IBM Blockchain

Trusted Identity

Decentralized Identity Introduction

Dan Gisolfi | CTO | gisolfi@us.ibm.com
Milan Patel | Product Manager | mspatel@us.ibm.com
Rachel Radulovich | Designer | rachel.elizabeth.radulovich@ibm.com

IBM

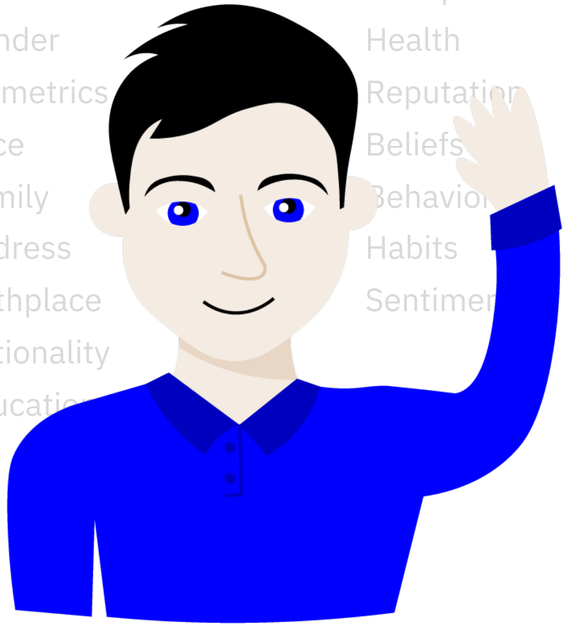
The Dimensions of our identity

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
Educatio

Profession
Workplace
Health
Reputation
Beliefs
Behavior
Habits
Sentimen



2. How I am represented:

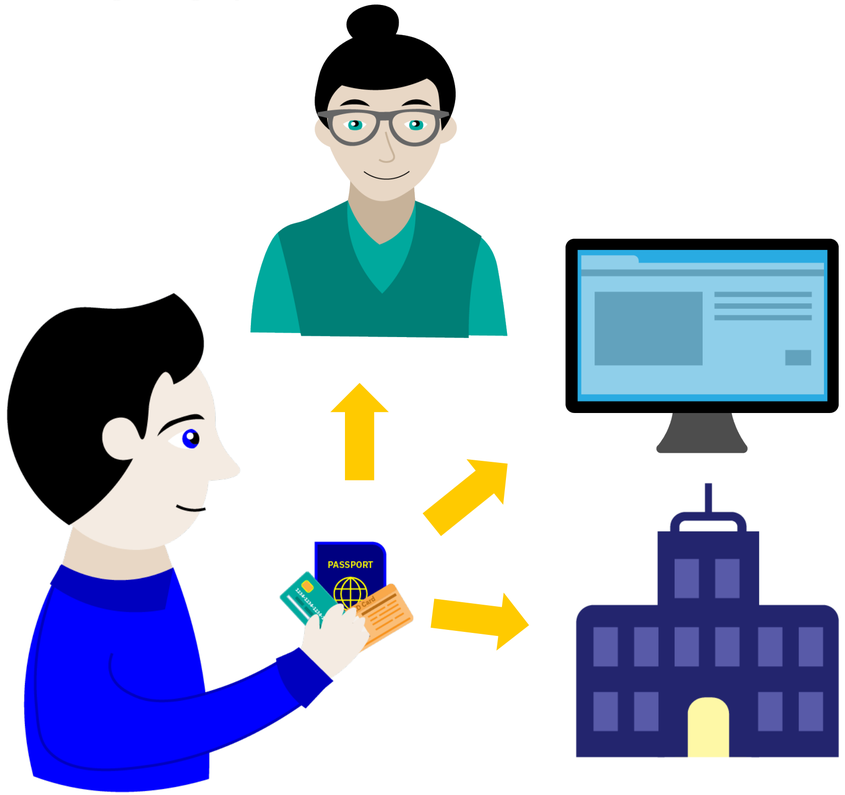
Identity Renderings: Digital or physical (paper/plastic) instrument as defined by providers.

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

Financial History
Medical History
Driving History
Social History

3. How I interact:

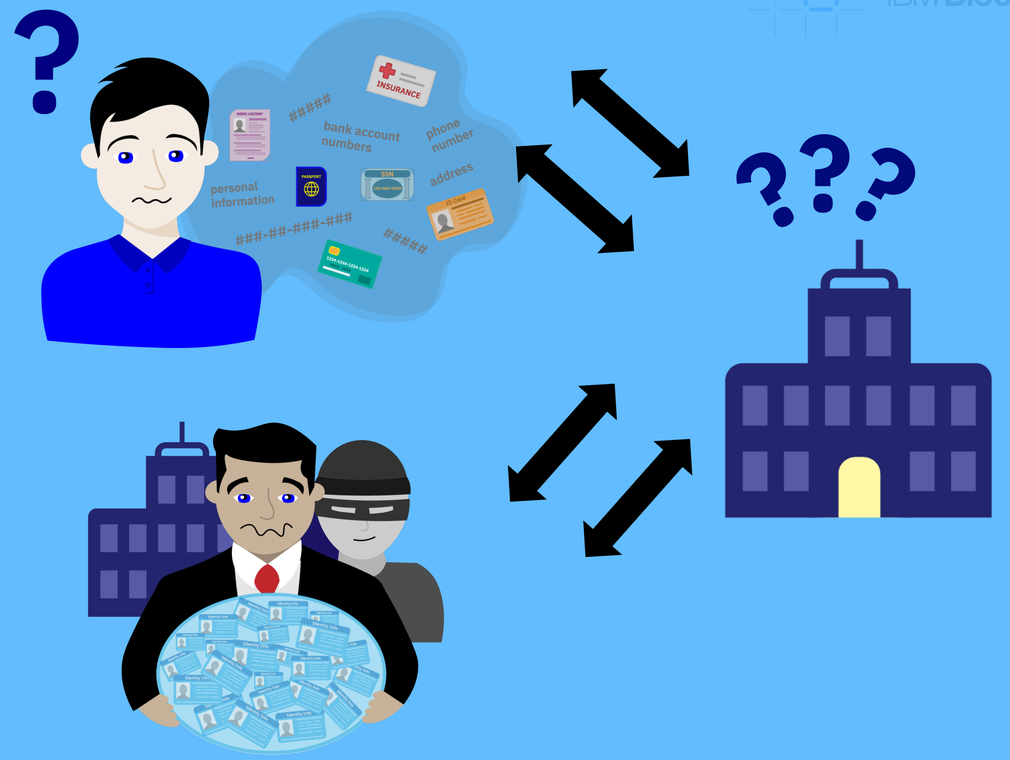
Identity Interactions: Situational usage such as pay, identify, participate, enter.



