



Build Your Identity Solution Using Hyperledger Aries

Thursday, January 20, 2022
8 AM - Noon PST / 11 AM - 3 PM EST

WORKSHOPS

Co-developed with: **Indicio**

Instructors:

Sam Curren



Lynn Bendixsen



Daniel Bluhm



Scott Harris





James Schulte
james@indicio.tech

Director of Business Development

Support and Help

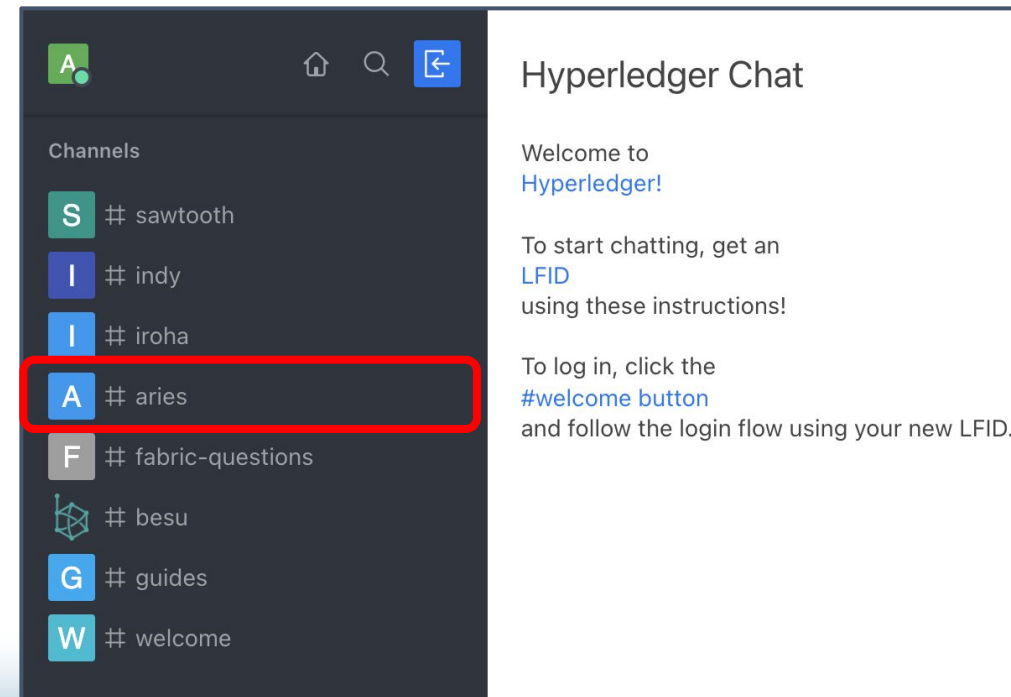
Workshop materials:

<https://wiki.hyperledger.org/display/events/Hyperledger+Aries+Training+Workshop+Prerequisites>

Have questions or need help during workshop?

Use the #aries channel on Hyperledger Chat

chat.hyperledger.org/home



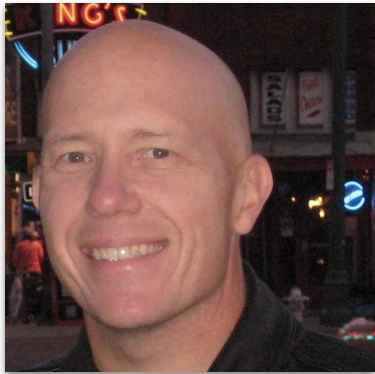
What is Decentralized Identity?

Scott Harris
VP Operations, Indico



HYPERLEDGER
FOUNDATION

Indicio



Scott Harris
scott@indicio.tech

VP Business Operations

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.

