# What is Decentralized Identity?

Scott Harris
VP Operations, Indicio

HYPERLEDGER FOUNDATION Indicio


# Scott Harris

scott@indicio.tech


VP Business Operations

HYPERLEDGER FOUNDATION Indicio

HYPERLEDGER FOUNDATION Indicio

# Internet and Identity

The Internet was created without a way of positively identifying the people and organizations who use it.

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

# TRUST

## The main reason we have identity systems is to establish trust.

LinkedIn

Welcome Back

Don't miss your next opportunity. Sign in to stay updated on your professional world.

Email or Phone

Password Show

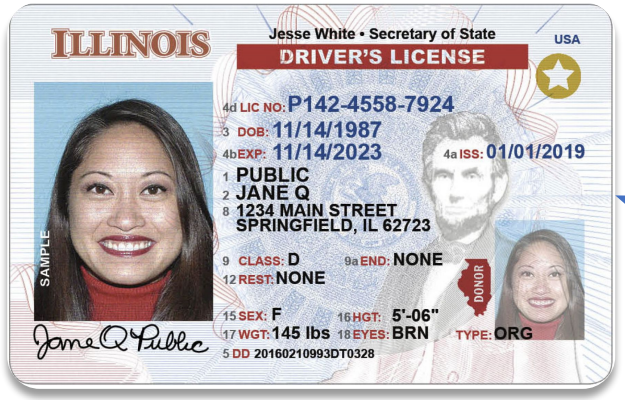
Sign in

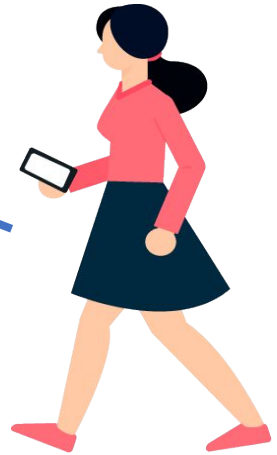
Forgot password?

New to LinkedIn? Join now

HYPERLEDGER FOUNDATION Indicio

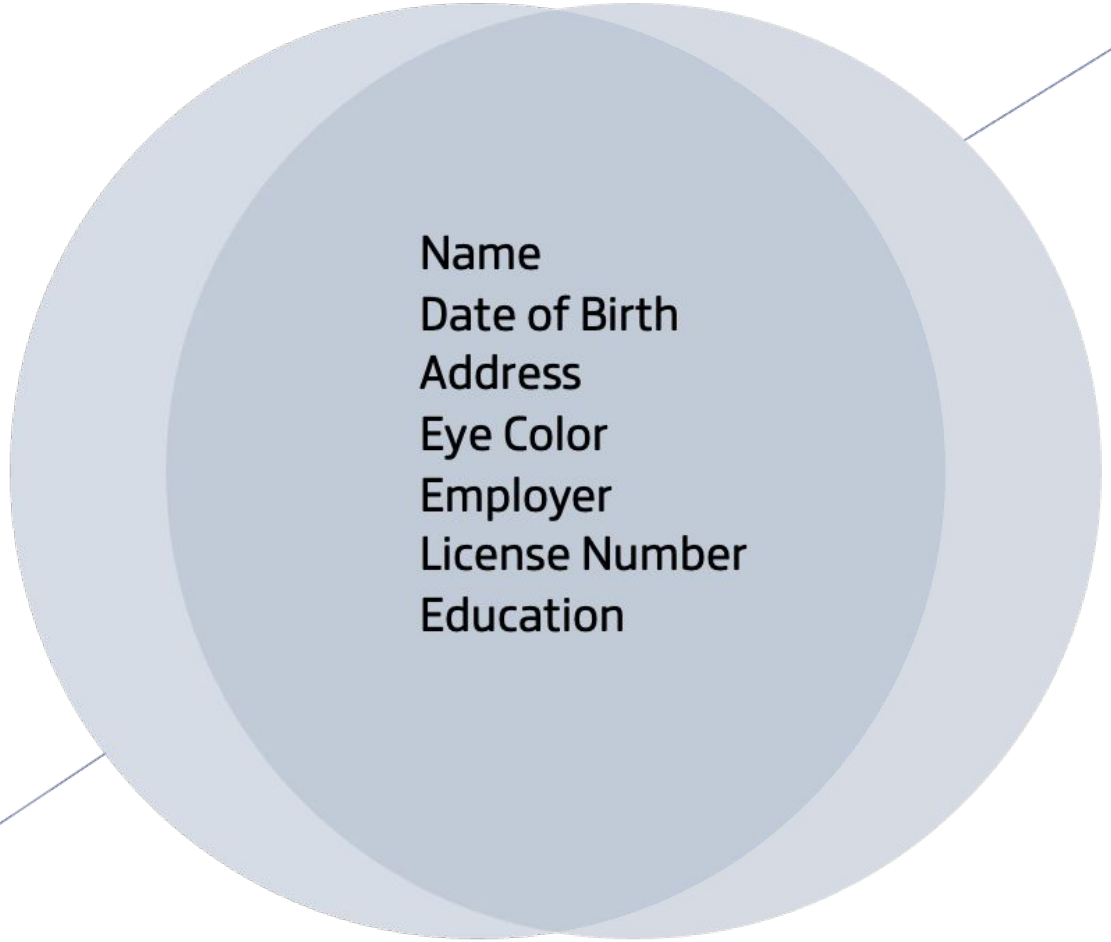
# What is identity?