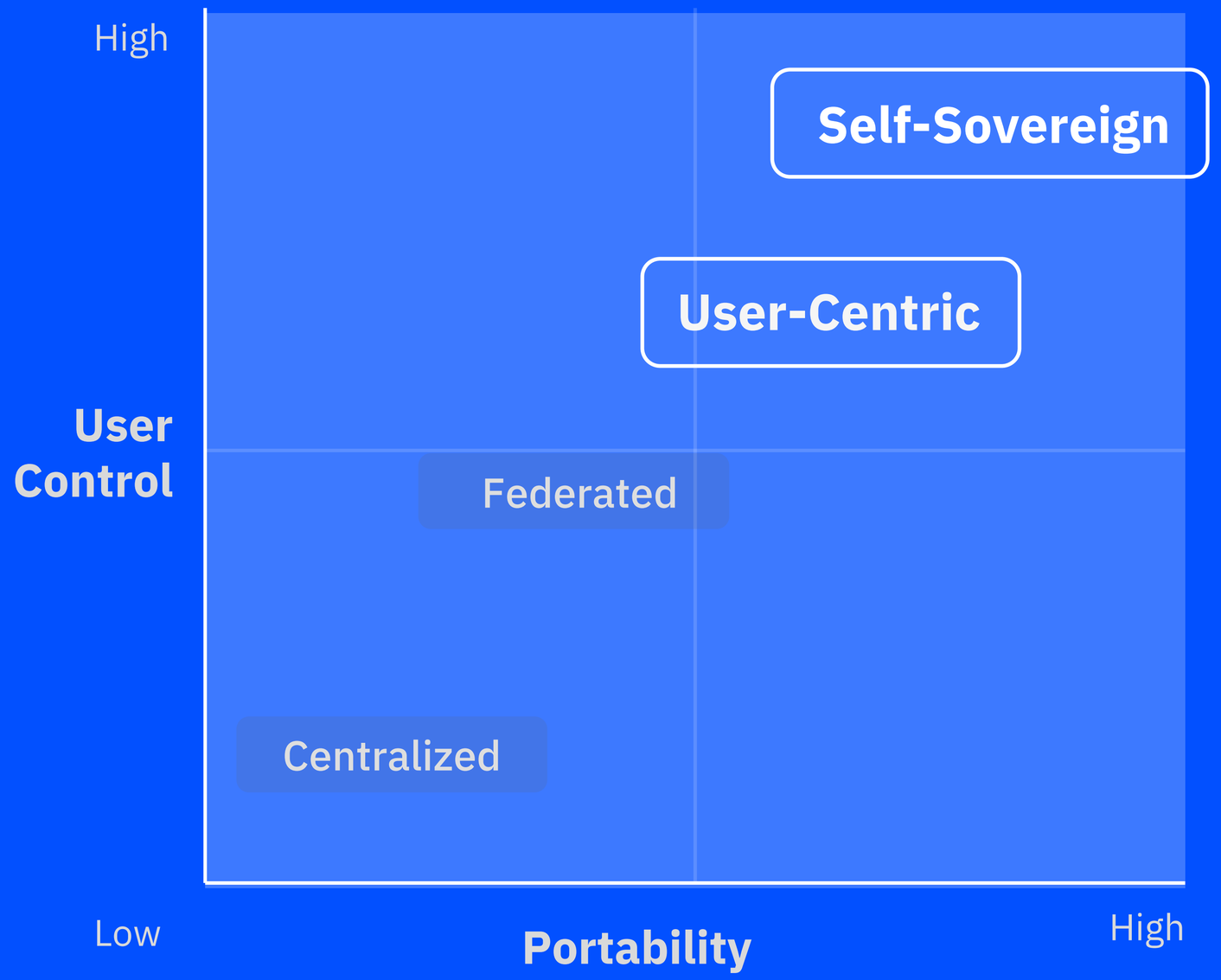
The Case for Change

Challenges and opportunity:

- Individuals and organizations are often **not in control over their identity**. Personal information is often shared without awareness and is a centralized source of sensitive data for hackers.
- **Centralized ID management** solutions are often cumbersome, hard to scale, expensive and complex to operate.
- **Security requirements** are growing in complexity, with more risks being passed down to the unaware end users. Information is **out of date** and **inconsistent** due to manual entries.
- **Login & password** do not provide adequate trust to adopt to digital channels and redefine engagements with customers. **Customer experience** can be redefined along with new **monetization models** and **cost savings.**

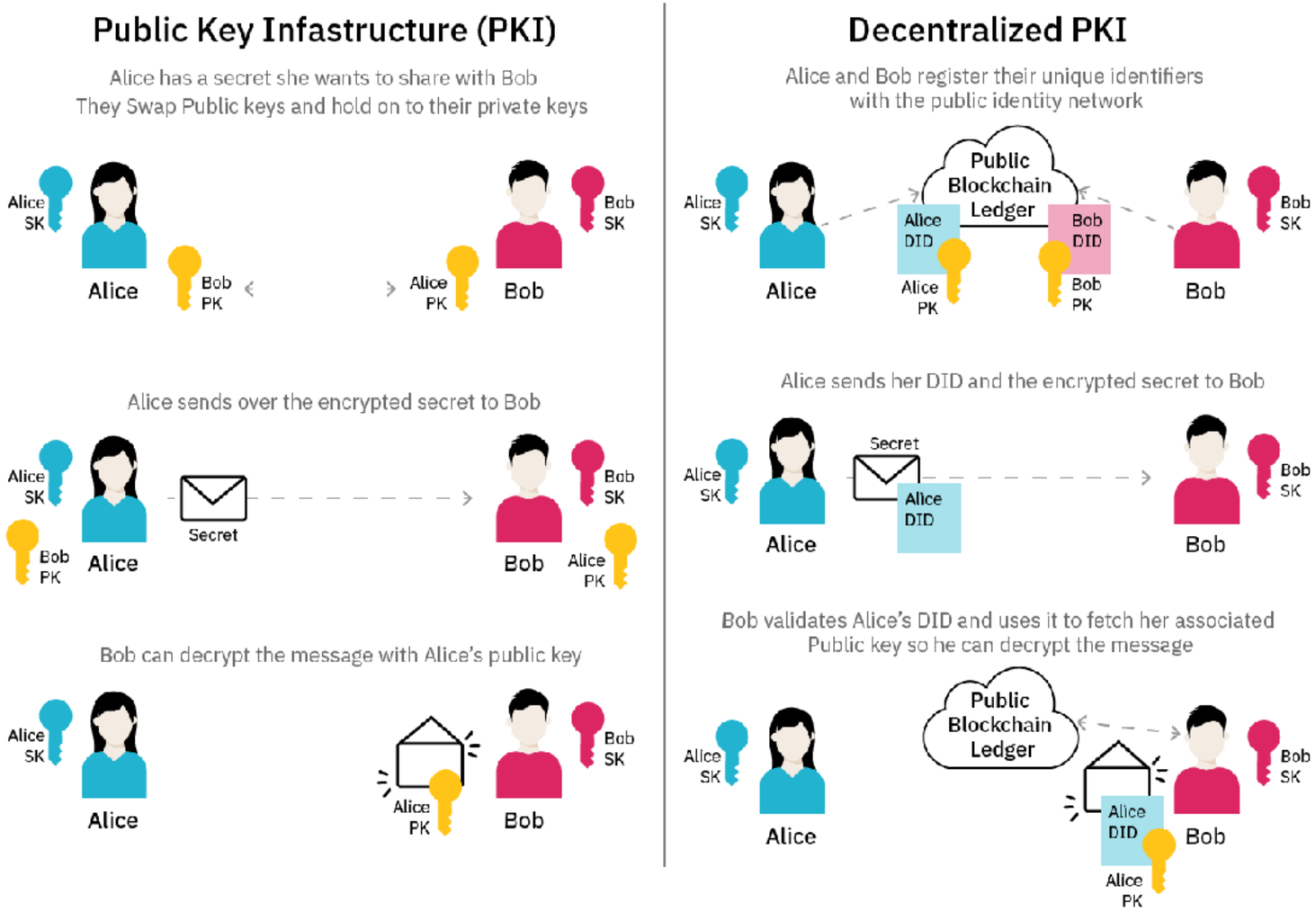


Rather than grant broad consent to countless apps and have their identity data spread across numerous providers, **there is an opportunity for a secure encrypted digital hub** where individual could store their identity credentials and control access to it.



