Identity Management on Blockchain

Speaker:

Shruti Kulkarni
Blockchain Architect, IBM

What is Identity?

Business Challenges

What is SSI?

Digital Identity Use Cases

What is Identity ?

The Dimensions of our identity

1. Me as an individual:

Identity: Unique traits associated with an individual; the owner of personal identification information.

Name
Age
Gender
Biometrics
Race
Family
Address
Birthplace
Nationality
Educati

Profession
Workplace
Health
Reputatio
Beliefs
Behavio
Habits
Sentimen

2. How I am represented:

Identity Renderings: Digital or physical (paper/plastic) instrument as defined by providers.

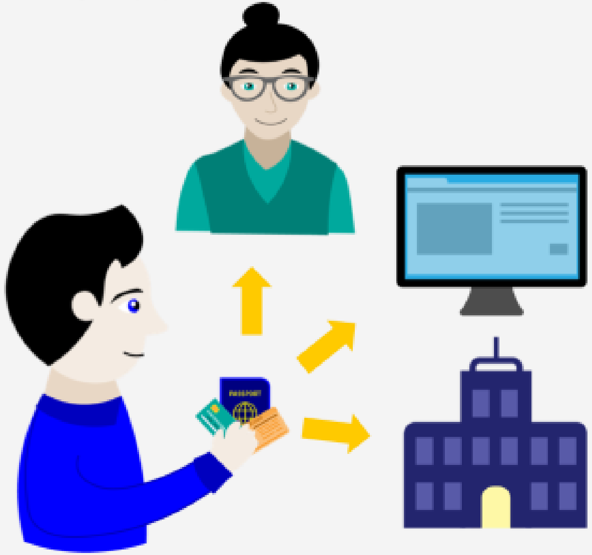
National ID
Work ID
Driving ID
Address History
Tax ID
Social Security ID
ory

Financial History
Medical History
Driving History
Social History

INSURANCE
WORK HISTORY
PASSPORT
ID Card
SSN
123-4567-8910
1234-1234-1234-1234

3. How I interact:

Identity Interactions: Situational usage such as pay, identify, participate, enter.



How do you prove that you are you?

- ❖In the real world?
- ❖On the internet?

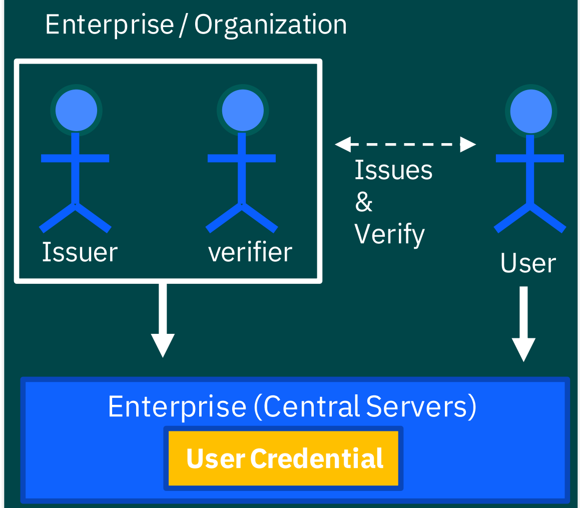
Business challenges

Enterprise today demands a new way of identity & authorization due to the following reasons:

- Hacker attacks are more due to centrally managed Identities.
- Central point of failure and multiple factor is overhead.
- Current approach is only based on Password control.
- Credentials are not controlled by the credential owners.
- Long term integrity of the identifier is questionable.
- More credentials are issued in the form of verify credentials.