# What is identity anyway?

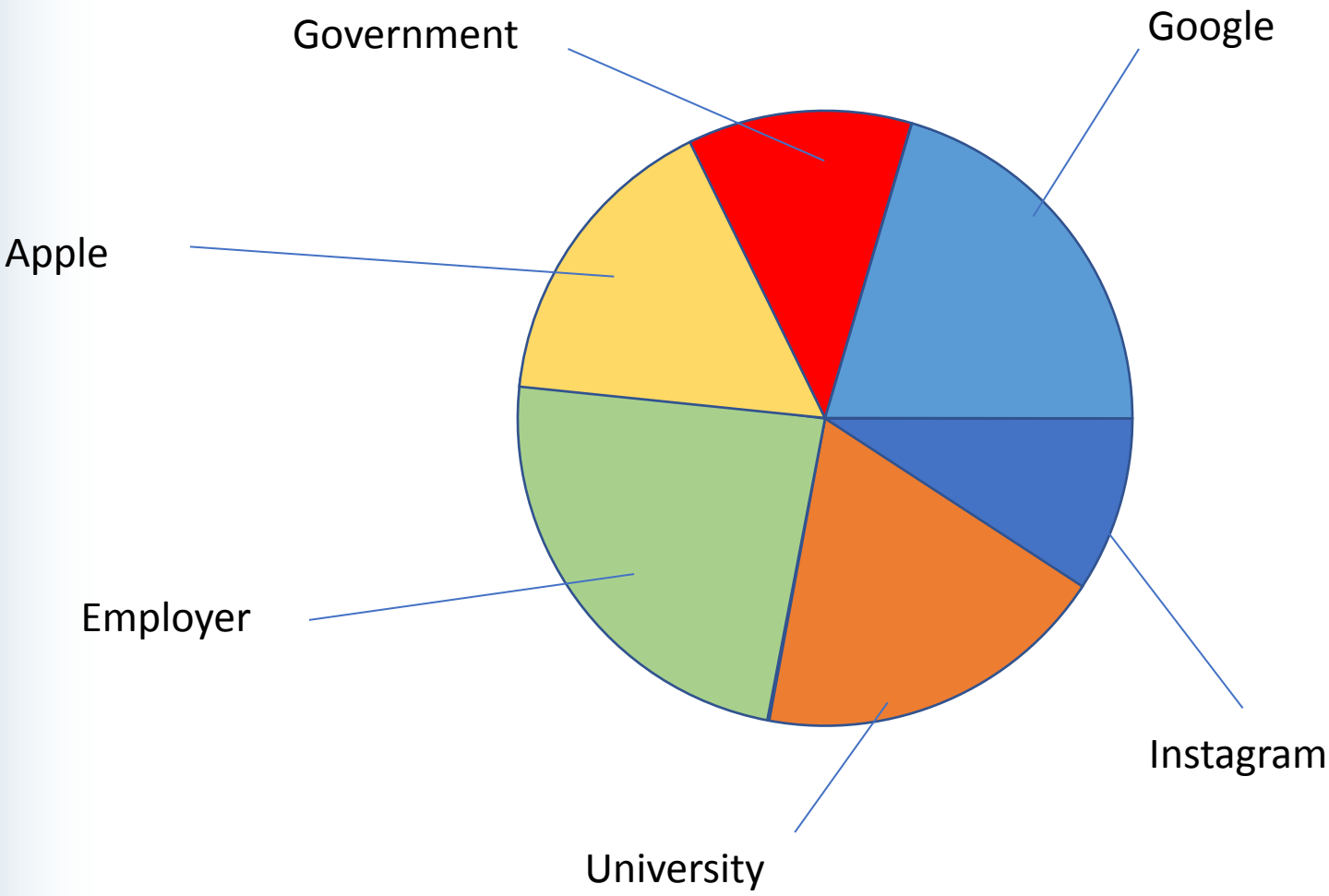
*Who is this person?*




Verifiable Credential

HYPERLEDGER FOUNDATION Indicio

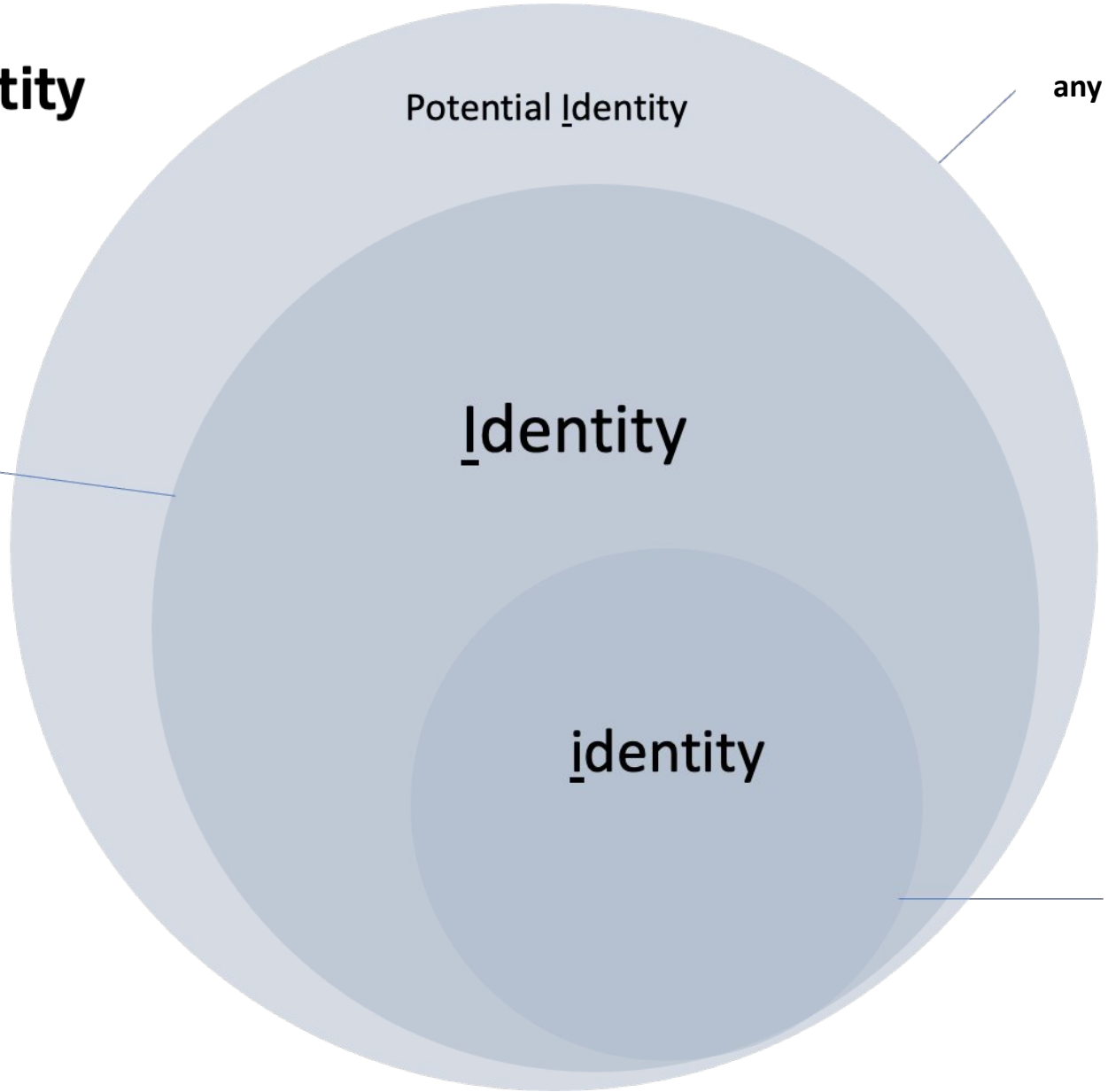
# What is “identity?”




Any given data point can be used to PROVE something about yourself, and therefore, *any data point* can become a constituent of your identity.

HYPERLEDGER FOUNDATION Indicio

# The Everything Identity




**any** data point that may be valuable and can be shared with consent

**any conceivable data point**

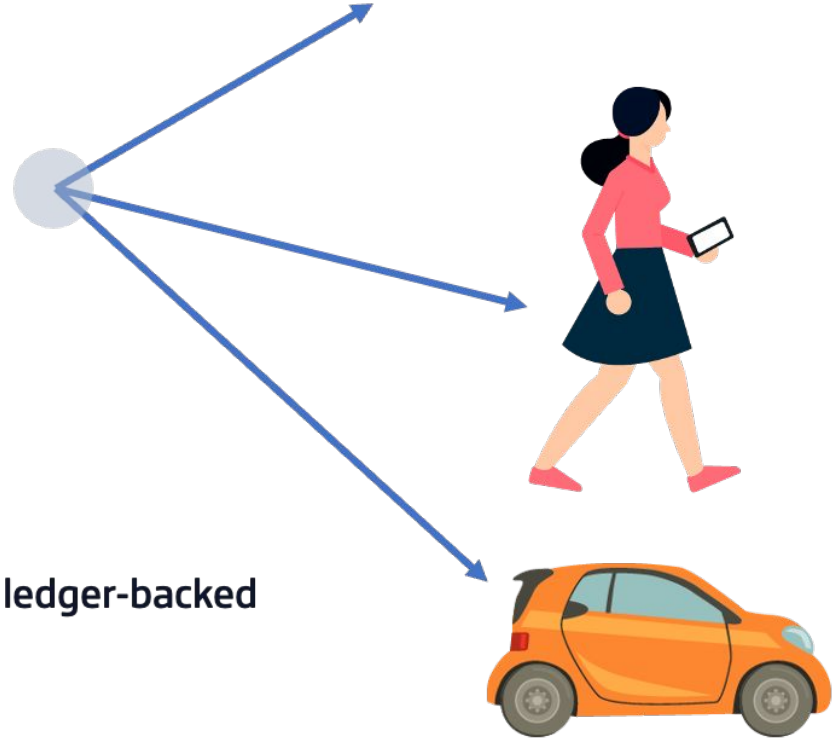
**traditional** biographic and demographic data about a person

HYPERLEDGER FOUNDATION

Indicio

# Identity is Everything!

**(and anything you want it to be)**



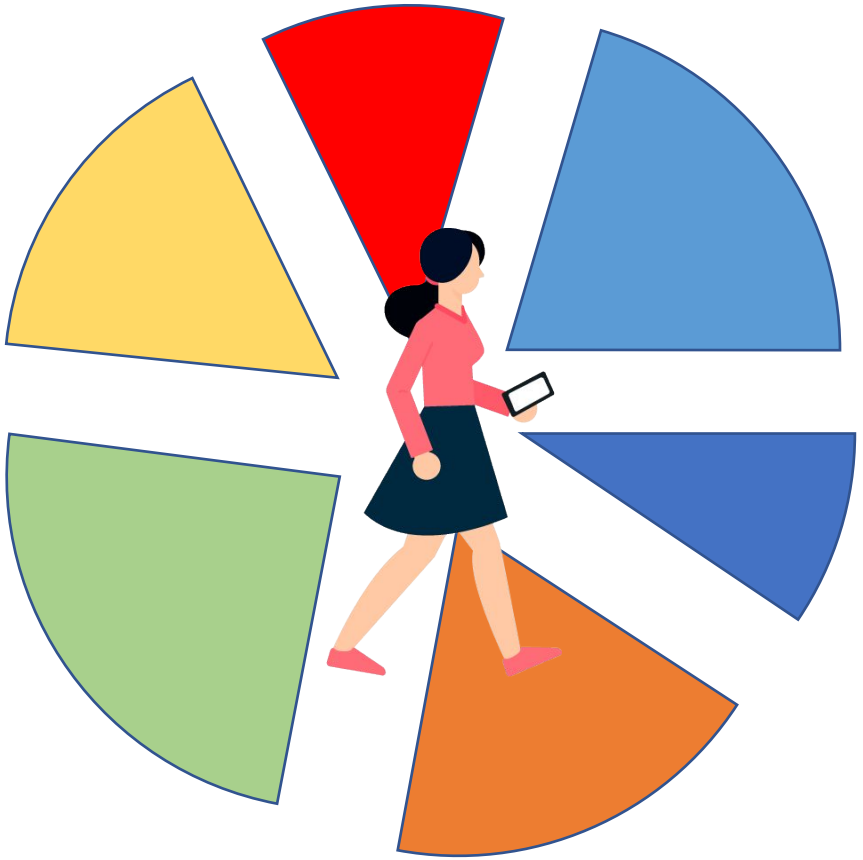
## Any data point that refers to a particular data subject.

- Database stores
- Biometric data or authentication
- Regulatory attestation authority

## All can be used as a form of identity with a ledger-backed Verifiable credential

HYPERLEDGER FOUNDATION Indicio

# Decentralization



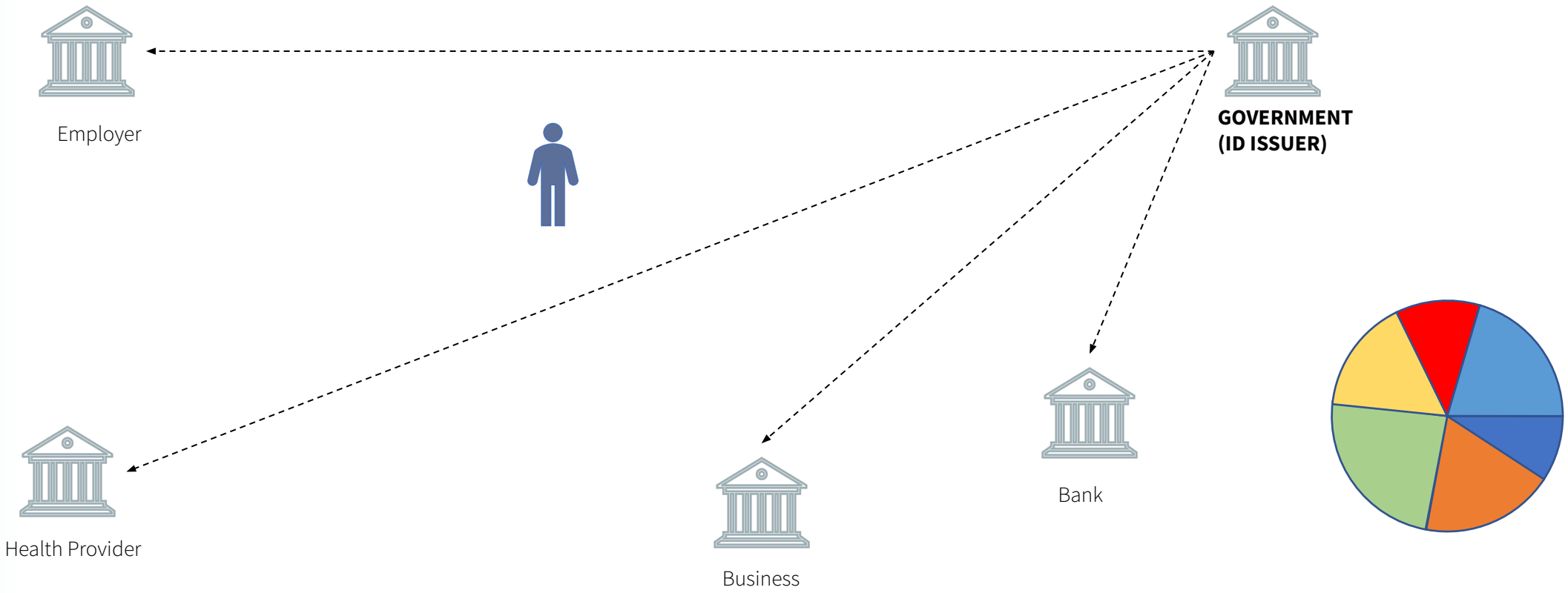
HYPERLEDGER FOUNDATION Indicio

# The problem with centralization

When data is controlled, shared and handled primarily by third parties (not the data subject),

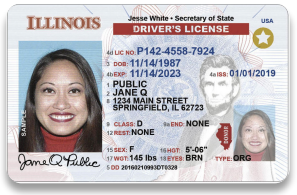
**consent, compliance, tracking and transparency are difficult to achieve**

To gain efficiency and trust, entities must integrate systems, which is difficult, costly, and compromises privacy