Self-Sovereign Identity: Why blockchain?

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



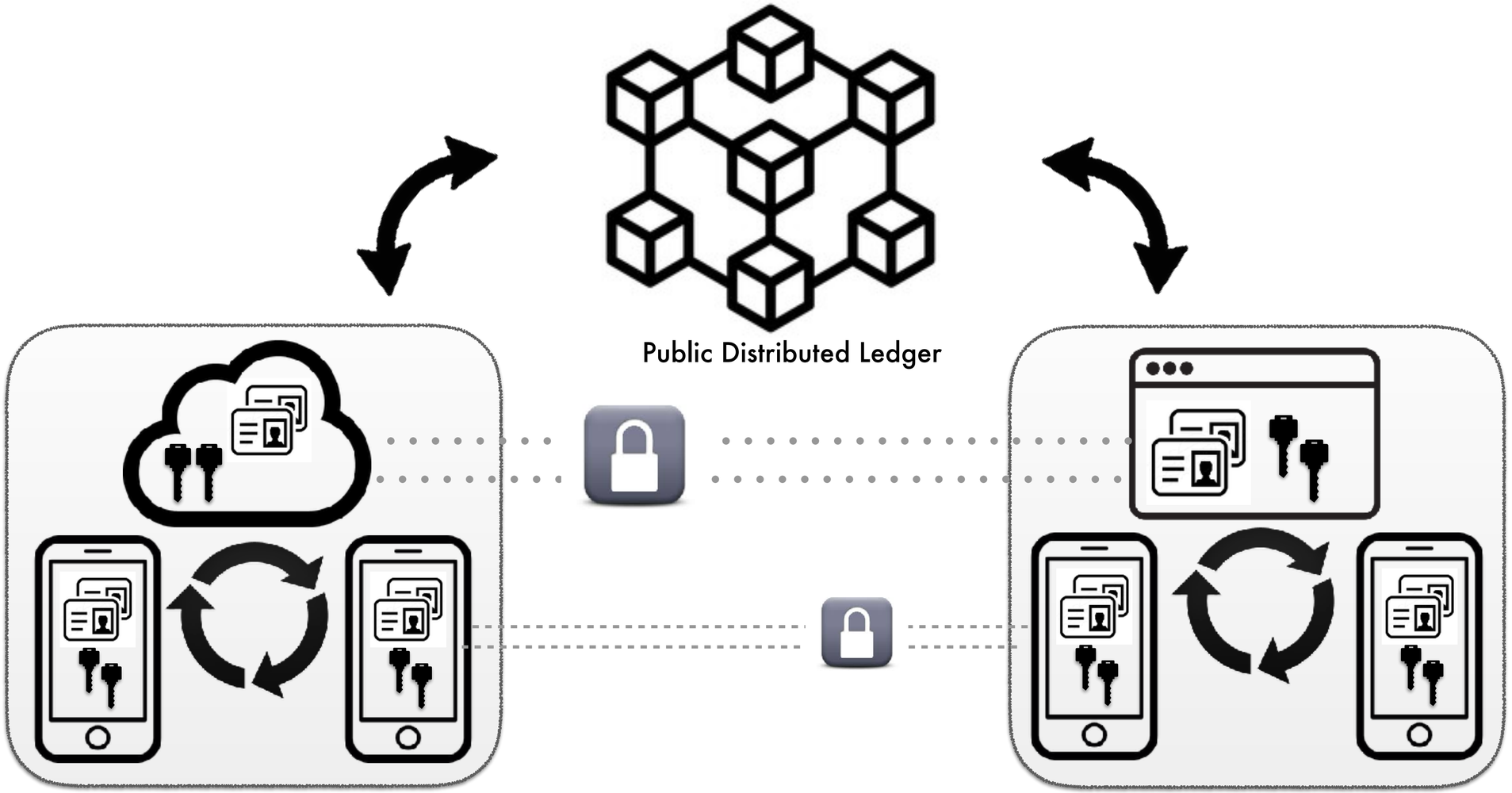
Blockchain provides:

- Immutable recordings of the lifecycle events associated with the binding between a public key and its owner.
- Secure and authentic exchange of keys which was not possible using PKI.

A blockchain ledger is <u>not</u> intended to be used for the storage of PII data.

Peer-to-peer interactions at the edges of the network

P2P network of distributed private agents working in parallel with the distributed ledger.



Self-Sovereign Identity Concepts

Three critical components that construct self-sovereign identity

Decentralized Identifier (DIDs)

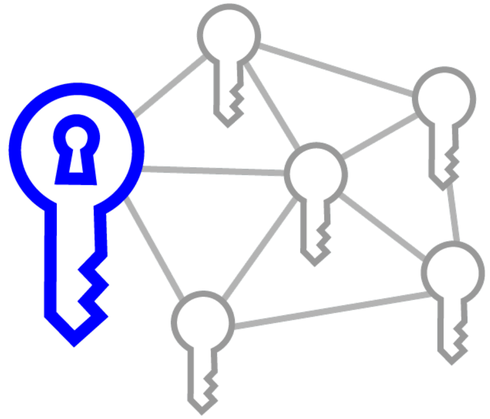
- User owned and governed
- New type of identifier for verifiable, self sovereign identity
- Fully under the control of person, institution, or thing
- URL to relate an identity for a trusted interaction with a subject
- Standardization for universal identifiers

Verifiable Credentials

- Cryptographically backed statements of truth
- Standard way of defining, exchanging, and verifying digital information
- Ecosystem of issues, verifiers, and owners

