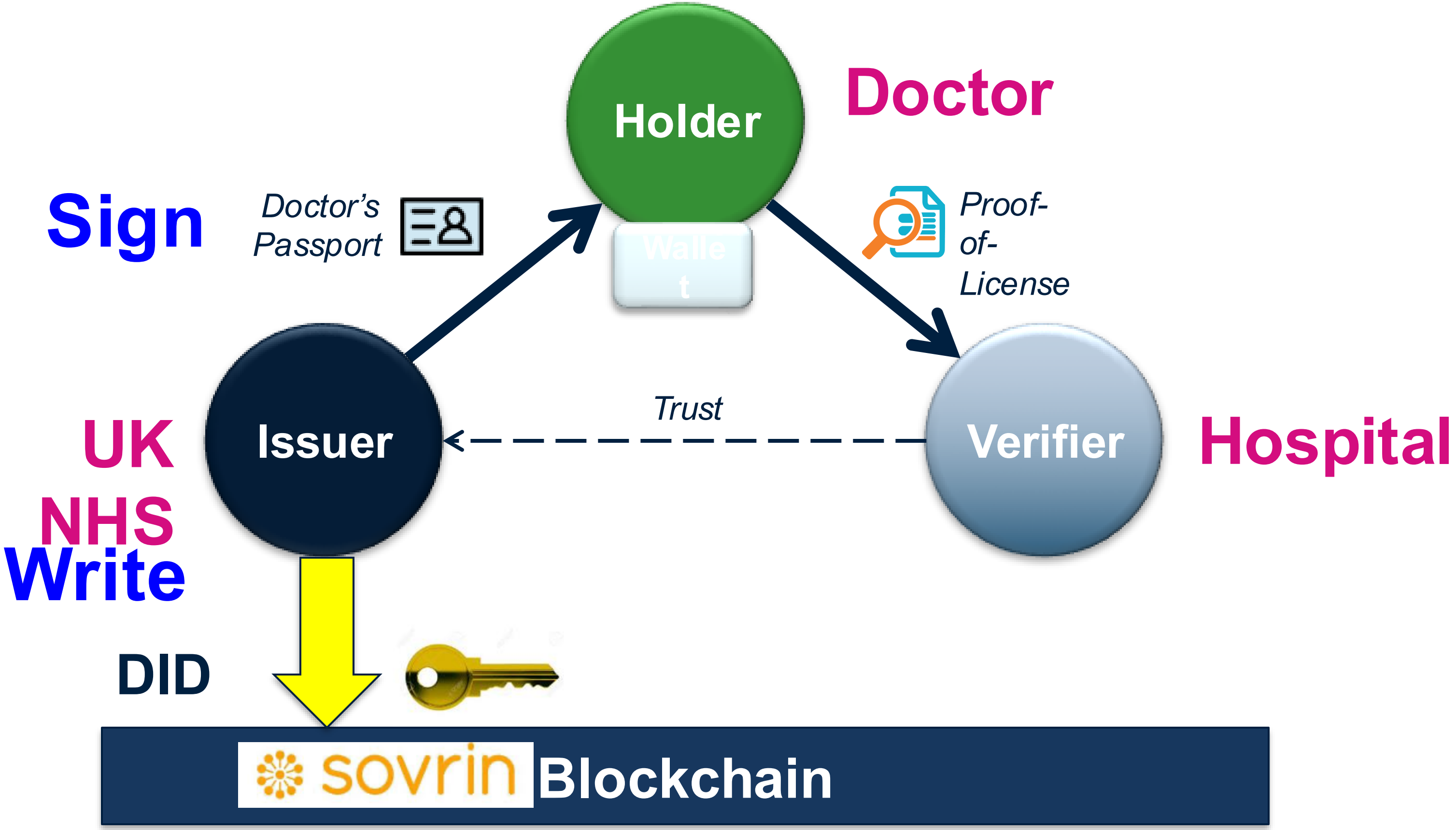
DID

sovrin Blockchain

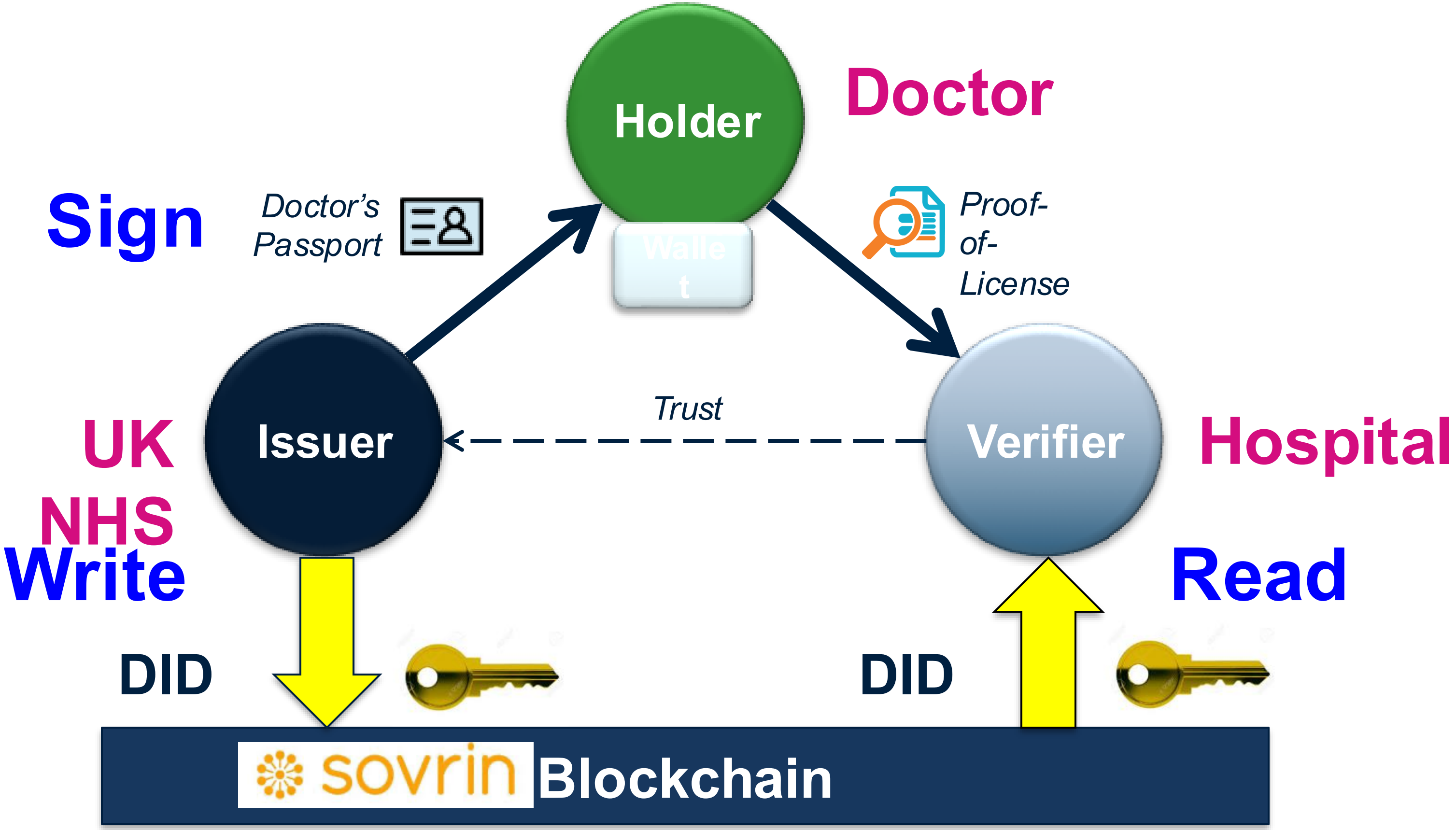
Doctor’s Passport Example



Doctor’s Passport Example



Doctor’s Passport Example



Holder

Walle
t

Doctor

Sign

Doctor’s Passport

Proof-of-License

UK NHS

Issuer

Trust

Verifier

Hospital

Write

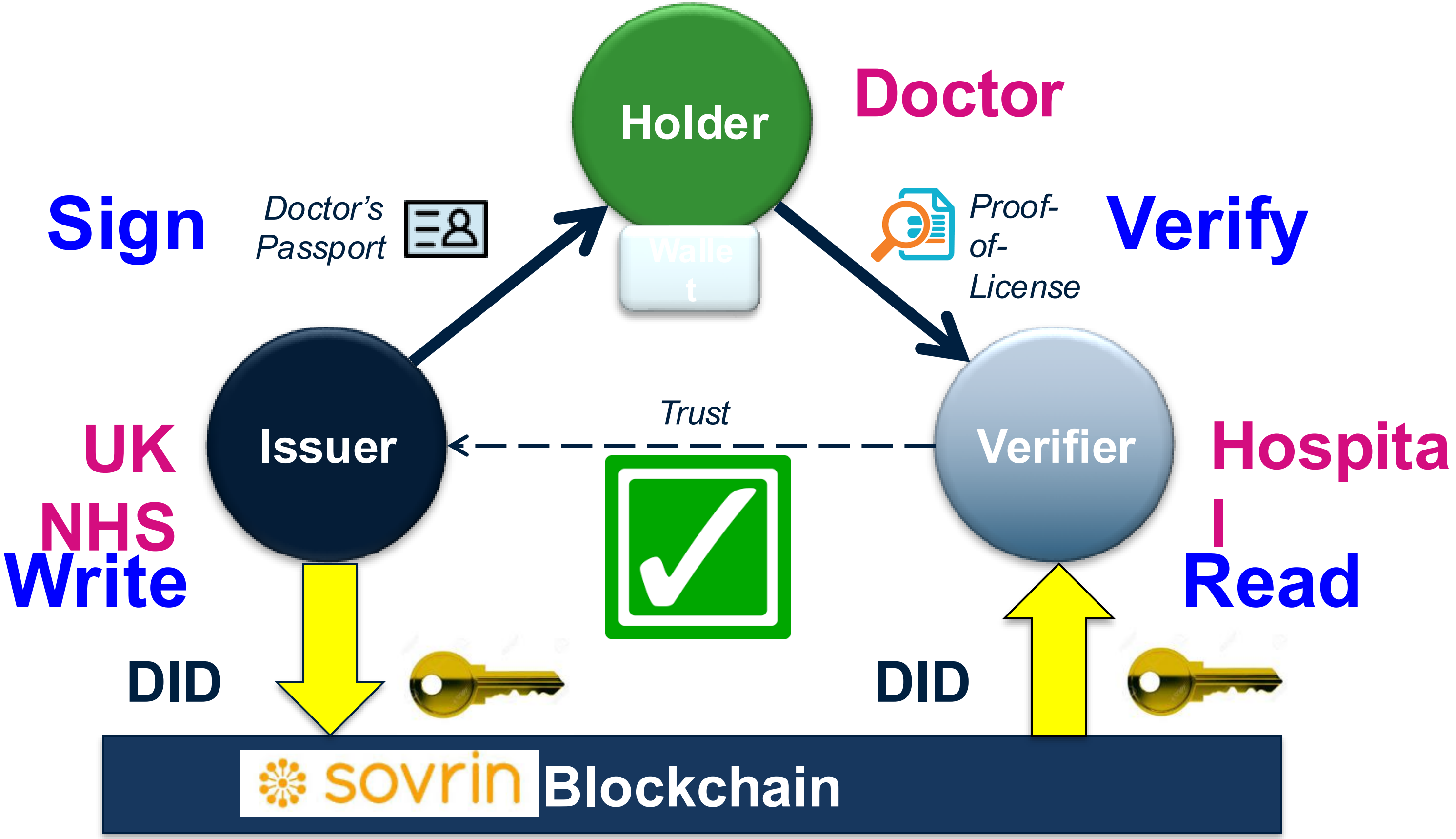
Read

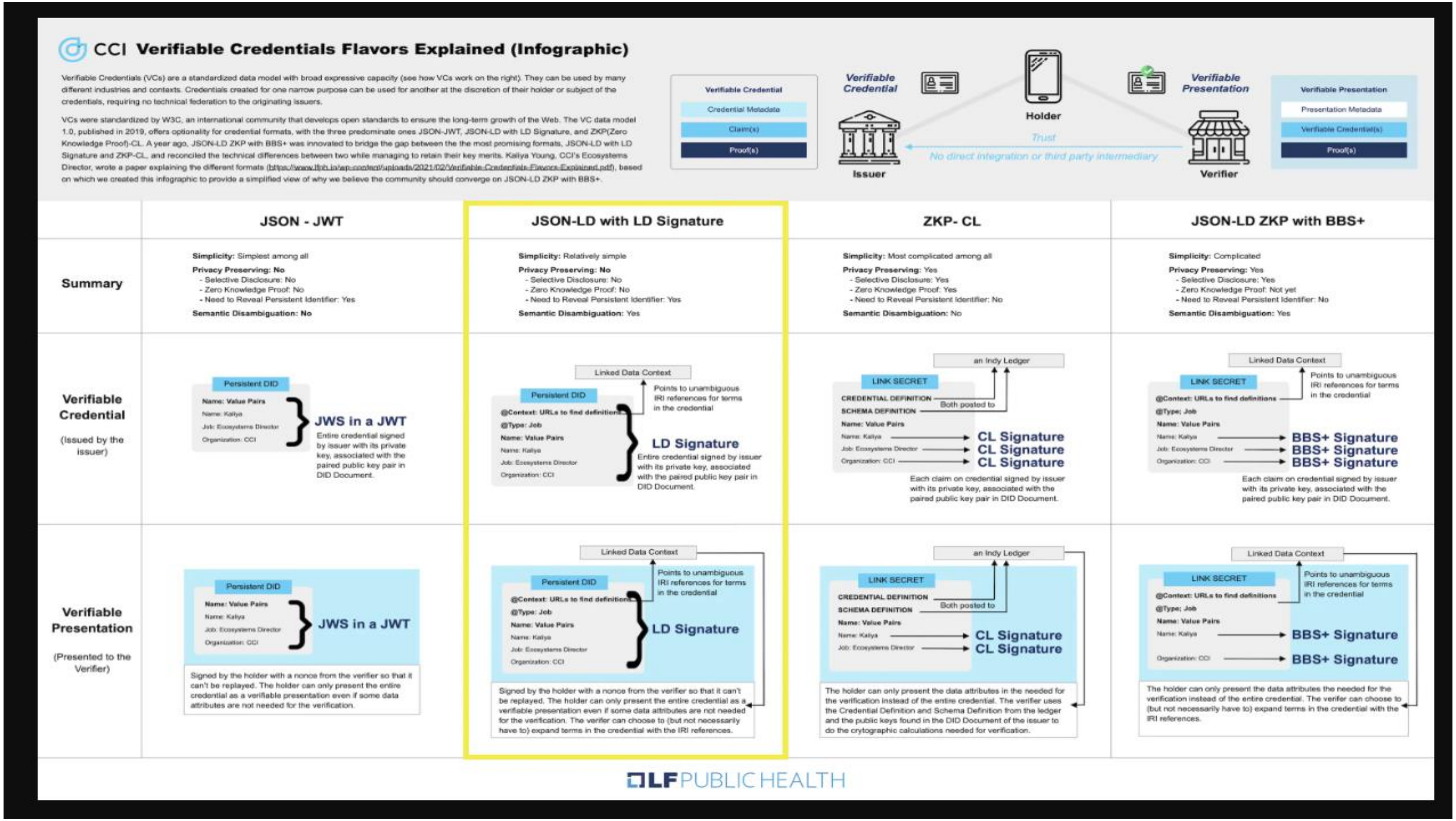
DID

DID

sovrin Blockchain

Doctor’s Passport Example





CCI Verifiable Credentials Flavors Explained (Infographic)