HYPERLEDGER FOUNDATION Indicio

# A digital model of the analog world




Government

HYPERLEDGER FOUNDATION

Indicio

# Trust:
## Then and now

HYPERLEDGER FOUNDATION

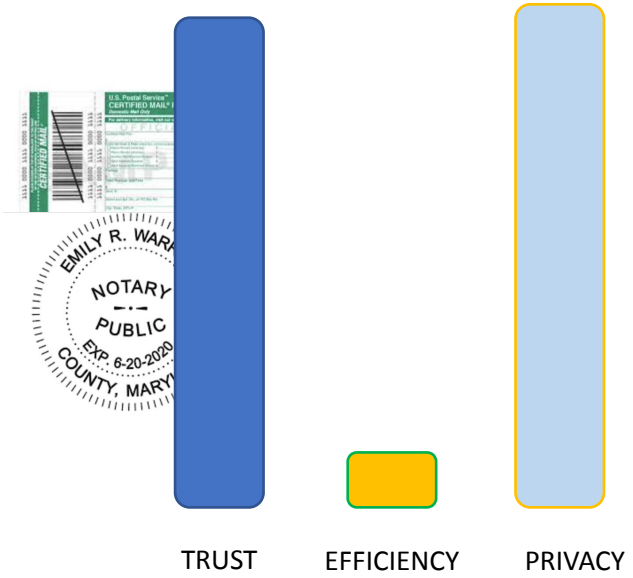
Indicio

# The goal of decentralized identity

Analog functionality with digital efficiency

## Analog World

3200 BC ~ 1964



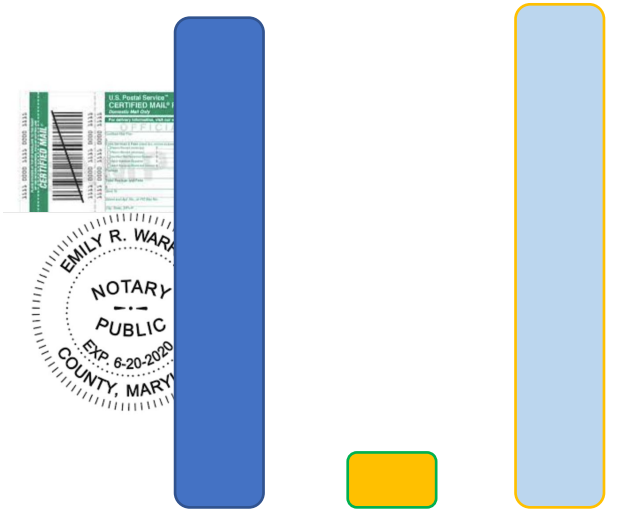

*Physical documents sent, shown, signed, notarized, sealed…*

# The goal of decentralized identity

Analog functionality with digital efficiency

## Analog World

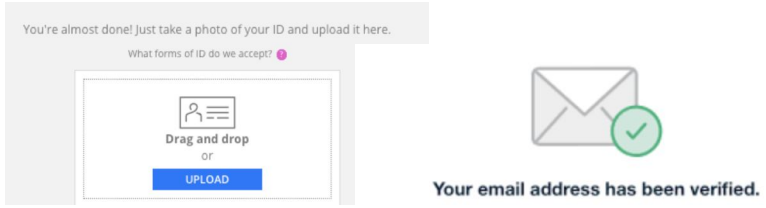
3200 BC ~ 1964

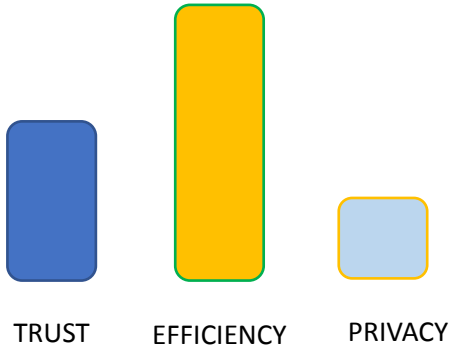



*Physical documents sent, shown, signed, notarized, sealed…*

## Hybrid World

~1964 - 2020



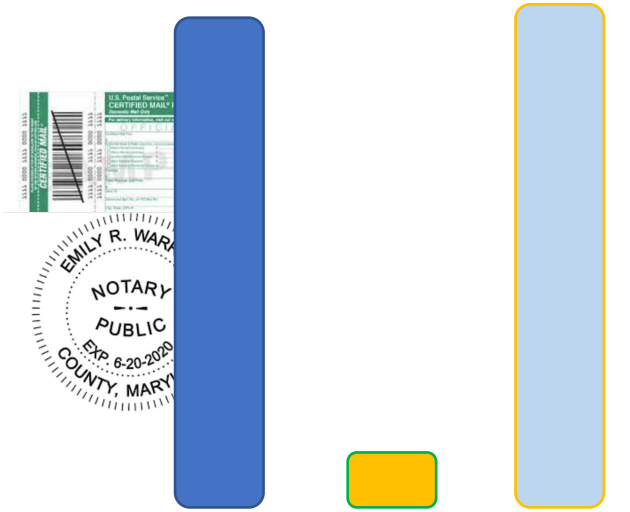

*Duplicate and/or digitized documents sent electronically*

# The goal of decentralized identity

Analog functionality with digital efficiency

## Analog World

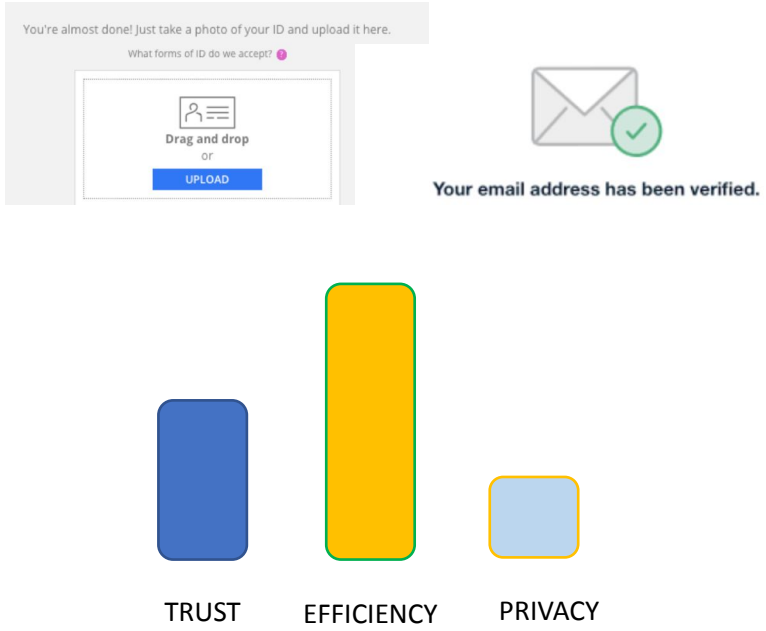
3200 BC ~ 1964




*Physical documents sent, shown, signed, notarized, sealed…*

## Hybrid World

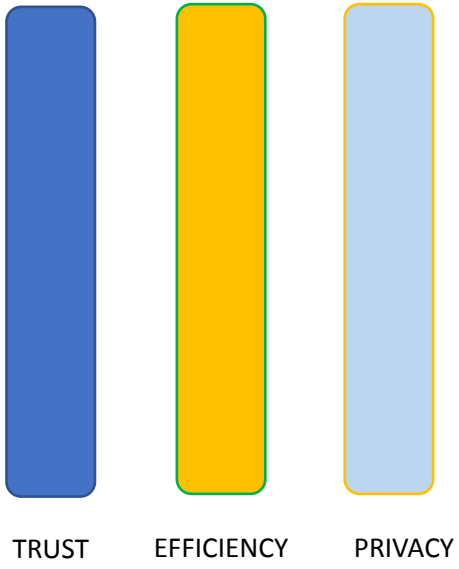
~1964 - 2020




*Duplicate and/or digitized documents sent electronically*

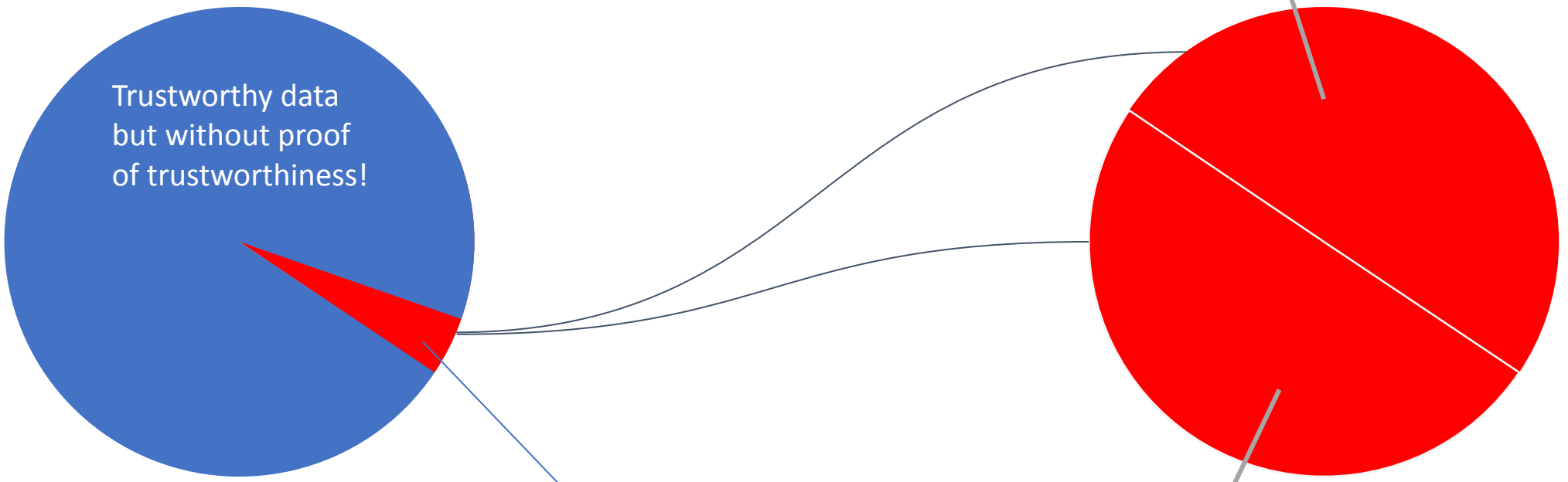
## Decentralized World

~2020 ---




*Verification of digital document authenticity and integrity is possible!*

# Trust in Data:
# Small percentage, big risk




**RISK COST**
from intake of untrustworthy data because you don't want to increase analysis costs

**ANALYSIS COST**
of work to prove trustworthy data is truly trustworthy and weed out untrustworthy data



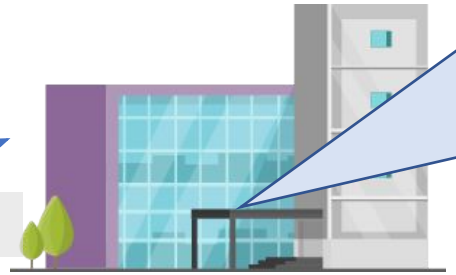
Indicio

# Placing Trust in Representations and Attestations

## Carries Cost and Risk in a Hybrid World


SCAN

Email/Upload



How do I know it's real?
How do I know it hasn't been digitally altered?

