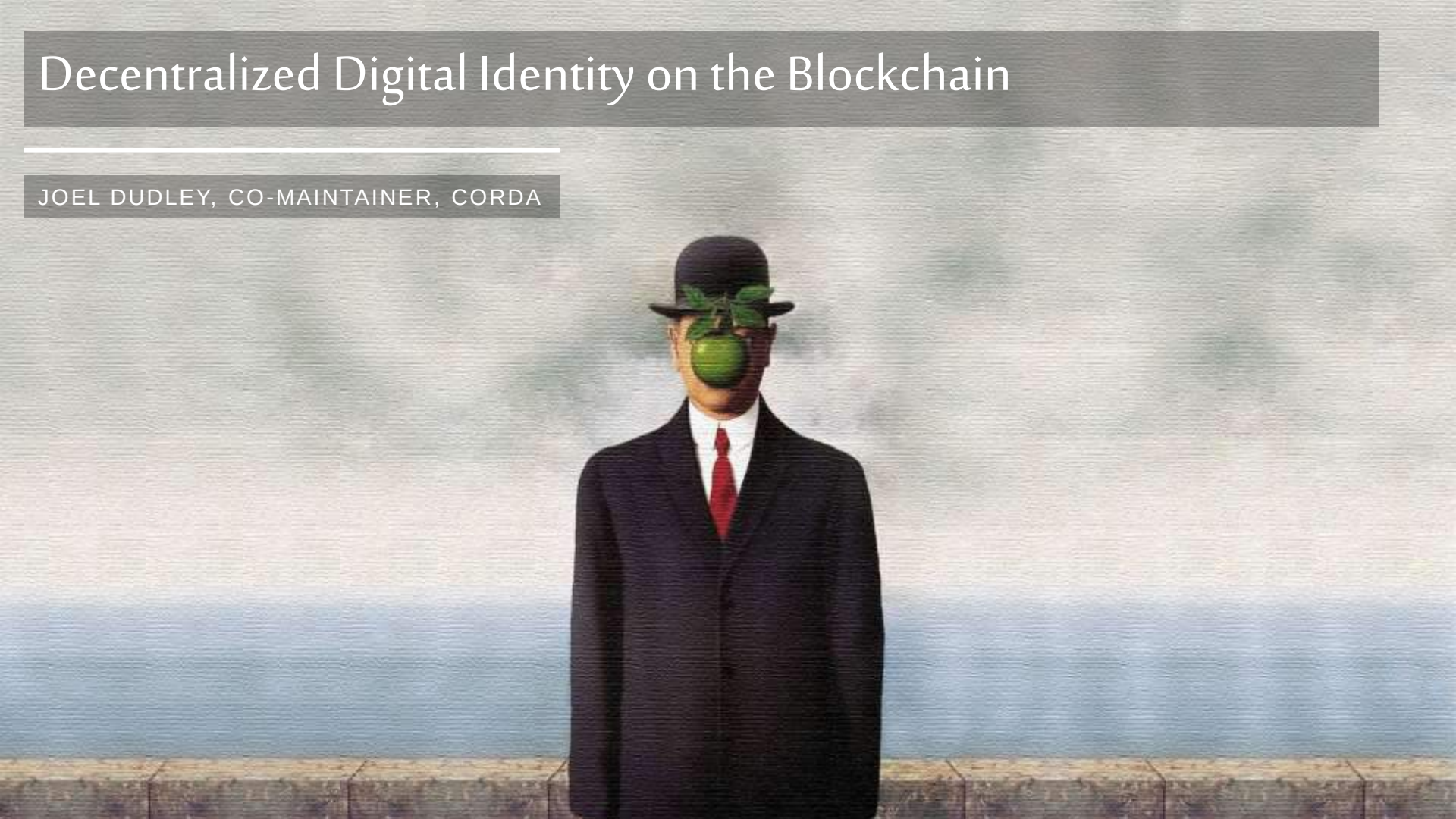
Decentralized Digital Identity on the Blockchain

JOEL DUDLEY, CO-MAINTAINER, CORDA



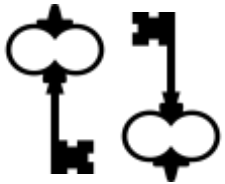
There is an identity problem today

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

We need digital credentials


```
{
  “properties”: {
    “id”: “I1234562”,
    “expiry”: “08-31-2018”,
    “first_name”: “Joel”,
    “last_name”: “Dudley”,
    “date_of_birth”: “01/01/1990”
  },
  “owner”: “Joel Dudley”,
  “owner_signature”: “E731EB6B61F1010ED7E7C787F”,
  “issuer”: “California DMV”,
  “issuer_signature”: “84102C2A86198312D86551A67”
}
```