Verifiable Credentials (VCs) are a standardized data model with broad expressive capacity (see how VCs work on the right). They can be used by many different industries and contexts. Credentials created for one narrow purpose can be used for another at the discretion of their holder or subject of the credentials, requiring no technical federation to the originating issuers.

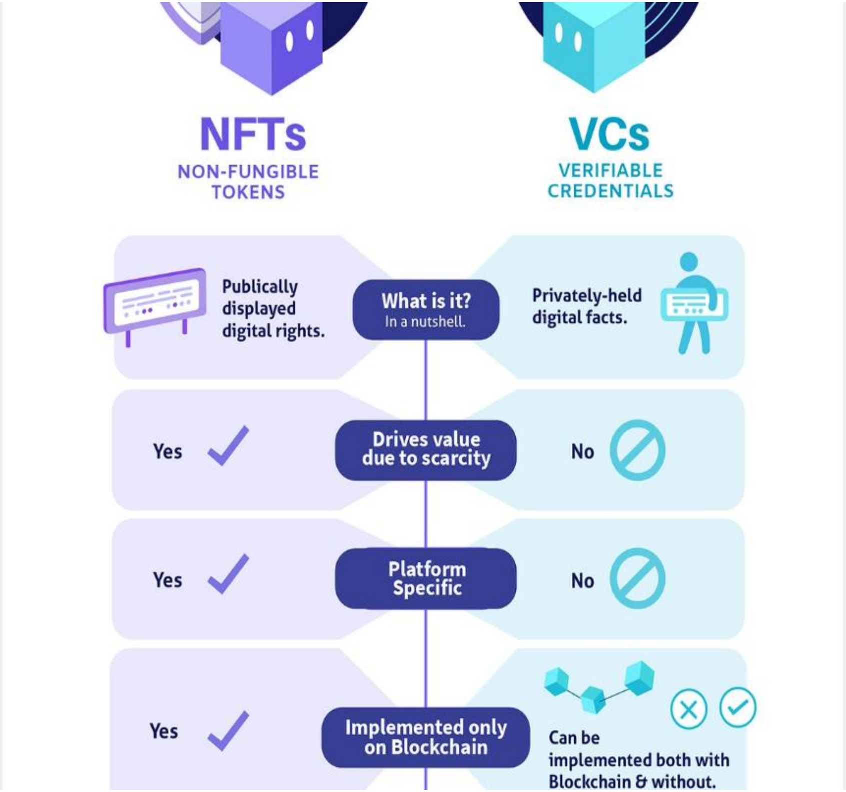
VCs were standardized by W3C, an international community that develops open standards to ensure the long-term growth of the Web. The VC data model 1.0, published in 2019, offers optionality for credential formats, with the three predominate ones JSON-JWT, JSON-LD with LD Signature, and ZKP(Zero Knowledge Proof)-CL. A year ago, JSON-LD ZKP with BBS+ was innovated to bridge the gap between the the most promising formats, JSON-LD with LD Signature and ZKP-CL, and reconciled the technical differences between two while managing to retain their key merits. Kaliya Young, CCI's Ecosystems Director, wrote a paper explaining the different formats (https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf), based on which we created this infographic to provide a simplified view of why we believe the community should converge on JSON-LD ZKP with BBS+.

	JSON - JWT	JSON-LD with LD Signature	ZKP- CL	JSON-LD ZKP with BBS+
Summary	**Simplicity:** Simplest among all **Privacy Preserving: No** - Selective Disclosure: No - Zero Knowledge Proof: No - Need to Reveal Persistent Identifier: Yes **Semantic Disambiguation: No**	**Simplicity:** Relatively simple **Privacy Preserving: No** - Selective Disclosure: No - Zero Knowledge Proof: No - Need to Reveal Persistent Identifier: Yes **Semantic Disambiguation:** Yes	**Simplicity:** Most complicated among all **Privacy Preserving:** Yes - Selective Disclosure: Yes - Zero Knowledge Proof: Yes - Need to Reveal Persistent Identifier: No **Semantic Disambiguation:** No	**Simplicity:** Complicated **Privacy Preserving:** Yes - Selective Disclosure: Yes - Zero Knowledge Proof: Not yet - Need to Reveal Persistent Identifier: No **Semantic Disambiguation:** Yes
Verifiable Credential (Issued by the issuer)	Persistent DID **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **JWS in a JWT** Entire credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	Linked Data Context Points to unambiguous IRI references for terms in the credential Persistent DID **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **LD Signature** Entire credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	an Indy Ledger LINK SECRET **CREDENTIAL DEFINITION** Both posted to **SCHEMA DEFINITION** **Name: Value Pairs** Name: Kaliya → **CL Signature** Job: Ecosystems Director → **CL Signature** Organization: CCI → **CL Signature** Each claim on credential signed by issuer with its private key, associated with the paired public key pair in DID Document.	Linked Data Context Points to unambiguous IRI references for terms in the credential LINK SECRET **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya → **BBS+ Signature** Job: Ecosystems Director → **BBS+ Signature** Organization: CCI → **BBS+ Signature** Each claim on credential signed by issuer with its private key, associated with the paired public key pair in DID Document.
Verifiable Presentation (Presented to the Verifier)	Persistent DID **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **JWS in a JWT** Signed by the holder with a nonce from the verifier so that it can't be replayed. The holder can only present the entire credential as a verifiable presentation even if some data attributes are not needed for the verification.	Linked Data Context Points to unambiguous IRI references for terms in the credential Persistent DID **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya Job: Ecosystems Director Organization: CCI **LD Signature** Signed by the holder with a nonce from the verifier so that it can't be replayed. The holder can only present the entire credential as a verifiable presentation even if some data attributes are not needed for the verification. The verifer can choose to (but not necessarily have to) expand terms in the credential with the IRI references.	an Indy Ledger LINK SECRET **CREDENTIAL DEFINITION** Both posted to **SCHEMA DEFINITION** **Name: Value Pairs** Name: Kaliya → **CL Signature** Job: Ecosystems Director → **CL Signature** The holder can only present the data attributes in the needed for the verification instead of the entire credential. The verifier uses the Credential Definition and Schema Definition from the ledger and the public keys found in the DID Document of the issuer to do the crytographic calculations needed for verification.	Linked Data Context Points to unambiguous IRI references for terms in the credential LINK SECRET **@Context: URLs to find definitions** **@Type: Job** **Name: Value Pairs** Name: Kaliya → **BBS+ Signature** Organization: CCI → **BBS+ Signature** The holder can only present the data attributes the needed for the verification instead of the entire credential. The verifer can choose to (but not necessarily have to) expand terms in the credential with the IRI references.

LF PUBLIC HEALTH

Source: https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

Comparing NFTs and VCs



NFTs NON-FUNGIBLE TOKENS		VCs VERIFIABLE CREDENTIALS
Publically displayed digital rights.	What is it? In a nutshell.	Privately-held digital facts.
Yes ✓	Drives value due to scarcity	No ⊘
Yes ✓	Platform Specific	No ⊘
Yes ✓	Implemented only on Blockchain	Can be implemented both with Blockchain & without.

SOULBOUND TOKENS

Transferability:

VCs: Can be shared and verified by others, but not transferred.

SBTs: Permanently tied to the holder’s wallet and cannot be transferred.

Purpose and Usage:

VCs: Used to prove qualifications, identity, and credentials.

SBTs: Used to represent personal, non-transferable attributes and reputation.

Verification:

VCs: Verified through cryptographic proofs by verifiers.

SBTs: Exist on the blockchain and represent unique attributes visible to all.

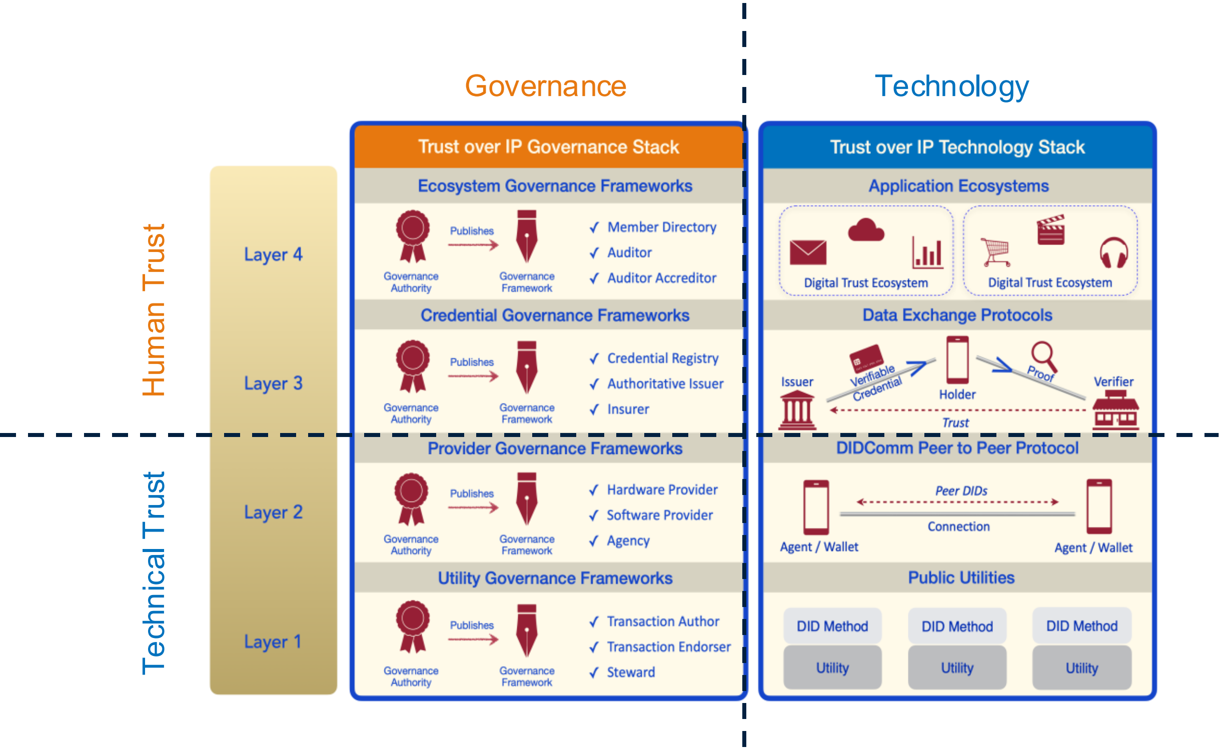
Privacy:

VCs: Can selectively disclose information to verifiers.

SBTs: Publicly visible on the blockchain, potentially less privacy.

