RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-R03

Decentralized Identity: No Promises Edition

Pamela Dingle
Director of Identity Standards
Microsoft
@pamelarosiedee

Preeti Rastogi
Principal Software Engineer
Microsoft
@PreetiRastogi13

Cast of Characters

Preeti Rastogi

- Developed my first online application using CICS on Mainframes
- 3 years as a developer in anti-malware security products
- 9 years as a security architect for enterprise mobile management
- Now part of the Decentralized Identity Engineering team at Microsoft

Pamela Dingle

- Installed my first directory in '99
- Wrote OSS RP code for infocards back in the day
- 8 years as an identity architect, 8 years in CTO office
- Now running a team of experts who design identity standards for Microsoft

RSAConference2019

We come from Different Perspectives

Preeti

Photo credit: David Guyler https://www.flickr.com/photos/daviegee/16840203586

In the U.S. and abroad, fundamental rights and services like voting, healthcare, housing and education are tethered to legal proof of identification – you can't participate if you don't have it. Yet nearly one in six people worldwide – the majority of them being women, children and refugees – live without it. The lack of legal documentation not only strips access to critical services, it puts those trapped in the "identity gap" at risk for larger issues including displacement and child trafficking.

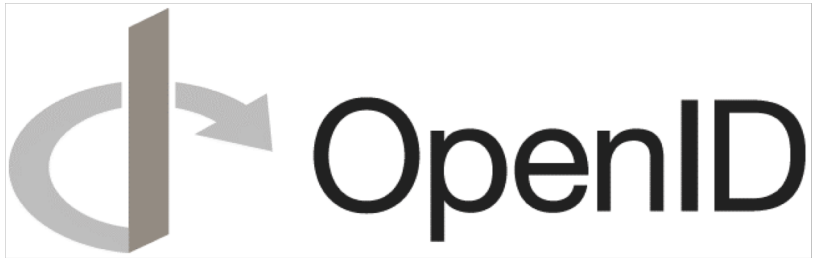
--- Excerpt from a Jan 22, 2018 blog by Peggy Johnson
https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/

Photo credit: David Guyler https://www.flickr.com/photos/daviegee/16840203586

Pam

Inspiration for the Laws of Identity

Protest drove change



Taught us about Discovery UX

First version was not 'consumer-grade'
(and some people liked it that way)

http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

Three ways to Get Around

when you travel

Photo Credit: Hernan Pinera https://www.flickr.com/photos/hernanpc/8139327438/

1. Local

Photo credit: Bernard Spragg https://www.flickr.com/photos/volvob12b/14333164242/

2. All Inclusive

Photo credit: Wessel Blokzijl https://www.flickr.com/photos/wblokzijl/44967804132/

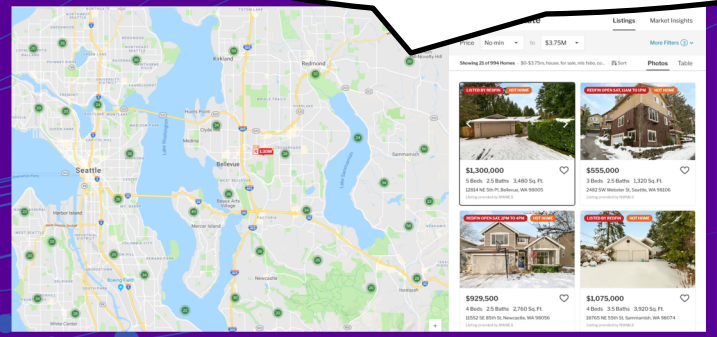
3. Yours

Photo credit: Pamela Dingle https://www.flickr.com/photos/pamelarosiedee/6889169915

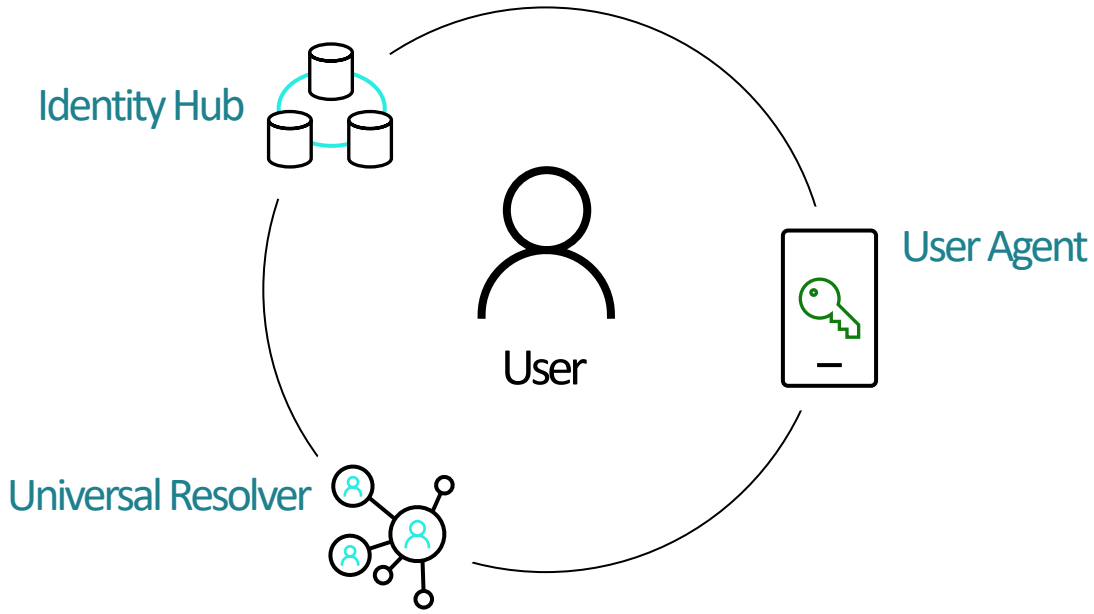
RSAConference2019

Scenario: Own and control your identity

Alice wants to buy a house!!!