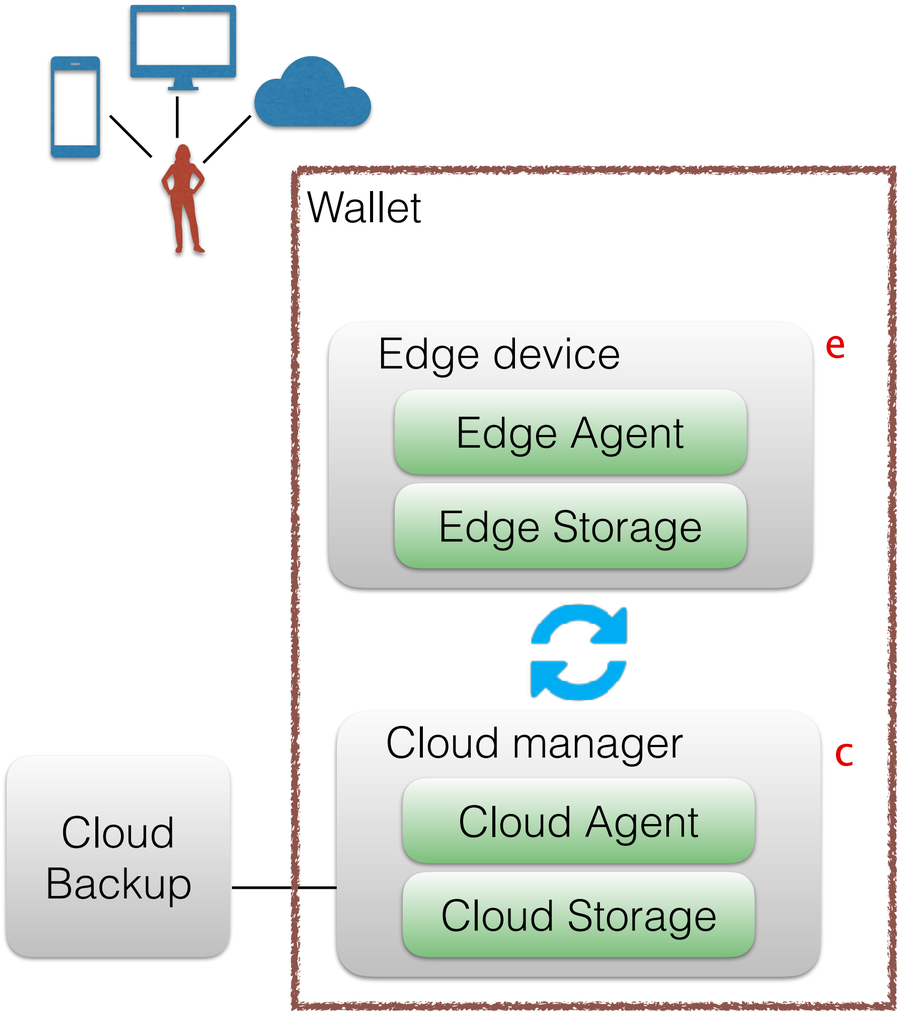
Decentralized Key Management

- User permissioning
- Entities own their own keys and have a “public key” ring for those they interact with
- “Public key” rings are used to resolve and verify interactions through DIDs



Trusted Identity Wallets

Each entity establishes a collection of infrastructure components to manage their identity relationships.



- **Wallet**: The corpus of edge devices and cloud manager that make up an entities self-sovereign identity infrastructure
  - **Agency** is a wallet provider that provides services for wallets
  - A wallet consist of edge devices and cloud manager
  - Cloud manager offloads the management and responsibilities to wallet providers and provide capabilities such as backup, recovery, etc
  - An entity (person, organization) may have several edge (“e”) devices in their Wallet
    - typically, e > 1 and c = 1
    - Entities can have multiple Cloud managers (“c”
  - Cloud manager can reside in one or more wallet provider (“Agency”) environments
  - Each cloud manager would have a Backup that may not be hosted within the same wallet provider (“Agency”) environments

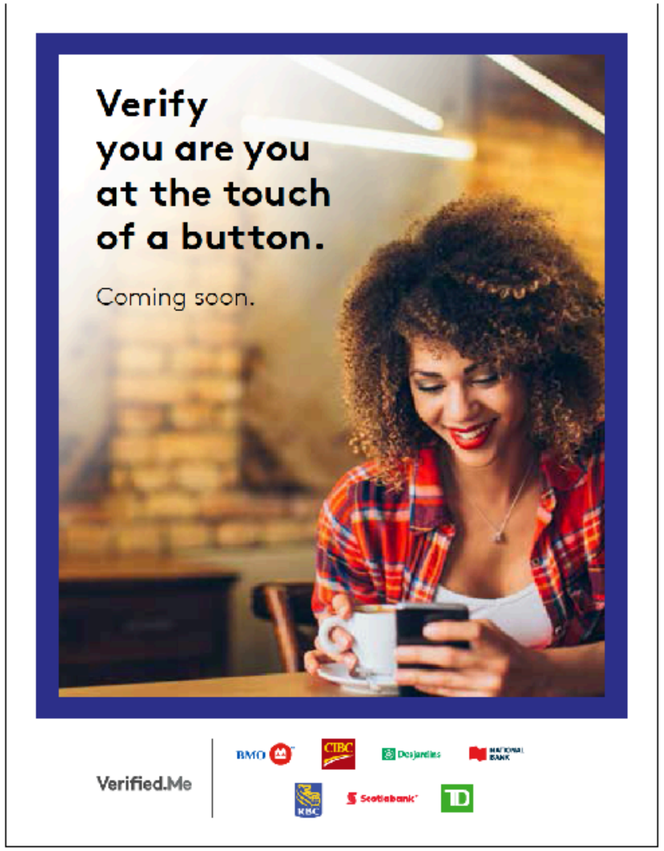
- **Edge device**: consist of physical devices (phones, laptops, etc)
  - **Edge Agent**: Manages generation and most key and link secret operations. Communicate directly, peer-to-peer, via a protocol such as Bluetooth, NFC, or another mesh network protocol. Edge agents may also establish secure connections with cloud manager agent or with others using DID TLS
  - **Edge Storage**: Manages key and data storage. Is the primary storage handler for private keys. Provides access to a secure element or Trusted Platform Module

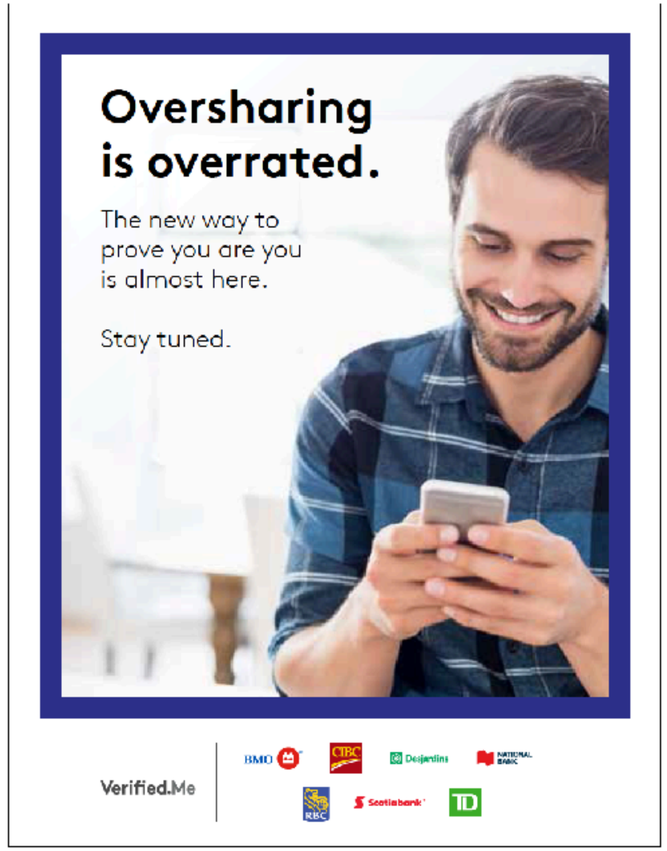
- **Cloud manager**: Hosted by a wallet provider. Provides the public end-point for interactions with the agents of connections
  - **Cloud Agent**: Designed to be available 24 x 7 to send and receive communications on behalf of the entity. Manages communications, encryption, key management, data management, and backup processes. Manages synchronization across all edge layer and backup instances. Uses DIDs and DID documents to automatically negotiate mutually authenticated secure connections
  - **Cloud Storage**: Manages keys, recovery shares, and data storage

IBM and SecureKey

Enabling a shift from single entity controlled identity to a centralized consortium model that reduces identity risk by leveraging blockchain immutability while monetizing the identity sharing economy.