Identity Journey

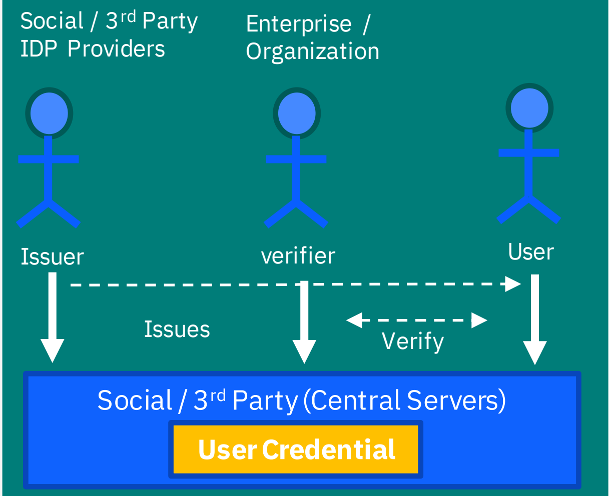
1. Centrally Managed



User Identity account owned by Organization.

- User has no control on their own data.
- User is powerless.
- Power exists with centralized identity organization authority.

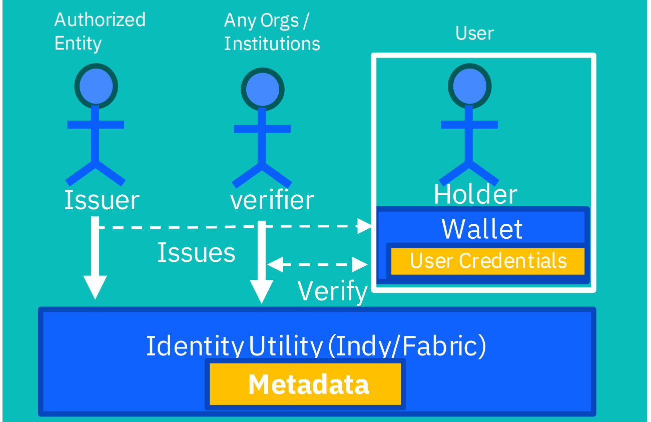
2. Federated Identity


Social / 3rd Party IDP Providers
Enterprise / Organization
Issuer
verifier
User
Issues
Verify
Social / 3rd Party (Central Servers)
User Credential

Federated identity by many different organization like google, Facebook, etc.

- User has no control on their own data.
- User is powerless.
- Power exists with federated identity organization authority. Federated identity organization authority has access and visibility into user usage patterns as well.

3. SSI model



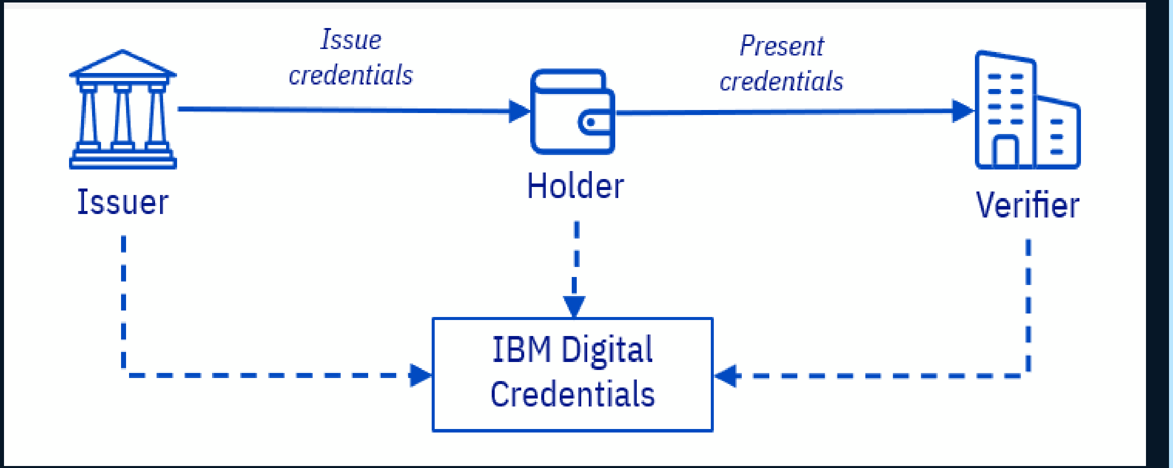
Individuals own their own identity. Credentials stored on Wallet.

- Users own their own credentials and stored in their digital wallet.
- Users decide when and where users want to use them. That improves privacy.
- Users are in control of when and with whom they share their information.

