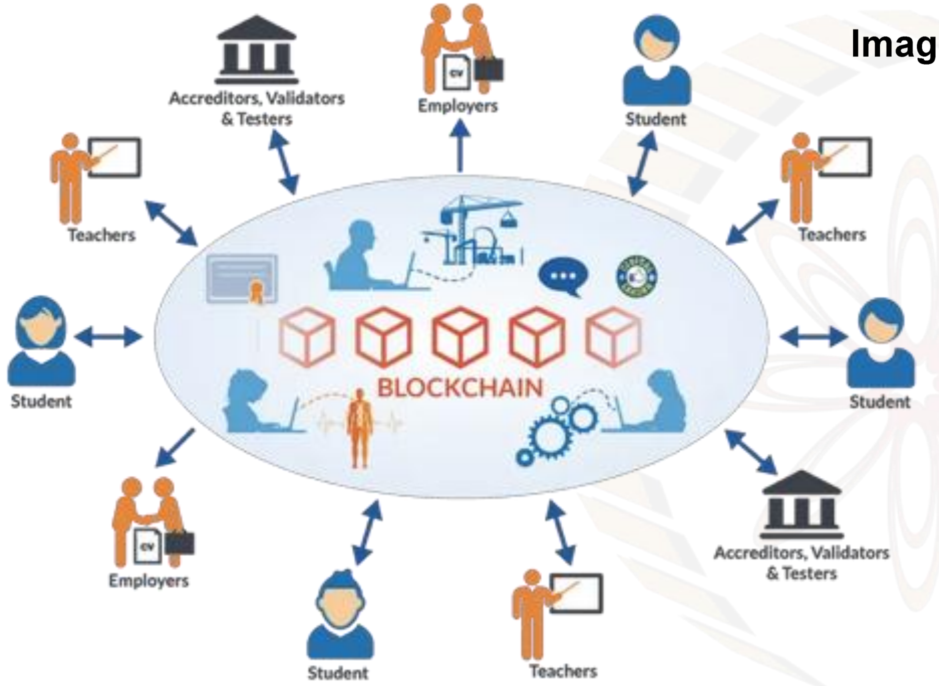
BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

Image Source: http://blockchain.open.ac.uk/



Blockchain in Government - III

Case Study I - Digital Identity

- People are known by their identities - drives every business and social interactions
- Identity is a collection of attributes
  - Name
  - Age
  - Financial history
  - Work history
  - Address history
  - Social history

Source: https://securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain/

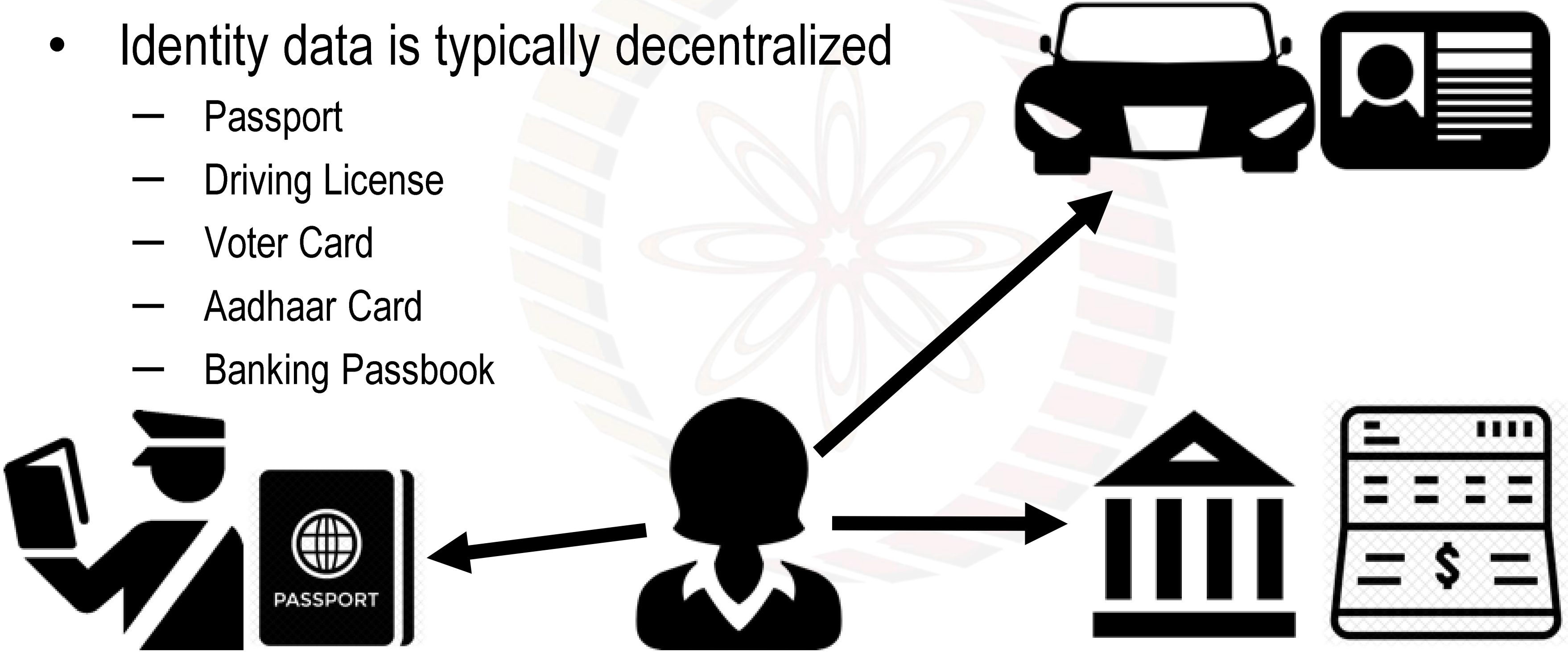
Digital Identity

- Individuals do not have any control over the information that comprises their identities

- **Identity fraud** - no visibility over the identity attributes
  - Authentication
  - Authorization
  - Verification