How do I know it's coming from the person they claim to be?

**No one has ever used a fake email, or had their email hacked, have they??**

**2FA with email is fine… really…**

# What is trust in data?

Trust in data comes from three parts:

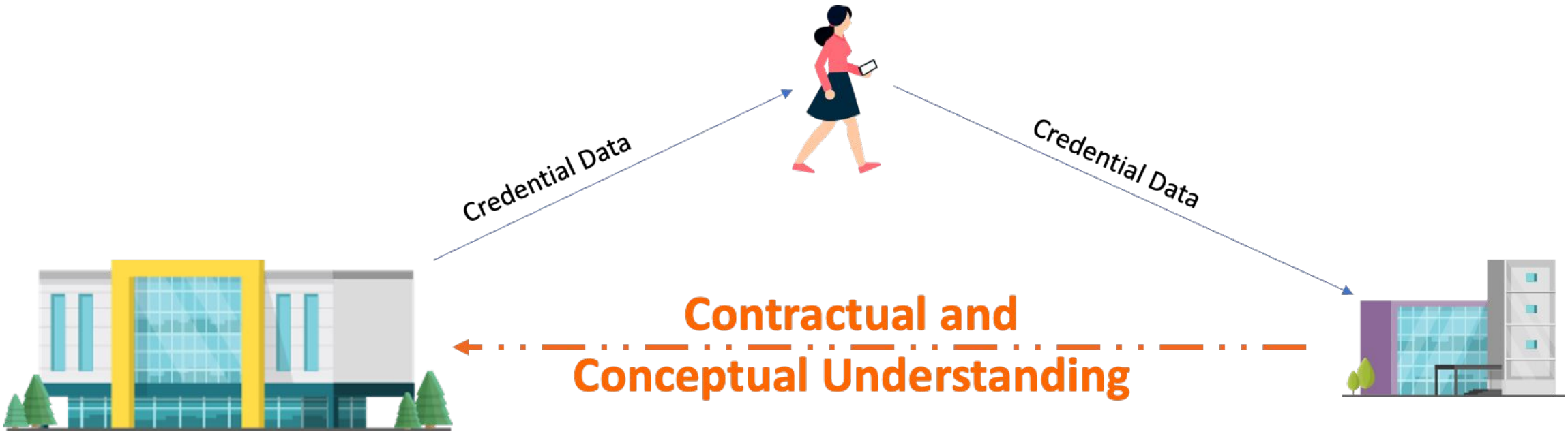
1. **Authenticity** Being able to identify the source of the data
   → *Does it come from the place it claims to be from?*
2. **Integrity** Being able to identify if the data is "real," or has arrived "as-issued"
   → *Has it been altered or tampered with?*

# What is trust in data?

Trust in data comes from three parts:

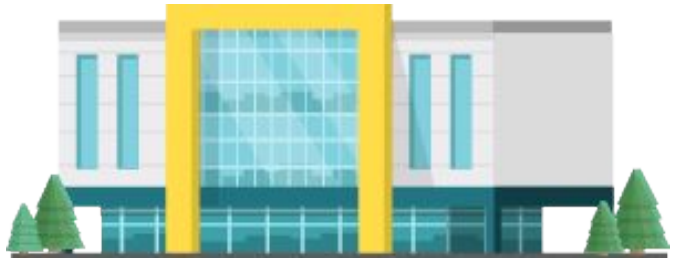
3 **Usefulness** Once provenance is assured, how well do I know the originator of the data?

→ *Do I trust their processes, regulatory environment and compliance practices?*



# Useless if untrustworthy?

**(it's actually more useful)**



Credential Issuer
(identity data source)

**INSTANT**
EFFICIENCY

**Trusted Source?**

**Untrusted Source?**

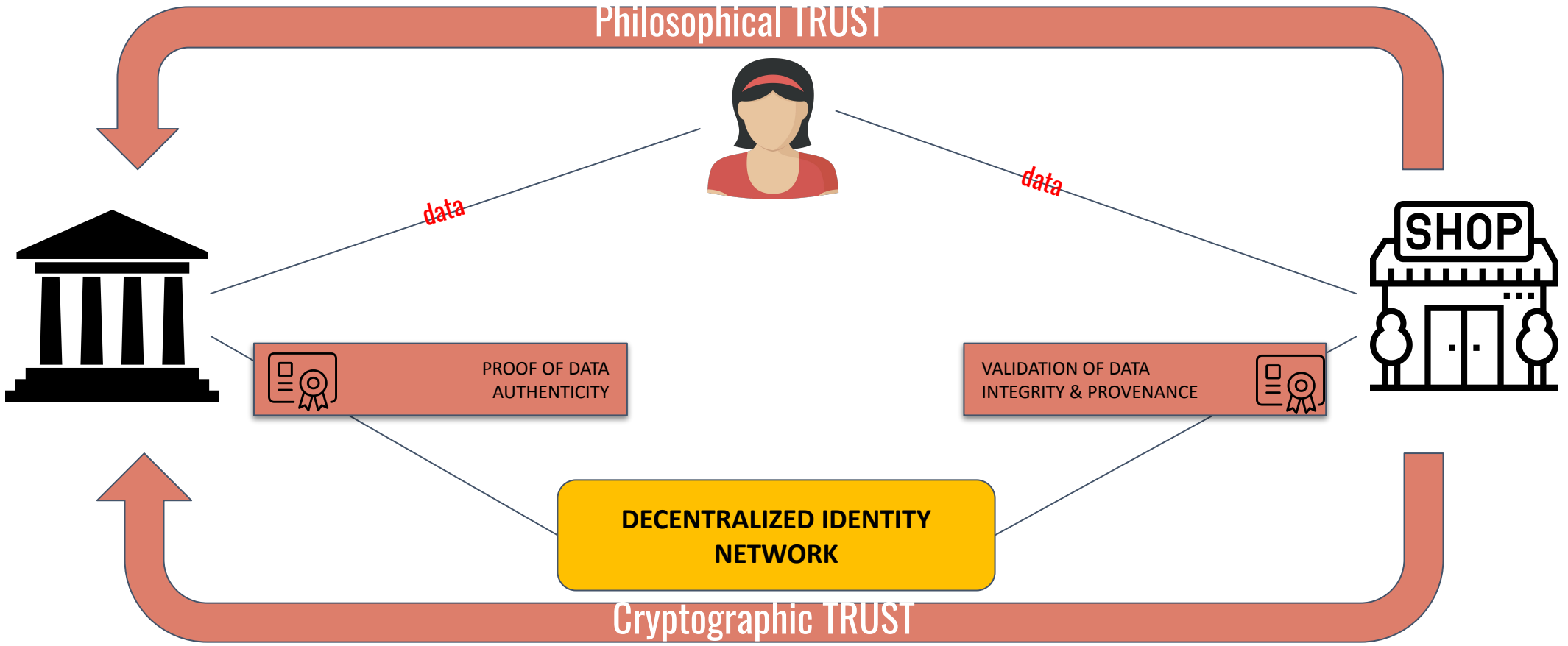
**INSTANT**
RISK
REDUCTION

Credential Verifier
(identity data receiver)