THE DECENTRALIZED IDENTITY STACK IN DETAIL

THE DECENTRALIZED IDENTITY STACK



Governance

Technology

Human Trust

Technical Trust

Layer 4

Layer 3

Layer 2

Layer 1

Trust over IP Governance Stack

Ecosystem Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Member Directory
- ✓ Auditor
- ✓ Auditor Accreditor

Credential Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Credential Registry
- ✓ Authoritative Issuer
- ✓ Insurer

Provider Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Hardware Provider
- ✓ Software Provider
- ✓ Agency

Utility Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Transaction Author
- ✓ Transaction Endorser
- ✓ Steward

Trust over IP Technology Stack

Application Ecosystems

Digital Trust Ecosystem

Digital Trust Ecosystem

Data Exchange Protocols

Issuer — Verifiable Credential → Holder — Proof → Verifier

Trust

DIDComm Peer to Peer Protocol

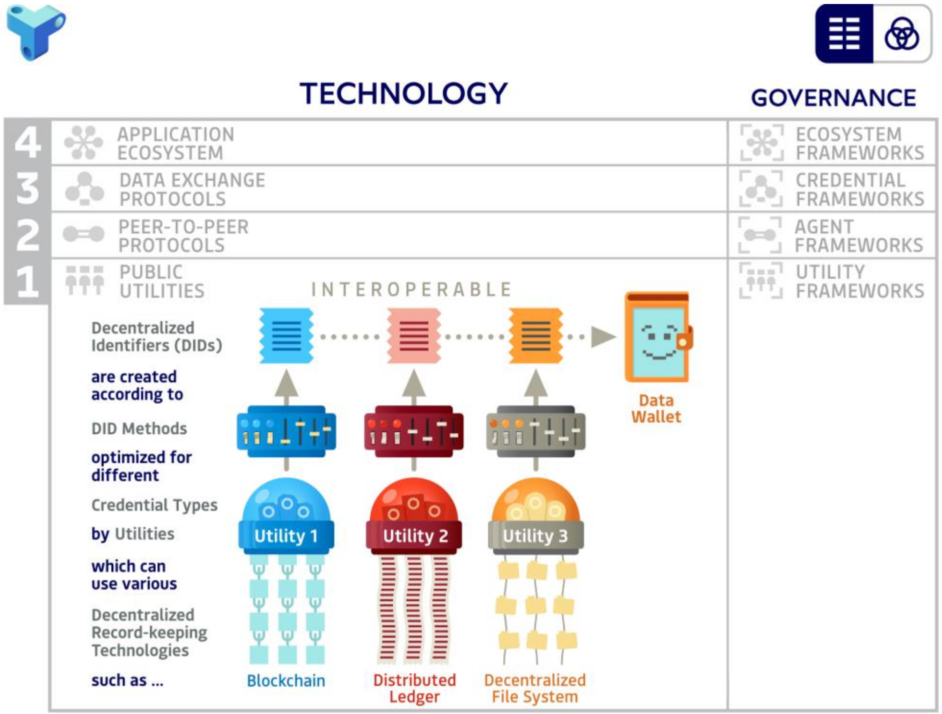
Agent / Wallet — Peer DIDs — Connection — Agent / Wallet

Public Utilities

DID Method	DID Method	DID Method
Utility	Utility	Utility

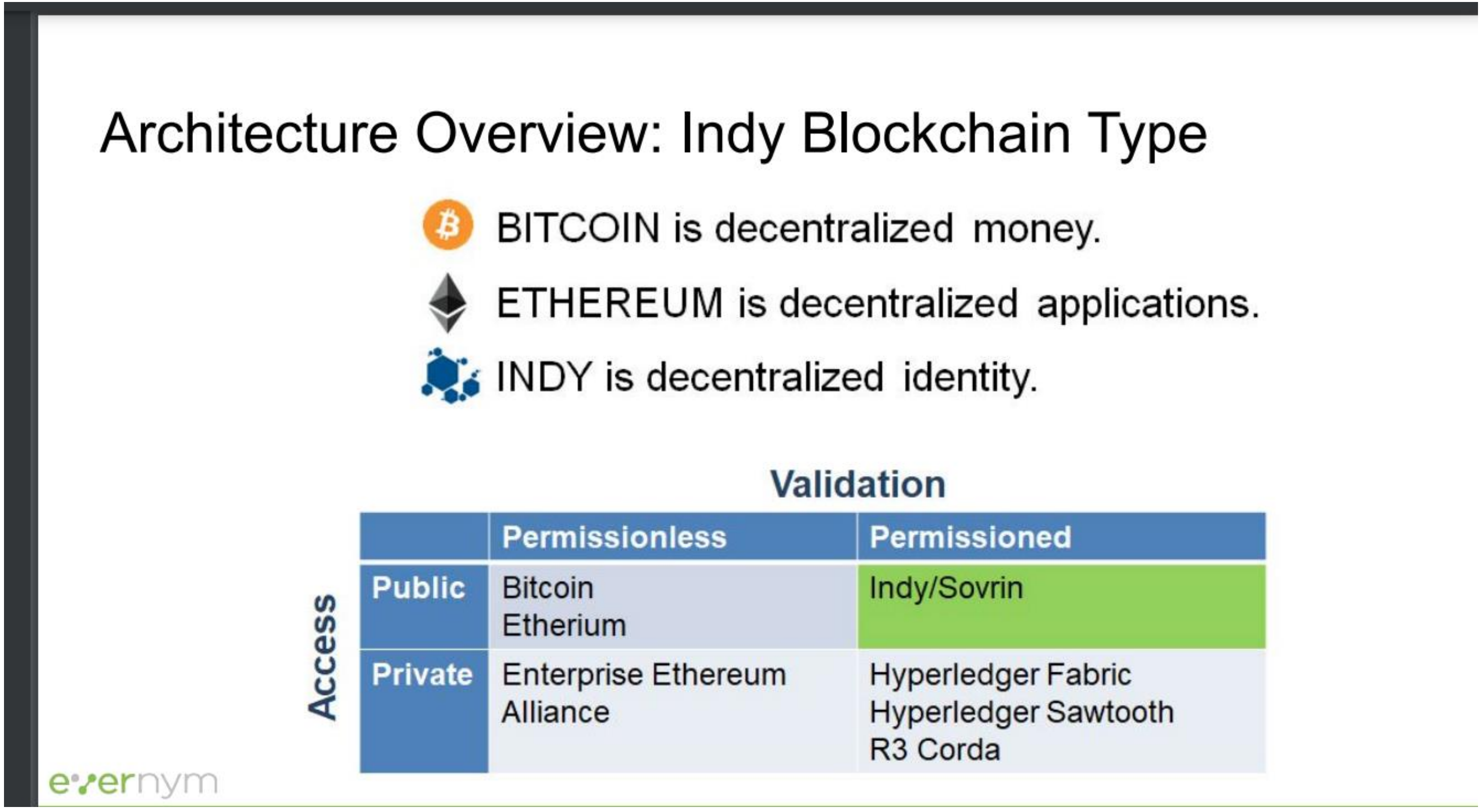
https://trustoverip.org/wp-content/toip-model/

TECHNOLOGY LAYER 1 (THE PUBLIC UTILITY LAYER)



Decentralized Identifiers (DIDs) are created according to DID Methods optimized for different Credential Types by Utilities which can use various Decentralized Record-keeping Technologies such as ...

HYPERLEDGER INDY



Architecture Overview: Indy Blockchain Type

- BITCOIN is decentralized money.
- ETHEREUM is decentralized applications.
- INDY is decentralized identity.

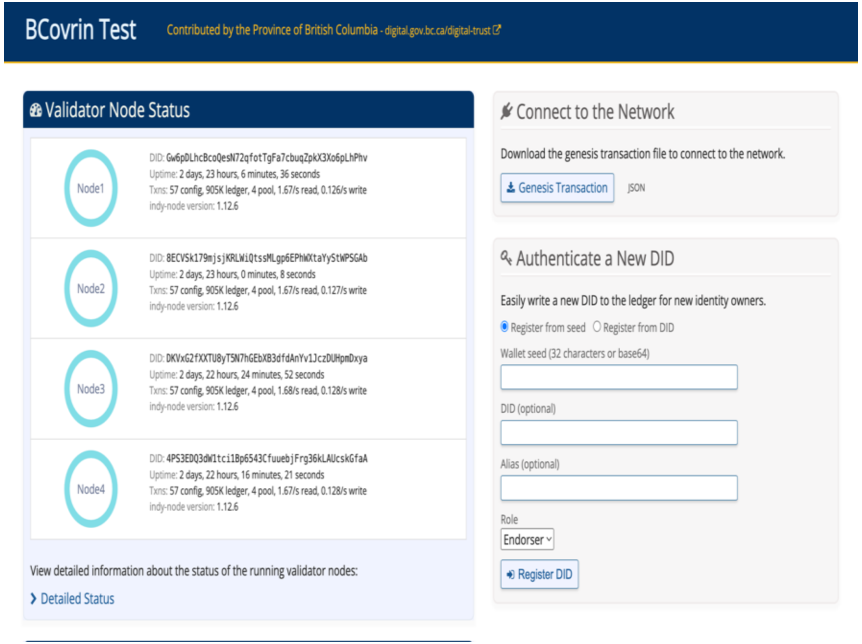
Validation

Access		Permissionless	Permissioned
	Public	Bitcoin Etherium	Indy/Sovrin
	Private	Enterprise Ethereum Alliance	Hyperledger Fabric Hyperledger Sawtooth R3 Corda

evernym

INDY IMPLEMENTATION: BCOVRIN TEST NET

Overview



BCovrin Test Contributed by the Province of British Columbia - digital.gov.bc.ca/digital-trust

Validator Node Status

Node1
DID: Gw6pDLhcBcoQesN72qfotTgFa7cbuqZpkX3Xo6pLhPhv
Uptime: 2 days, 23 hours, 6 minutes, 36 seconds
Txns: 57 config, 905K ledger, 4 pool, 1.67/s read, 0.126/s write
indy-node version: 1.12.6

Node2
DID: 8ECVSk179mjsjKRLWiQtssMLgp6EPhWXtaYyStWPSGAb
Uptime: 2 days, 23 hours, 0 minutes, 8 seconds
Txns: 57 config, 905K ledger, 4 pool, 1.67/s read, 0.127/s write
indy-node version: 1.12.6

Node3
DID: DKVxG2fXXTU8yT5N7hGEbXB3dfdAnYv1JczDUHpmDxya
Uptime: 2 days, 22 hours, 24 minutes, 52 seconds
Txns: 57 config, 905K ledger, 4 pool, 1.68/s read, 0.128/s write
indy-node version: 1.12.6

Node4
DID: 4PS3EDQ3dW1tci1Bp6543CfuuebjFrg36kLAUcskGfaA
Uptime: 2 days, 22 hours, 16 minutes, 21 seconds
Txns: 57 config, 905K ledger, 4 pool, 1.67/s read, 0.128/s write
indy-node version: 1.12.6

View detailed information about the status of the running validator nodes:

› Detailed Status

Connect to the Network

Download the genesis transaction file to connect to the network.

Genesis Transaction JSON

Authenticate a New DID

Easily write a new DID to the ledger for new identity owners.

● Register from seed ○ Register from DID

Wallet seed (32 characters or base64):

DID (optional):

Alias (optional):

Role: Endorser

Register DID

[Source: http://test.bcovrin.vonx.io/](http://test.bcovrin.vonx.io/)

This Medium post describes the Hyperledger Indy blockchain in details: https://drlee.io/identity-on-the-blockchain-with-hyperledger-indy-architecture-by-ernesto-net-7ce1a7e2732c

-It is a permissioned ledger

-It has no native cryptocurrency or token

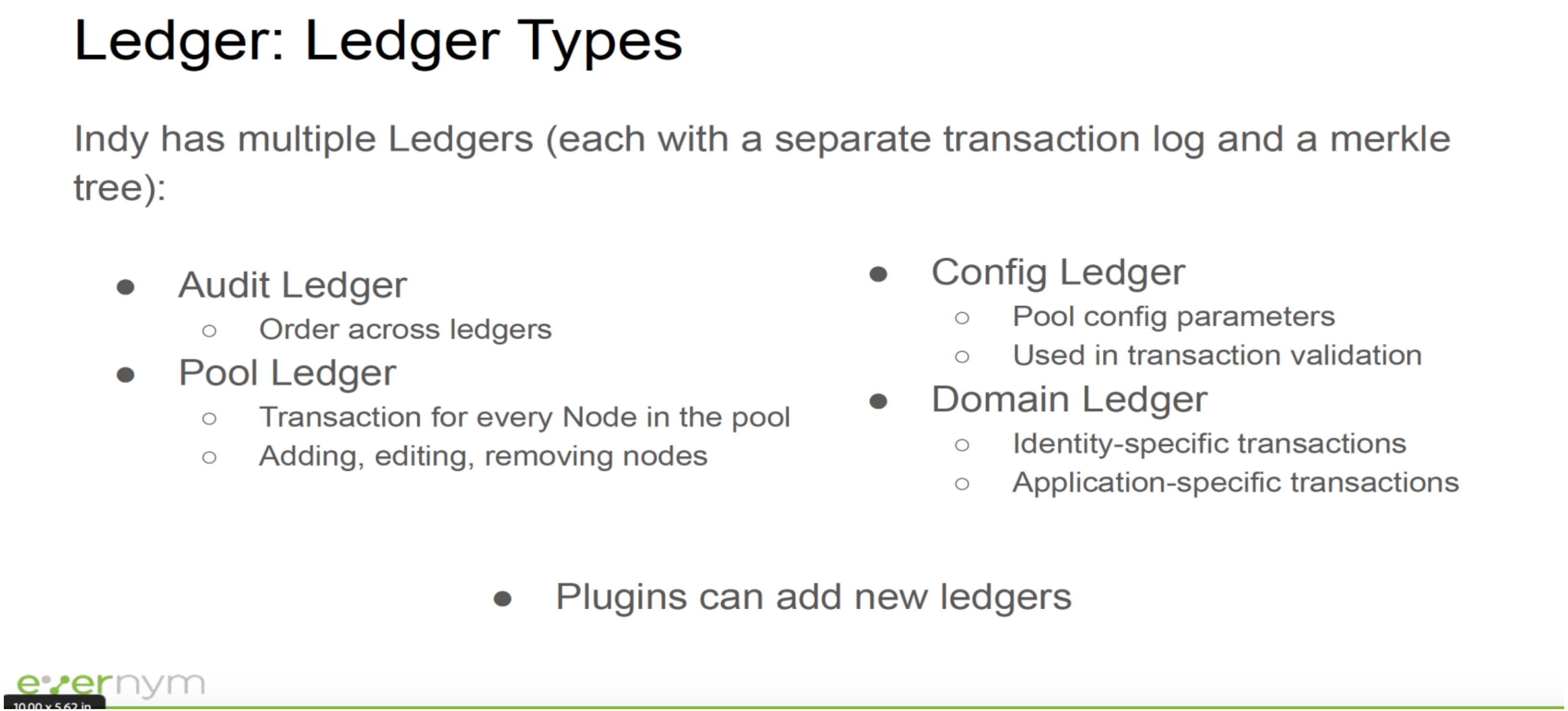
-It operates the Plennum consensus protocol (RBPT), which is a variant of the Byzantine Fault Tolerant protocol (more than 1/3 corrupt nodes can corrupt the ledger).