- SecureKey Founded in 2008 and partnered with IBM in 2017
- Focus: National consortium verification networks
- Working with 7 of the largest banks in Canada for a national identity consortium verification network
  - Built on Hyperledger Fabric using IBM Blockchain Platform



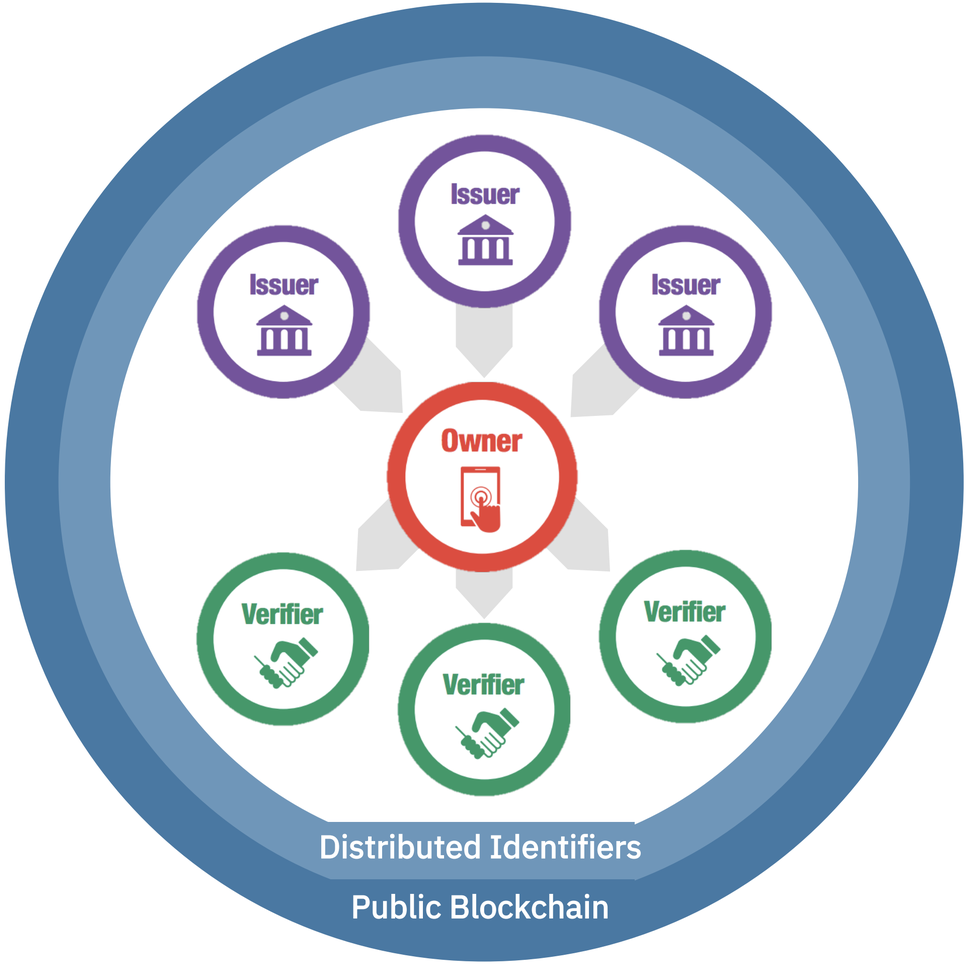


IBM and Sovrin Foundation

A decentralized, global public utility for self-sovereign identity which pertains to the management of lifetime portable identity for any person, organization, or thing.

- An ecosystem model whereby users generate and manage their own digital identity without relying on a central repository.
  - Identity is derived through Distributed certified credentials
  - Trust Frameworks: Global Public and Domain Specific (Business, Legal, Technical)
  - Built-for security and scale: push identity to the edges of the networks
  - Built using Hyperledger Indy

- IBM Role
  - Founding Steward in Sovrin Network
  - Member of Technical Governance Board for the non-profit Sovrin Foundation, founded in 2016
  - Help establish and help organizations participate



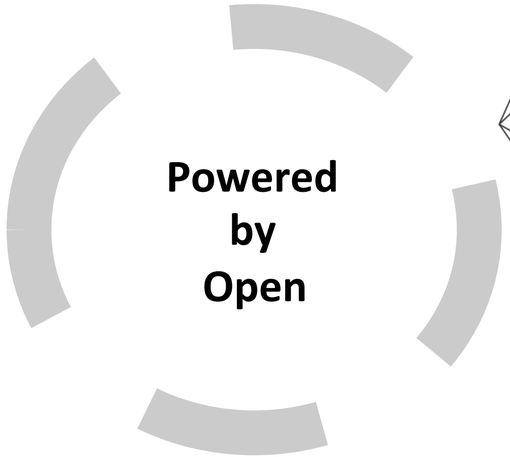
Open Network, Source Code and Standards

DIF

- Foundation of self-sovereign identity providers – building the missing identity layer
- Focus on identity registration, identity hubs, and resolving of identifiers
- Community driven, community supported (Sovrin, Uport, Microsoft, etc)
- IBM is a member

W3C®

- Standards specification of verifying and exchanging credentials
- Standardizing schemas and operations for Decentralized Identifiers (DIDs)
- IBM is an Observer/Contributor



sovrin
identity for all

- Non-profit foundation governing network to achieve self-sovereign identity
- **Member of DIF**
- **Contributor of Indy codebase**
- **IBM is a founding member (steward)**