Using digital credentials to rent a car



1. Create keypair

"Here's my driver's licence. I own pubkey x"

2. Get attestations

Digital driver's licence credential signed by DMV and "owned by" pubkey x

1. Signature proving I own pubkey x
2. Part of DMV-signed credential proving I have driving licence

3. Use attestations

"OK, you can go pick up your rental car"

Icon made by Freepik from www.flaticon.com

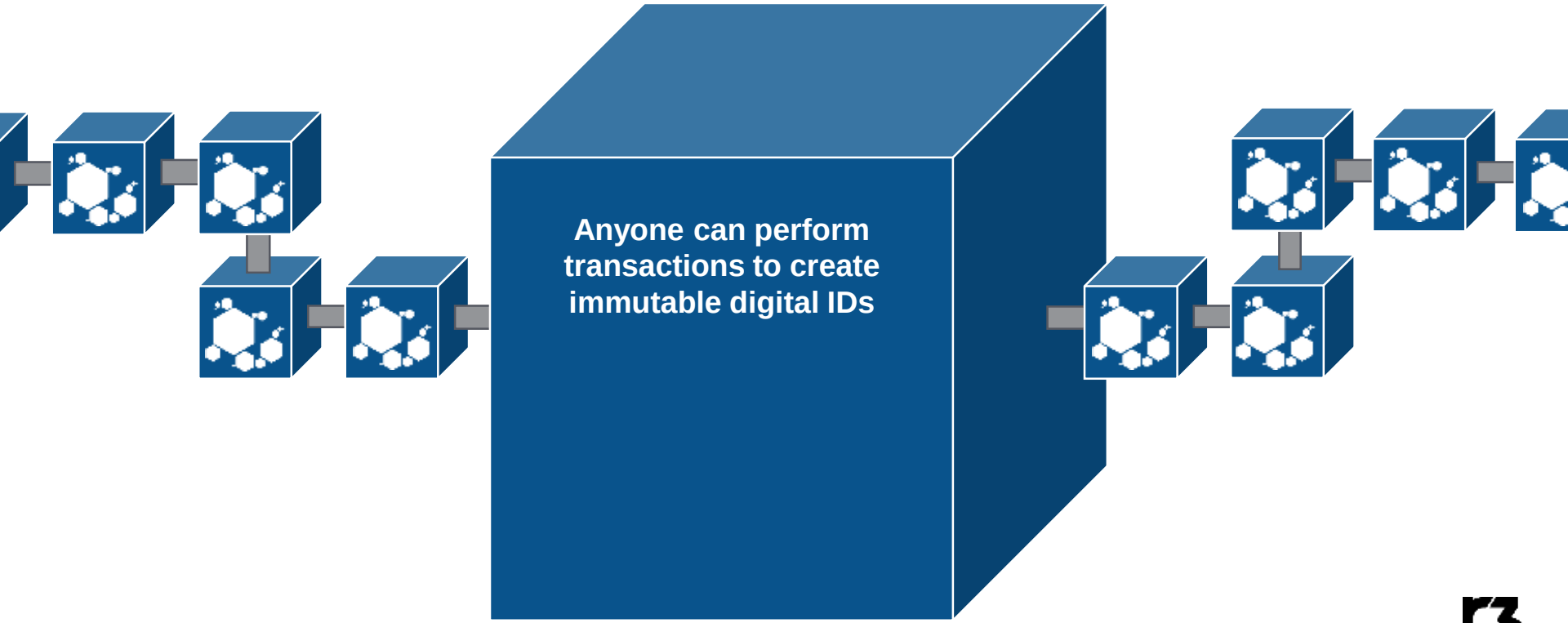
Problem: how can we link the owner and issuer to their public keys?


```
{
  “properties”: {
    “id”: “I1234562”,
    “expiry”: “08-31-2018”,
    “first_name”: “Joel”,
    “last_name”: “Dudley”,
    “date_of_birth”: “01/01/1990”
  },
  “owner”: “Joel Dudley”,
  “owner_signature”: “E731EB6B61F1010ED7E7C787F”,
  “issuer”: “California DMV”,
  “issuer_signature”: “84102C2A86198312D86551A67”
}
```