-It can handle a high volume of transactions

-Immutability guarantees will depend on who controls the ledger nodes (e.g., single entity or decentralized entities)

Transactions between peers are not stored in the ledger

EACH NODE RUNS FOUR TYPES OF LEDGERS



Ledger: Ledger Types

Indy has multiple Ledgers (each with a separate transaction log and a merkle tree):

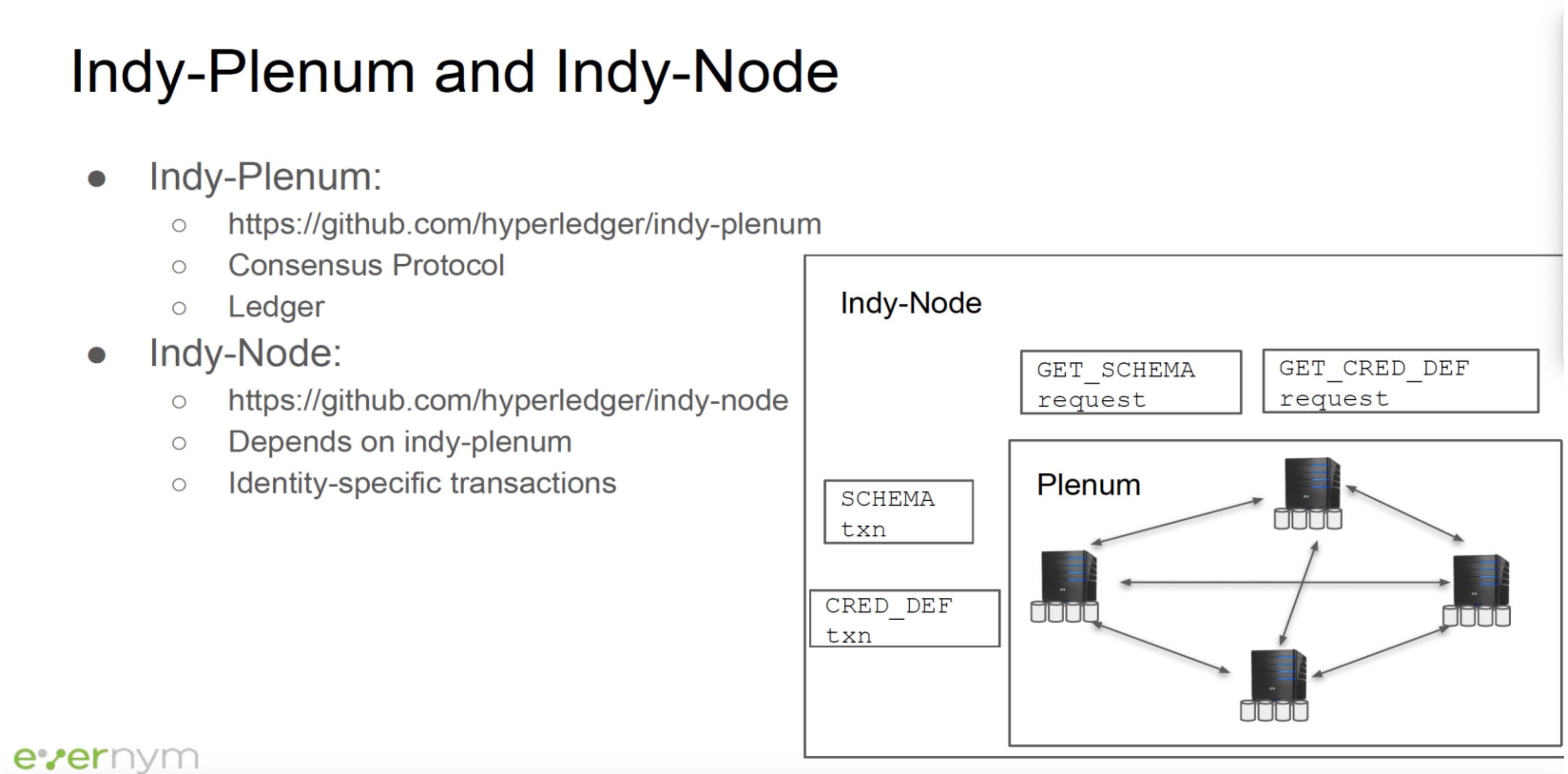
- Audit Ledger
  - Order across ledgers
- Pool Ledger
  - Transaction for every Node in the pool
  - Adding, editing, removing nodes
- Config Ledger
  - Pool config parameters
  - Used in transaction validation
- Domain Ledger
  - Identity-specific transactions
  - Application-specific transactions

- Plugins can add new ledgers

evernym

10.00 x 5.62 in

ARCHITECTURE OVERVIEW – CONSENSUS



Indy-Plenum and Indy-Node

- Indy-Plenum:
  - https://github.com/hyperledger/indy-plenum
  - Consensus Protocol
  - Ledger
- Indy-Node:
  - https://github.com/hyperledger/indy-node
  - Depends on indy-plenum
  - Identity-specific transactions

evernym

BYZANTINE FAULT TOLERANCE OVERVIEW

Definition: Byzantine Fault Tolerance (BFT) refers to the system's ability to function correctly and reach consensus even when some nodes in the network act maliciously or unpredictably.

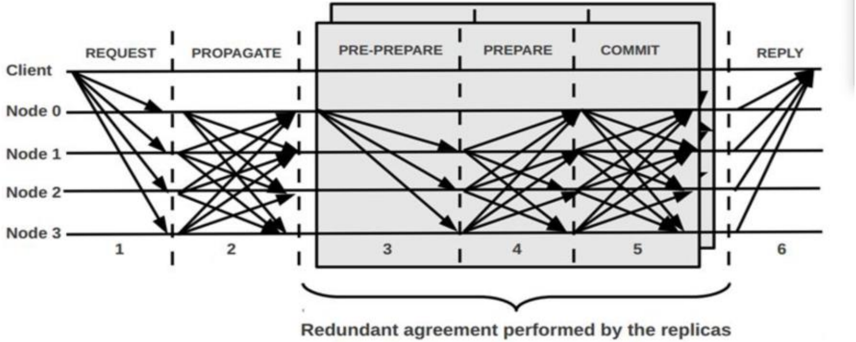
Importance: Ensures reliability and security in distributed systems where nodes may fail or act maliciously.

Basic Concept:

- **Fault Model:** Assumes that nodes can fail in arbitrary ways, including lying or colluding.
- **Consensus Objective:** Achieve agreement among non-faulty nodes on a common state or value.
- **Node Requirements:** Typically, to tolerate 'f' faulty nodes, a total of '3f + 1' nodes are needed.
- **Message Passing:** Nodes exchange messages to share their state and validate others' states to reach consensus.

REDUNDANT BYZANTINE FAULT TOLERANT MECHANISM

- **Redundancy Principle:** Incorporates additional nodes and layers of redundancy to enhance fault tolerance.
- **Phases of Consensus:**
  - **Pre-prepare:** Leader proposes a value.
  - **Prepare:** Nodes validate the proposal and broadcast their validation.
  - **Commit:** Nodes validate the prepare phase and broadcast commitment.
- **Final Decision:** Nodes make a final decision based on received messages from other nodes.
- **Redundancy Strategy:** Adds more nodes and layers to handle more complex fault scenarios.



CRYPTOGRAPHY OVERVIEW

Ledgers:

- Merkle Tree (Ledger)
- Patricia Merkle Trie (State)

Node-to-Node Communication:

- ZMQ (libsodium) as secure transport
  - CurveCP handshake
  - Authenticated Encryption

Authentication: Poly1305 MAC

Symmetric key crypto: XSalsa20

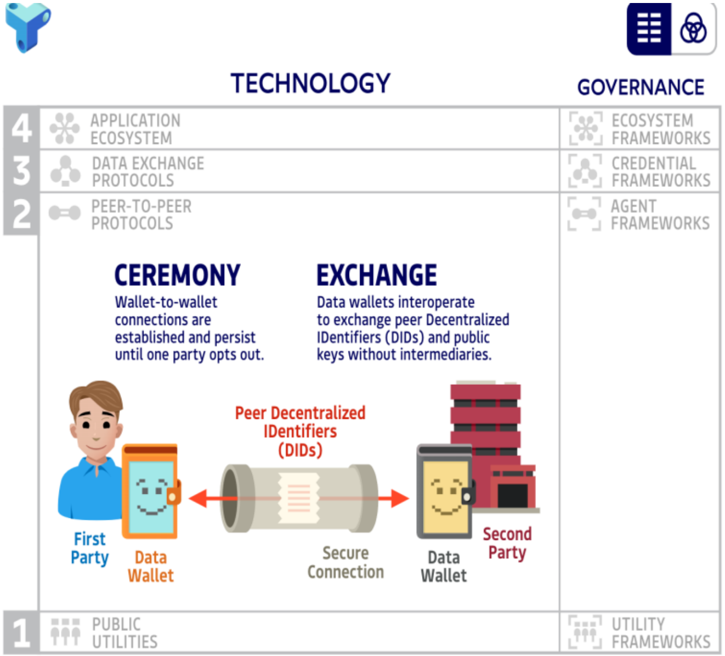
Public Key Crypto: Curve25519

- No Digital Signatures
  - BLS multi-signature to sign merkle roots

Client-to-Node communication:

- Ed25519 Digital Signatures

TECHNOLOGY LAYERS 2 & 3 (DIDCOMM & DATA EXCHANGE)

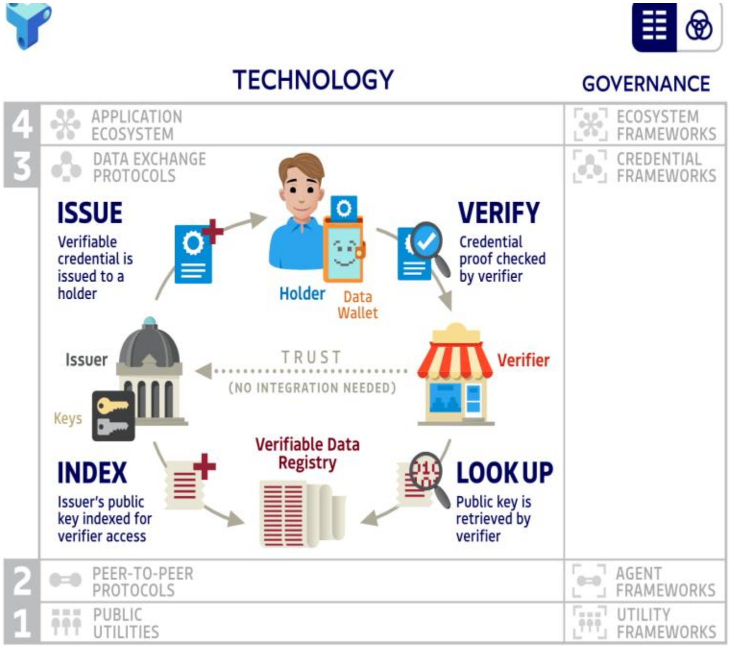


CEREMONY

Wallet-to-wallet connections are established and persist until one party opts out.

EXCHANGE

Data wallets interoperate to exchange peer Decentralized IDentifiers (DIDs) and public keys without intermediaries.



ISSUE

Verifiable credential is issued to a holder

VERIFY

Credential proof checked by verifier

INDEX

Issuer's public key indexed for verifier access

LOOKUP

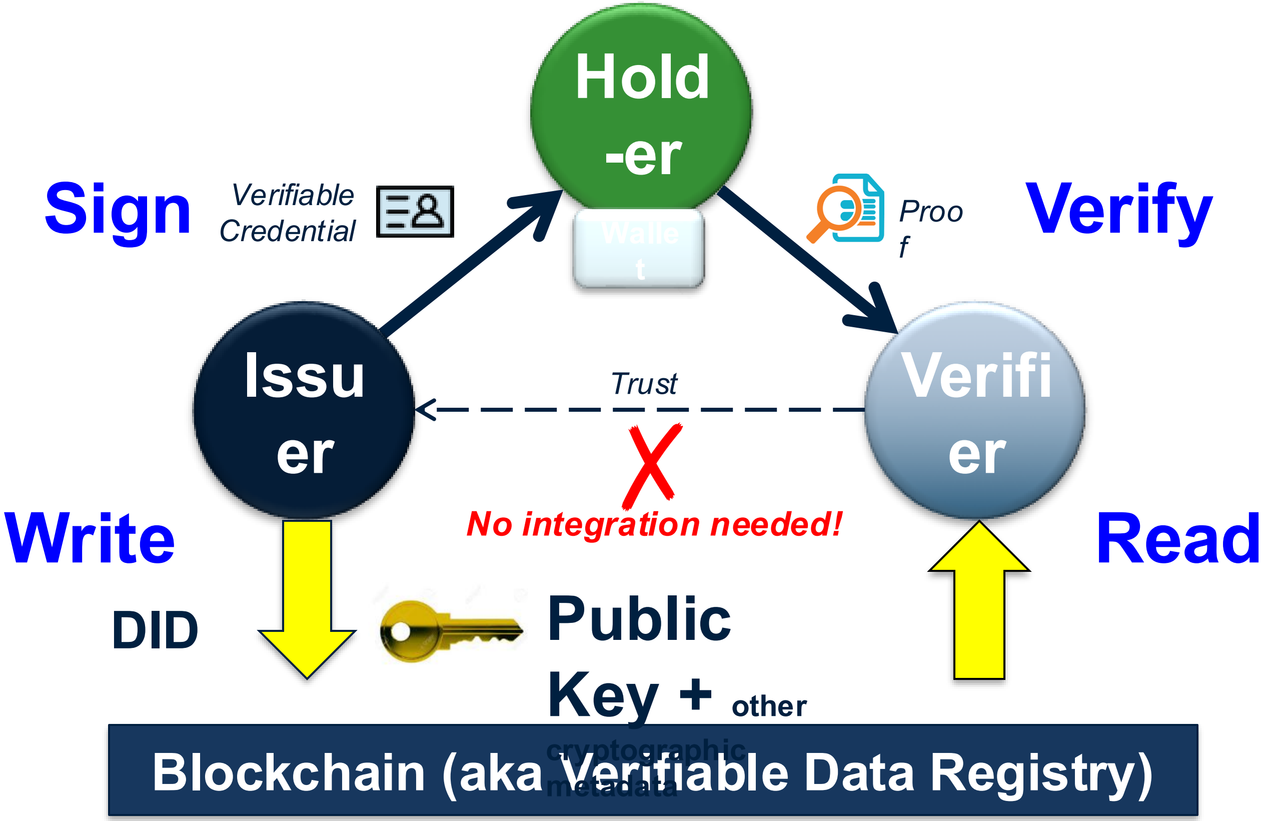
Public key is retrieved by verifier

Decentralized Identity Components

The essence Decentralized-ID is in creating open standards for a privacy preserving internet-wide identity layer — not owned by any one particular organization, but interoperable between all.