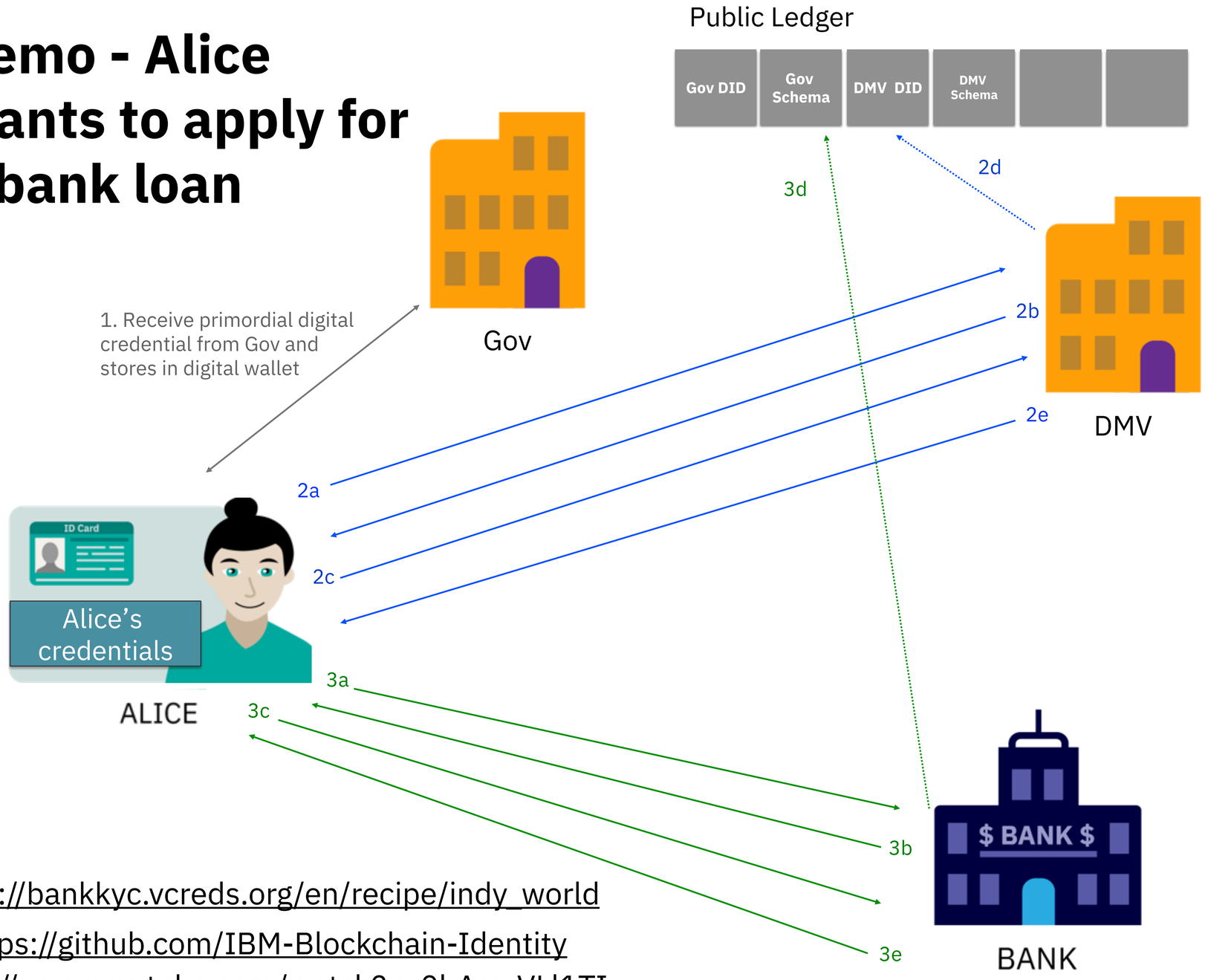
HYPERLEDGER

- Open Source Blockchain Project for Fabric and Indy
- Indy is code base for Sovrin Trust Framework
- Designed for scale and optimized for identity solutions
- Ecosystem, Community, Accelerant for our platform
- IBM is a member and active contributor to both Indy and Fabric

OASIS

- Standardizing protocols for communication between encrypted systems
- Decentralized Key Management System
- IBM is an Observer

Demo - Alice wants to apply for a bank loan



2a. Alice request for a digital drivers license

2b. DMV challenges Alice to prove attributes attested by known, trusted issuer on the network (Gov)

2c. Alice presents credentials stored in her wallet from a known, trusted issuer on the network (Gov)

2d. DMV verifiers credentials presented by Alice and issuer of presented credentials (Gov) on the public ledger

2e. DMV issues Alice a verifiable credential that is stored in her digital wallet

3a. Alice request for a loan application

3b. Bank challenges Alice to prove attributes attested by known, trusted issuer on the network (Gov and DMV)

3c. Alice presents credentials stored in her wallet from a known, trusted issuer on the network (Gov and DMV)

3d. Bank verifiers credentials presented by Alice and issuer of presented credentials (Gov ID and DMV) on the public ledger

3e. Bank issues Alice a verifiable credential that is stored in her digital wallet for issuing her loan

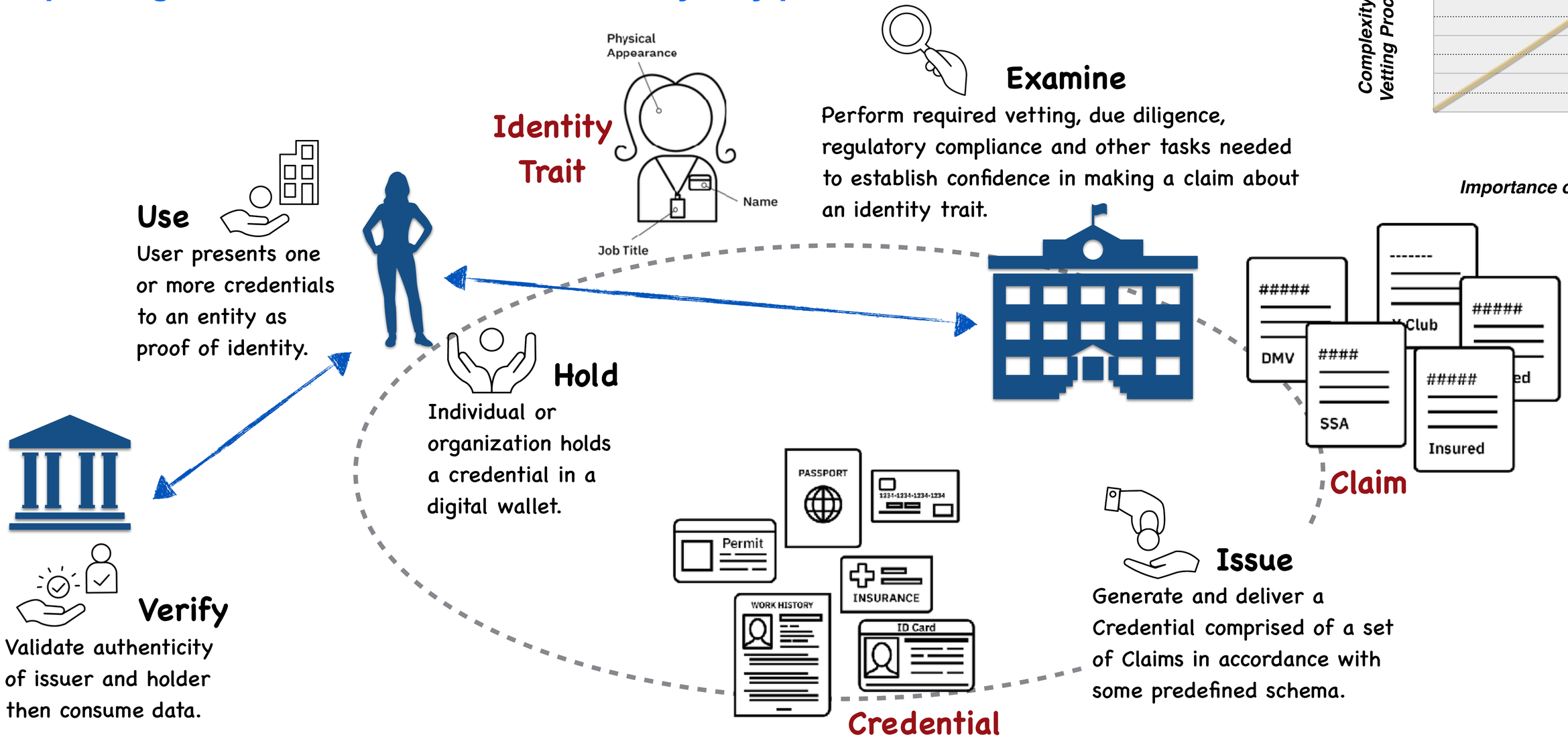
https://bankkyc.vcreds.org/en/recipe/indy_world