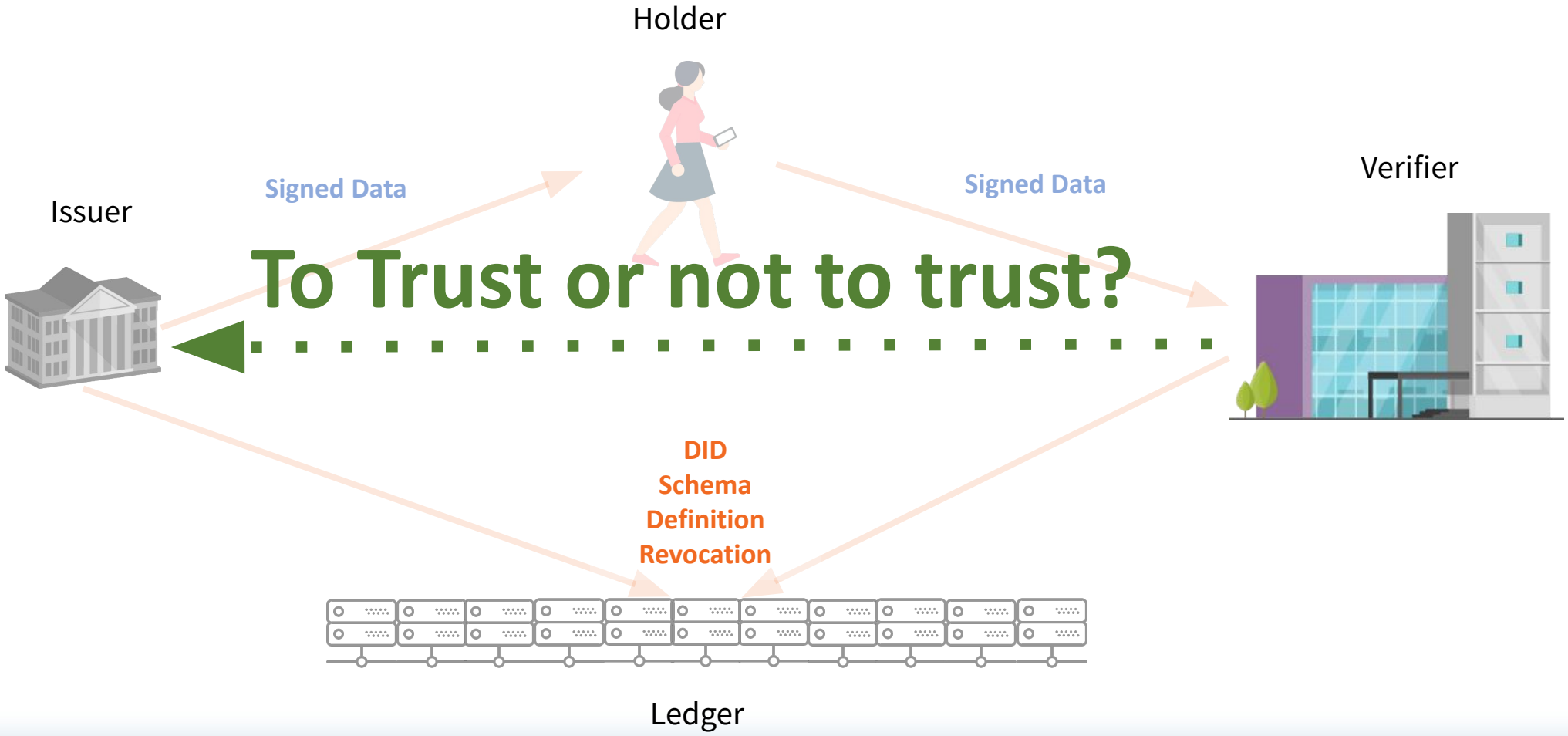


Indicio

# The Trust Model

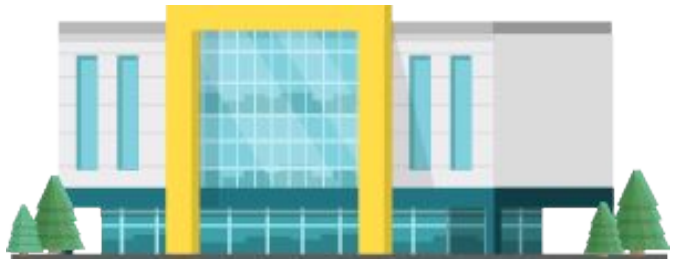


# That is the question:
# And the answer is up to each participant – autonomy and control

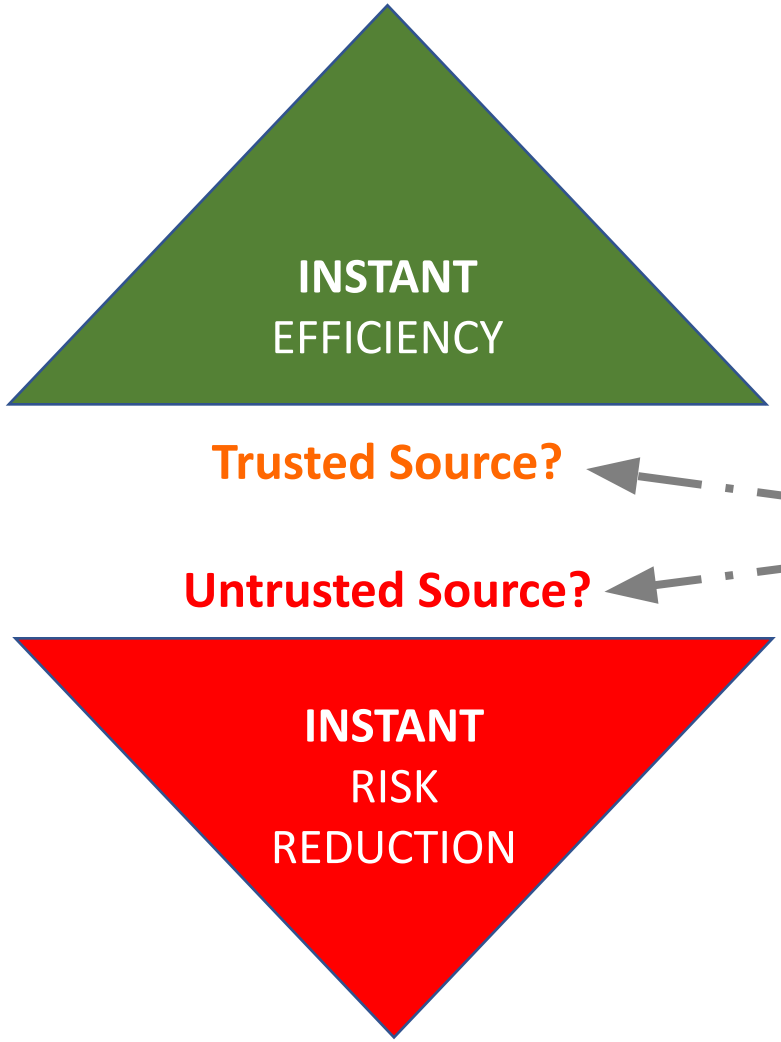


# Instantly Actionable Data

## Verified Data increases efficiency and reduces risk instantly



Credential Issuer
(identity data source)




Credential Verifier
(identity data receiver)



Indicio

# Efficiency and Trust without Integration or Centralization

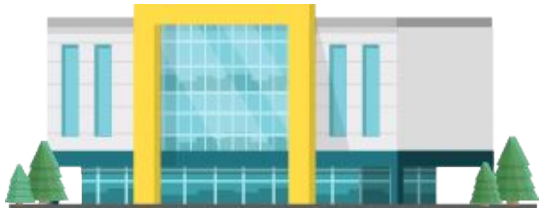
## Fostering commercial relationships via credential value

Verifiable DTC
Passport Biometric
Data

**Border Control Agency**

**Airline for efficient proof of identity for other services**

Bags, Alcohol purchase,
Unaccompanied Minor Transport



**Financial Services**

Trusted issuers have already done KYC/AML processes


**Hotel for efficient check-in**

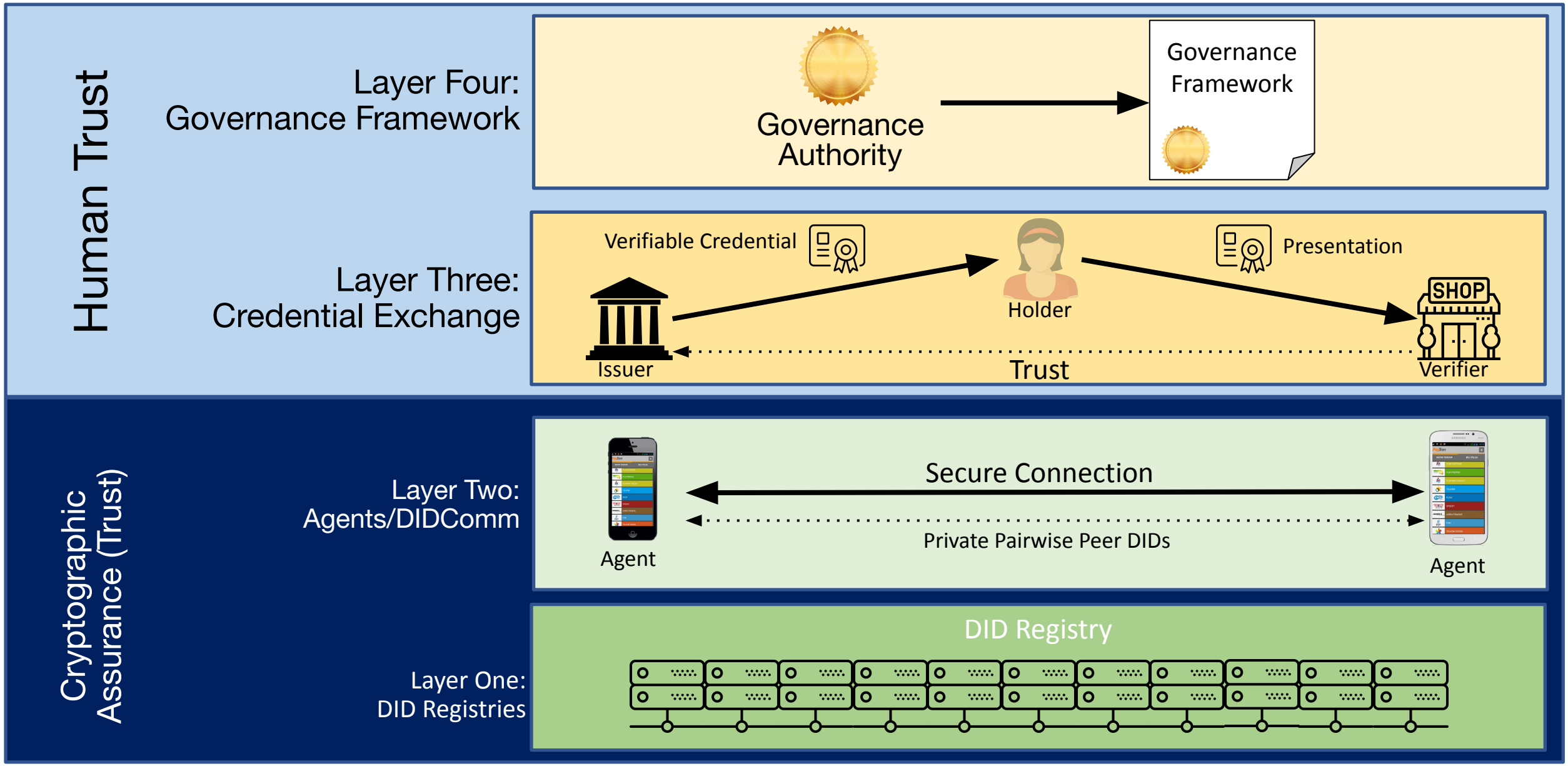
Instant proof of identity and check-in

**Car Rental for instant pick-up**

Use to sign rental agreements, purchase ancillary services and efficiently move through a complicated workflow