- DIDs
- DID Method (embedded in a DID Document)
- DID Specification
- DIDComm (Exchange Protocols)
- Verifiable Credential
- Agent/Digital Wallet

How Layer 3 works: Verifiable Credential Trust Triangle



Hold
-er

Walle
t

Sign

Verifiable Credential

*Proo
f*

Verify

Issu
er

Trust

X

No integration needed!

Verifi
er

Write

Read

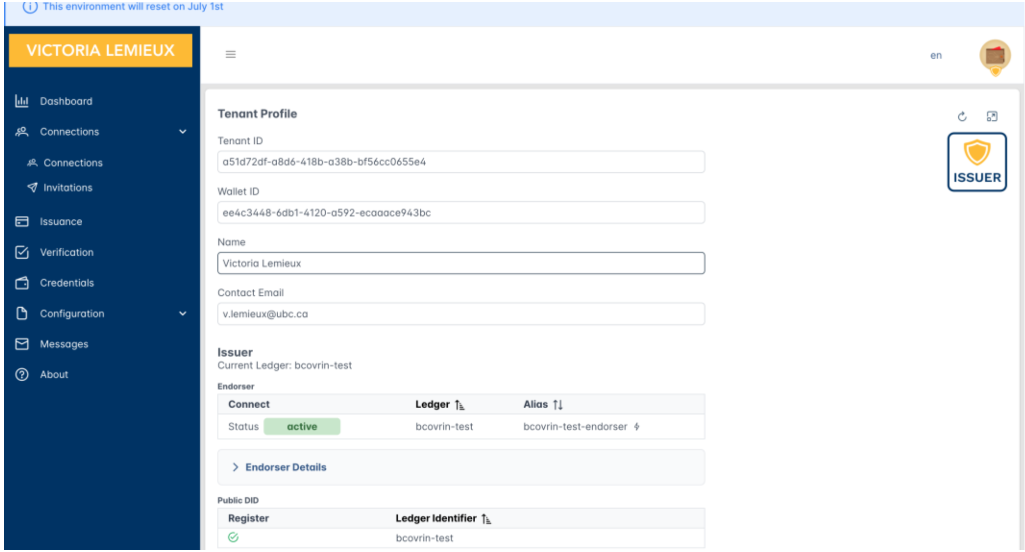
DID

Public Key + other cryptographic metadata

Blockchain (aka Verifiable Data Registry)

UBC iSchool

PARTIES (AGENTS) INTERACT USING THEIR WALLETS



ⓘ This environment will reset on July 1st

Tenant Profile

Tenant ID: a51d72df-a8d6-418b-a38b-bf56cc0655e4

Wallet ID: ee4c3448-6db1-4120-a592-ecaaace943bc

Name: Victoria Lemieux

Contact Email: v.lemieux@ubc.ca

Issuer

Current Ledger: bcovrin-test

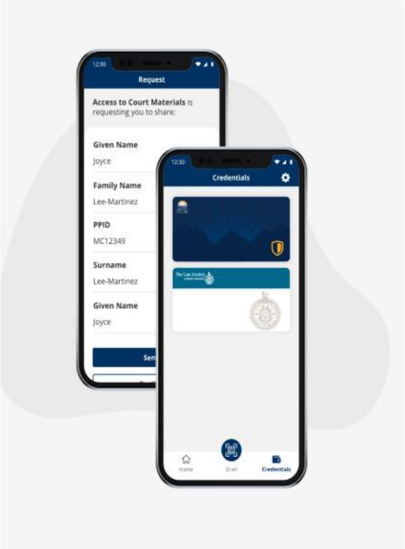
Endorser

Connect	Ledger	Alias
Status active	bcovrin-test	bcovrin-test-endorser

› Endorser Details

Public DID

Register	Ledger Identifier
✓	bcovrin-test



Access to Court Materials is requesting you to share:

Given Name: Joyce

Family Name: Lee-Martinez

PPID: MC12349

Surname: Lee-Martinez

Given Name: Joyce

Cloud Wallet

Mobile Wallet

Agent/Digital Wallet

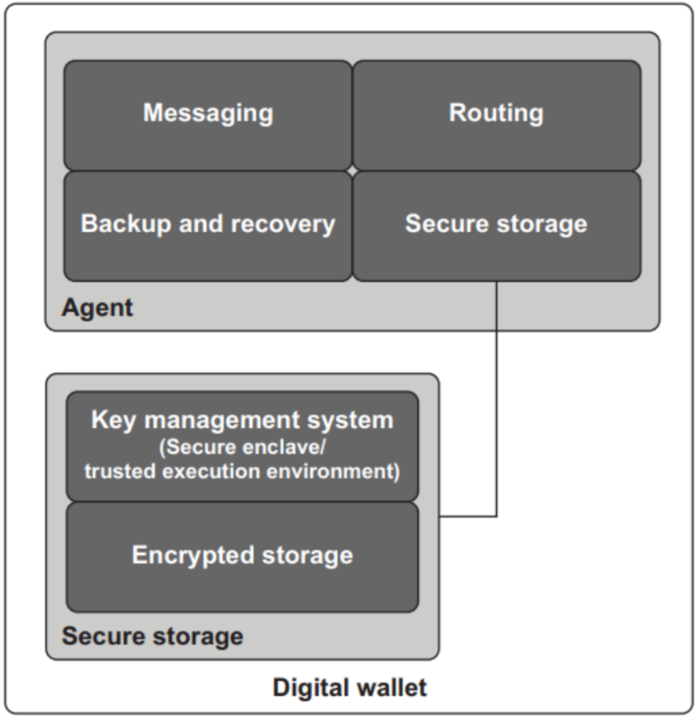


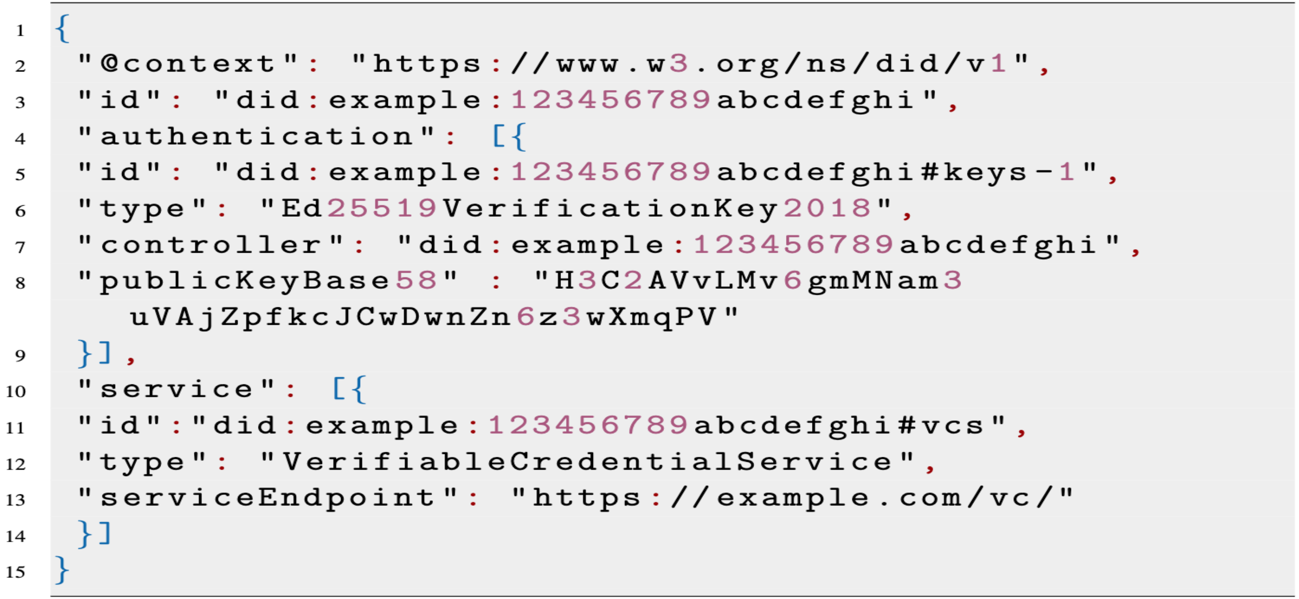
Fig. 4. Conceptual architecture of a typical SSI digital wallet and agent.[58]

REGISTERING A DID IN AN SSI BLOCKCHAIN REGISTRY USING HYPERLEDGER INDY (REFER TO LAB #!)

$$\underbrace{\text{did}}_{\text{DID Scheme}} : \underbrace{\text{example}}_{\text{DID Method}} : \underbrace{\text{123456789abcdefghijk}}_{\text{Method-Specific Identifier}}$$

DID Method

Listing 1. Example DID Document



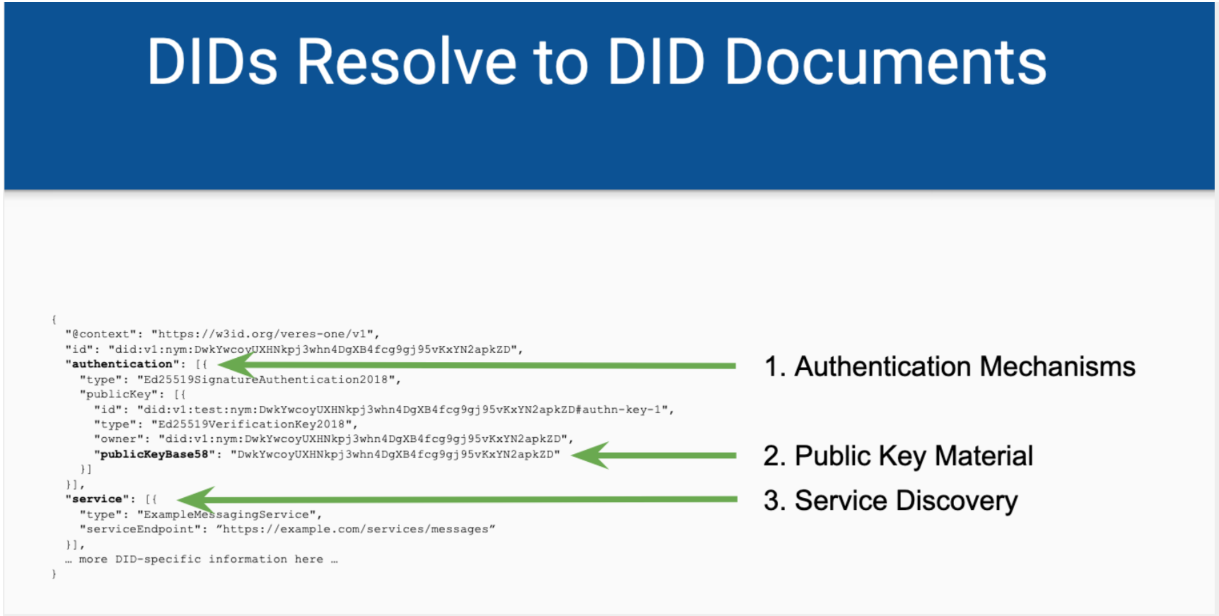
```
{
 "@context": "https://www.w3.org/ns/did/v1",
 "id": "did:example:123456789abcdefghi",
 "authentication": [{
 "id": "did:example:123456789abcdefghi#keys-1",
 "type": "Ed25519VerificationKey2018",
 "controller": "did:example:123456789abcdefghi",
 "publicKeyBase58" : "H3C2AVvLMv6gmMNam3
   uVAjZpfkcJCwDwnZn6z3wXmqPV"
 }],
 "service": [{
 "id":"did:example:123456789abcdefghi#vcs",
 "type": "VerifiableCredentialService",
 "serviceEndpoint": "https://example.com/vc/"
 }]
}
```

Latest (2022) W3C Rubric for choosing a DIDMethod: https://w3c.github.io/did-rubric/

DIDDocs and Specifications

DIDS RESOLVE TO DIDDOCS

ENSURES INTEROPERABILITY BETWEEN DID SCHEMES, ALLOWING ANY STORAGE SYSTEM TO INTERACT WITH AND RESOLVE A DID.