Digital Identity

- Identity data is typically decentralized
  - Passport
  - Driving License
  - Voter Card
  - Aadhaar Card
  - Banking Passbook



Digital Identity - Single Sign On (SSO)

- Single identity for various purposes
  - No need to maintain multiple identity documents

- Widely conceptualized in software industry
  - One password to access multiple services

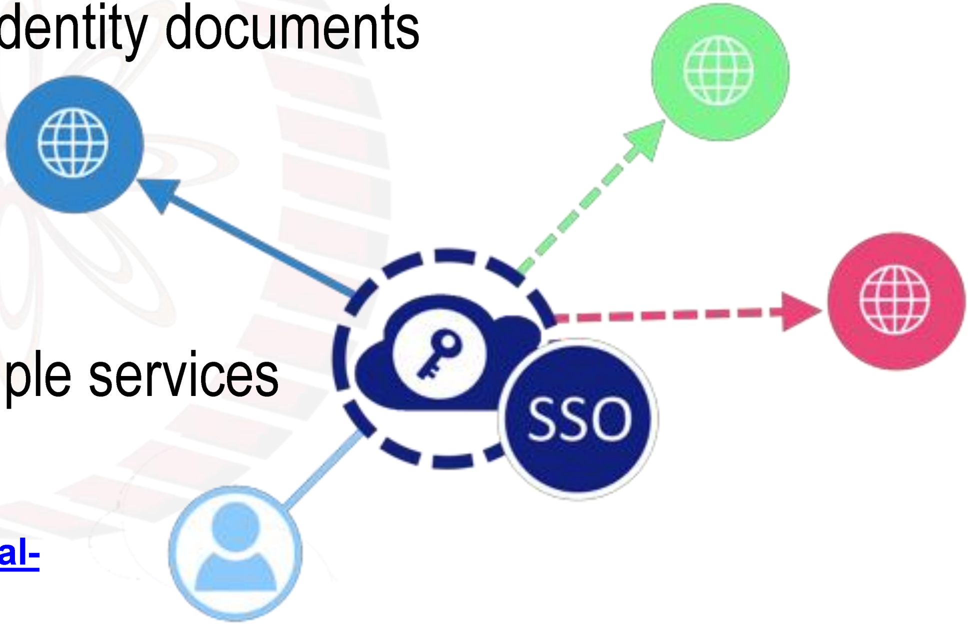
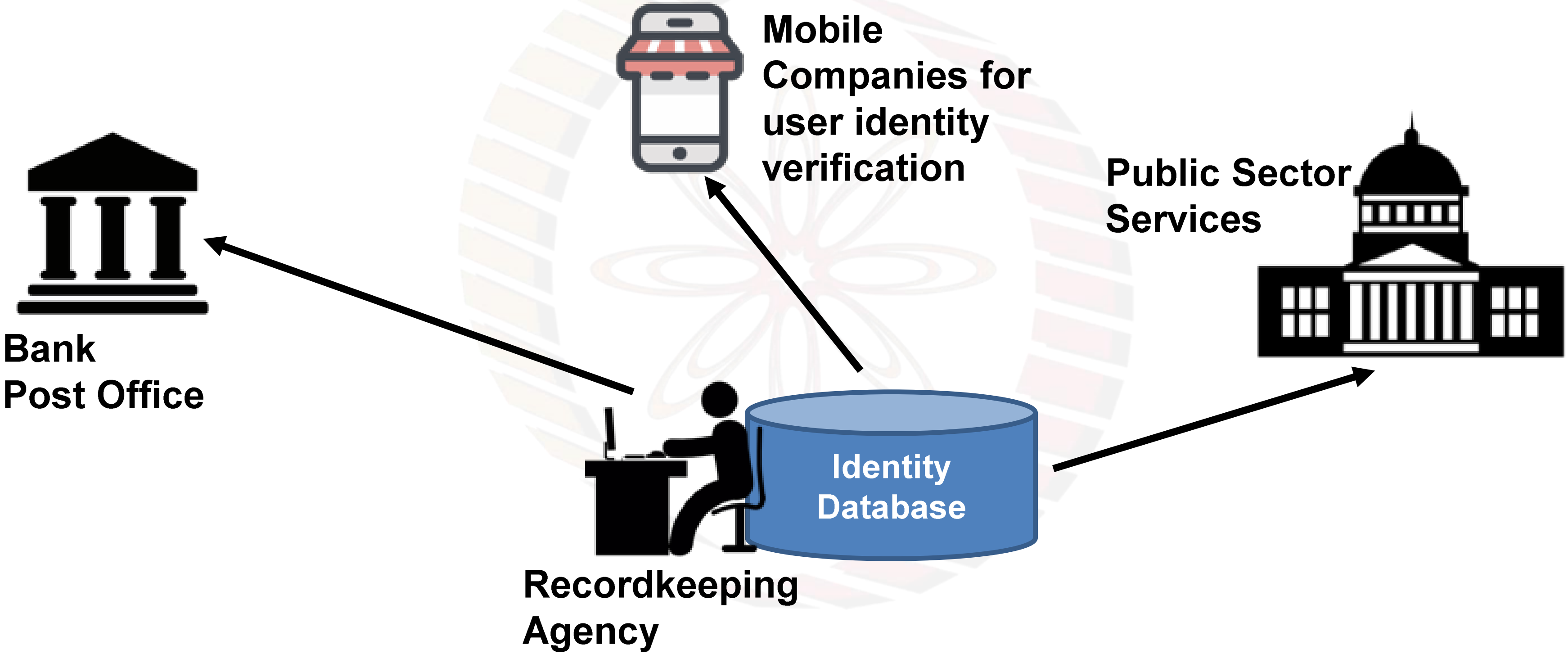


Image Source: https://www.e-spincorp.com/global-theme-and-feature-topics/single-sign-on-sso/