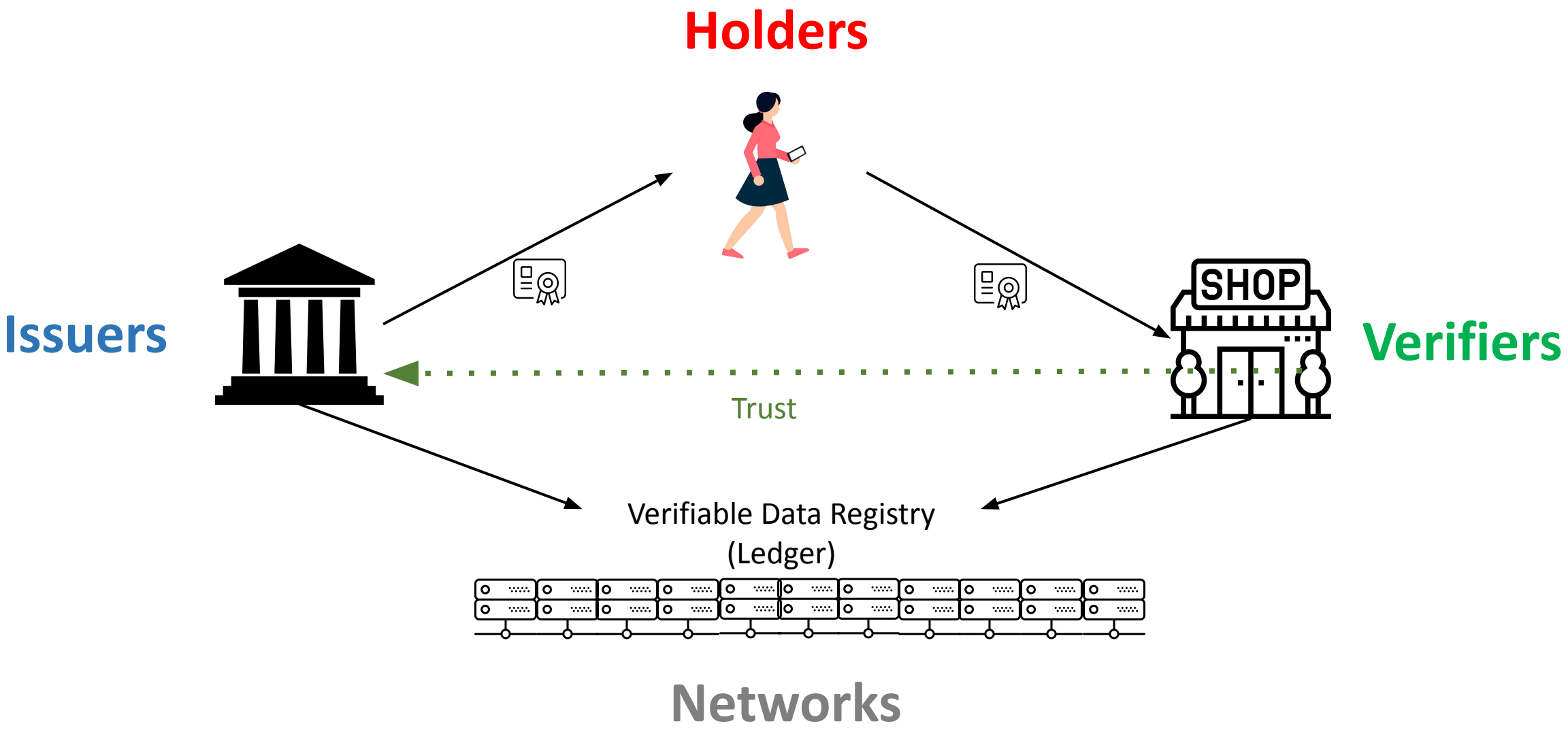


Indicio

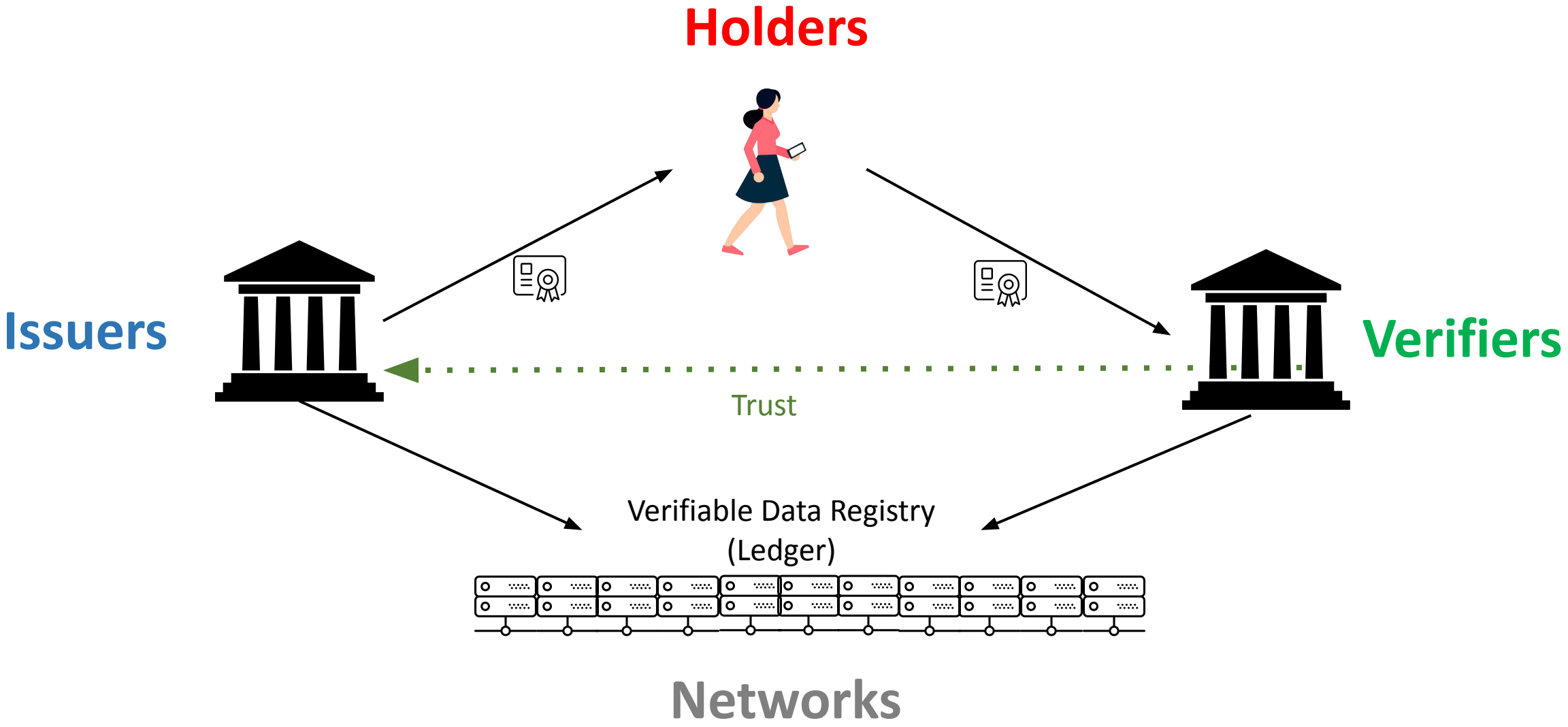


# The Verifiable Credential Trust Triangle

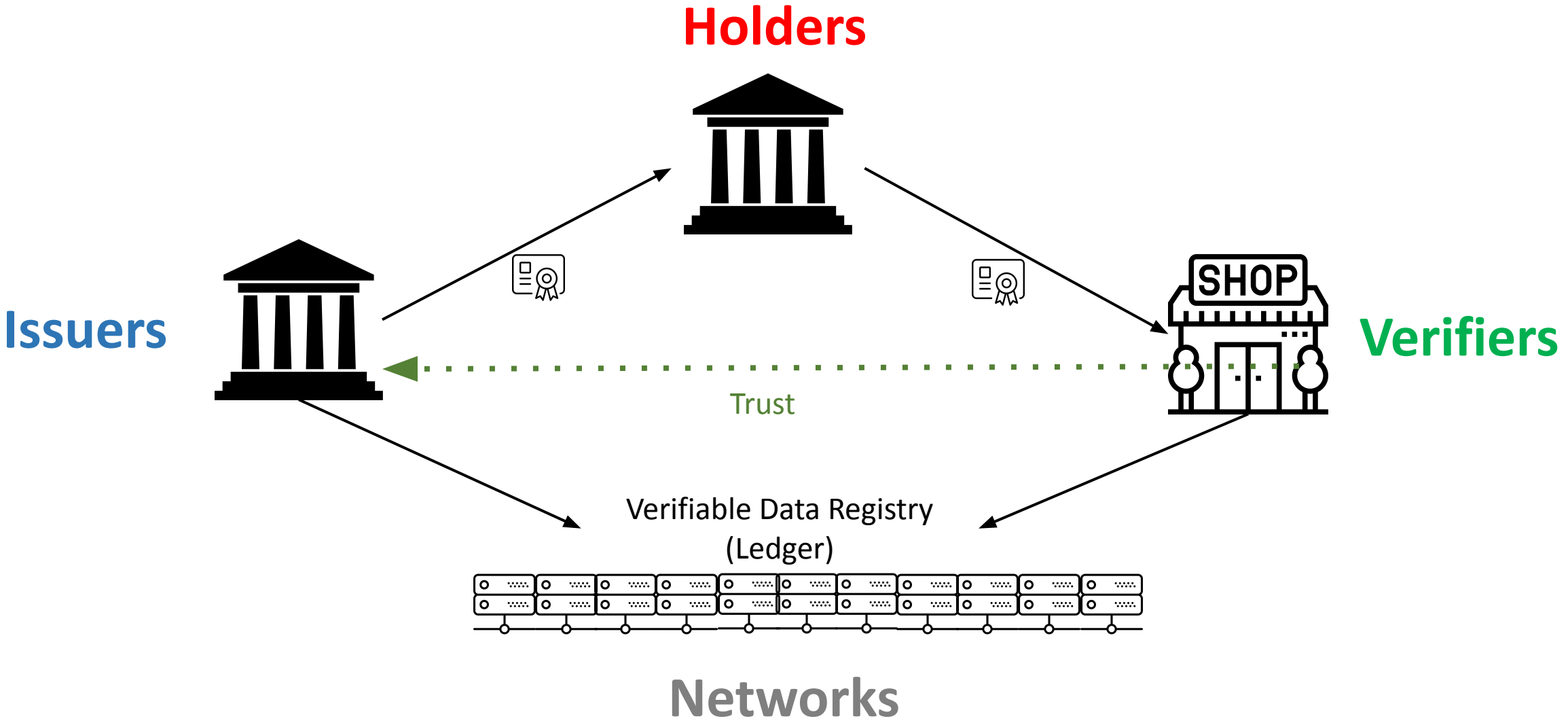
The participants:



# Roles are not mutually exclusive



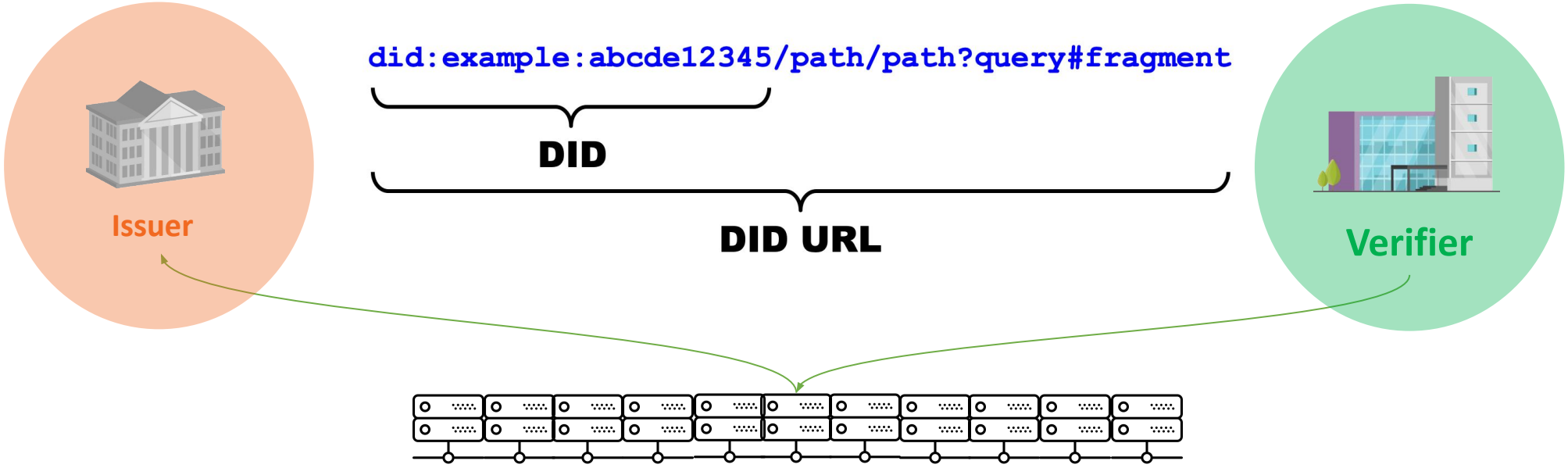
# Roles are not mutually exclusive



# Decentralized Identifiers (DIDs)

## Secrets management

- A Decentralized Identifier (DID) is a URL that returns a DID Document
- A DID subject is an entity (person, organization, or thing)