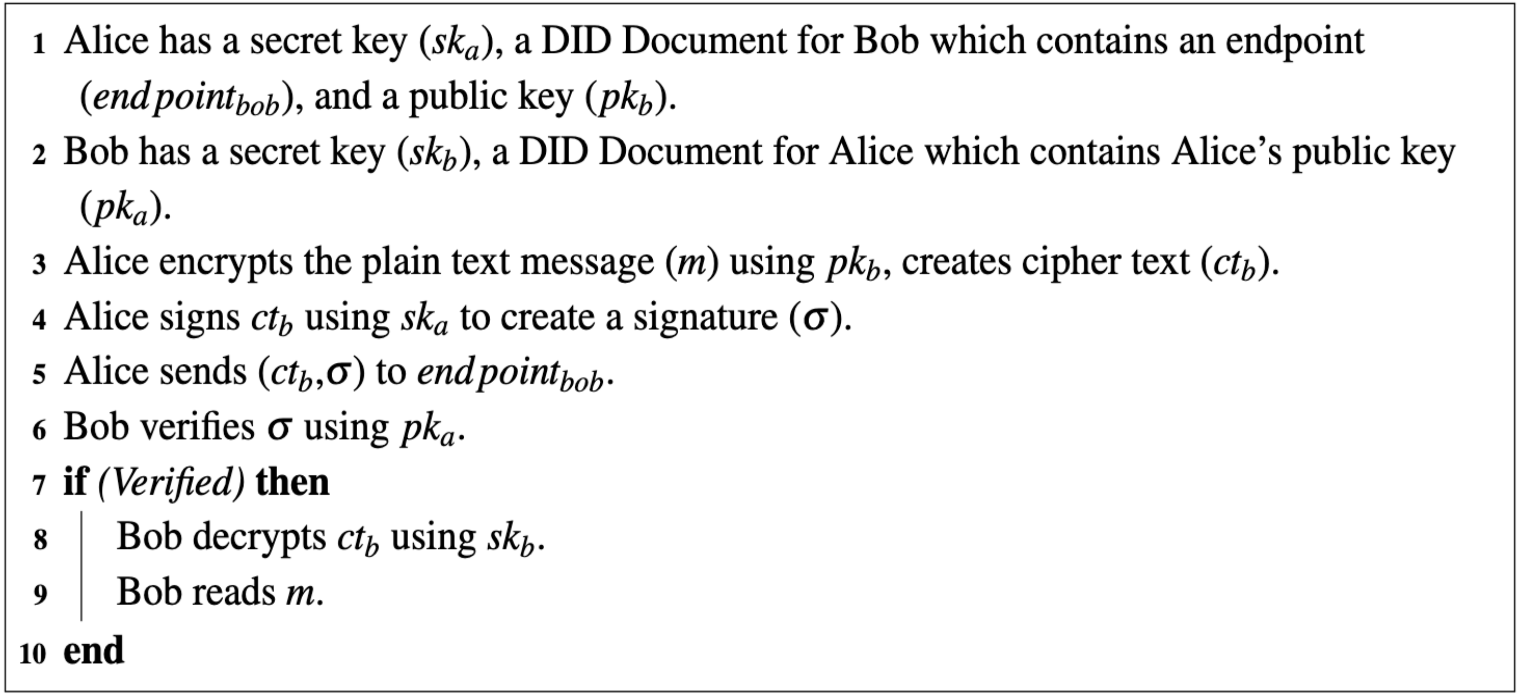


DIDs Resolve to DID Documents

```
{
  "@context": "https://w3id.org/veres-one/v1",
  "id": "did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id": "did:v1:test:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#authn-key-1",
      "type": "Ed25519VerificationKey2018",
      "owner": "did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
      "publicKeyBase58": "DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD"
    }]
  }],
  "service": [{
    "type": "ExampleMessagingService",
    "serviceEndpoint": ”https://example.com/services/messages”
  }],
  … more DID-specific information here …
}
```

1. Authentication Mechanisms
2. Public Key Material
3. Service Discovery

DIDComm (Exchange Protocols)



```
Alice has a secret key ($sk_a$), a DID Document for Bob which contains an endpoint ($endpoint_{bob}$), and a public key ($pk_b$).
Bob has a secret key ($sk_b$), a DID Document for Alice which contains Alice's public key ($pk_a$).
Alice encrypts the plain text message ($m$) using $pk_b$, creates cipher text ($ct_b$).
Alice signs $ct_b$ using $sk_a$ to create a signature ($\sigma$).
Alice sends ($ct_b$,$\sigma$) to $endpoint_{bob}$.
Bob verifies $\sigma$ using $pk_a$.
if (Verified) then
    Bob decrypts $ct_b$ using $sk_b$.
    Bob reads $m$.
end
```

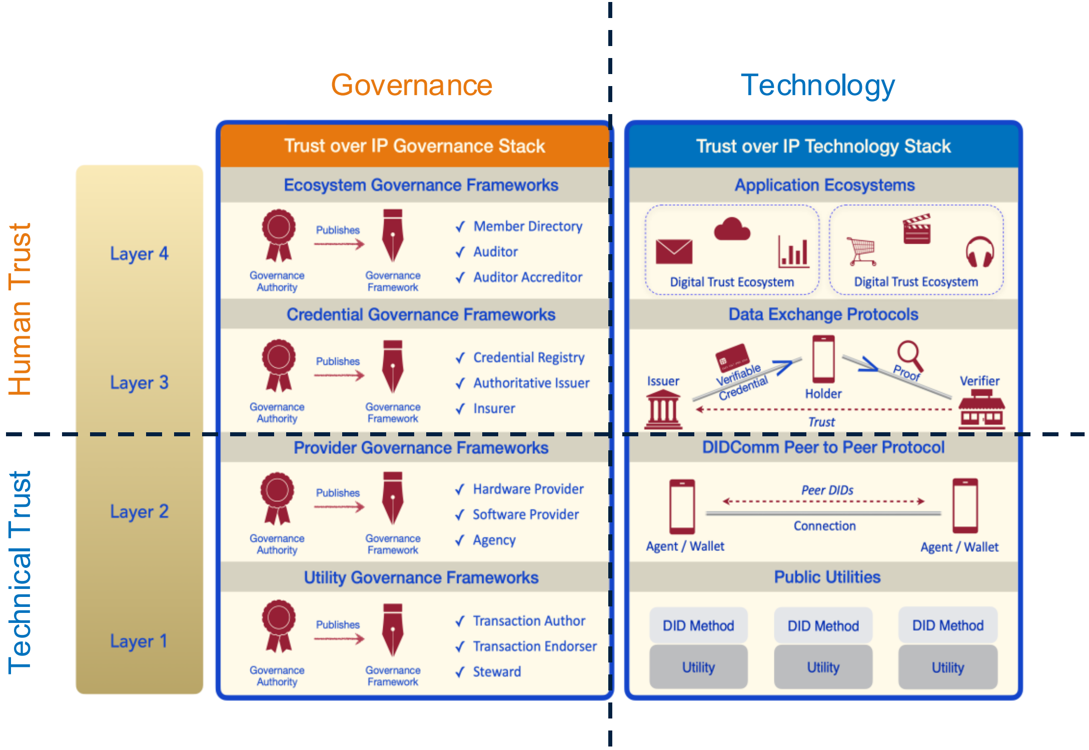
Variety of exchange protocols

- DIDComm (DIF)
- CHAPI (DIF)
- OIDC4VC (OpenID)
- mDL (ISO/IEC)
- WACI-Pex (DIF)
- VC-HTTP-API (CCG)

See: https://decentralized-id.com/ecosystem/

GOVERNANCE

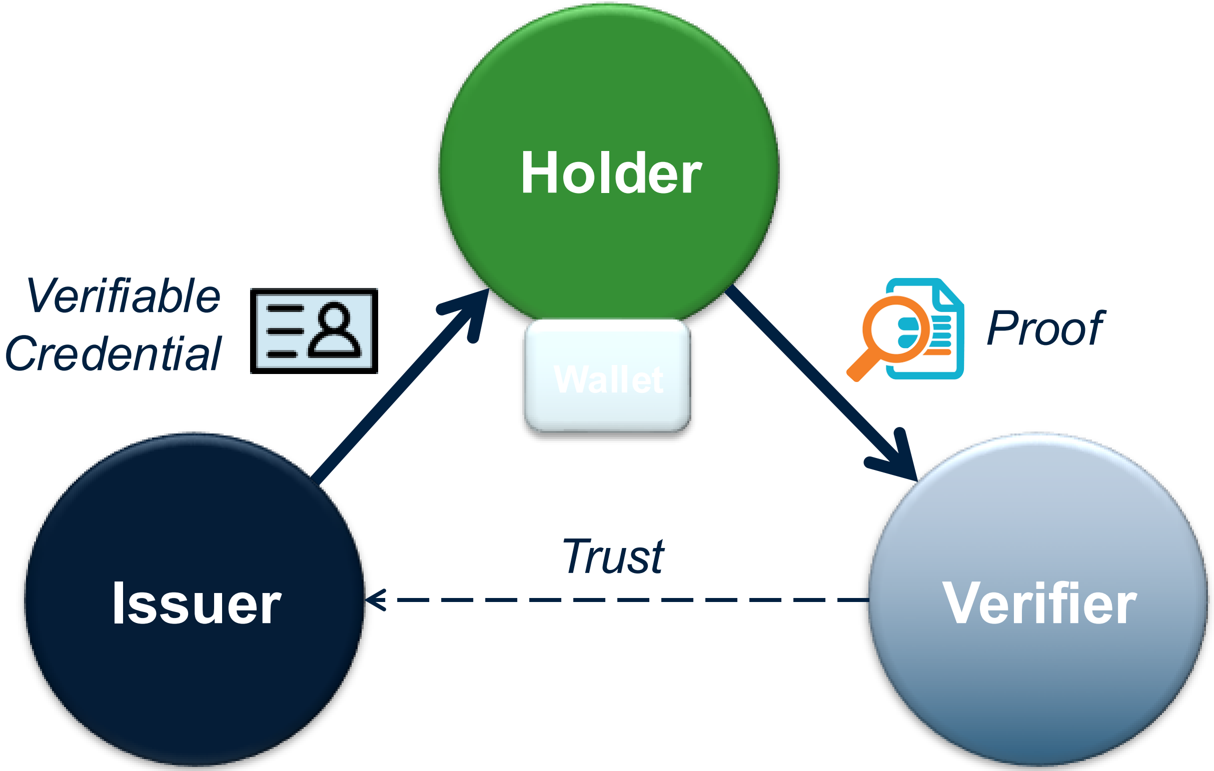
THE DECENTRALIZED IDENTITY STACK



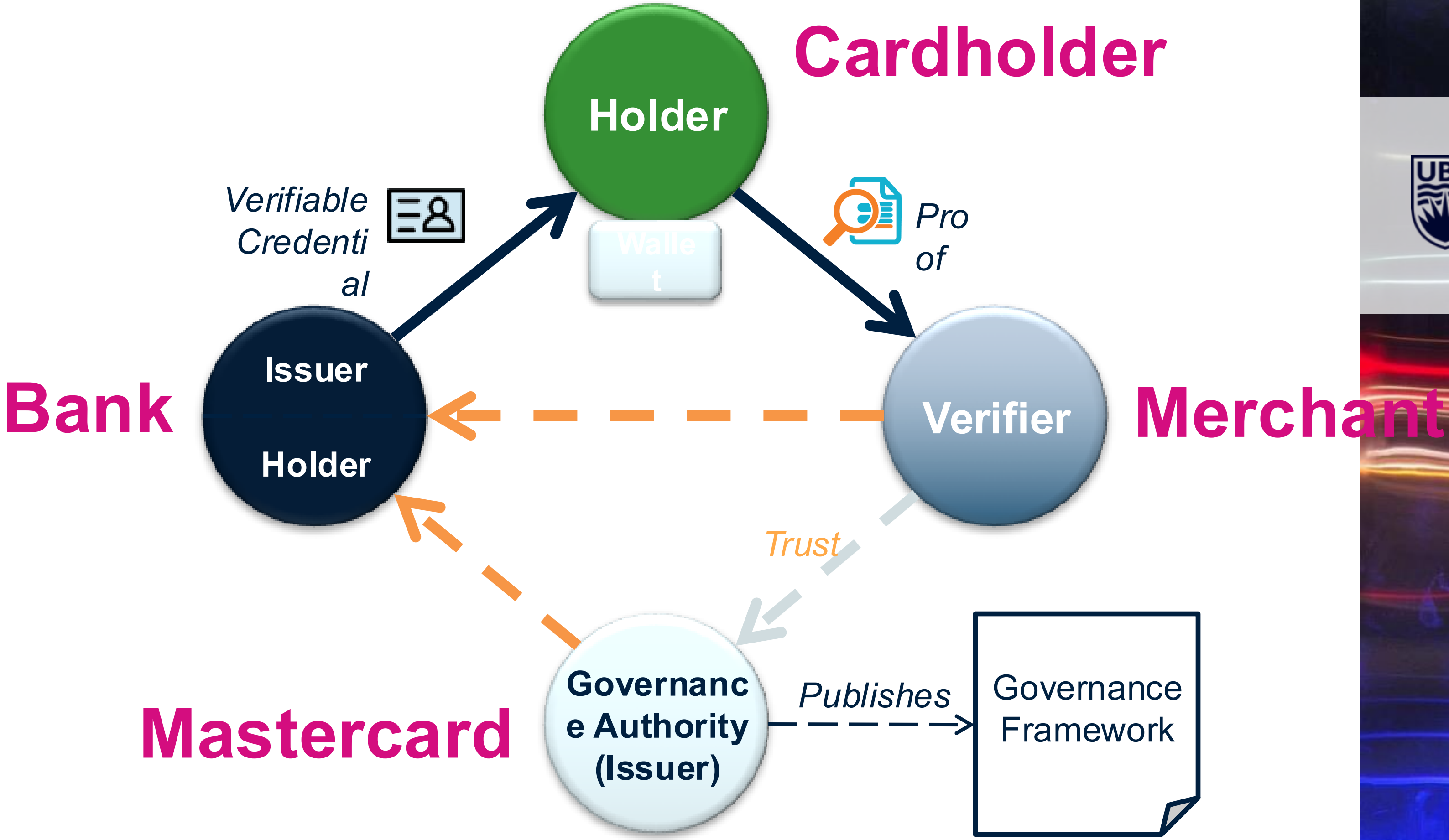
		Governance	Technology
		Trust over IP Governance Stack	Trust over IP Technology Stack
Human Trust	Layer 4	Ecosystem Governance Frameworks Governance Authority – Publishes → Governance Framework ✓ Member Directory ✓ Auditor ✓ Auditor Accreditor	Application Ecosystems Digital Trust Ecosystem Digital Trust Ecosystem
	Layer 3	Credential Governance Frameworks Governance Authority – Publishes → Governance Framework ✓ Credential Registry ✓ Authoritative Issuer ✓ Insurer	Data Exchange Protocols Issuer – Verifiable Credential → Holder – Proof → Verifier Trust
Technical Trust	Layer 2	Provider Governance Frameworks Governance Authority – Publishes → Governance Framework ✓ Hardware Provider ✓ Software Provider ✓ Agency	DIDComm Peer to Peer Protocol Agent / Wallet – Peer DIDs / Connection – Agent / Wallet
	Layer 1	Utility Governance Frameworks Governance Authority – Publishes → Governance Framework ✓ Transaction Author ✓ Transaction Endorser ✓ Steward	Public Utilities DID Method / Utility DID Method / Utility DID Method / Utility