SSO and Decentralization



Fundamental Principles of Digital Identity Management

- **Self-Sovereign Identity (Privacy Control)**
  - Individual should have full control and ownership of their identity information
  - Individuals can control the usage of their own identity profile for business and social interactions (Consent - agreement for information usage)
  - **Burden at individual user?**

Fundamental Principles of Digital Identity Management

- **Distributed Trust Model**
  - Multiple different vendors can access identity profile for different purposes
  - **However, individual should agree on the usage of identity attributes**
  - **Every identity attribute may not be accessible to all**

Why Blockchain for Identity Management

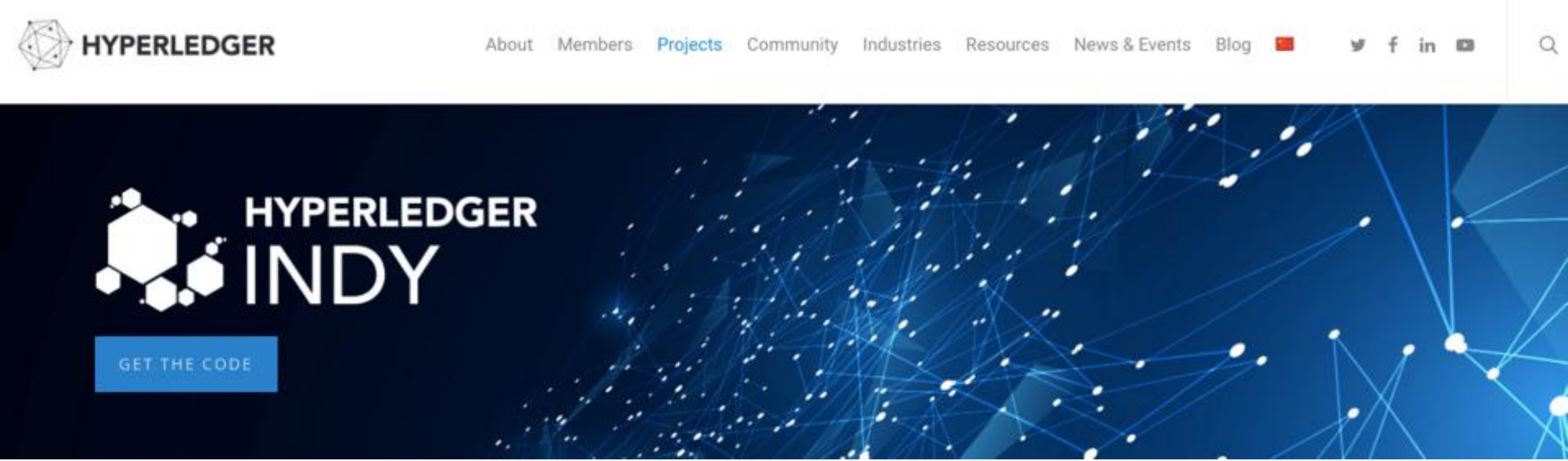
- **User centric design**
  - user can give (a) ***consent*** *for identity usage* and (b) ***control*** *identity attributes and identity profile*

- Automated and real-time verification of identity through smart contracts - can verify identity without revealing the identity data

- No one can tamper with the identity information of individuals; Auditable records of information access

Hyperledger Indy

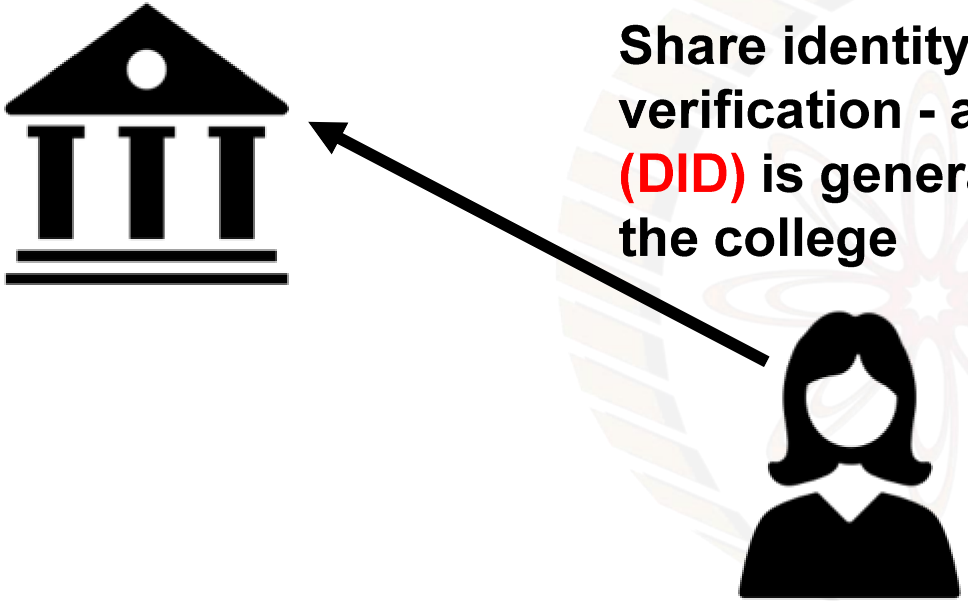
- Distributed Ledger platform for decentralized identity management