The User Agent generates keys

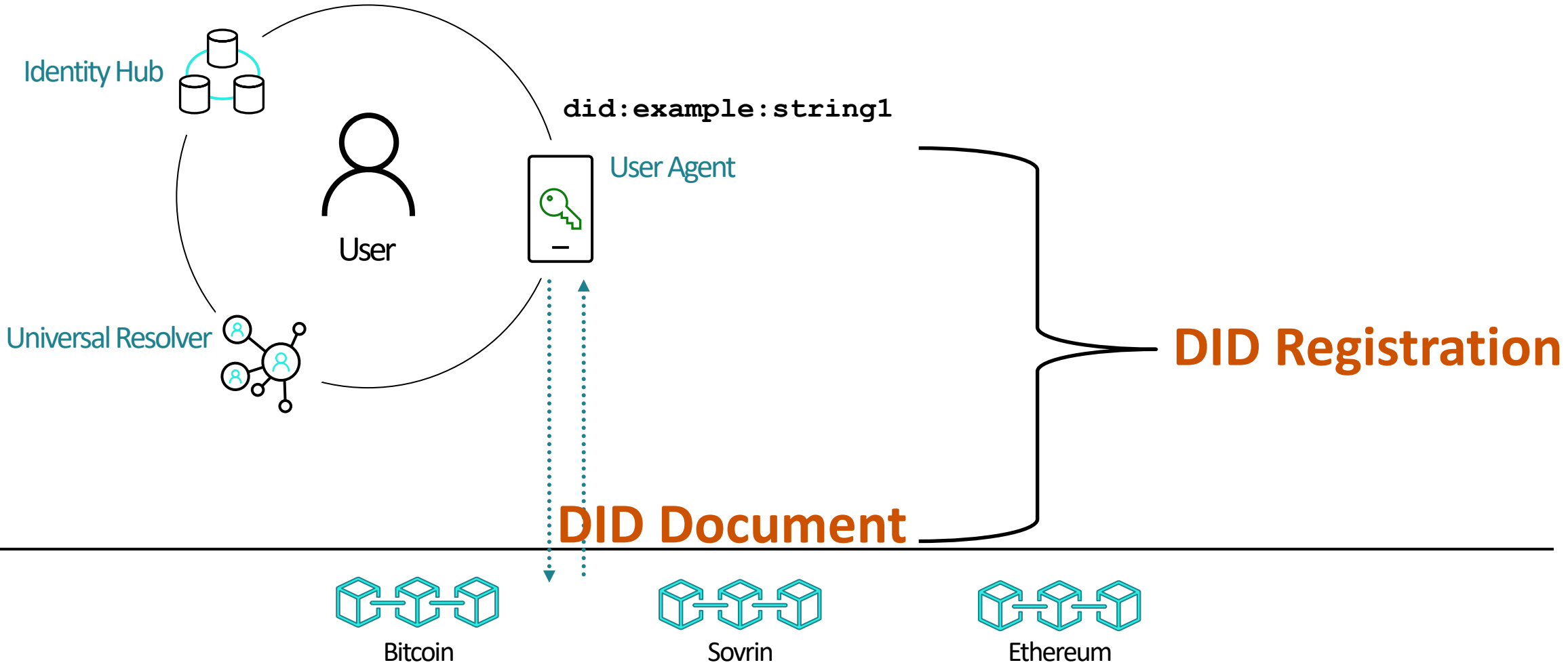


Bitcoin

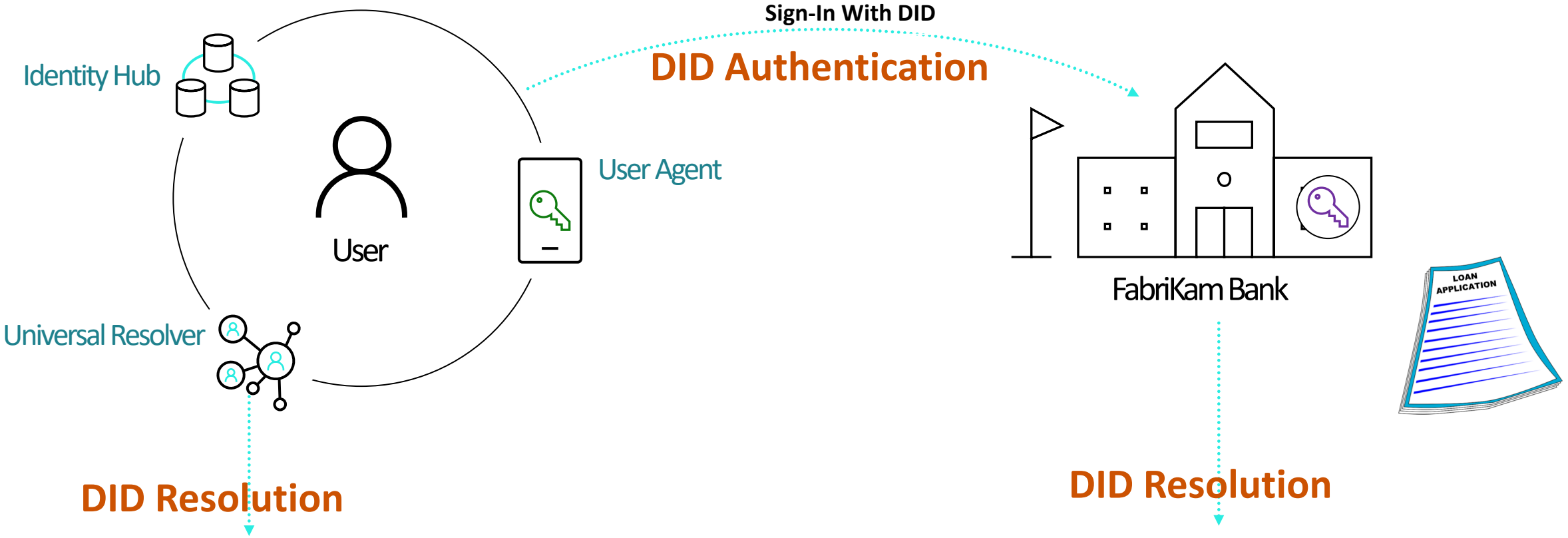
Sovrin

Ethereum

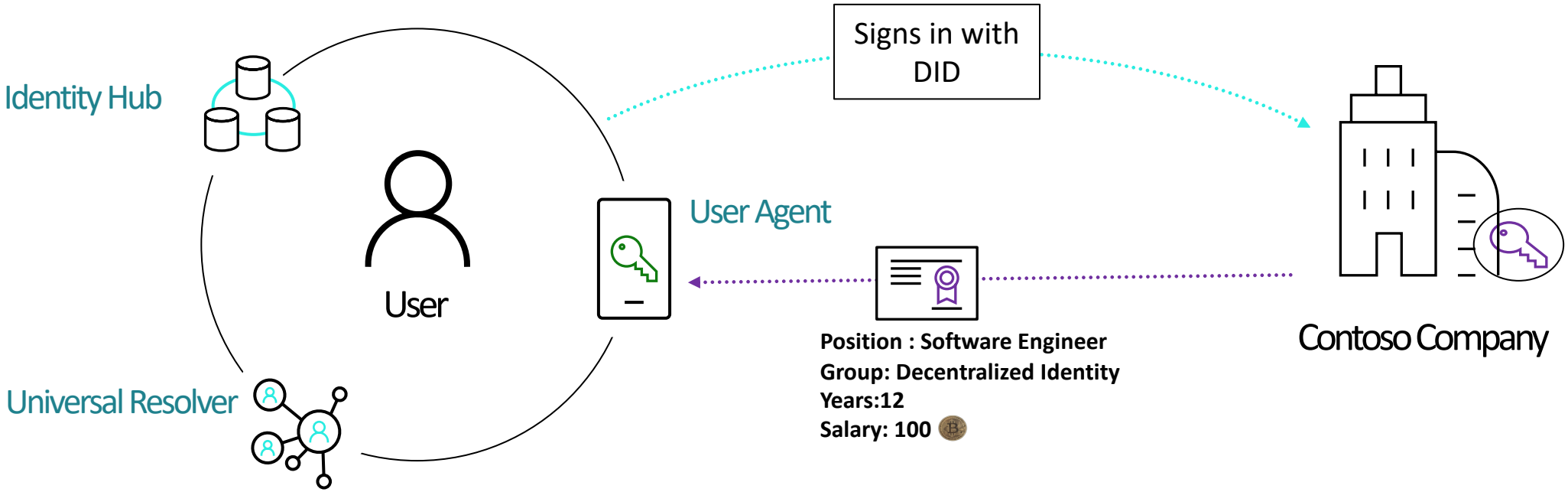
Alice creates a Decentralized ID on the blockchain