Show

Sign in

[Forgot password?](#)

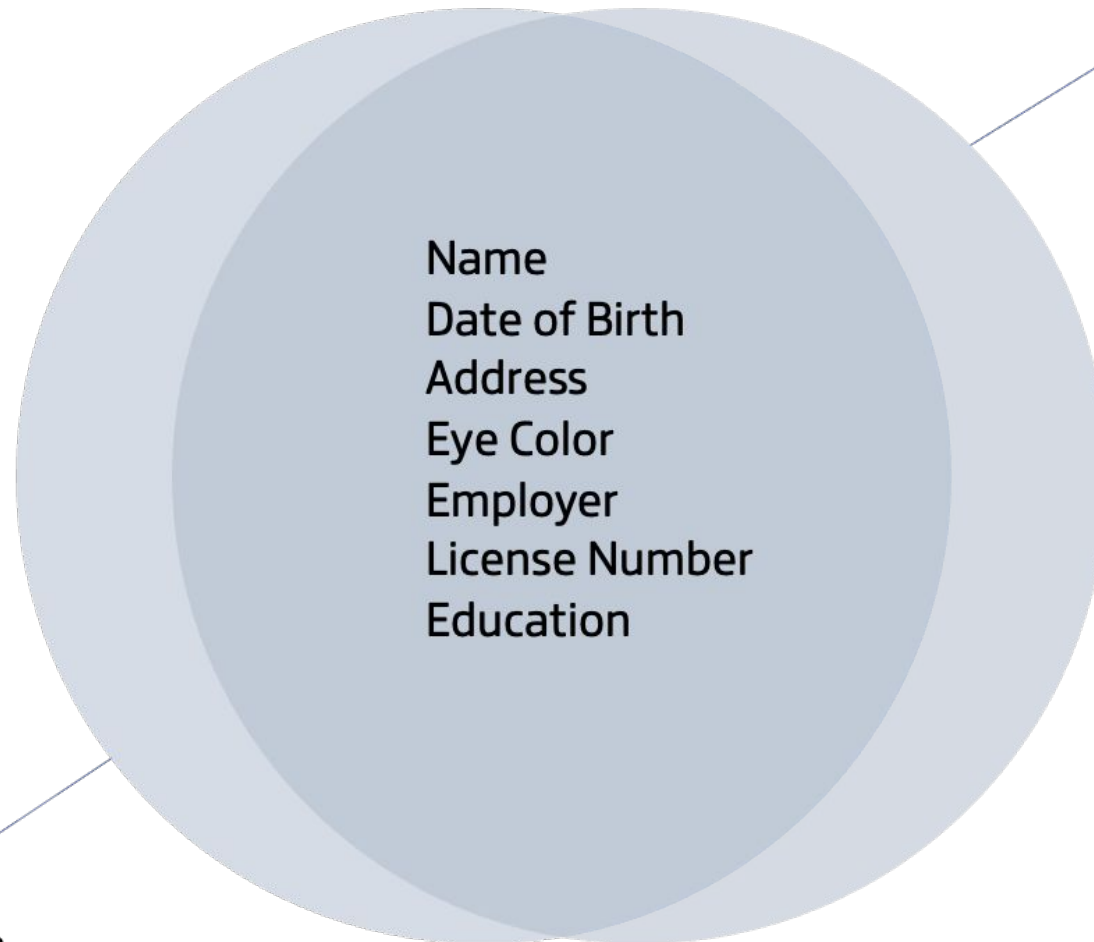
New to LinkedIn? [Join now](#)



Indicio

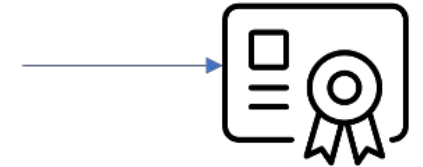
What is intity anyway?

Who is this person?