Hyperledger Indy

Want to have my degree transcript to apply for a job

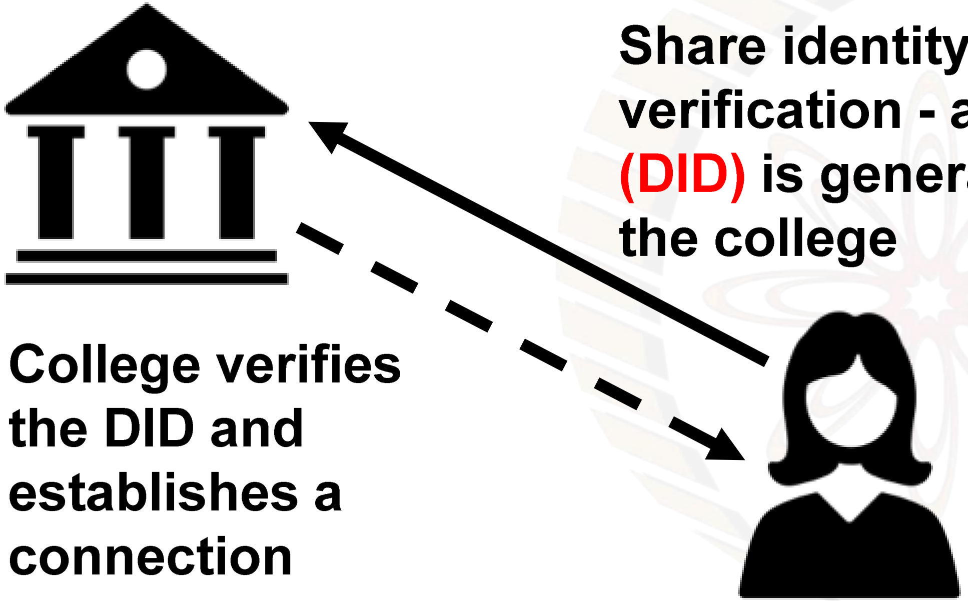
Hyperledger Indy



Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

Want to have my degree transcript to apply for a job

Hyperledger Indy

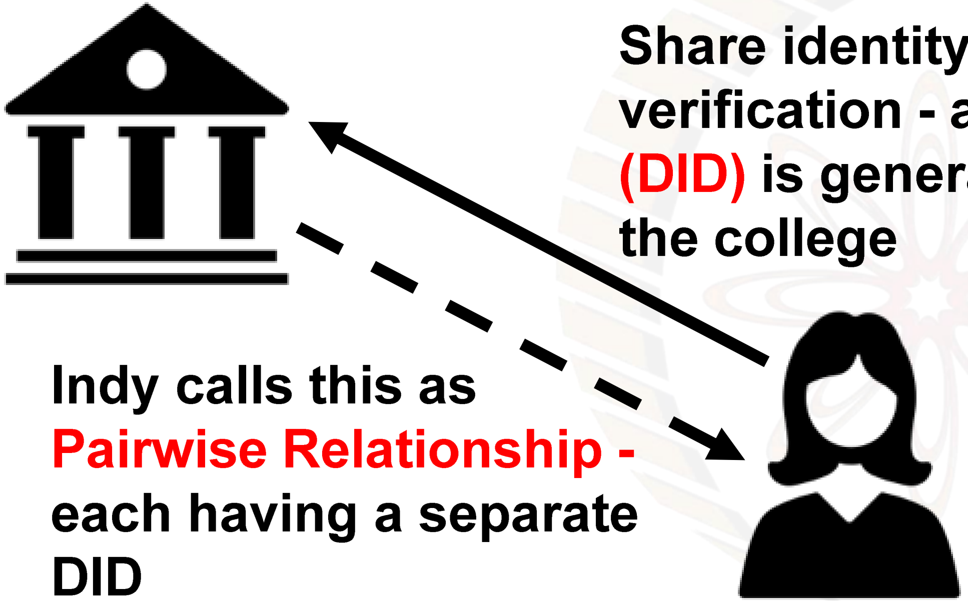


Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

College verifies the DID and establishes a connection

Want to have my degree transcript to apply for a job

Hyperledger Indy

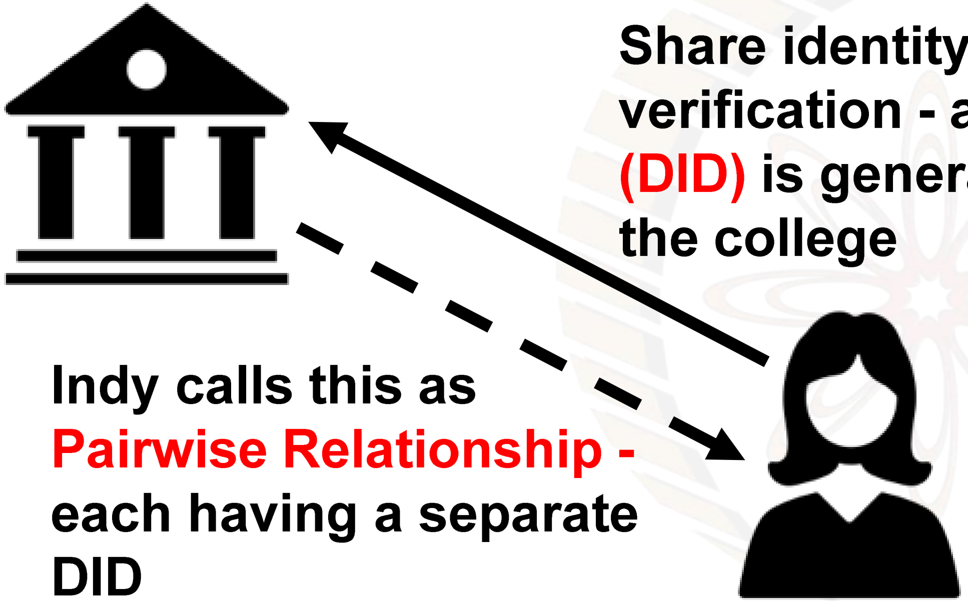


Share identity for college verification - a **distributed identifier (DID)** is generated and shared with the college