Organization centrally managed & controlled model → **Individual owned & controlled model**

Shifting to user / individual control

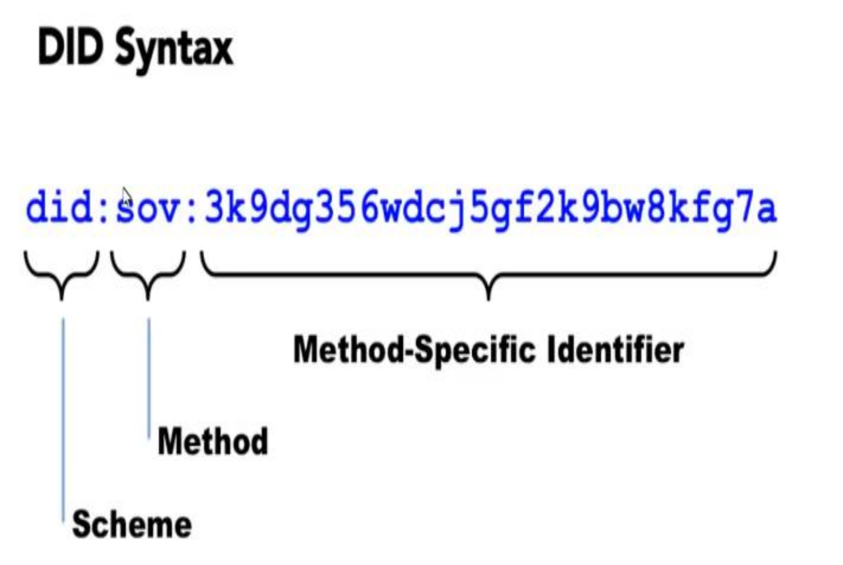
SSI Concepts



- Self-sovereign identity (SSI) is a term used to describe the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities
- With SSI, the power to control personal data resides with the individual, and not an administrative third party granting or tracking access to these credentials
- You no longer have to give up control of personal information to dozens of databases each time you want to access new goods and services, with the risk of your identity being stolen by hackers
- In SSI, there are 3 personas – Issuer, Holder or Prover and Verifier

Decentralized Identifiers (DID)

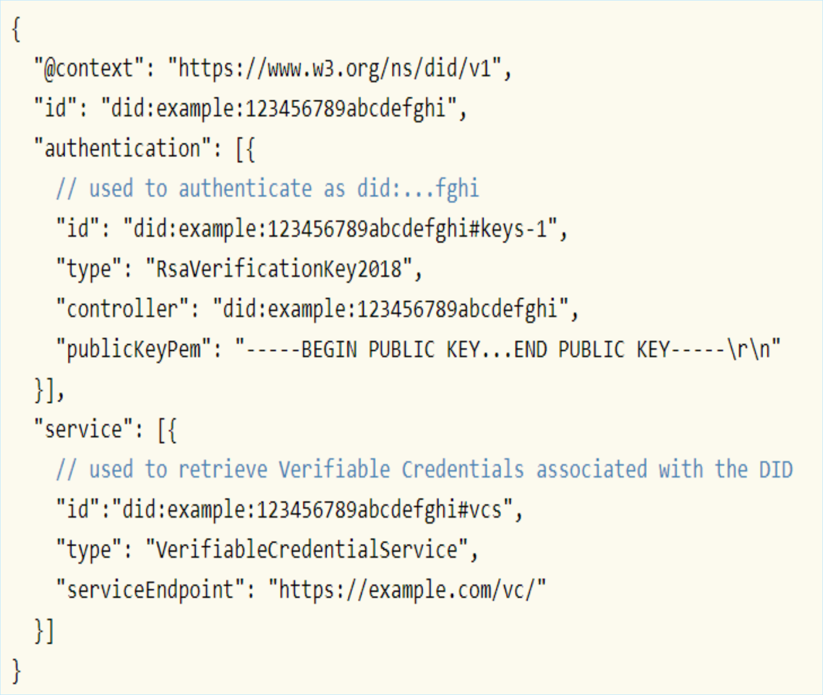
- DID is a globally unique identifier (e.g., UUID) that has no special cryptographic properties
- DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority
- DIDs point to a DID document in the ledger. DID document describes verification methods (such as public keys) and services that can be used to interact with a DID controller
- DIDs can be Verinyms or Blinded
- Each DID is associated with one or more public keys created by the DID owner (and the owner holds the corresponding private keys), and one or more endpoints - addresses where messages can be delivered for that identity