Resolution of a DID to a DID Document provides means to:

- Authenticate keys
- Send messages to the Subject

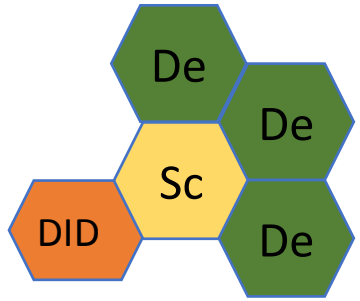


Indicio

# DID-Schema-Definition

## Relationships

Definitions provide a means of managing relationships between verifiers, holders and issuers, where the issuer *defines* the attributes available to a particular set of verifiers

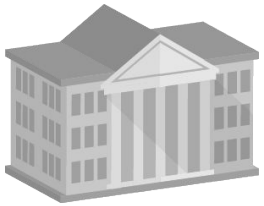



*Driver License 1.0*
Last Name
First Name
Date of Birth
Eye Color
License Number
Issue Date
Expiration Date

De

*Driver License 1.0*
Last Name
First Name
Date of Birth
~~Eye Color~~
~~License Number~~
~~Issue Date~~
Expiration Date

De



Gov


Sc

*Driver License 1.0*
Last Name
First Name
Date of Birth
Eye Color
License Number
Issue Date
Expiration Date

De

*Driver License 1.0*
Last Name
First Name
Date of Birth
~~Eye Color~~
License Number
Issue Date
Expiration Date

Indicio

# Hyperledger Indy Network

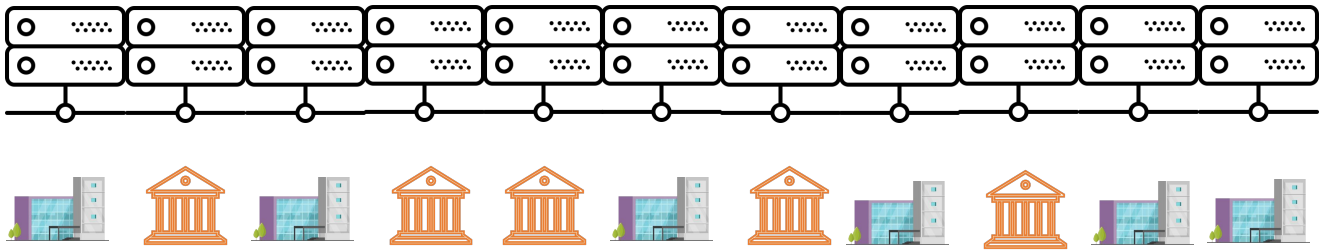


Indicio

# Hyperledger Indy Network

**Nodes**

support and create a network





Indicio

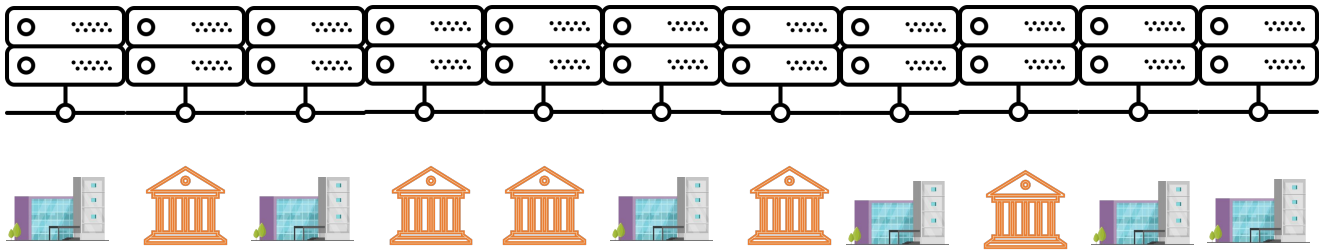
# Hyperledger Indy Network

Enterprise Agent

Edge Agents

**“Agents”**

Are simply **software programs** that act on behalf of a participant to perform a function of interacting with the network and ledger

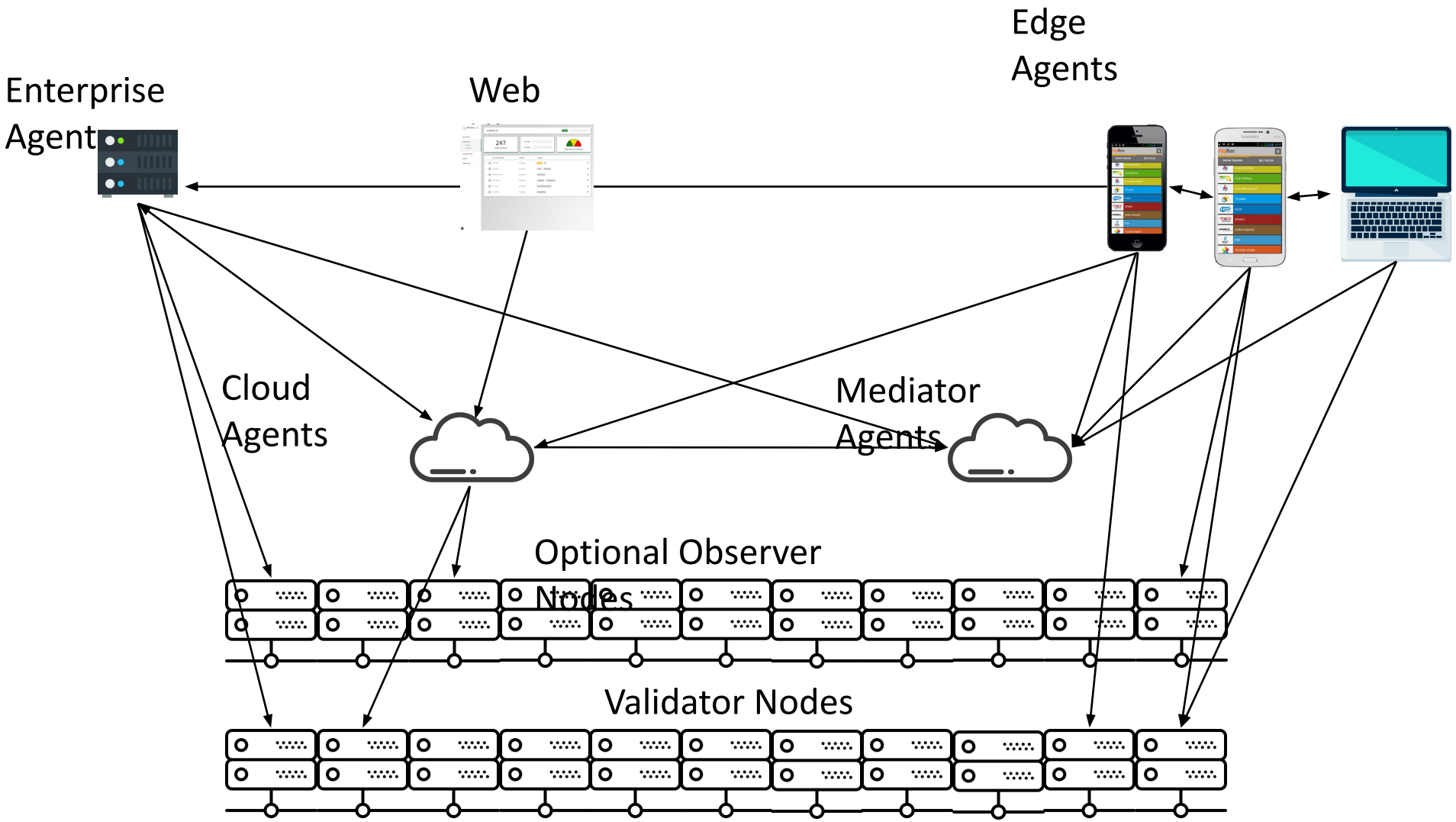




Indicio

# Hyperledger Indy Network

How is it organized?