Indy calls this as **Pairwise Relationship** - each having a separate DID

Want to have my degree transcript to apply for a job

Hyperledger Indy



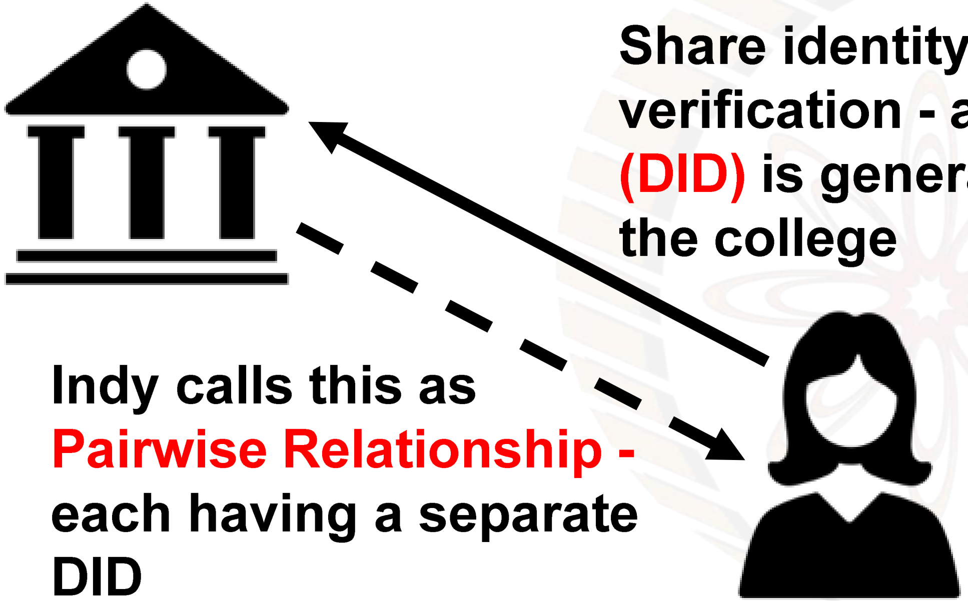
Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

Indy calls this as Pairwise Relationship - each having a separate DID

Trust Anchors - Pairwise relationships are added to the ledger by the Anchors, after verification of the DID (Consensus)

Want to have my degree transcript to apply for a job

Hyperledger Indy



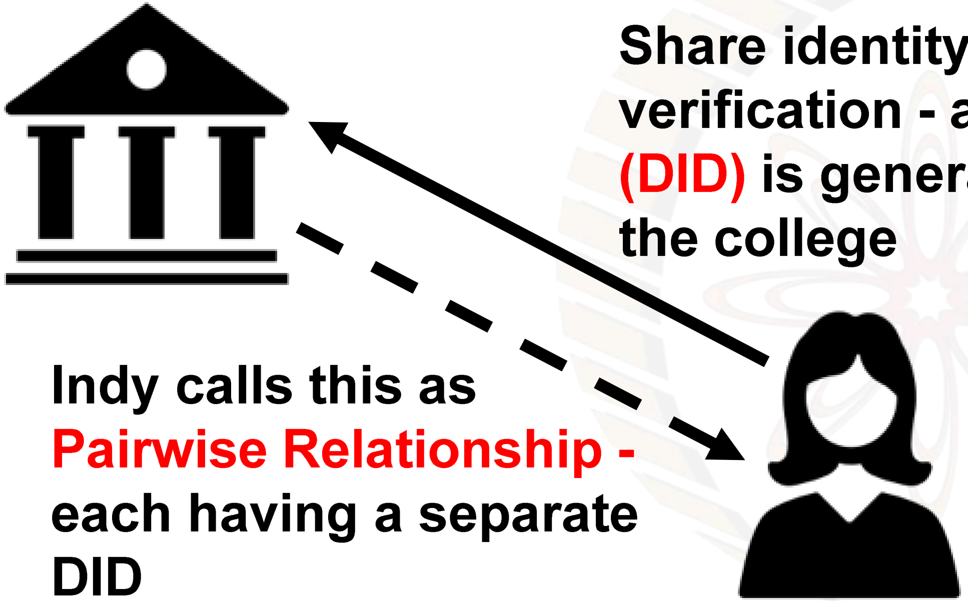
Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

Indy calls this as Pairwise Relationship - each having a separate DID

Trust Anchors - Use Alice’s public key to verify the DID (Consensus)

- Note: Trust anchors neither know Alice not her college - privacy is preserved through DID

Hyperledger Indy



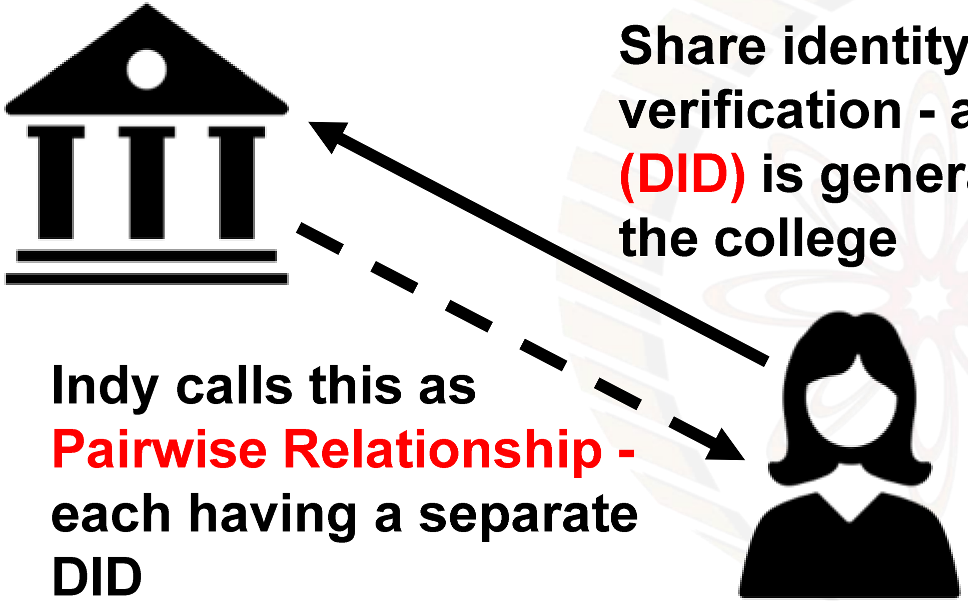
Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

Indy calls this as Pairwise Relationship - each having a separate DID

DID is not the self-sovereign identity of Alice

- Is the identity card for college usage
- Trust anchors will check that this i-card is not forged