Alice logs on to the bank and starts a loan application



Alice goes to her company to get signed employment details



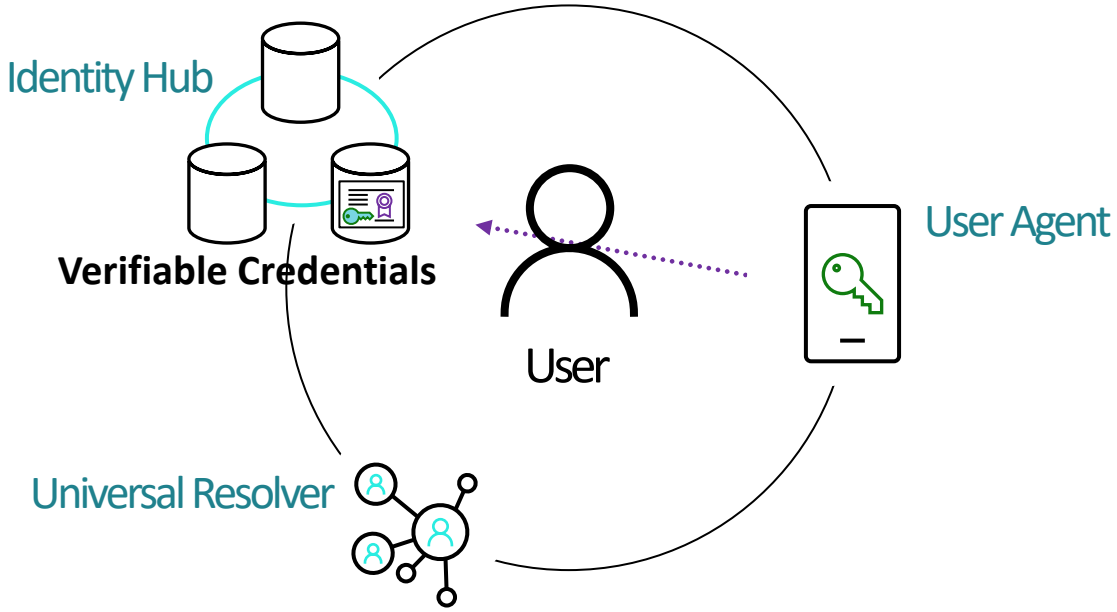
Verifiable Credentials

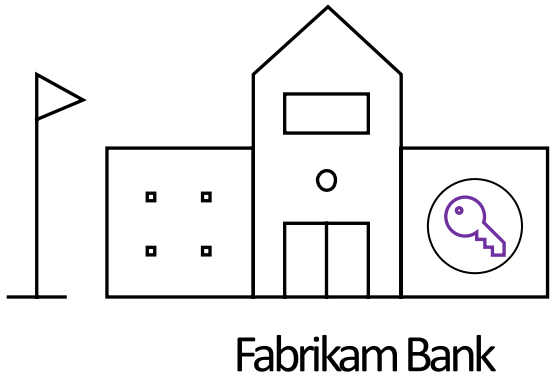
Bitcoin

Sovrin

Ethereum

The User Agent signs and stores it in Alice's identity hub



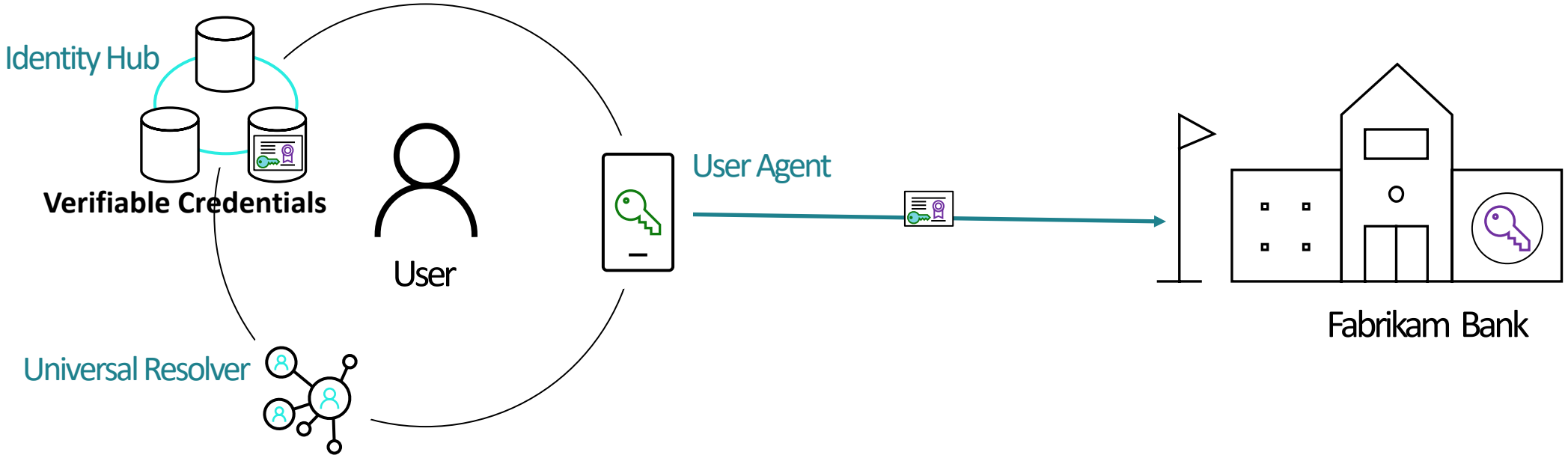


Bitcoin

Sovrin

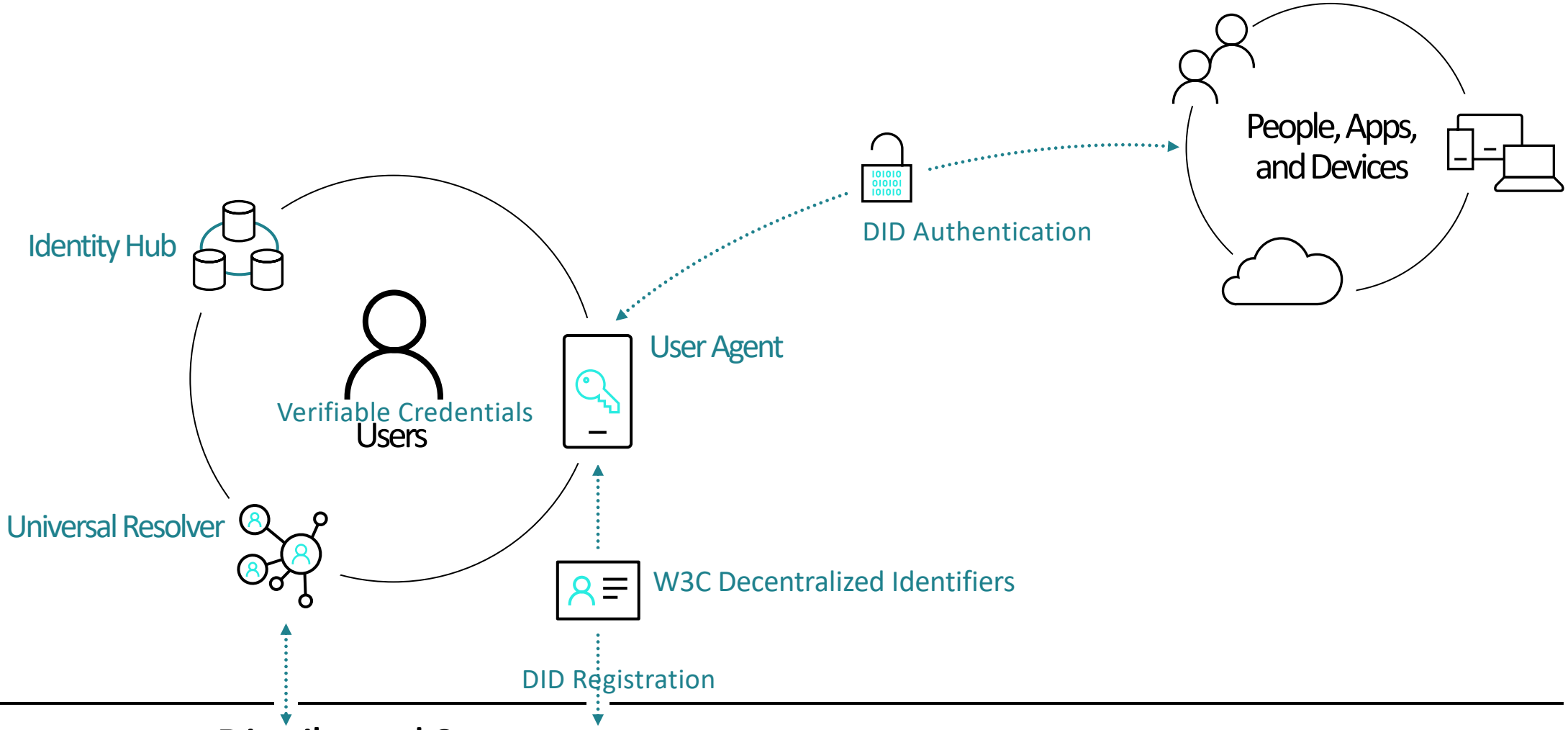
Ethereum

Now Alice can present her signed employment details to the bank



Bitcoin Sovrin Ethereum

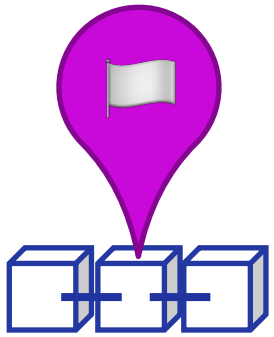
Decentralized Identity Building Blocks



RSAConference2019

How can an individual participate in a public key cryptography driven interaction model?

The Trust Model behind Decentralized Identity



- Publish user-controlled public keys
  - A ledger-stored document is immutable*
    - Once confirmed, a given document (transaction) cannot be deleted or changed
    - Updates require a new transaction hashed to the old with private keys
- An immutable document on a ledger has advantages (also disadvantages)
  - Unlikely that any one entity can make your document disappear
    - IFF your ledger stays healthy and has reasonable byzantine tolerance
  - Discovery document itself contains no PII
  - BUT corresponding identifier is public. Public identifiers can be correlated

The Immutable Bit – DID Document


```
{
  "@context":      "https://w3id.org/btcr/v1",
  "id":            "did:btcr:8kyt-fzzq-qqqq-ase0-d8",
  "publicKey":     [{
                    "id": "did:btcr:8kyt-fzzq-qqqq-ase0-d8#keys-2",
                    "type": "RsaVerificationKey2018",
                    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n",
                    "owner": "did:btcr:8kyt-fzzq-qqqq-ase0-d8"
                   }],
  "authentication": [{