DID Syntax
did:sov:3k9dg356wdcj5gf2k9bw8kfg7a
Method-Specific Identifier
Method
Scheme

DID W3C Link: https://www.w3.org/TR/did-core/

DID Document

- DIDs point to a DID document in the ledger.
- DID Document is a JSON-LD document describing the entity identified by the DID
- DID document consists of
  - The DID (for self description)
  - A set of cryptographic material (for verification)
  - A set of auth protocols (for authentication)
  - A set of service endpoints (for interaction)
  - Timestamps (for audit history)
  - Signature (for integrity)



```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

DID W3C Link: https://www.w3.org/TR/did-core/

Credential Schema

- Credential Schema is the base semantic structure that describes the list of attributes which one particular Credential can contain

- A Credential Schema can be created and saved in the Ledger by any Trust Anchor

- Creating the schema will require DID of the schema issuer, name of the schema, version of the schema, list of schema attributes description

```
transcript = {
    'name': 'Transcript',
    'version': '1.2',
    'attributes': ['first_name', 'last_name', 'degree',
'status', 'year', 'average', 'ssn’]
}

job_certificate = {
        'name': 'Job-Certificate',
        'version': '0.2',
        'attributes': ['first_name', 'last_name', 'salary',
'employee_status', 'experience']
    }
```

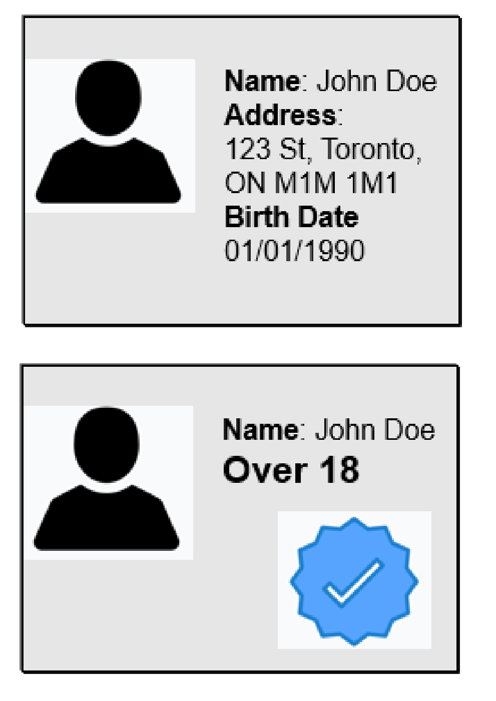
Verifiable Credential (VC)

- Claim is a statement about a subject
- Credential is a set of one or more claims made by an issuer e.g. name, date of birth
- VCs are cryptographically created statements of one entity (Issuer) about another entity (Holder)
- VC provide minimum disclosure & zero-knowledge proofs
- VCs are all digital and under the owner’s control

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
"https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type": ["VerifiableCredential","UniversityDegreeCredential"],
  "credentialSchema": {
    "id": "did:example:schema:3jf74yr7dsjw83jf",
    "type": "CLCredentialDefinition2019"
  },
  "issuer": "https://example.edu/issuers/14",
  "credentialSubject": {
    "givenName": "Jane",
    "familyName": "Doe",
    "degree": {
"name": "Bachelor of Science in Mechanical Engineering",
      "college": "College of Engineering"
    }
  },   "proof": {…} }
```

W3C VC Data Model: https://www.w3.org/TR/vc-data-model/
W3C VC Implementation: https://www.w3.org/TR/vc-imp-guide/