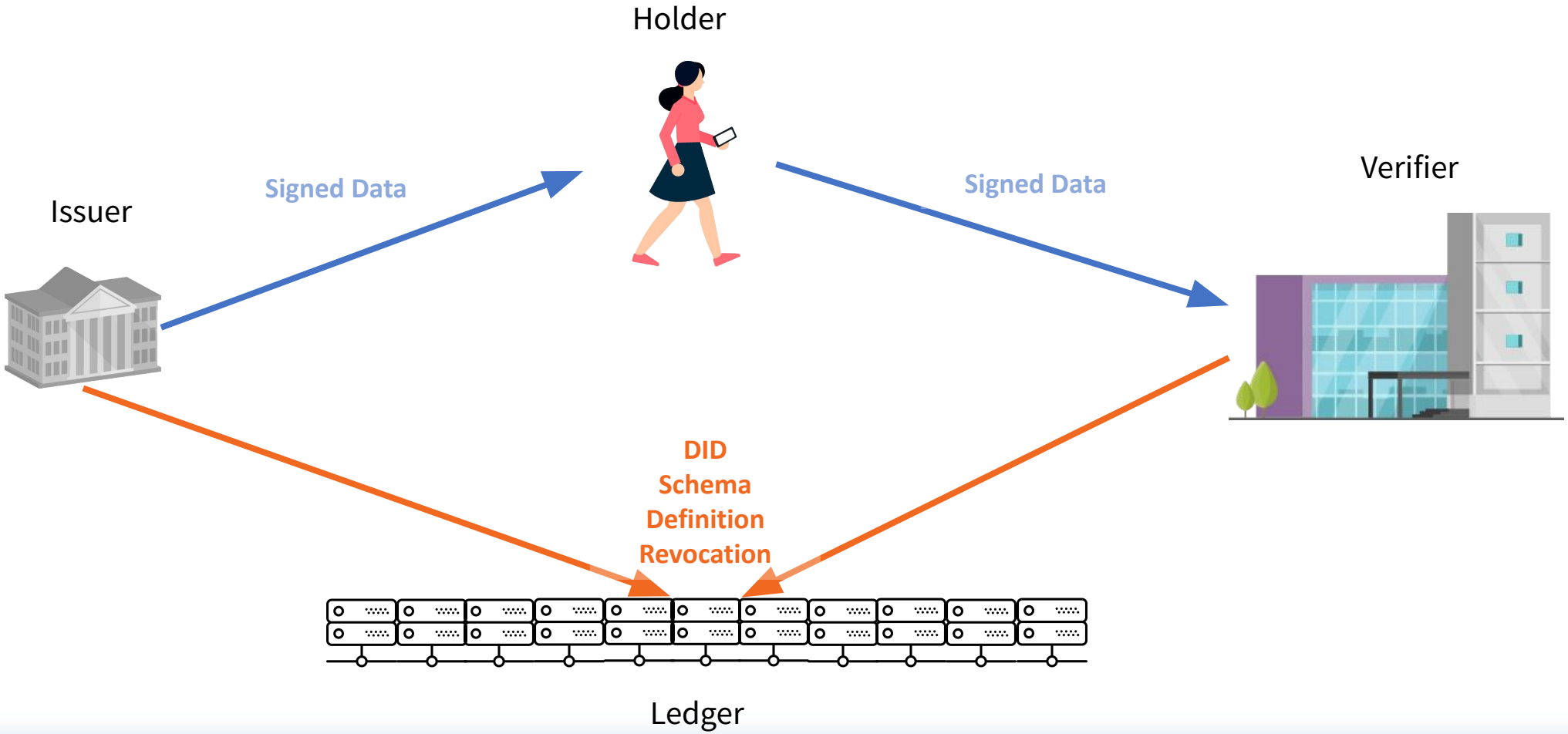



Indicio

# PII (and all Credential Data) stays with data's owner or authorized controller

Privacy-by-design and compliance protections

**The ledger is a means of verifying the authenticity/source and integrity of data!**



HYPERLEDGER FOUNDATION Indicio

# Code architecture

Enterprise, Mobile Apps

Hyperledger Indy Plugins

Aries Agent

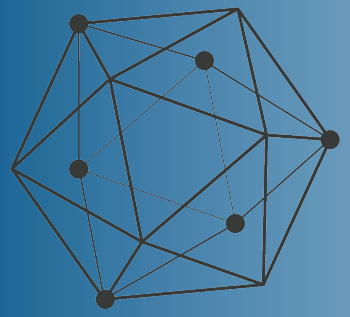
Hyperledger Indy Node (Identity Transactions)

Aries SDK

Hyperledger Indy Plenum (Consensus)

Indy Resolver

Hyperledger Ursa (Cryptography Library)

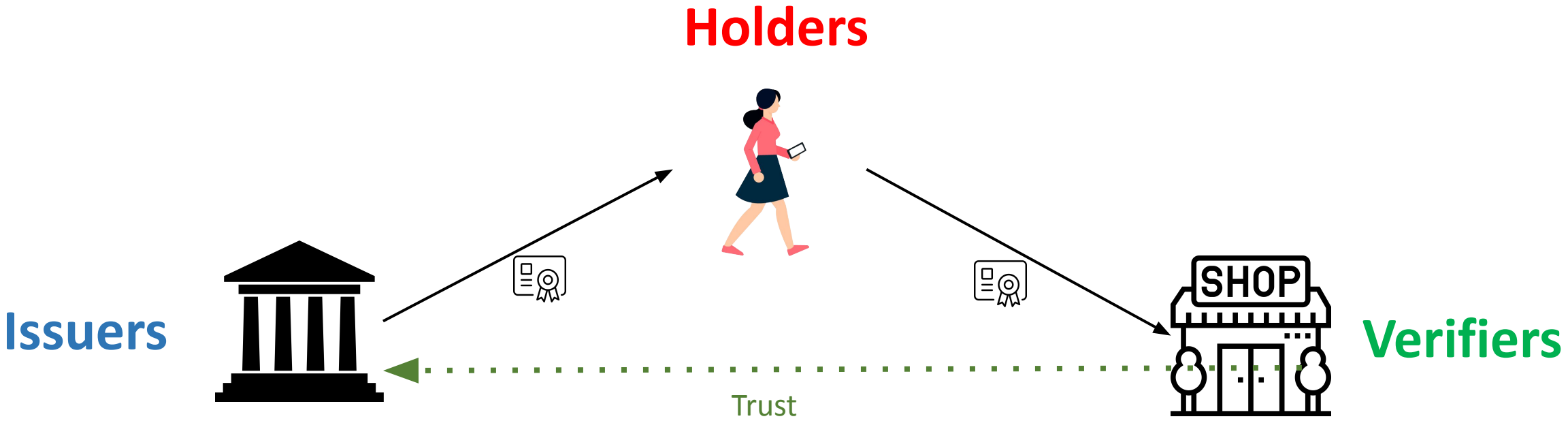


# Notes on components
## roles and conventions

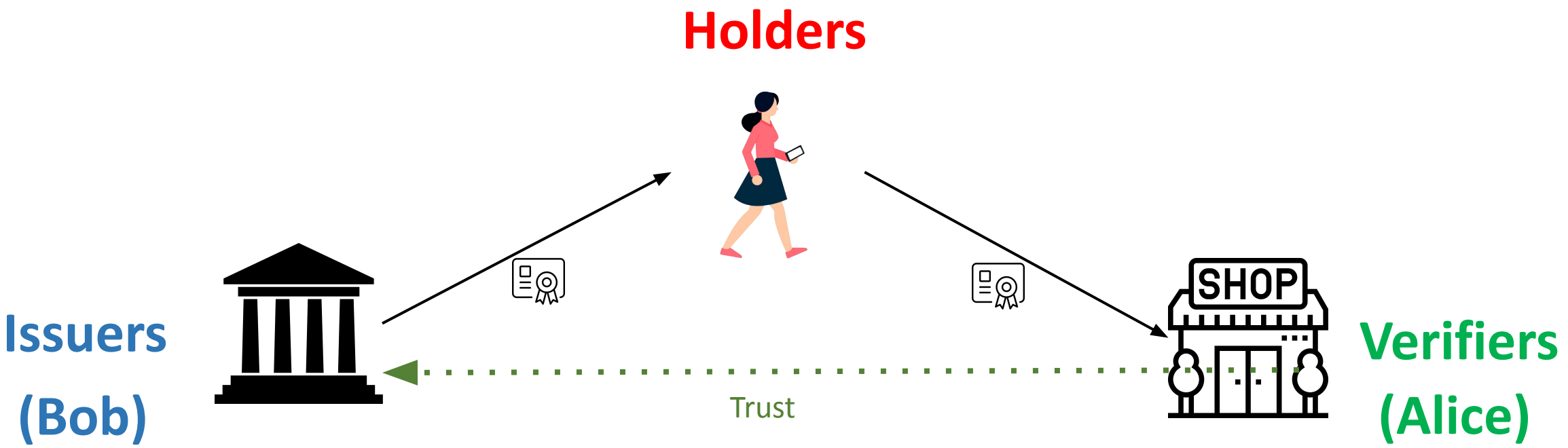
HYPERLEDGER FOUNDATION

Indicio

# Roles and Convention

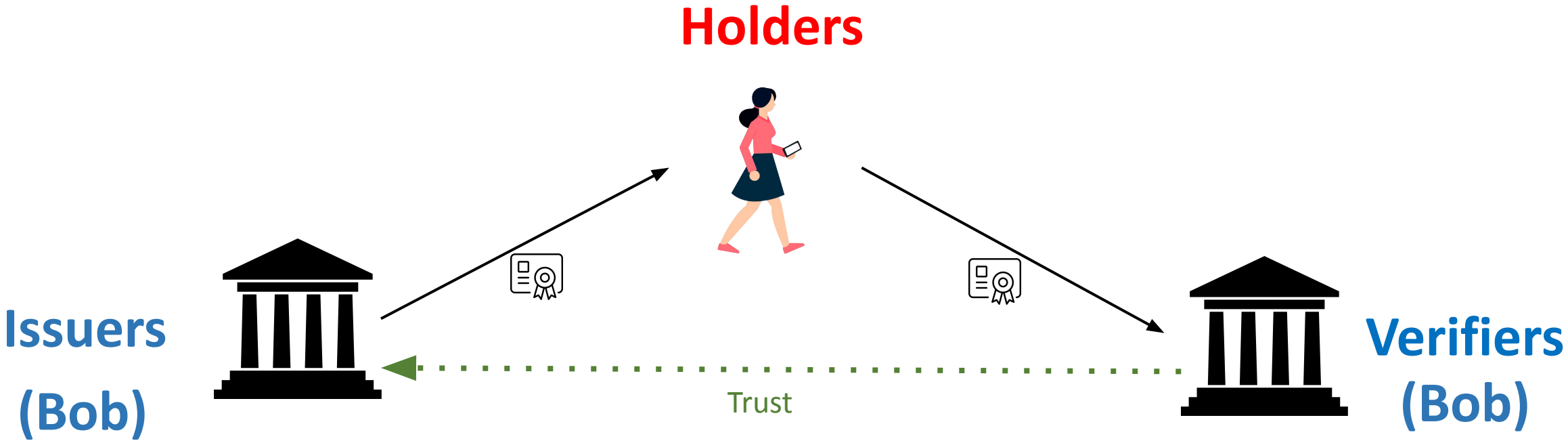


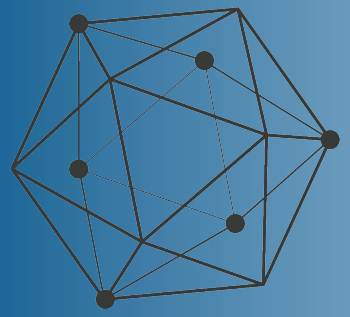
# Stories of Bob and Alice



# Roles may overlap

## Particularly those of ***Issuer*** and ***Verifier***





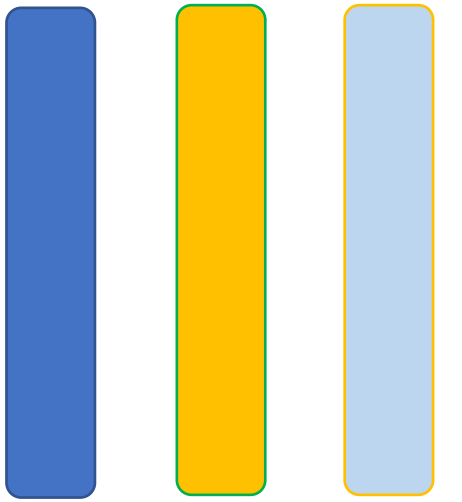
# Value

HYPERLEDGER FOUNDATION

Indicio

**Decentralized World**

~2020 ---




*Verification of digital document authenticity and integrity is possible!*

# Privacy

## Protecting individual data through **Privacy by Design**

- Use of Decentralized Identifiers (DIDs)
- Peer DIDs are pairwise unique
- No PII on the ledger!
- Zero-knowledge methods
- Verifiers don’t contact issuers
- Compliance

# Next:
# Technical Overview of Decentralized Identity

Tuesday 27 February 2023 12:00 EST

HYPERLEDGER FOUNDATION

Indicio