https://trustoverip.org/wp-content/toip-model/

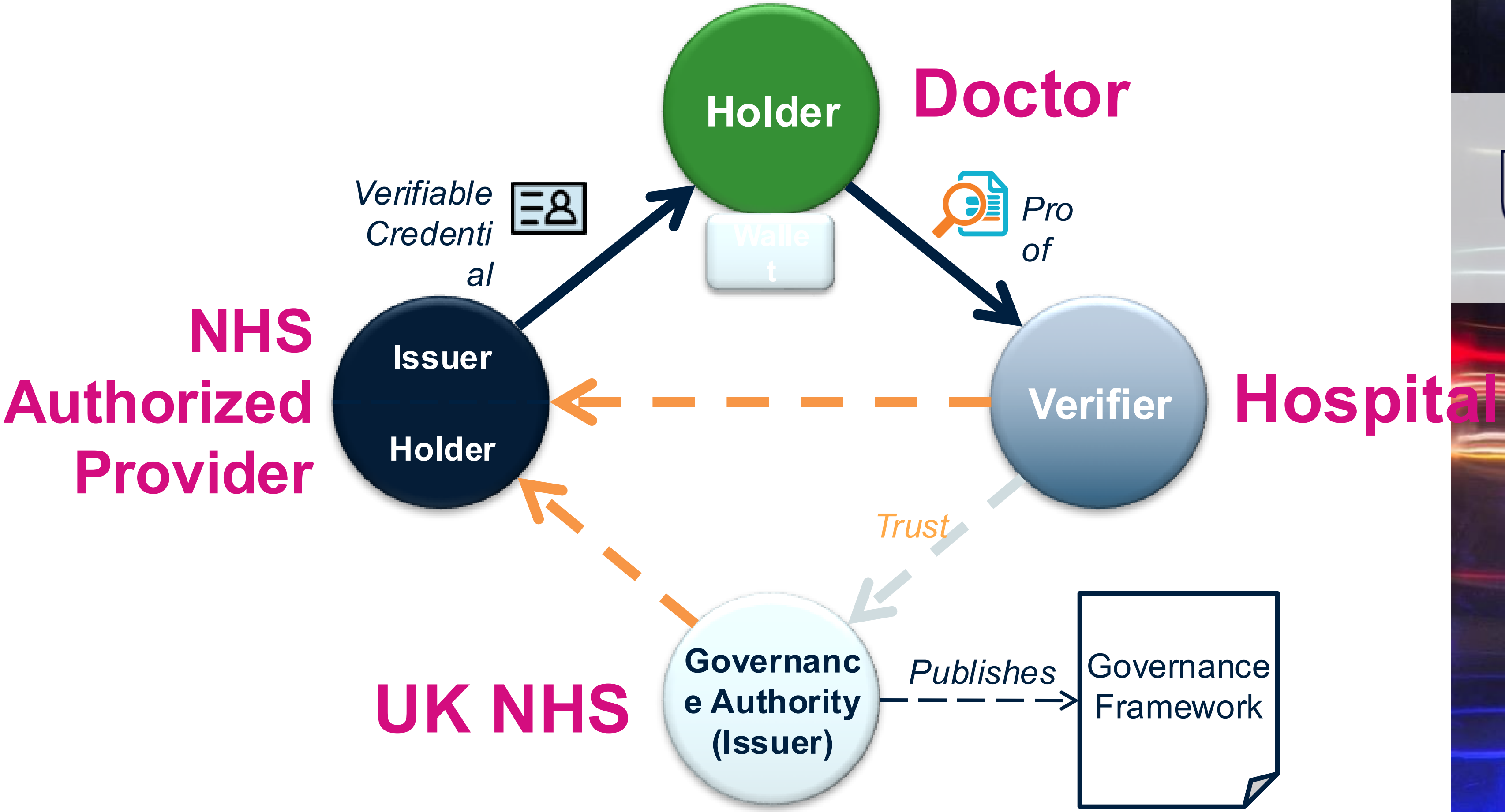
How can verifiers know all the issuers?



The governance trust triangle



Example: the doctor’s passport



Holder

Doctor

Walle
t

Verifiable
Credenti
al

Pro
of

NHS
Authorized
Provider

Issuer

Holder

Verifier

Hospital

Trust

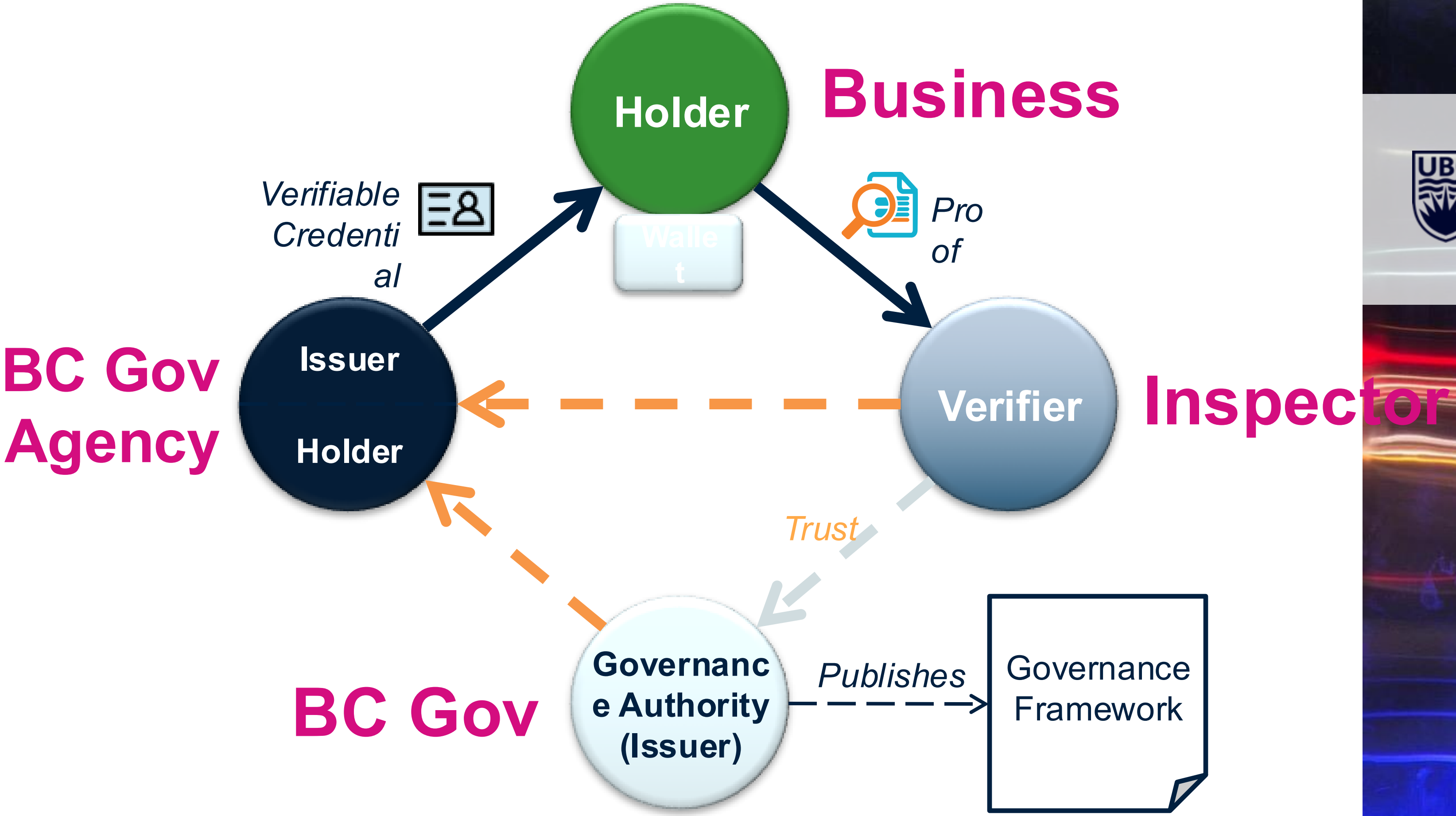
UK NHS

Governanc
e Authority
(Issuer)

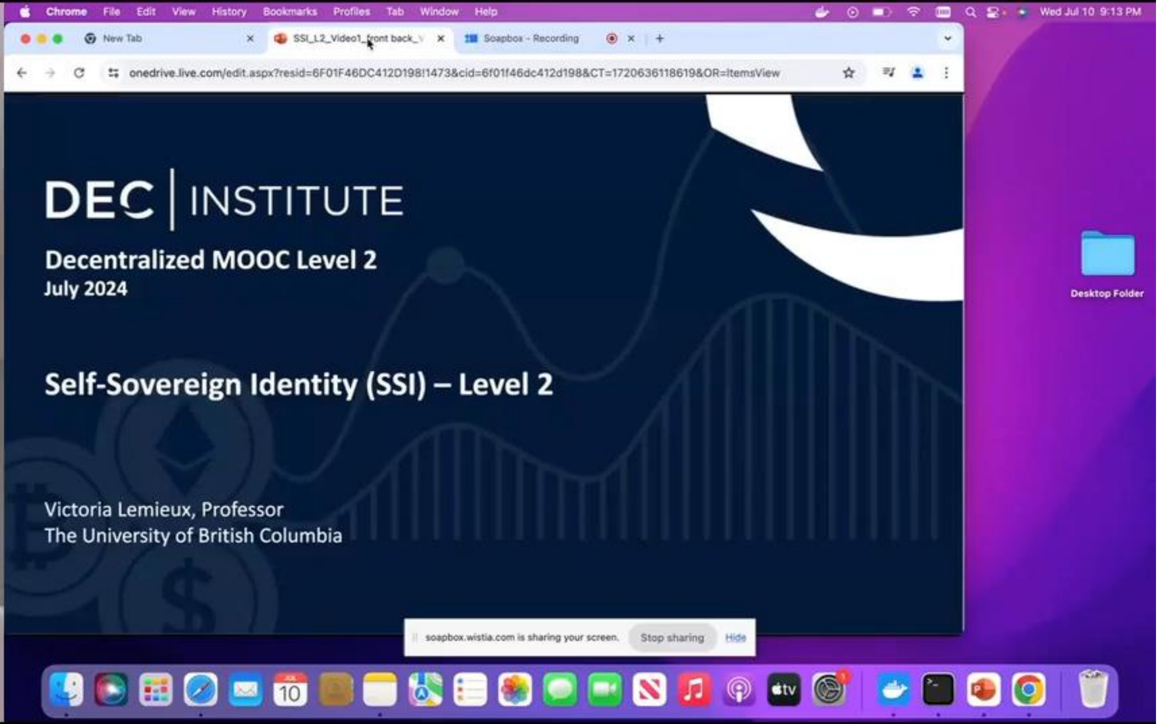
Publishes

Governance
Framework

Example: BC Gov digital trust ecosystem



SETTNG UP AN SSI BLOCKCHAIN REGISTRY (DEMO)


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed Jul 10 9:13 PM
New Tab
SSI_L2_Video1_front back_
Soapbox - Recording
onedrive.live.com/edit.aspx?resid=6F01F46DC412D198!1473&cid=6f01f46dc412d198&CT=1720636118619&OR=ItemsView
Desktop Folder
soapbox.wistia.com is sharing your screen.
Stop sharing
Hide

DEC | INSTITUTE

Decentralized MOOC Level 2
July 2024

Self-Sovereign Identity (SSI) – Level 2

Victoria Lemieux, Professor
The University of British Columbia

EXCHANGING AND VERIFYING VERIFIABLE CREDENTIALS (DEMO)

My files - OneDrive
SSI_L2_Video2_front back_
Soapbox - Recording
onedrive.live.com/edit.aspx?resid=6F01F46DC412D198!1475&cid=6f01f46dc412d198&CT=1721159345402&OR=ItemsView

DEC | INSTITUTE

Decentralized MOOC Level 2
April 2024

Self-Sovereign Identity (SSI) – Level 2

Victoria Lemieux, Professor
The University of British Columbia

CASE STUDIES

USE CASE EXAMPLE 1: ACCESS TO COURT SERVICES

Solution

The Law Society of British Columbia collaborated with the B.C. Government’s Digital Trust and Identity Program on a project that established 3 new pillars of digital trust.