https://github.com/IBM-Blockchain-Identity

https://www.youtube.com/watch?v=0bAewVLl1TI

Identity instruments, roles, and interactions

Depending on the situation context, an entity may perform one or more roles.



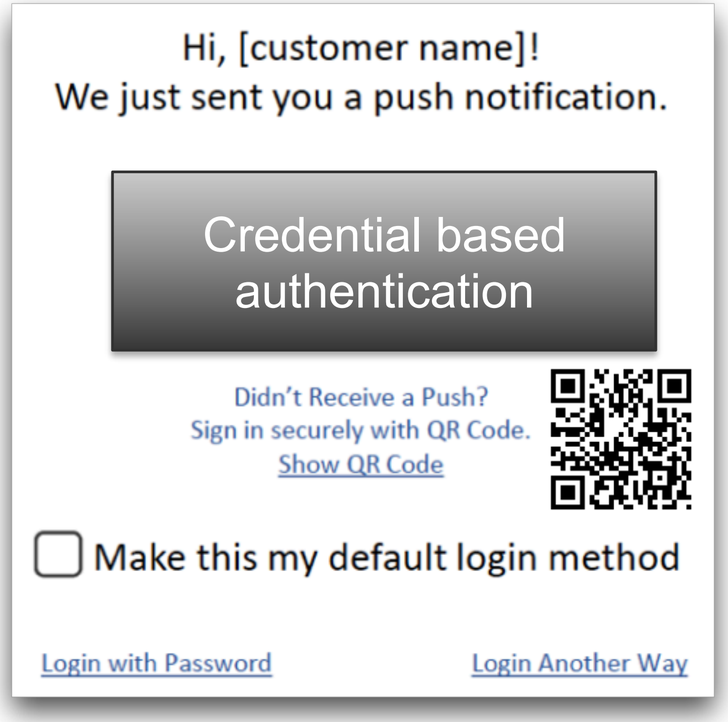
Business Pattern: Password-less Authentication

Leverage blockchain backed verifiable credentials to replace username/password

Password-less Authentication motivations and client drivers

- Customer problem 1: Customers want to reduce fraud associated with poor username/password authentication

- Customer problem 2: Customers want to provide new/real-time engagements



Business Pattern: Multi-source credentials for KYC

Initiatives involving the government are compounded in multi-source credentials

SSI for Financial Aid requiring multi-source identity

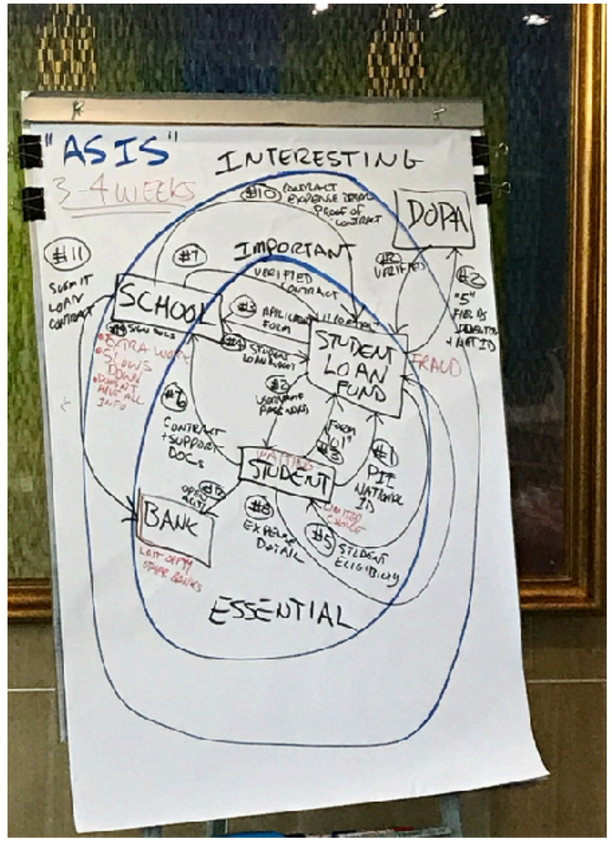
Problem

There is a lack of trust in the current financial aid application process. (a) Students often “self attest” to their education degrees (b) Families often lie about how much income they make (c) the Student Loan Fund takes on tremendous risk due to incorrect information (d) everything is manual, time consuming, uploading of physical documents, taking up to 4 weeks to process