Certificate authorities

HYPERLEDGER
INDY

HLP Indy uses blockchain to create a decentralised identity system



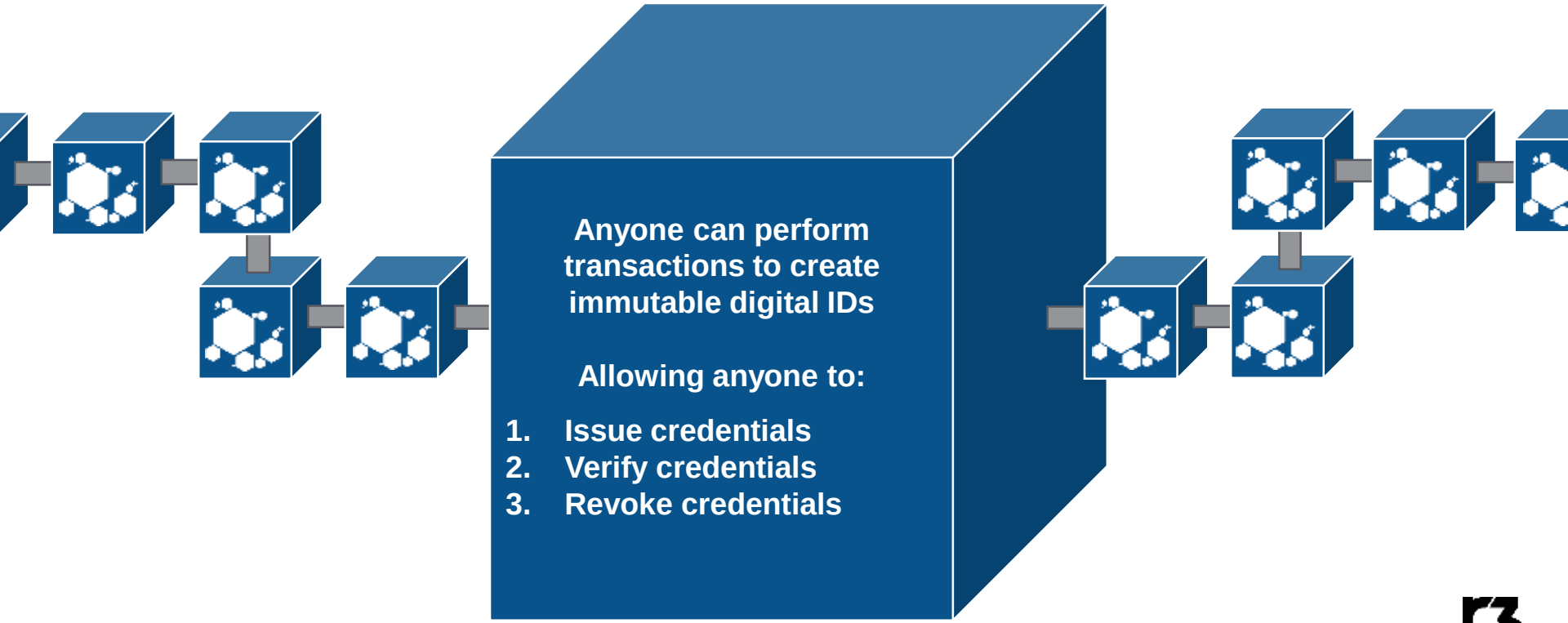
Digital identifier (DID) and DID document example

did:example:123456789abcdefghi


```
{
   “@context”: “https://w3id.org/did/v1”,
   “id”: “did:example:123456789abcdefghi”,
   “publicKey”: [{
                “id”: “did:example:123456789abcdefghi#keys-1”,
                “type”: “RSAVerificationKey2018”,
                “owner”: “did:example:123456789abcdefghi”,
                “publicKeyPem”: “-----BEGIN PUBLIC KEY…END PUBLIC KEY-----\r\n”
   }],
   “authentication”: [{
                “type”: “RsaSignatureAuthentication2018”,
                “publicKey”: “did:example:123456789abcdefghi#keys-1”
   }],
   “service”: [{
                “type”: “ExampleService”,
                “serviceEndpoint”: “https://example.com/endpoint/8377464”
   }]
}
```


Based on Self-Sovereign Identity with Hyperledger Indy, Calvin Cheng, FOSSASIA 2018