Hyperledger Indy

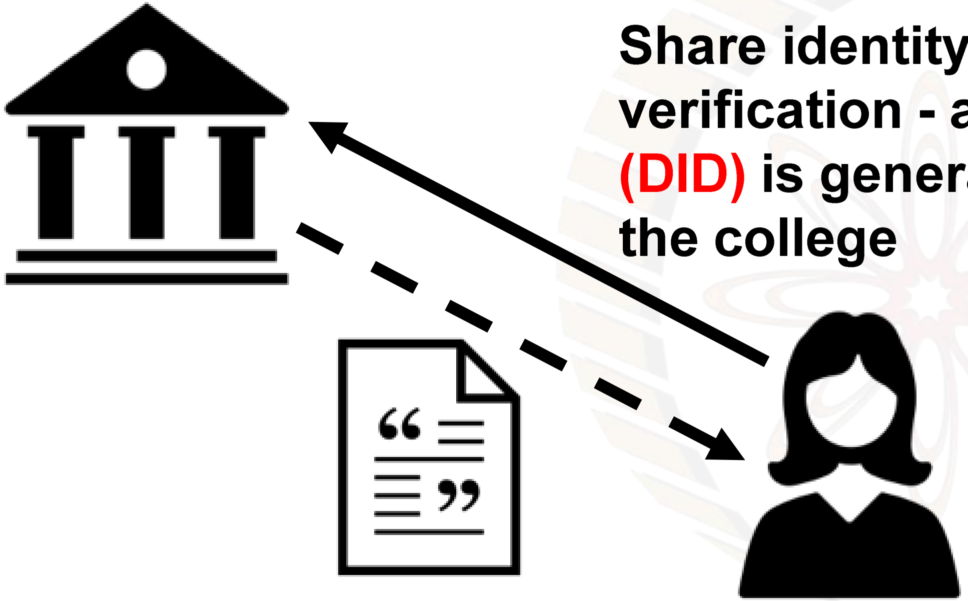


Share identity for college verification - a distributed identifier (DID) is generated and shared with the college

Indy calls this as Pairwise Relationship - each having a separate DID

The collection of all the DIDs can be thought of as the self-sovereign identity of Alice

Hyperledger Indy



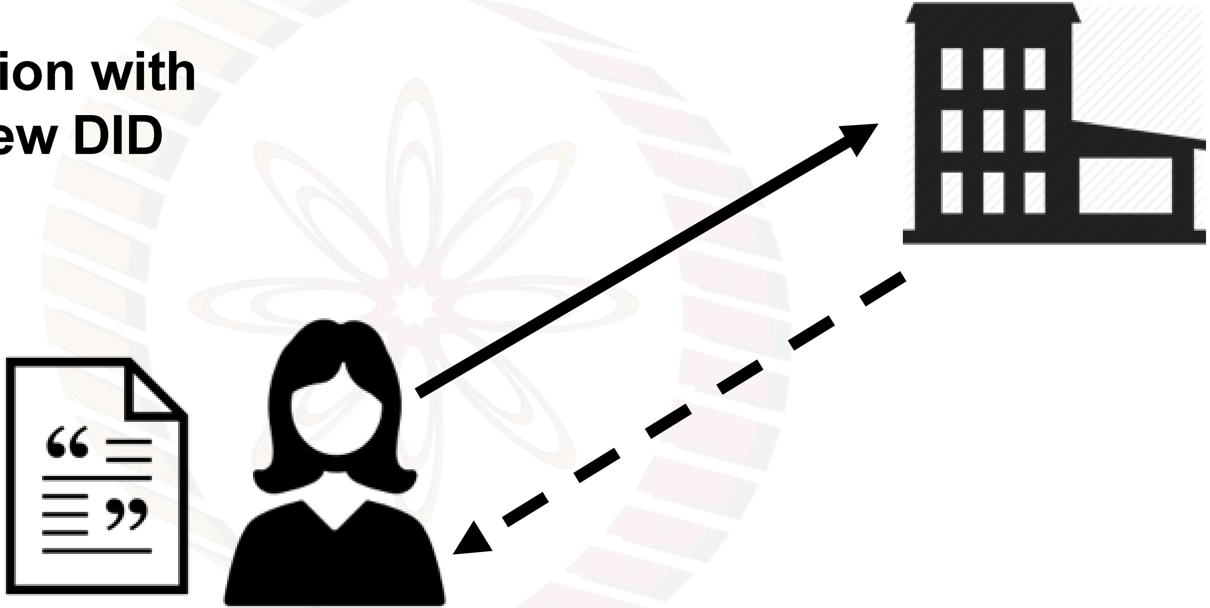
Share identity for college verification - a **distributed identifier (DID)** is generated and shared with the college

Once the consensus is reached, the connection can be accepted and information can be shared