- The Law Society of BC issued a Member Card digital credential to a lawyer, proving they’re a lawyer in good standing
- A Person credential, an online identity based on information from their BC Services Card, was also issued to the lawyers
- Both digital credentials were integrated into the BC Wallet, a user-friendly and secure digital wallet smartphone app
- Lawyers then used their digital credentials and BC Wallet for swift and secure access to court services.

https://digital.gov.bc.ca/digital-trust/justice-project/

USE CASE EXAMPLE 2: MANAGE CONSENT FOR HEALTH DATA EXCHANGE

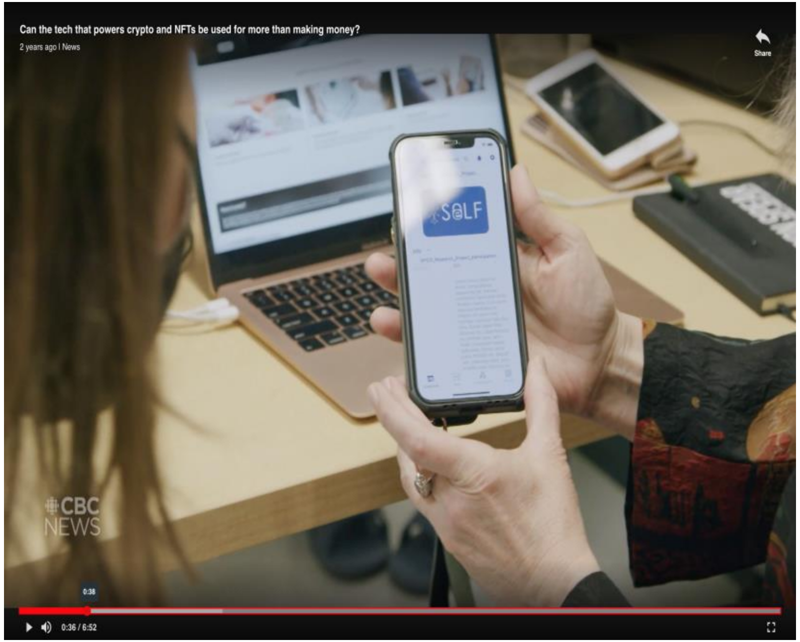
Solution

Health researchers must comply with laws and regulations that require them to:

- Validate a person’s identity
- Provide proof of consent for data sharing (What data? What use? How long?)
- Retain audit-ready consent evidence (for both partners + regulators)

Compliance with laws and regulations can slow health innovation, such as the discovery of new treatments for Cancer

Molecular You, a health intelligence company, and Blockchain@UBC at The University of British Columbia developed a solution to manage granular and dynamic consent using verifiable credentials



Can the tech that powers crypto and NFTs be used for more than making money?

2 years ago | News

https://www.cbc.ca/player/play/video/1.6412429

USE CASE EXAMPLE 3: PROOF OF SUSTAINABLE MINING

Solution

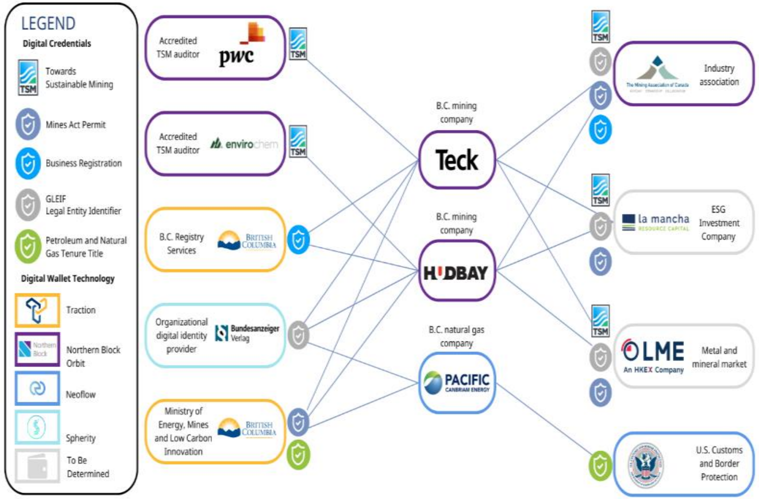
The Towards Sustainable Mining Program (TSM) program of the Mining Association of Canada (MAC) measures mining companies against 9 protocols.

- Commitment to biodiversity
- Water stewardship
- Health and safety
- Participating mines must report their progress annually.

Through collaboration with the Energy & Mines Digital Trust, MAC is exploring the opportunity for mining operators to submit their TSM scores using digital credentials, fulfilling their membership requirements securely and efficiently.

Mines can continue to use digital credentials to share their ESG performance to anyone who asks, including customers and investors.

Driving progress for natural resource operators in B.C.



LEGEND

Digital Credentials

- TSM Towards Sustainable Mining
- Mines Act Permit
- Business Registration
- GLEIF Legal Entity Identifier
- Petroleum and Natural Gas Tenure Title

Digital Wallet Technology

- Traction
- Northern Block Orbit
- Neoflow
- Spherity
- To Be Determined

Accredited TSM auditor — pwc

Accredited TSM auditor — envirochem

B.C. Registry Services — British Columbia

Organizational digital identity provider — Bundesanzeiger Verlag

Ministry of Energy, Mines and Low Carbon Innovation — British Columbia

B.C. mining company — Teck

B.C. mining company — HUDBAY

B.C. natural gas company — PACIFIC CANBRIAM ENERGY

The Mining Association of Canada — Industry association

la mancha RESOURCE CAPITAL — ESG Investment Company

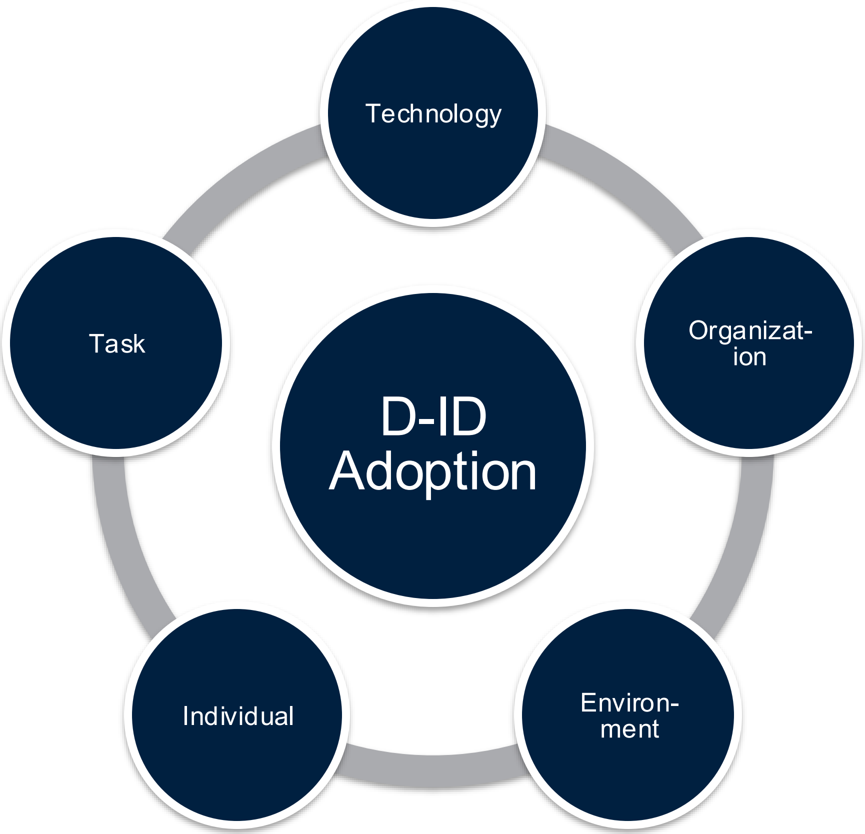
LME An HKEX Company — Metal and mineral market

U.S. Customs and Border Protection

https://digital.gov.bc.ca/2024/06/25/energy-mines-digital-trust-pilot/

ISSUES AND CHALLENGES

Technology adoption means Addressing issues and challenges . . .



CRITICAL ANALYSIS

QR Code Security

- Observation: QR codes can be insecure and subject to Man-in-the-Middle Attacks (a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two user parties). However, EDMT uses DiDComm which signs all messages passed between peers, ensuring that communications cannot be intercepted and forged.
- Suggestion: Always use DiDcomm for credential exchange (or some other secure form of communication)

CRITICAL ANALYSIS

Competence of Authority for Credential Issuance

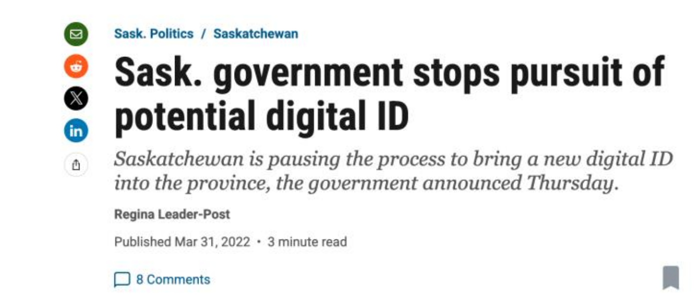
- Observation: Our demo does not incude a check that the credential is issued by the competent authority

- Suggestion: Need to set up a governance framework so that subsequent verifications check to ensure that the credential has been digitally signed by the competent authority (their VerKey which can be searched up on the blockchain)

CRITICAL ANALYSIS

Social Trust in the Governance Authority

- Observation: Individuals may not trust the credential issuing authority e.g., a government
- Suggestion: Need to set up a governance framework so that there are safeguards and limitations to avoid abuse of power/human rights violations/exclusion of disadvantaged groups



Sask. Politics / Saskatchewan

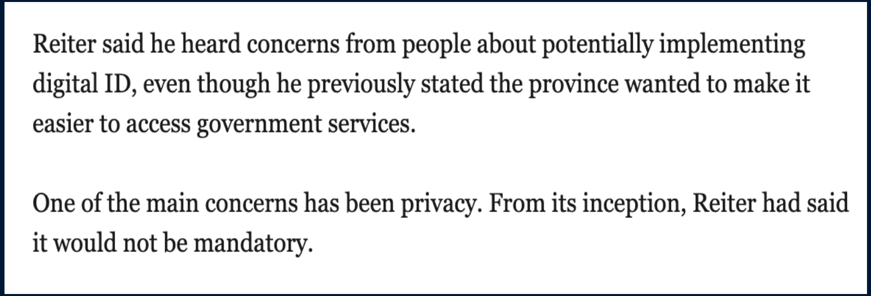
Sask. government stops pursuit of potential digital ID

Saskatchewan is pausing the process to bring a new digital ID into the province, the government announced Thursday.

Regina Leader-Post

Published Mar 31, 2022 • 3 minute read

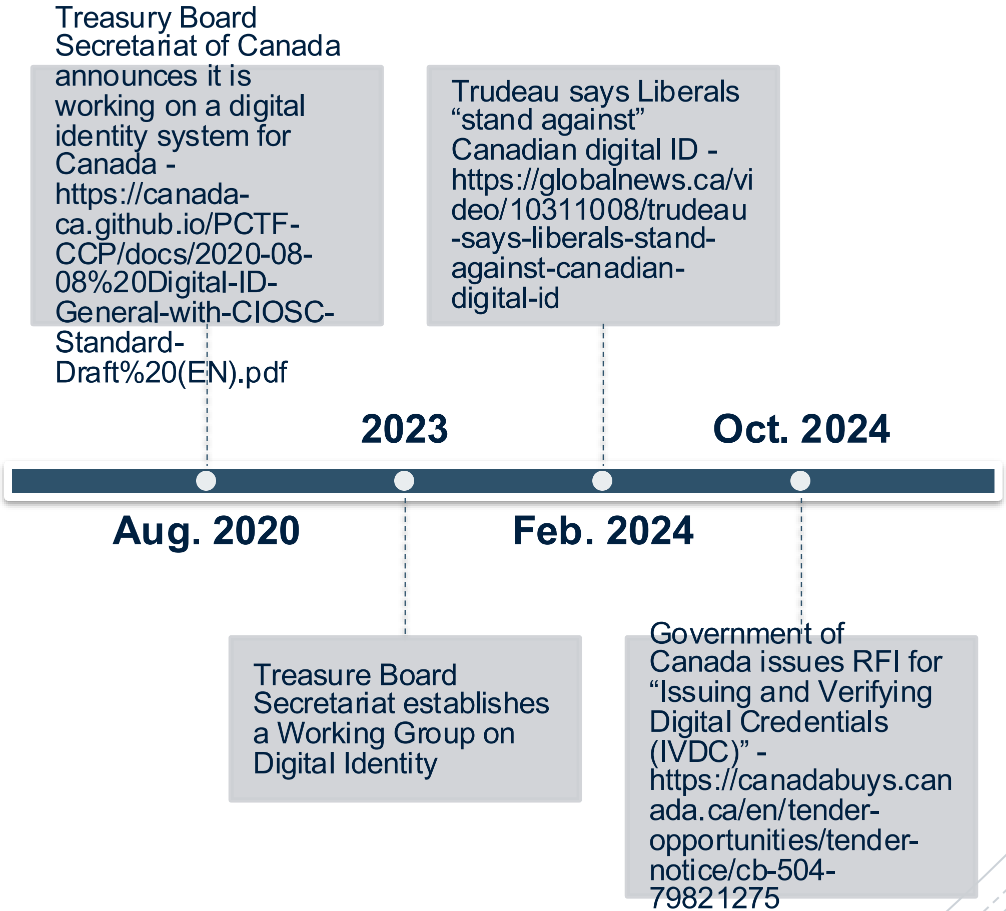
8 Comments



Reiter said he heard concerns from people about potentially implementing digital ID, even though he previously stated the province wanted to make it easier to access government services.

One of the main concerns has been privacy. From its inception, Reiter had said it would not be mandatory.

Decentralized identity in Canada – Watch this space!



Aug. 2020

Treasury Board Secretariat of Canada announces it is working on a digital identity system for Canada - https://canada-ca.github.io/PCTF-CCP/docs/2020-08-08%20Digital-ID-General-with-CIOSC-Standard-Draft%20(EN).pdf

2023

Treasure Board Secretariat establishes a Working Group on Digital Identity

Feb. 2024

Trudeau says Liberals “stand against” Canadian digital ID - https://globalnews.ca/video/10311008/trudeau-says-liberals-stand-against-canadian-digital-id

Oct. 2024

Government of Canada issues RFI for “Issuing and Verifying Digital Credentials (IVDC)” - https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-504-79821275

THE UNIVERSITY OF BRITISH COLUMBIA

School of Information

Faculty of Arts