Zero Knowledge Proof



Name: John Doe
Address:
123 St, Toronto,
ON M1M 1M1
Birth Date
01/01/1990

Name: John Doe
Over 18

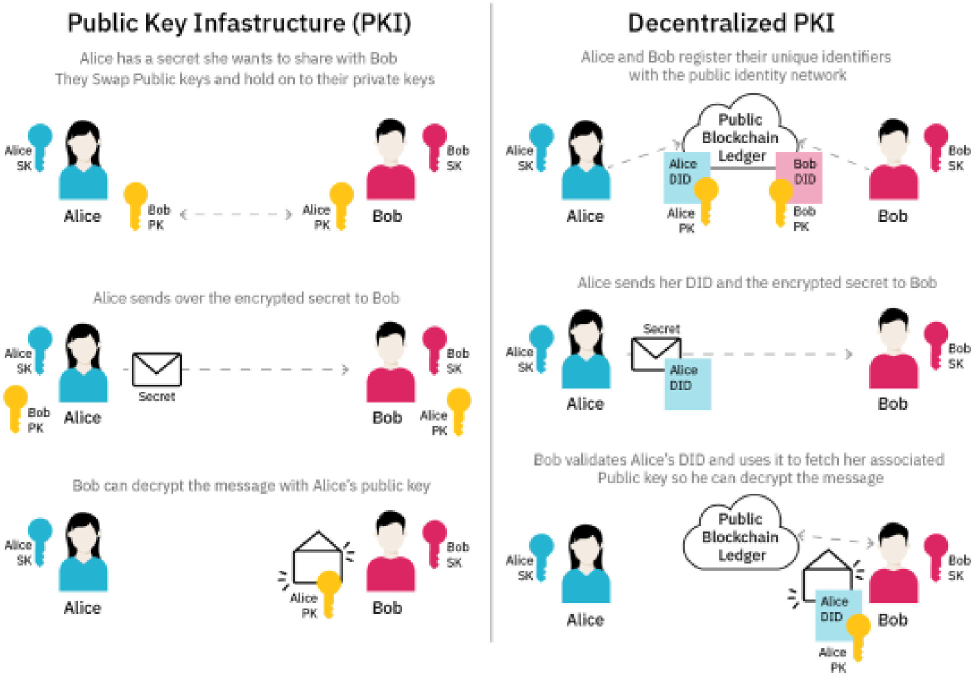
- A Zero Knowledge Proof allows the prover to prove to the verifier that some or all of the data in a set of Claims is true without revealing any additional information, including the identity of the Prover

- ZKPs are probabilistic and have different forms

- The 3 properties of ZKP are:
  - Completeness : The verifier is convinced
  - Soundness: If the prover cheats, the verifier will detect it
  - Zero-knowledge: Did the verifier really learn nothing else?

Why Blockchain for Decentralized Identity

Blockchain technology is a catalyst for rebooting the web of trust vision by providing an infrastructure of identity and public exchange that is publicly accessible



Public Key Infastructure (PKI)

Alice has a secret she wants to share with Bob
They Swap Public keys and hold on to their private keys