HLP Indy uses blockchain to create a decentralised identity system

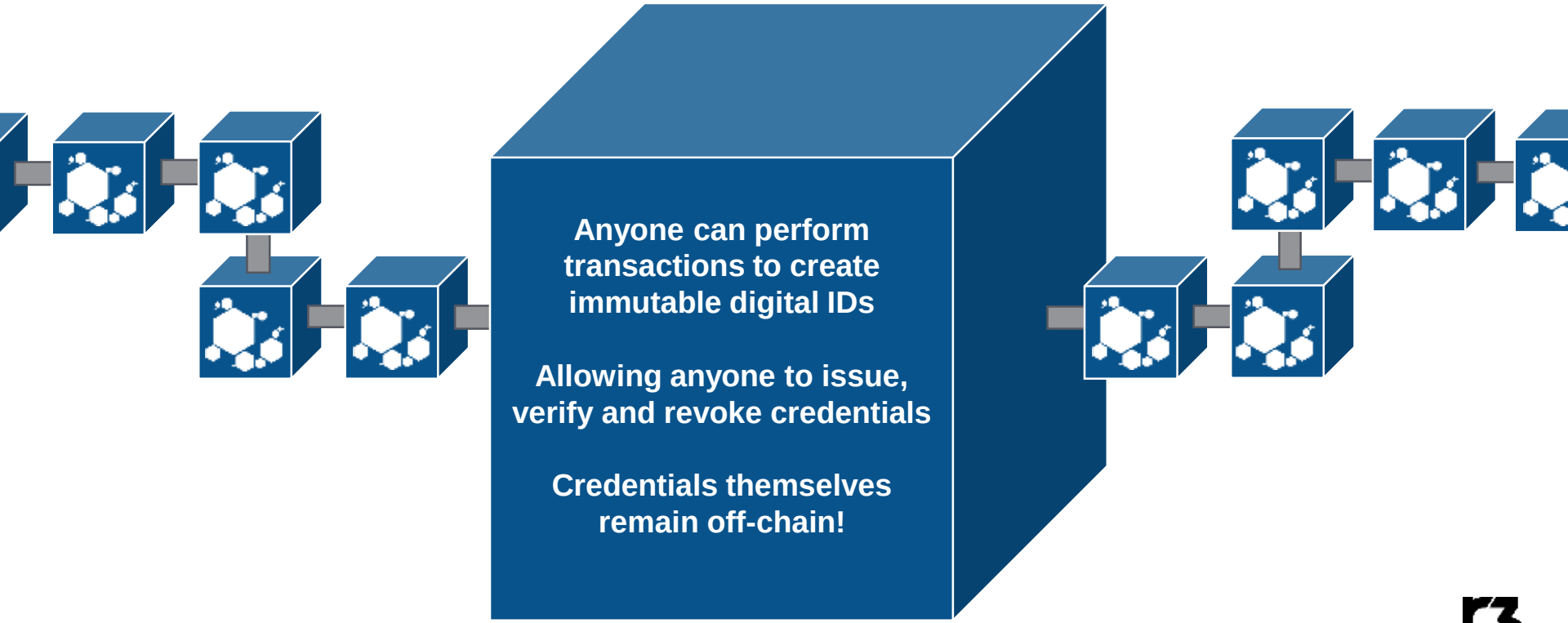


Verifiable claim example


```
{
    “@context”: “https://w3id.org/security/v1”,
    “id”: “http://example.gov/credentials/3732”,
    “type”: [“Credential”, “ProofOfAgeCredential”],
    “issuer”: “https://dmv.example.gov”,
    “issued”: “https://dmv.example.gov”,
    “claim”: {
                “id”: “did:example:ebfeb1f712ebc6f1c276e12ec21”,
                “ageOver”: 21
    },
    “revocation”: {
                “id”: “http://example.gov/revocations/738”,
                “type”: “SimpleRevocation2017”
    },
    “signature”: {
                “type”: “LinkedDataSignature2015”,
                “created”: “2016-06-18T21:19:10Z”,
                “creator”: “https://example.com/jdoe/keys/1”,
                “domain”: “json-ld.org”,
                “nonce”: “598c63d6”,
                “signatureValue”: “BavEll0/I1zpYw8XNi1bgVg/sCne…”
    }
}
```


Based on Self-Sovereign Identity with Hyperledger Indy, Calvin Cheng, FOSSASIA 2018

HLP Indy uses blockchain to create a decentralised identity system



Using digital credentials to rent a car on Indy

Joel creates a new DID for speaking to the DMV and writes it to the ledger

Joel looks up the DMV's DID on the ledger and gets their endpoint

Joel looks up the DMV's DID on their website

Alamo

Using digital credentials to rent a car on Indy

Joel creates a secure connection to the DMV and sends his newly created DID and proof of his identity

Secure channel

The DMV provides Joel with a signed digital driving licence credential over the secure connection (it is not written to ledger!)