                      "type": "RsaSignatureAuthentication2018",
                      "publicKey": "#keys-2"
                     }],
  "service":       [{
                    "type": "BTCREndpoint",
                    "serviceEndpoint": https://mydomain.com/ddo.jsonld
                   }]
}
```


* Real doc, edited for brevity

Decentralized Identifiers (DIDs)

```
did:method:<specific-idstring>
```

- A collision-free unique ID
- Method is a documented algorithm that describes how a specific idstring can 'resolve' to a document on a ledger
- Specification: https://w3c-ccg.github.io/did-spec/

DID Methods

- Deterministic representation
- Specification link encoded in DID Document @context
- Open source "driver" code registered with universal resolver at http://uniresolver.io

Method	DID Prefix	DLT/Network
Sovrin	did:sov:	Sovrin
Bitcoin Reference	did:btcr:	Bitcoin
Ethereum UPort	did:uport:	Ethereum
Blockstack	did:stack:	Ethereum
Veres One	did:v1:	Veres One
Ockam	did:ockam:	Ockam

Full list of DID methods at https://w3c-ccg.github.io/did-method-registry

BTCR DID Method (https://w3c-ccg.github.io/didm/btcr)

`did:btcr:TXREF-EXT(TX)`

- Defining org: W3C credentials community group (W3C CCG)
- Ledger: Bitcoin (public permissionless)
- Resolution:
  - DID-specific identifier is a TX ref
  - Once the base TX is located, newer blocks are walked if they exist
  - DID document is the last TX in the chain
- Great intro by Kim Hamilton Duffy: https://www.youtube.com/watch?v=SBesOFNlLoo

RSAConference2019

DEMO – BTCR
Registering and Resolving a DID

BTCR Playground
https://weboftrustinfo.github.io/btcr-tx-playground.github.io/

Proof of control of Decentralized Identifiers

- Challenge & Response
- Transport Protocols
  - HTTP Post
  - QR Code
  - Mobile Deep Link
  - JavaScript Browser API
  - BlueTooth
  - NFC