Alice sends over the encrypted secret to Bob

Bob can decrypt the message with Alice's public key

Decentralized PKI

Alice and Bob register their unique identifiers
with the public identity network

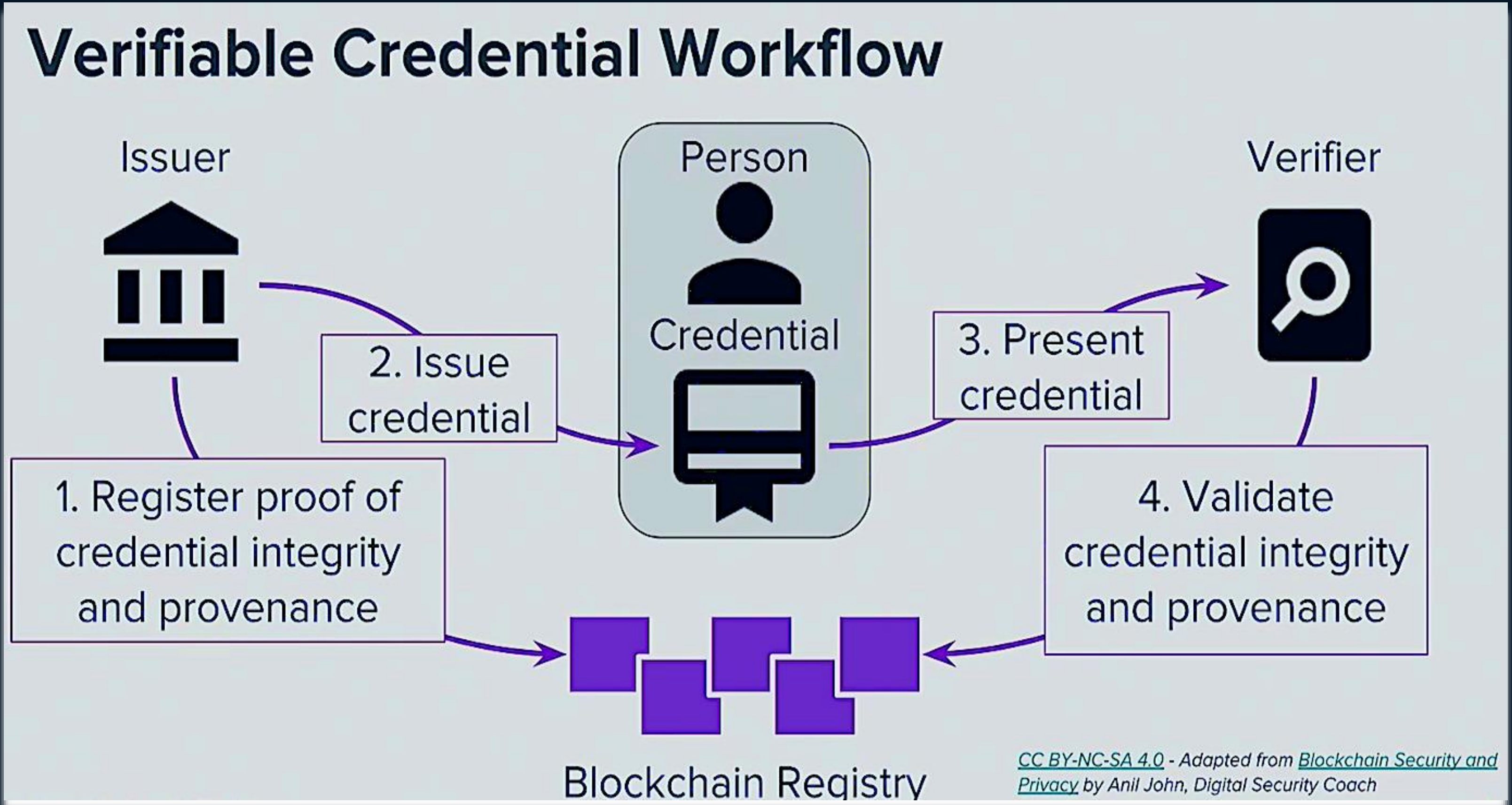
Alice sends her DID and the encrypted secret to Bob

Bob validates Alice's DID and uses it to fetch her associated
Public key so he can decrypt the message

1. **Distributed**: No single point of failure as multiple organizations operate nodes in a permissioned way
2. **No call back**: Verifiers never go back to issuers, instead they go to a globally distributed ledger to perform verification
3. **Selective disclosure**: Fine granularity in sharing the pertinent information required to establish trust based on business policy

PII is NEVER stored on the Blockchain

How does it work?



Verifiable Credential Workflow

Issuer

Person

Credential

Verifier

1. Register proof of credential integrity and provenance

2. Issue credential

3. Present credential

4. Validate credential integrity and provenance

Blockchain Registry

CC BY-NC-SA 4.0 - Adapted from Blockchain Security and Privacy by Anil John, Digital Security Coach

Decentralized Identity Use Cases

- Secure Identity Verification.
- Healthcare Records.
- Supply chain management.
- Learning or Education credentials.
- Employment Records.

Thank you

Questions? Tweet us or
go to ibm.com/blockchain

@IBMBlockchain

IBM Blockchain

IBM Blockchain