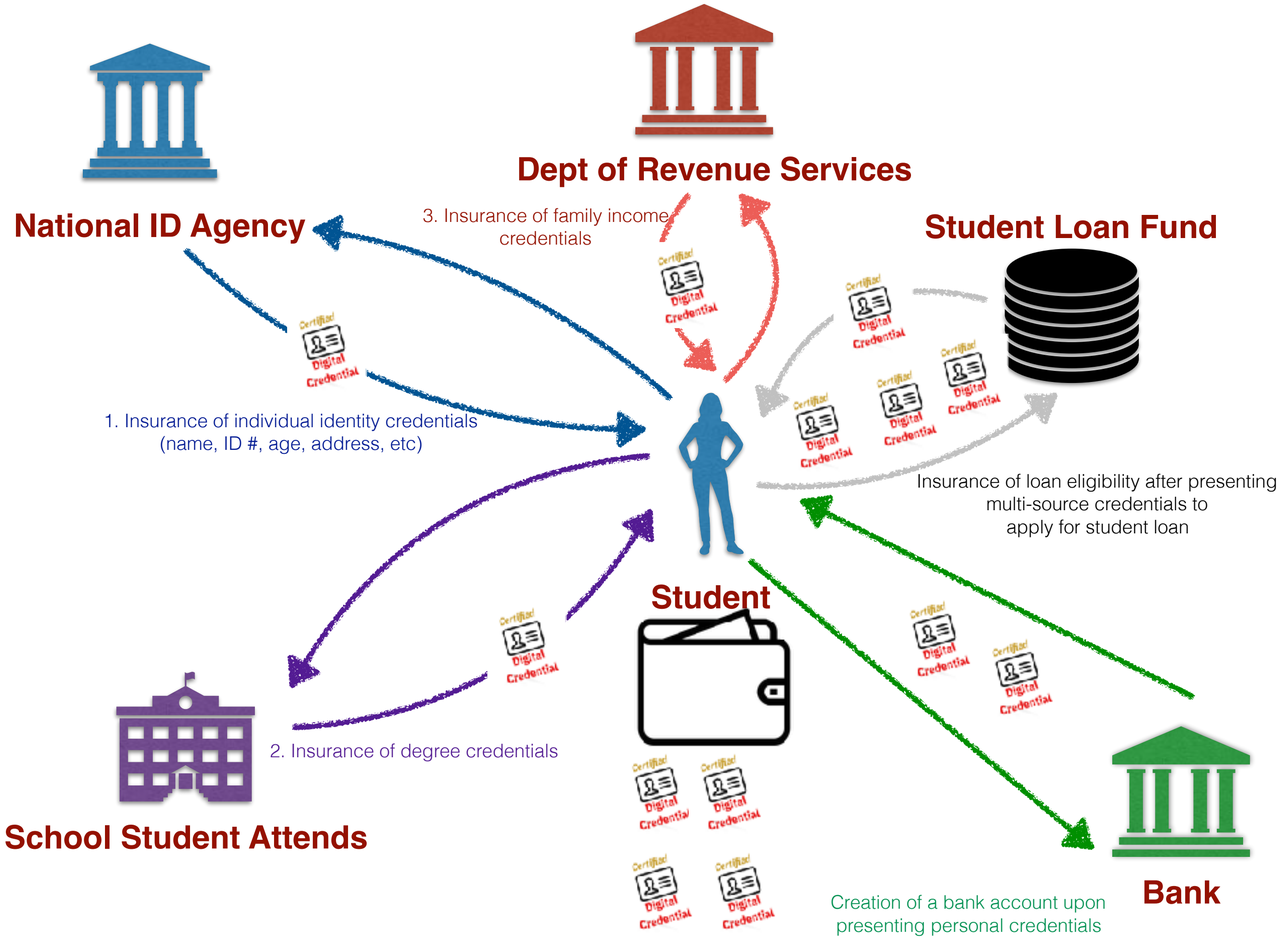
To-be experience

With self sovereign identity, (a) individuals control the flow of credentials (b) issuers and verifiers of identity can ensure trusted relationships (c) trusted digital experience reduces the time and risk of issuing student financial aids (d) credentials can be used across a global public framework

AS IS



TO BE



Why IBM for decentralized identity?

Establish permissioned decentralized identity networks

- IBM Cloud global footprint for high availability
- High level of security with Secure Services Container on System Z

Participate in decentralized identity networks

- Identity network choice based on identity needs
- Interoperate across many networks – DIF, W3C, Hyperledger, Oasis, etc

Transform business process workflow with industry expertise and AI

- Harmonize business standards regulations with Promontory
- Infuse decentralized identity in Watson services for higher value add

Design Thinking Workshop with Blockchain Identity

OFFERING OVERVIEW

Apply IBM Design Thinking principles to evaluate current business processes, identify the identity use case/ecosystem, and define the minimum viable prototype (MVP) for your blockchain solution.

What does the client receive?

IBM provides one week of blockchain solution design, including a two-day, in-person workshop, with one blockchain identity architect and design facilitator.

Typical workshop participants from the client organization:

- Client executive sponsor
- Business process subject matter experts
- IT (in support of business)
- Product owner / Project manager
- Sponsor user

Deliverable: Workshop outcomes deck and blockchain identity MVP project definition

MVP (Minimum Viable Prototype) Build-up with Blockchain Identity

OFFERING OVERVIEW

Develop a functioning blockchain identity prototype using agile methodologies, leveraging experts in IBM Blockchain Identity, UX/UI design and development, and cloud architecture.

What does the client receive?

IBM provides an application development team consisting of the following hours per week:

- At minimum, two Cloud Garage developers for 40 hours each.
- One Cloud Garage Blockchain architect for 32 hours.
- One or more Cloud Garage designer for 32 hours each.
- Additional developers can be provided per the SOW for 40 hours each.
- Project manager can be added but at an additional cost

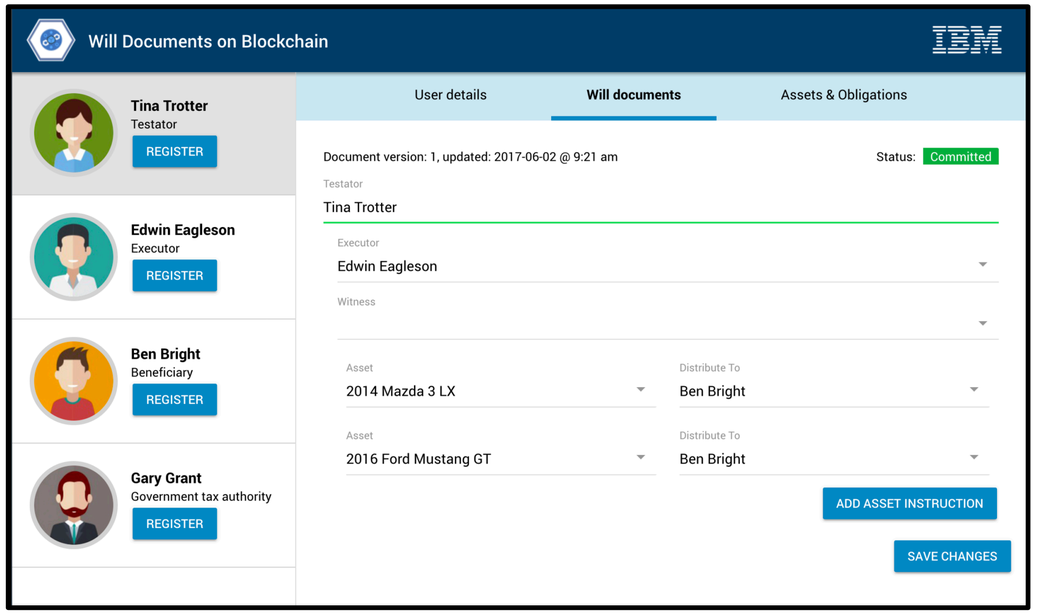
What does the client provide?

Client will provide a team to assist the application development team with the following hours per week:

- At minimum, one client developer for 40 hours each.
- One solution manager for 40 hours.

Typical project timeframe: 6-12 weeks, depending on scope

Deliverable: MVP application, including source code, delivered on IBM Cloud



Sovrin Steward Hosting with Blockchain Identity

OFFERING OVERVIEW

IBM as a cloud provider can provide value to Sovrin Steward by deploying validator nodes with high availability and security.

What does the client receive?

- Highly available validator node deployed on IBM Cloud
- Compliance and support for validator node as defined in the Sovrin Steward Agreement
- Rapid deployment and managed validator node experience
- Support with additional Steward

Deliverable: Validator node deployed onto IBM Cloud with compliance, support, and management outlined by Sovrin Steward Agreement

Sovrin Steward Service provided by IBM

- Secure, managed steward deployments
- 3 node kubernetes deployment hosted on IBM Cloud
- Global Availability

IBM **Blockchain**

IBM

IBM Blockchain

Trusted Identity

Thank you!