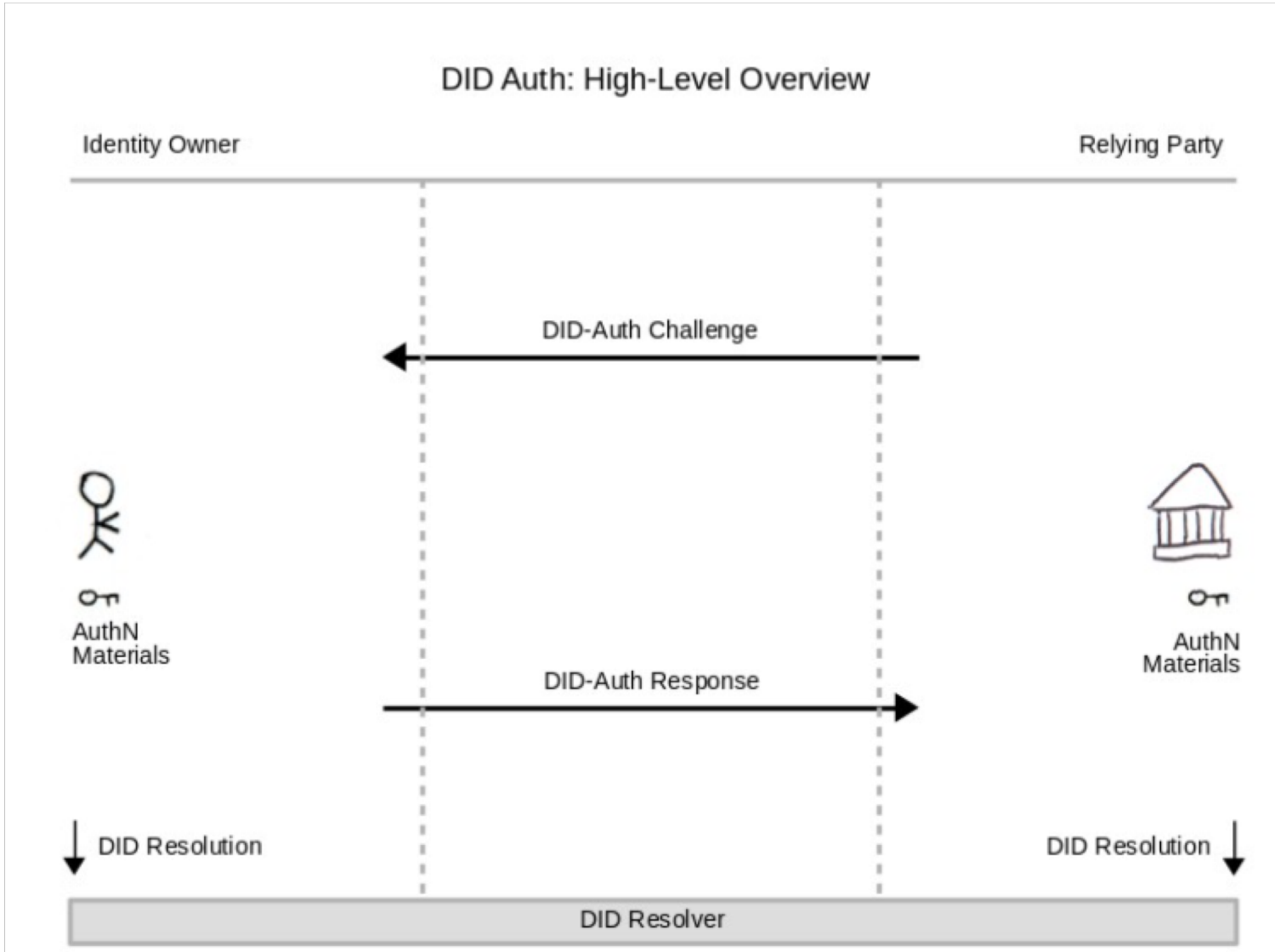


Diagram source: Markus Sabadello, https://www.youtube.com/watch?v=Yq8yFYdCnxU

Various forms of DID Auth Interactions

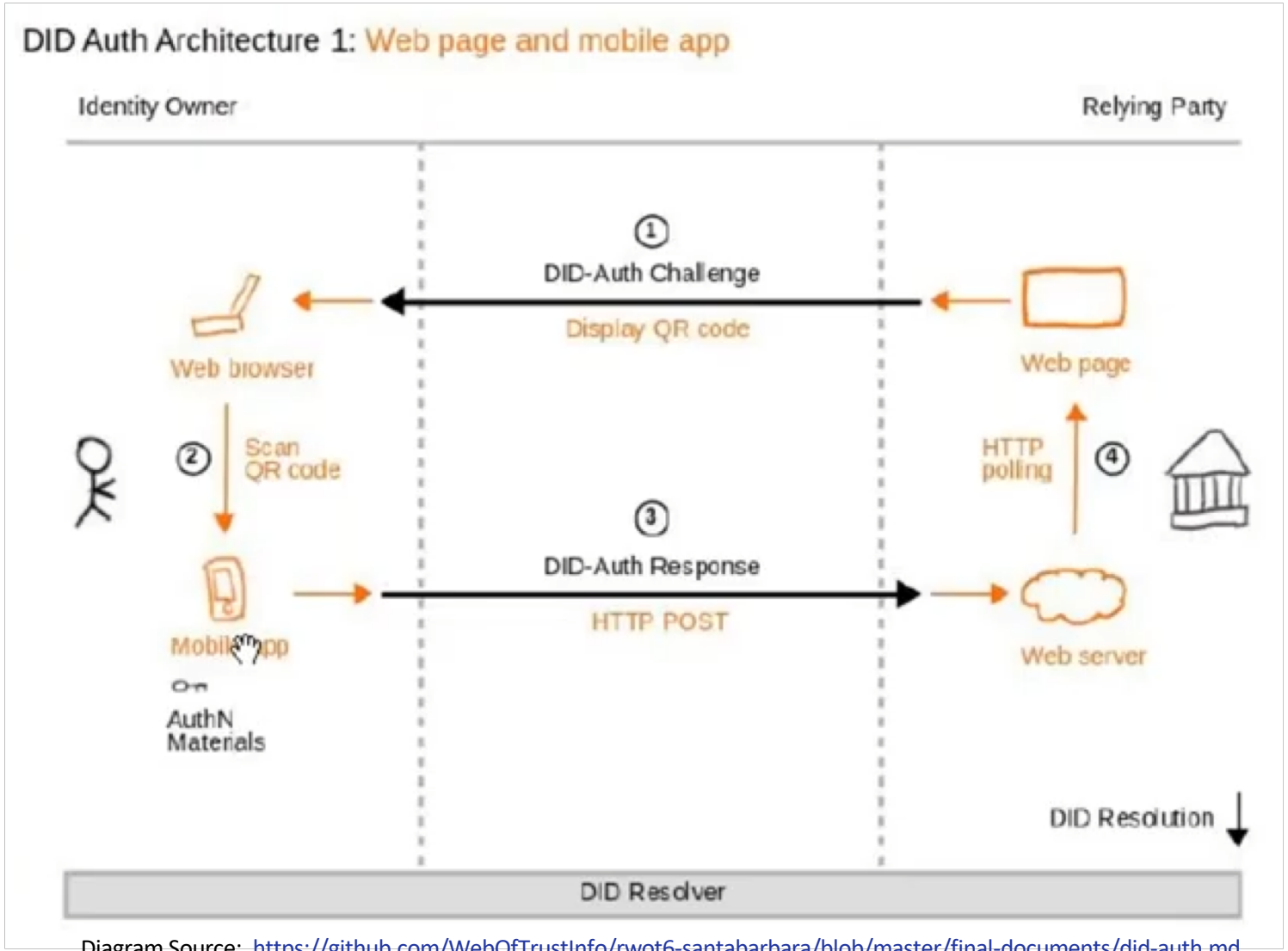


Diagram Source: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md

RSAConference2019

DEMO – Proof of control of DID

Authenticating with DIDs via Self-Issued OIDC

Challenge

```
HTTP/1.1 302 Found
Location: openid://?
   scope=openid
   &request=
   {
      "iss": "did:doc:bankapplication",
      "response_type": "id_token",
      "client_id": "app://claims",
      "scope": "openid",
      "state": af0ifjsldkj
      "nonce": "drnEJZTtfh",
      "claims":{
         "id_token":{
            "age": {"essential": true}
         }
      }
   }
   &state=af0ifjsldkj
```

- Self-issued OpenID Connect is built into the core specification
- Uses JWS/JWE
- Compatible with centralized systems!