Want to have my degree transcript to apply for a job

Hyperledger Indy

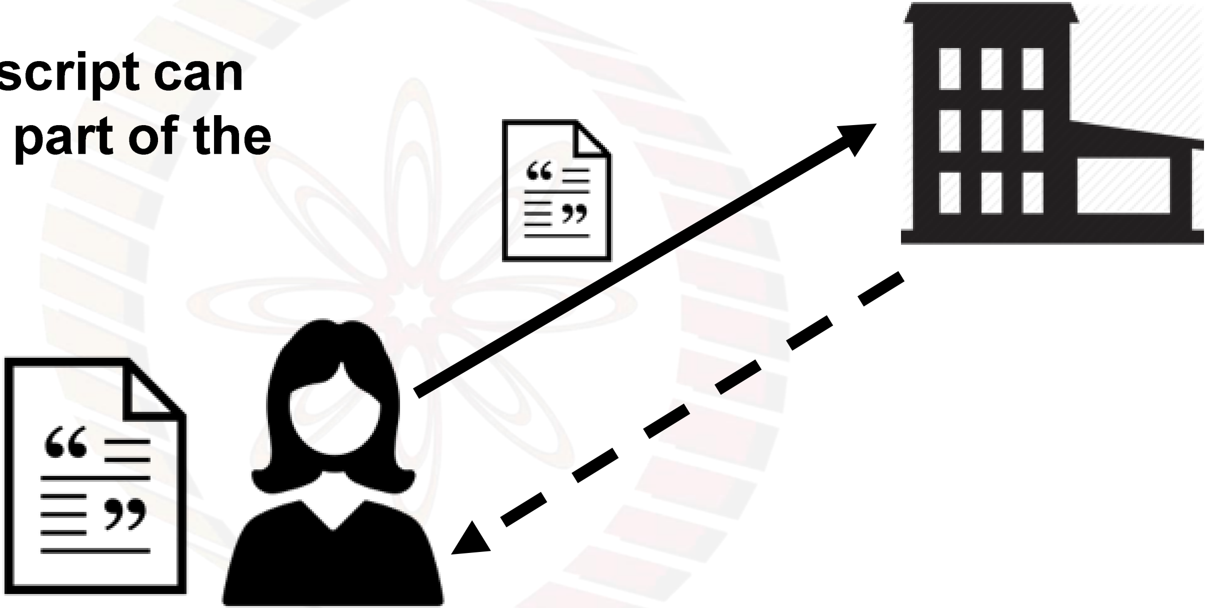
Creates a connection with the office with a new DID



Want to have my degree transcript to apply for a job

Hyperledger Indy

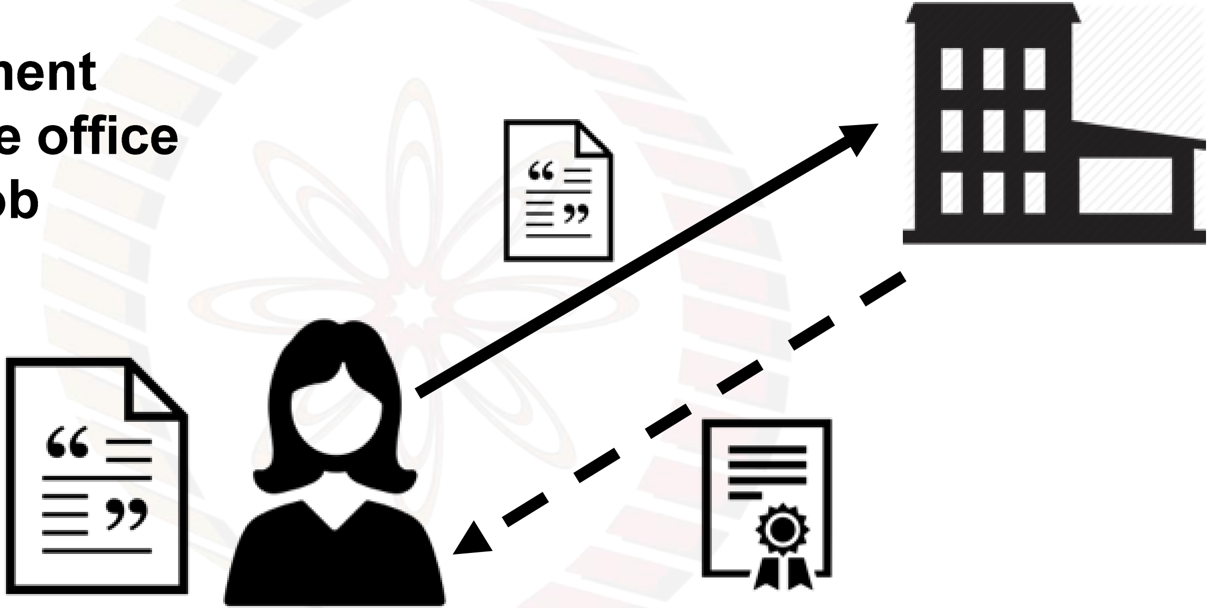
This time, the transcript can be embedded as a part of the DID



Want to have my degree transcript to apply for a job

Hyperledger Indy

Receives employment certificate once the office selects her for a job



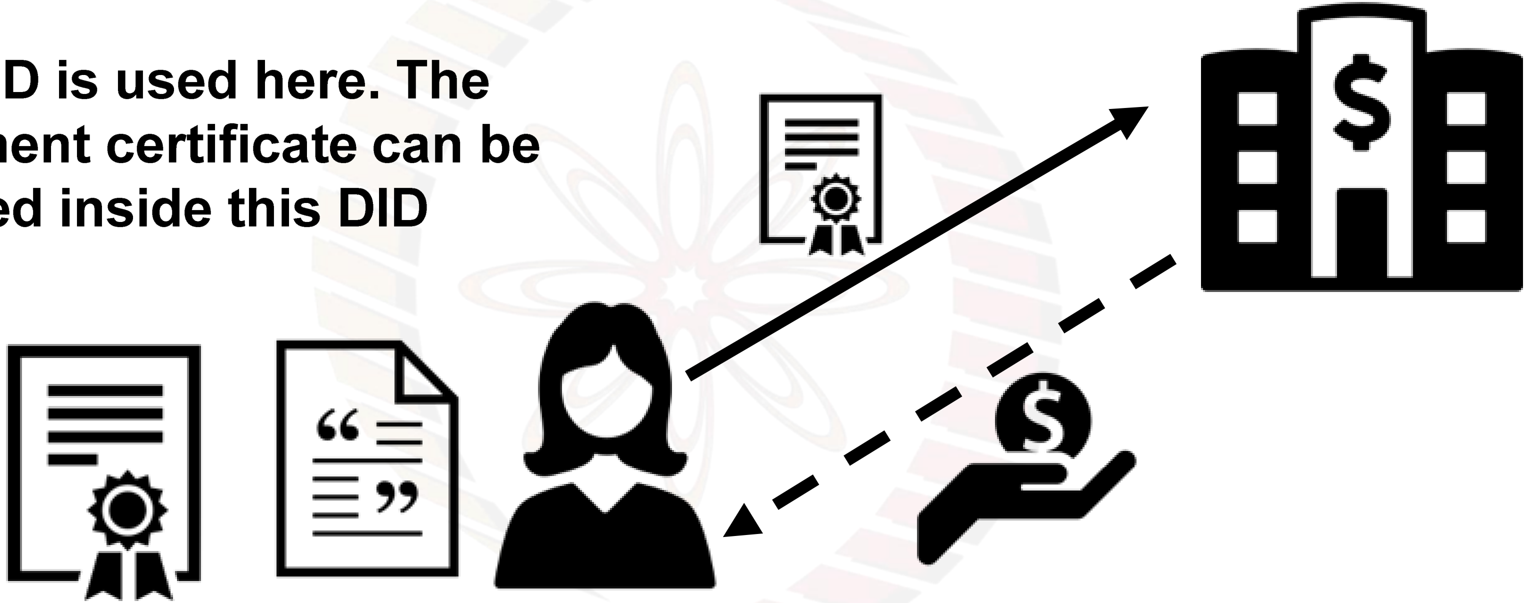
Want to have my degree transcript to apply for a job