Alamo

Using digital credentials to rent a car on Indy

Joel creates a new DID for speaking to Alamo and writes it to the ledger

Joel looks up Alamo's DID on the ledger and gets their endpoint

Joel looks up Alamo's DID on their website

Alamo

Using digital credentials to rent a car on Indy

Joel creates a secure connection to Alamo and sends his newly created DID

Secure channel

Alamo sends Joel a request for the *can drive* attribute of his digital driving licence credential from the DMV

Alamo

Using digital credentials to rent a car on Indy

Alamo retrieves the DMV's DID from the ledger

Alamo verifies the *can drive* attribute by comparing the credential's signature to the DMV's public key

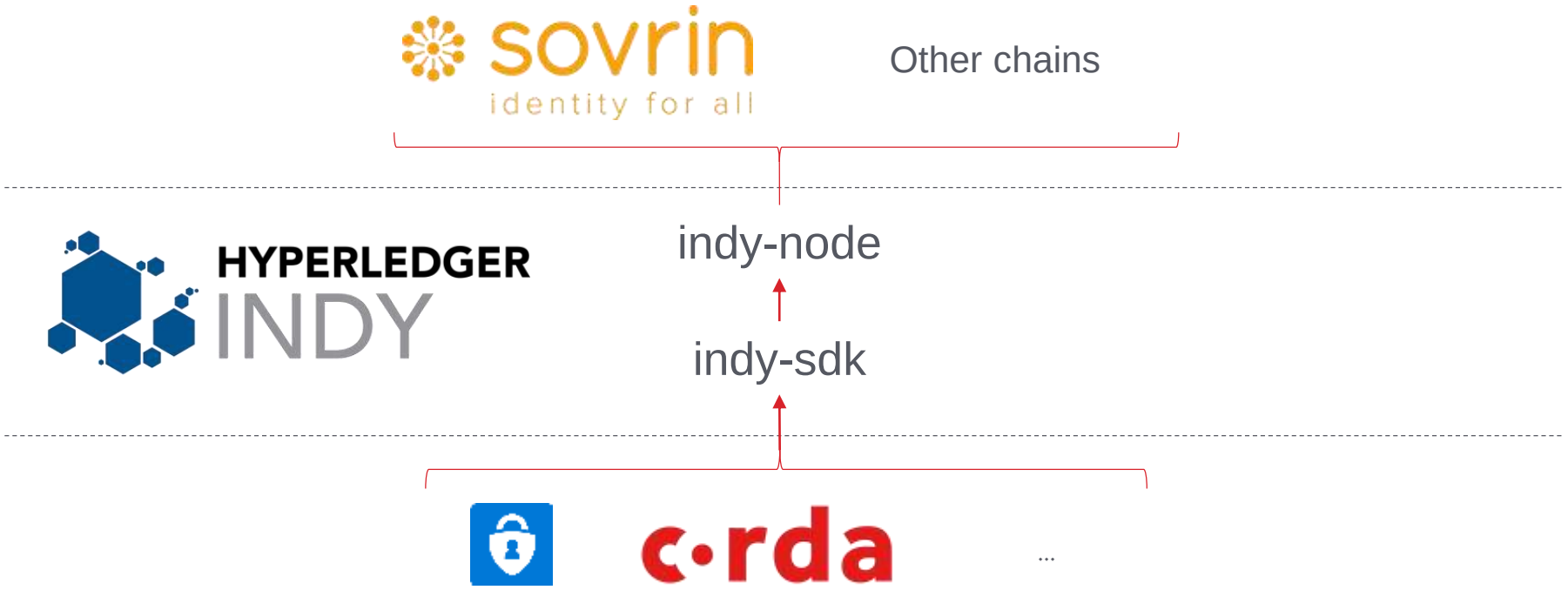
Joel sends a proof where he only reveals the *can drive* attribute of his digital driving licence credential

Secure channel

Alamo sends through authorisation to pick up the rental car

Alamo

HLP Indy is an toolkit for running and interacting with ID blockchains



HYPERLEDGER
INDY

&

corda

: ID wallet on Indy used for bank customer KYC on Corda

gemalto
security to be free

Bank A | Bank B | Regulator

User sends passport photo and photo to open account

Authenticate new customer

Create account on-ledger

Report on accounts

Bank writes digital identity claim to Indy

Provide verifiable claim

Authenticate individual

User shares identity claim from Indy to authenticate with another bank

Create account on-ledger

Icon made by Freepik from www.flaticon.com

r3

Thank you

www.r3.com

New York
11 West 42nd Street, 8th Floor
New York, NY 10036

London
2 London Wall Place,
London, EC2Y 5AU

Singapore
80 Robinson Road, #09-04
Singapore, 068898