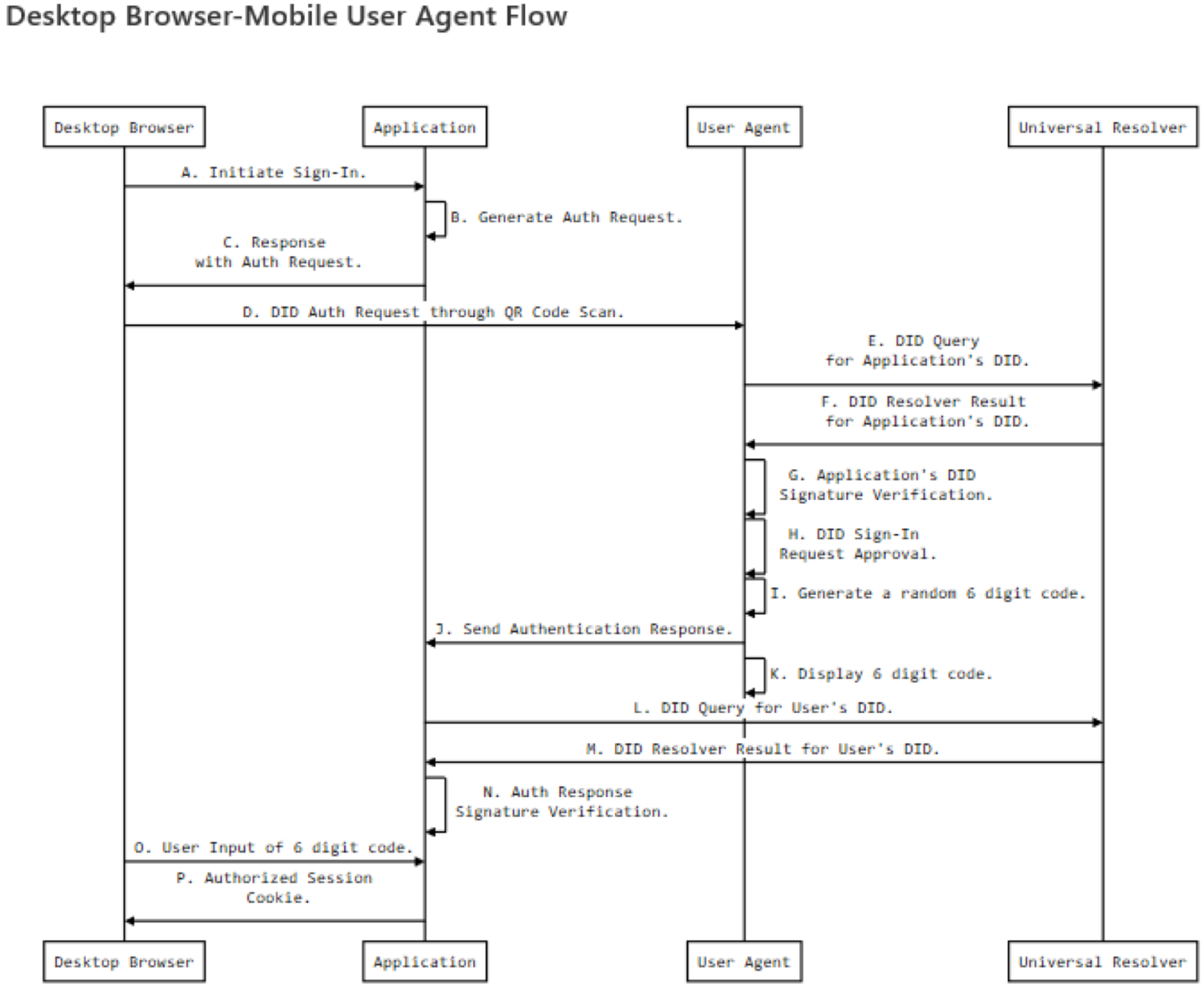
Response

```
HTTP/1.1 302 Found
  Location: app://claims#
    id_token=eyJ0 ... NiJ9.eyJ1c ... I6IjlifX0.DeWt4Qu ... ZXso
    &state=af0ifjsldkj=
```

Payload:

```
{
  "iss": "https://self-issued.me",
  "sub": [Base64UrlEncoded Thumbprint],
  "aud": "app://claims",
  "nonce": "drnEJZTtfh",
  "state": af0ifjsldkj,
  "exp": 1311281970,
  "iat": 1311280970,
  "sub_jwk": {
    "kty":"RSA",
    "n": "0vx7agoebGcQSuuPiLJXZptN9nndrQmbXEps2aiAFbWhM78LhWx
    4cbbfAAtVT86zwu1RK7aPFFxuhDR1L6tSoc_BJECPebWKRXjBZCiFV4n3oknjhMs
    tn64tZ_2W-5JsGY4Hc5n9yBXArwl93lqt7_RN5w6Cf0h4QyQ5v-65YGjQR0_FDW2
    QvzqY368QQMicAtaSqzs8KJZgnYb9c7d0zgdAZHzu6qMQvRL5hajrn1n91CbOpbI
    SD08qNLyrdkt-bFTWhAI4vMQFh6WeZu0fM4lFd2NcRwr3XPksINHaQ-G_xBniIqb
    w0Ls1jF44-csFCur-kEgU8awapJzKnqDKgw",
    "e":"AQAB"
  },
  "did": "did:ion:EiDhJDBj8OHAyENIS5Bbyn0MYPSb4wUCps9Hi7sj_-V0BQ"
  "age": 35
}
```

Swimlane
(to look at later)



uPort

- Built on Ethereum
- uPort Identity
  - Keypair or Smart Contract address
- Main 3 components
  - Smart Contracts
  - Developer libraries
  - Mobile app
- Personal data stored off-chain: IPFS, AWS, Azure, Dropbox