Hyperledger Indy

Hurray! Got the job … Now I need a car ... Need some loan

Hyperledger Indy

A new DID is used here. The employment certificate can be embedded inside this DID



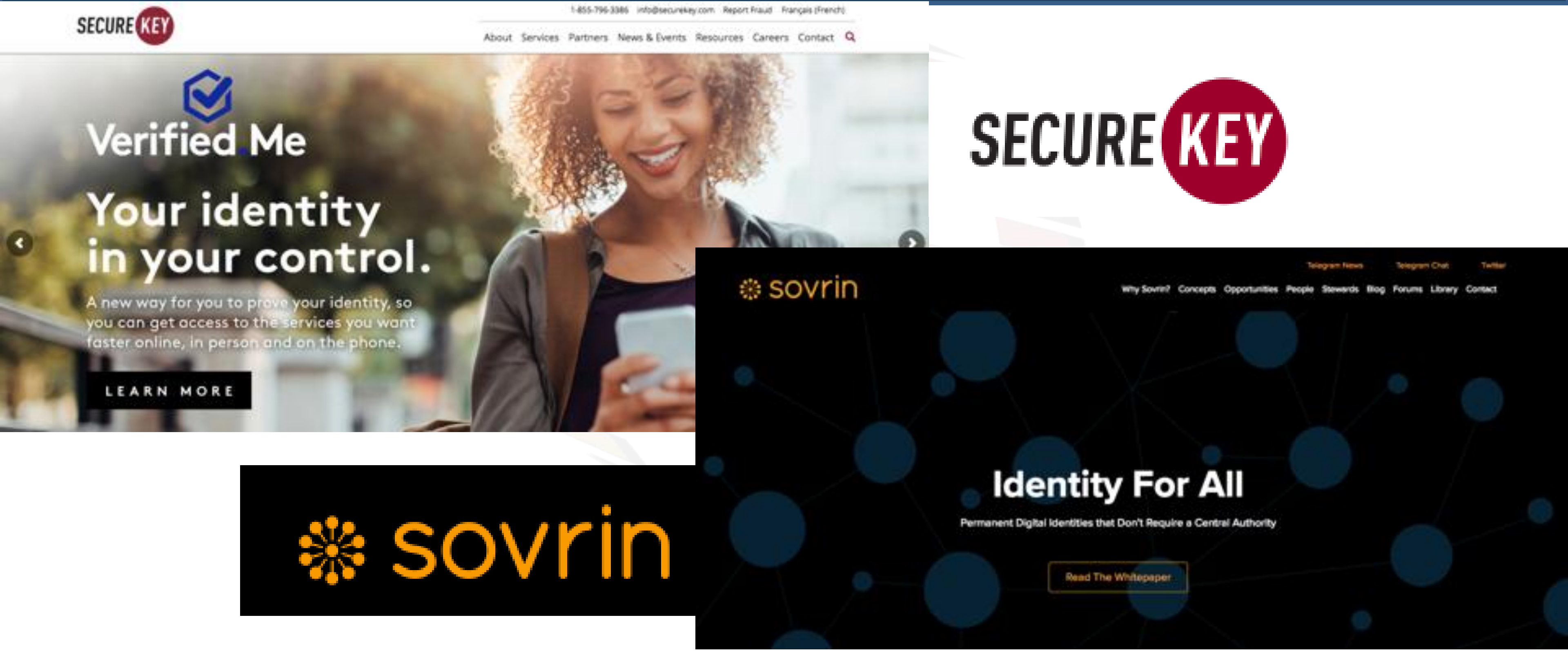
Hurray! Got the job … Now I need a car ... Need some loan

Hyperledger Indy - Plenum Consensus

- **Plenum** - a distributed ledger platform (similar to smart contracts, but tuned for verifying digital identity)
- Uses Redundant Byzantine Fault Tolerant (RBFT) algorithm for consensus
  - Multiple instances of BFT with multiple primaries - avoid malicious primaries
  - Master and Backup instances among the primaries
  - Master serializes the requests, backups validate the same
  - Backups detect faulty master and replace it

Aublin, Pierre-Louis, Sonia Ben Mokhtar, and Vivien Quéma. "RBFT: Redundant byzantine fault tolerance." *IEEE 33rd ICDCS*, 2013.

Startups for Digital Identity



Your identity in your control.

A new way for you to prove your identity, so you can get access to the services you want faster online, in person and on the phone.

Identity For All

Permanent Digital Identities that Don't Require a Central Authority

Open Standards for Digital Identity

- IBM and Hyperledger have signed on with the Decentralized Identity Foundation (DIF) - a consortium to promote interoperability and standards for blockchain based identity system (2017)

Blockchain

Paving the Road to Self-Sovereign Identity with Blockchain, Open Standards

https://www.ibm.com/blogs/think/2017/10/self-sovereign-id-blockchain/

Interesting Reads

- Sovrin White Paper - https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust

A White Paper from the Sovrin Foundation

Version 1.0

January 2018

thank you!