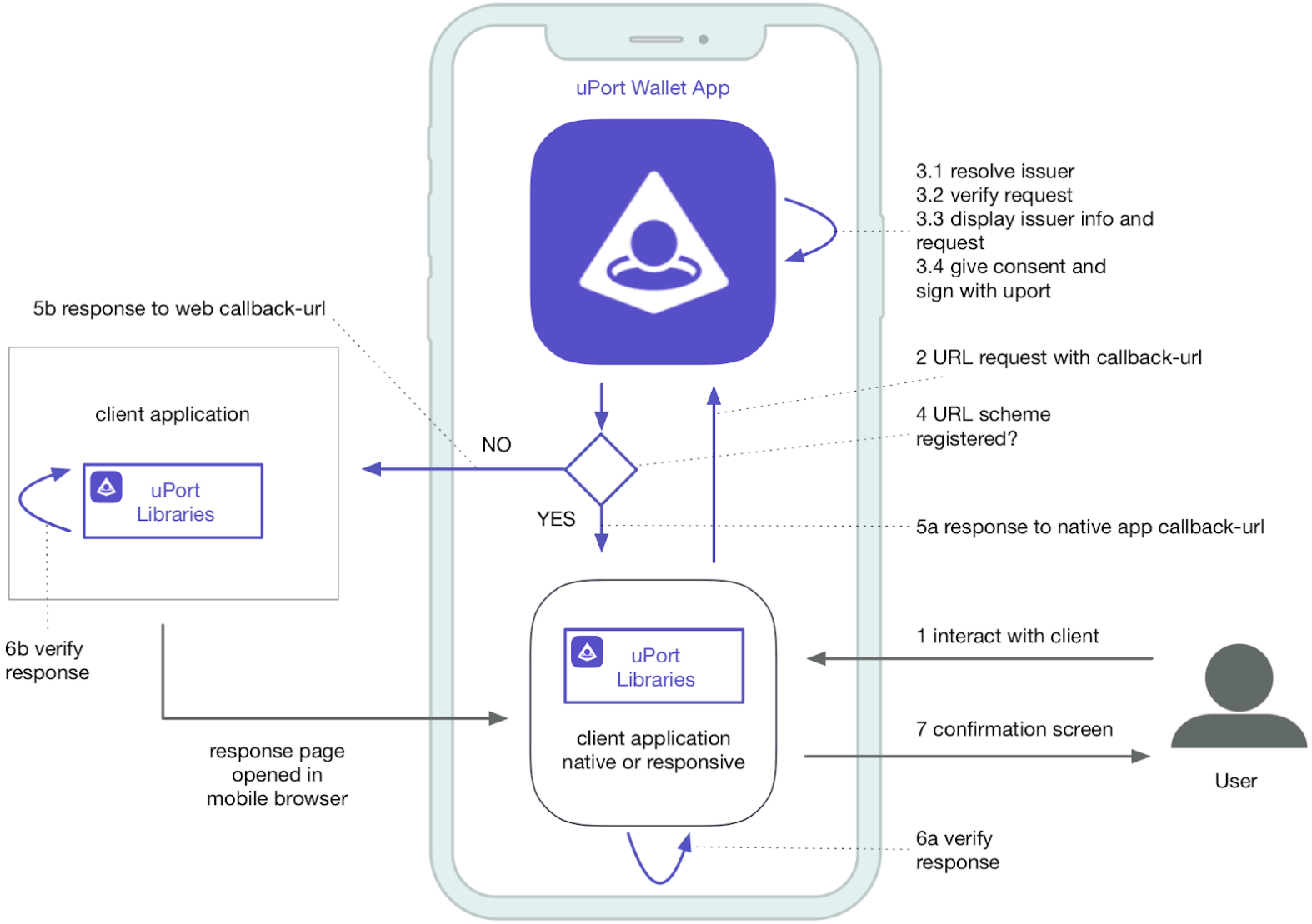


Diagram courtesy of uPort

Verifiable Credentials https://w3c.github.io/vc-data-model/

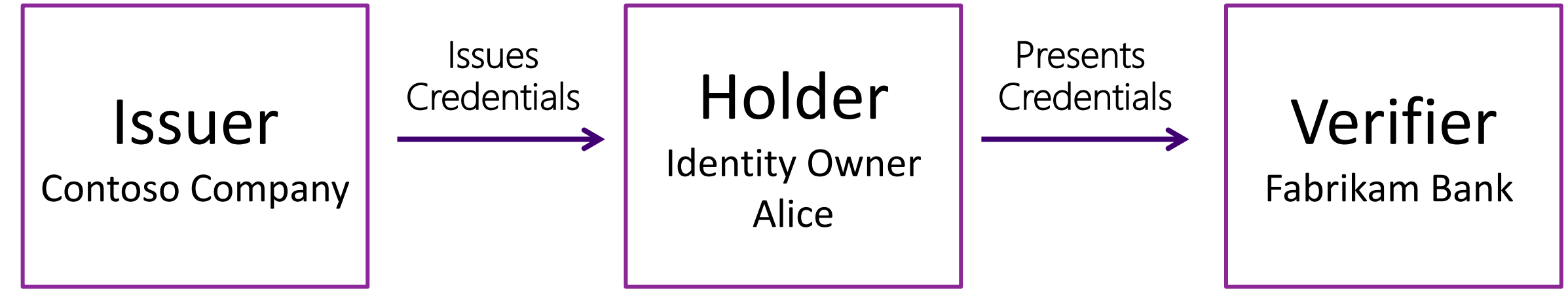


Diagram adapted from link in title

RSAConference2019

DEMO – uPort
Exchange of Verifiable Credentials

uPort : Creation and Issuance of Verifiable Credentials

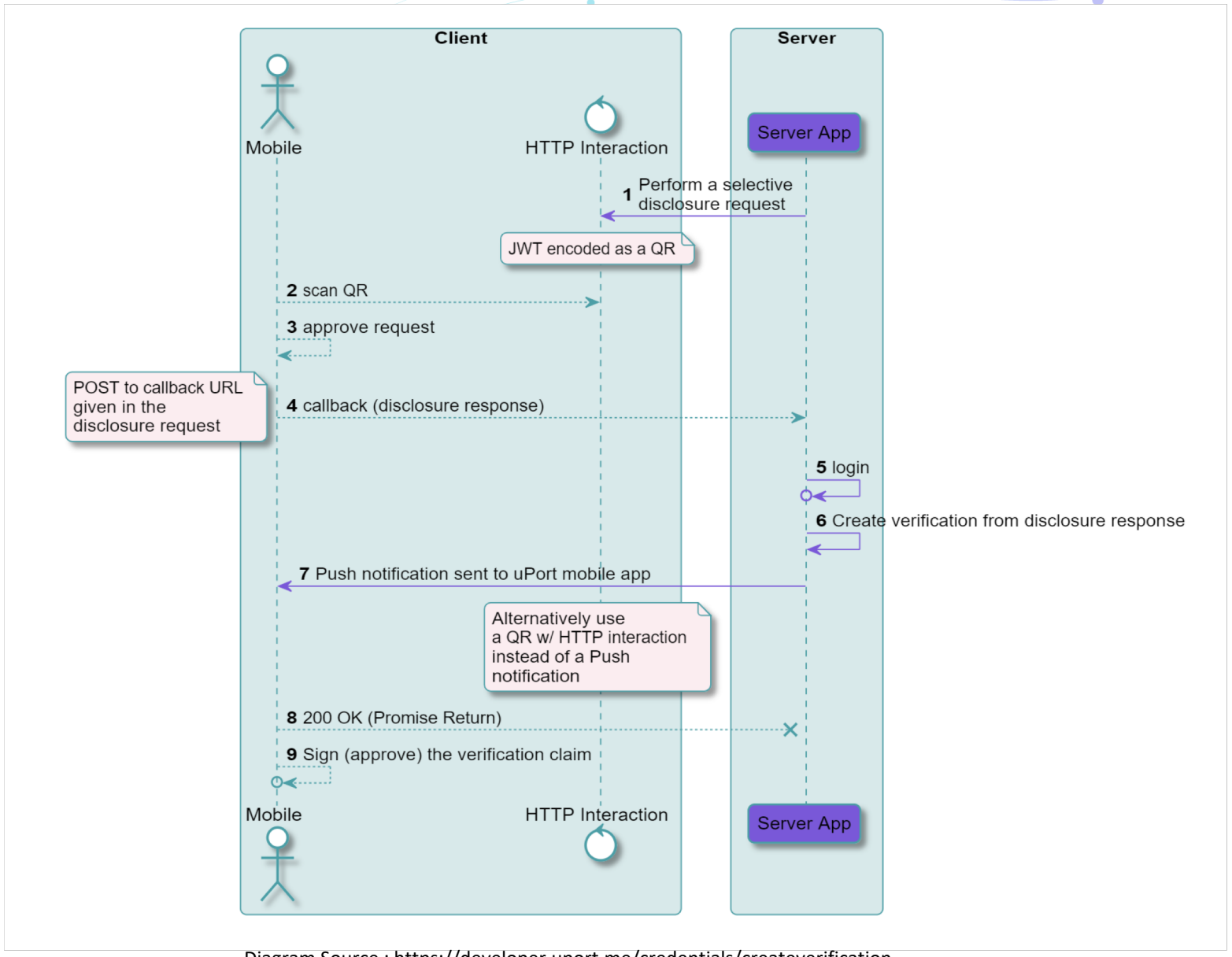


Diagram Source : https://developer.uport.me/credentials/createverification

uPort : Verifiable Presentation

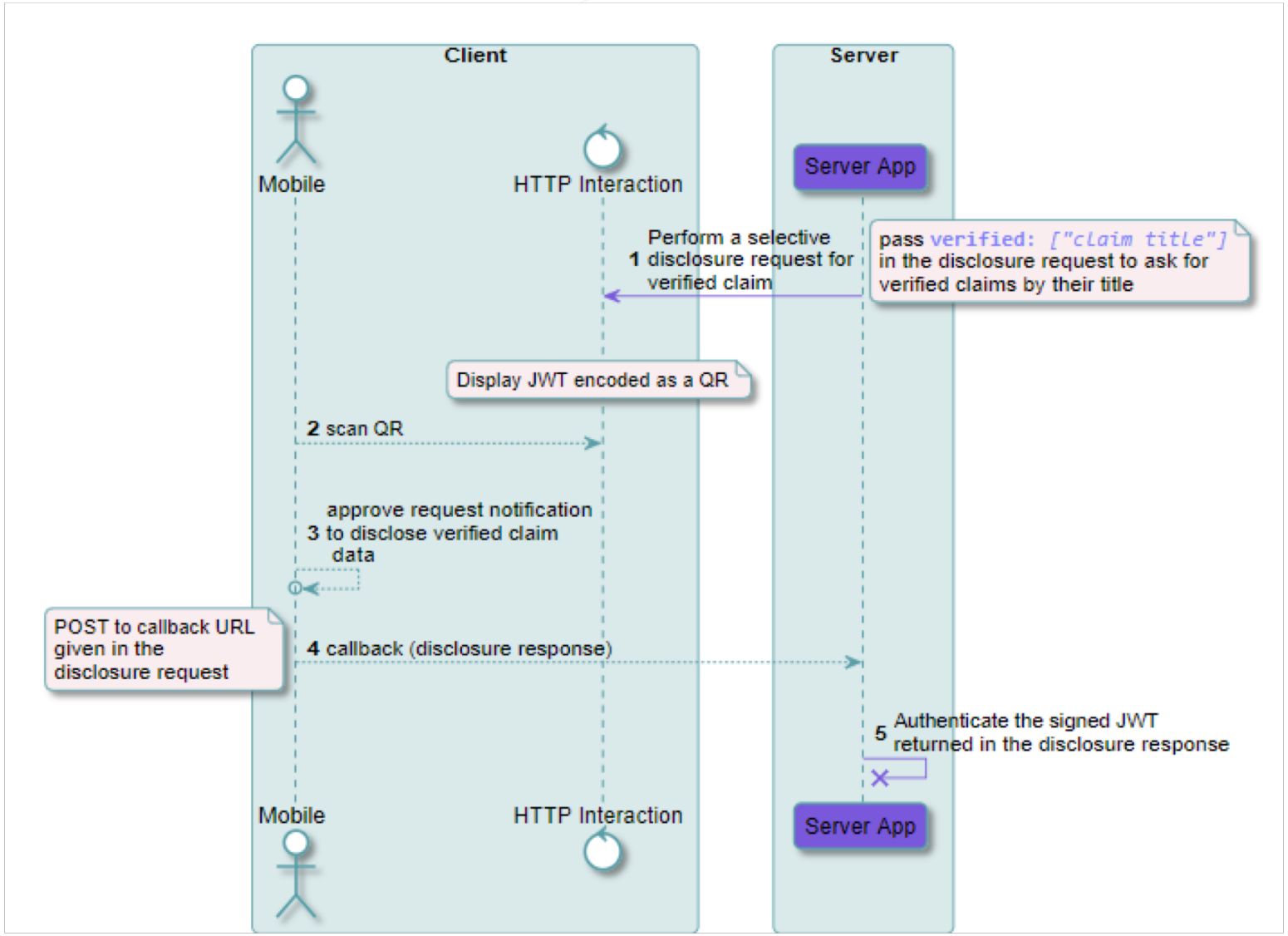


Diagram Source : https://developer.uport.me/credentials/createverification

Sovrin [DID method, Foundation, Ledger]

- Defining orgs:
  - Indy Hyperledger Project
  - Sovrin Foundation & Alliance
  - Evernym
- Ledger: Sovrin ledger (public permissioned)
  - 4 different ledgers
- Resolution:
  - standard Sovrin GET_NYM transaction, validated at multiple validators or signature of aggregator score validated

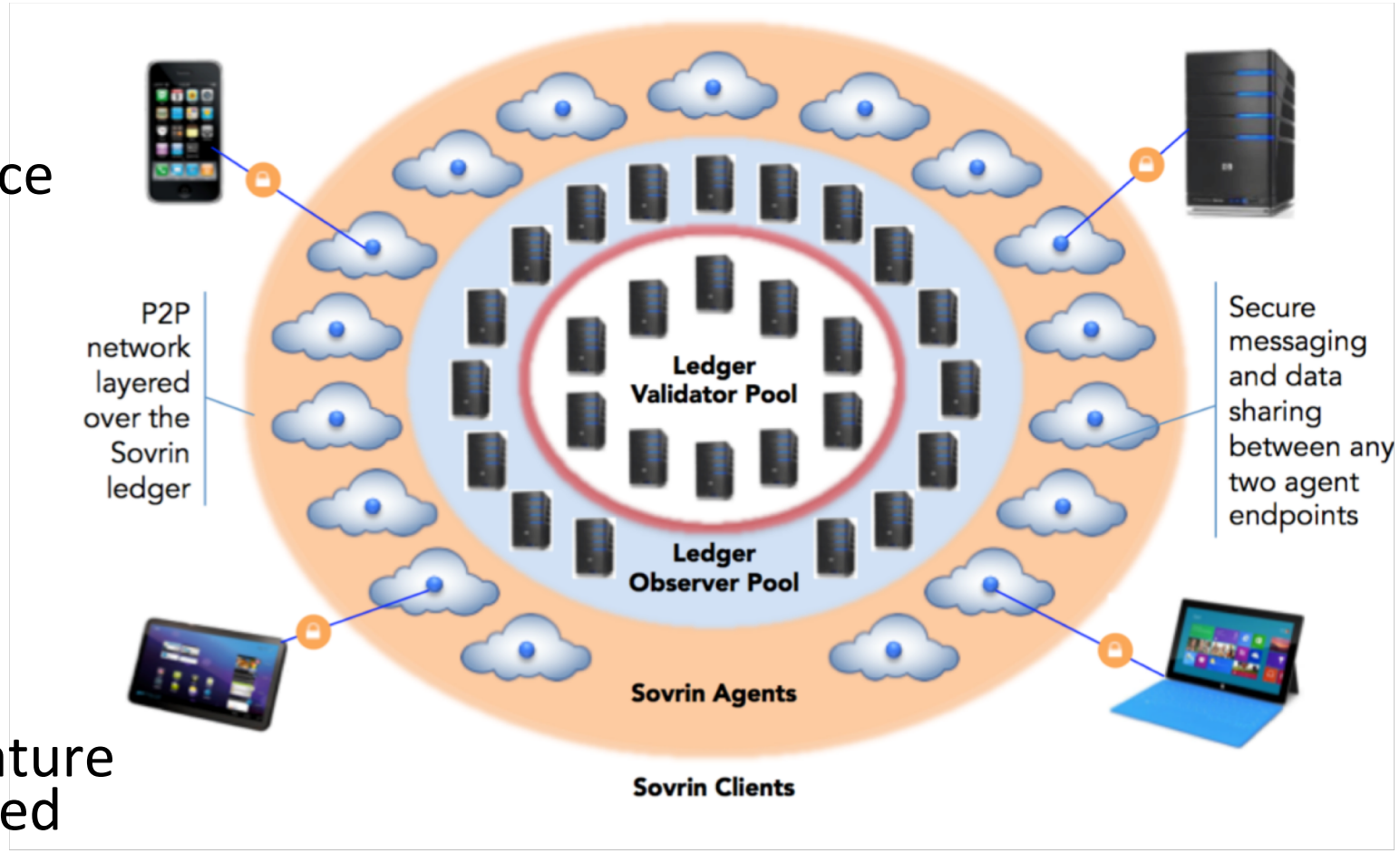


Diagram Source: https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf

What Have we Shown You

- Stuff that is reasonably standardized now
  - DIDs, DID documents, DID resolver
- Stuff that needs to be standardized
  - DID auth, pairwise identifiers
- Stuff that should be standardized
  - DID registration, Account Recovery

- The community is working hard to ensure their worlds can intersect – there is work to do but lots of energy to see it done

How can You Apply this Knowledge

- Join the Decentralized Identity Foundation: http://identity.foundation
- Go get your own DID!
  - uPort Getting Started: http://developer.uport.me
  - BTCR Playground: https://weboftrustinfo.github.io/btcr-tx-playground.github.io/
  - Indy Hyperledger Walkthrough: https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md
  - Ockam SDK: https://github.com/ockam-network/ockam
  - Veres One Quickstart: https://veres.one/developers/guides/
- Have an informed opinion
  - Know the difference between PII off-chain and Trust data on-chain
  - If you hate it, get involved and change what you hate
  - If you love it, get involved and make it better
- If you want to understand the ideology behind Self-sovereign identity (built on the technology of decentralized identity) try this video: https://youtu.be/2g6KSv1aeuI

RSAConference2019

Thank You – Questions?

@pamelarosiedee @decentralizedID

aka.ms/didwhitepaper