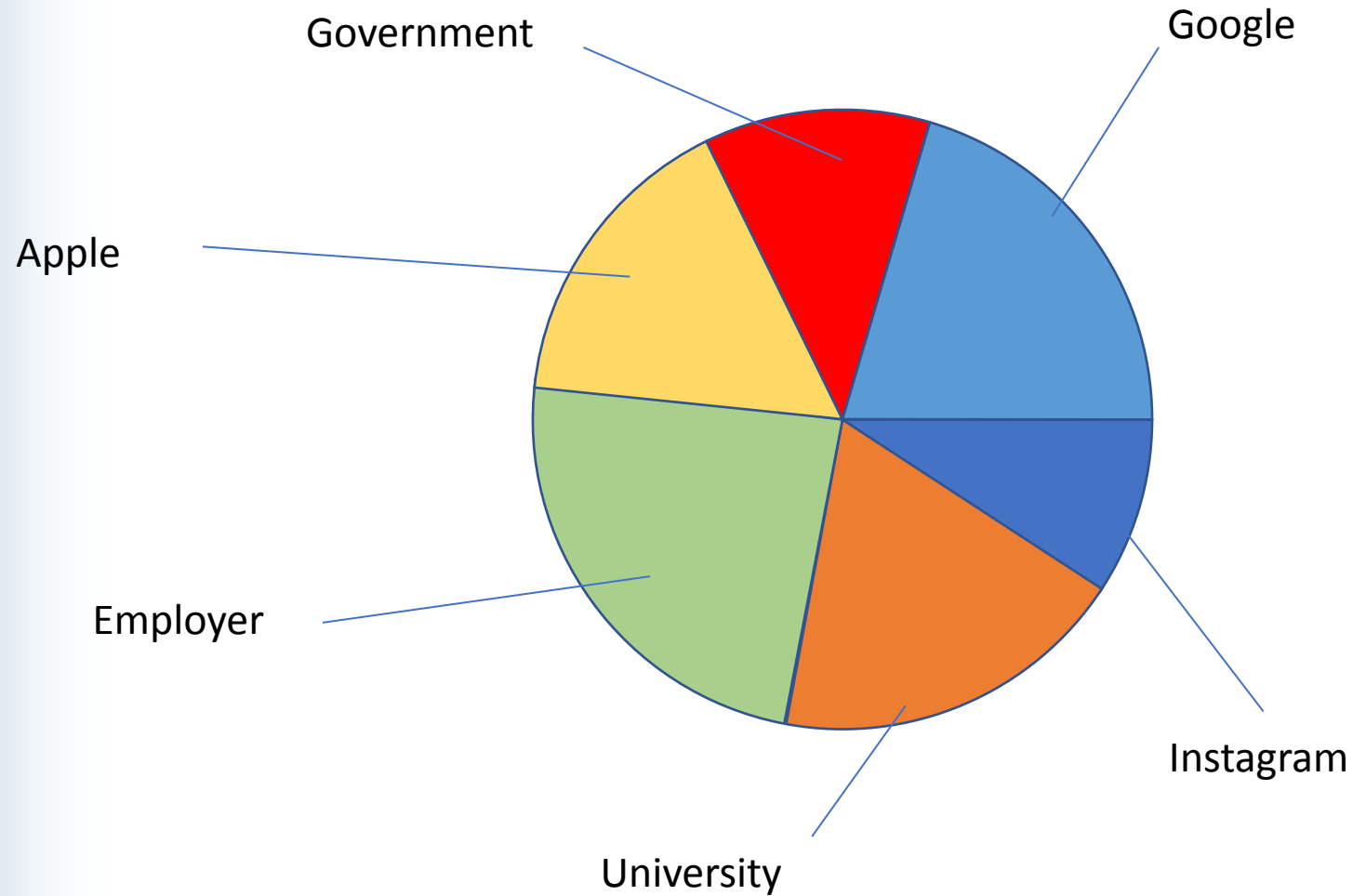
Biographic Data

Demographic Data

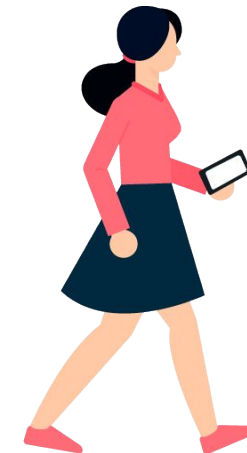


Verifiable
Credential

What is “identity?”

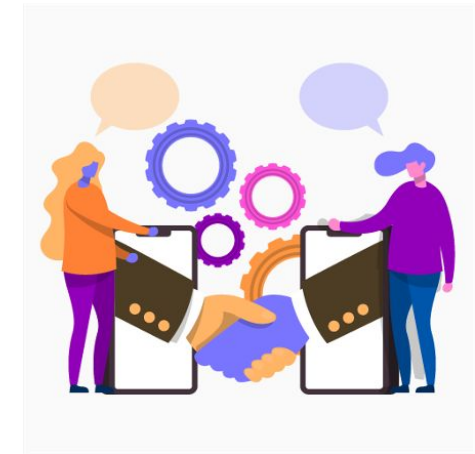
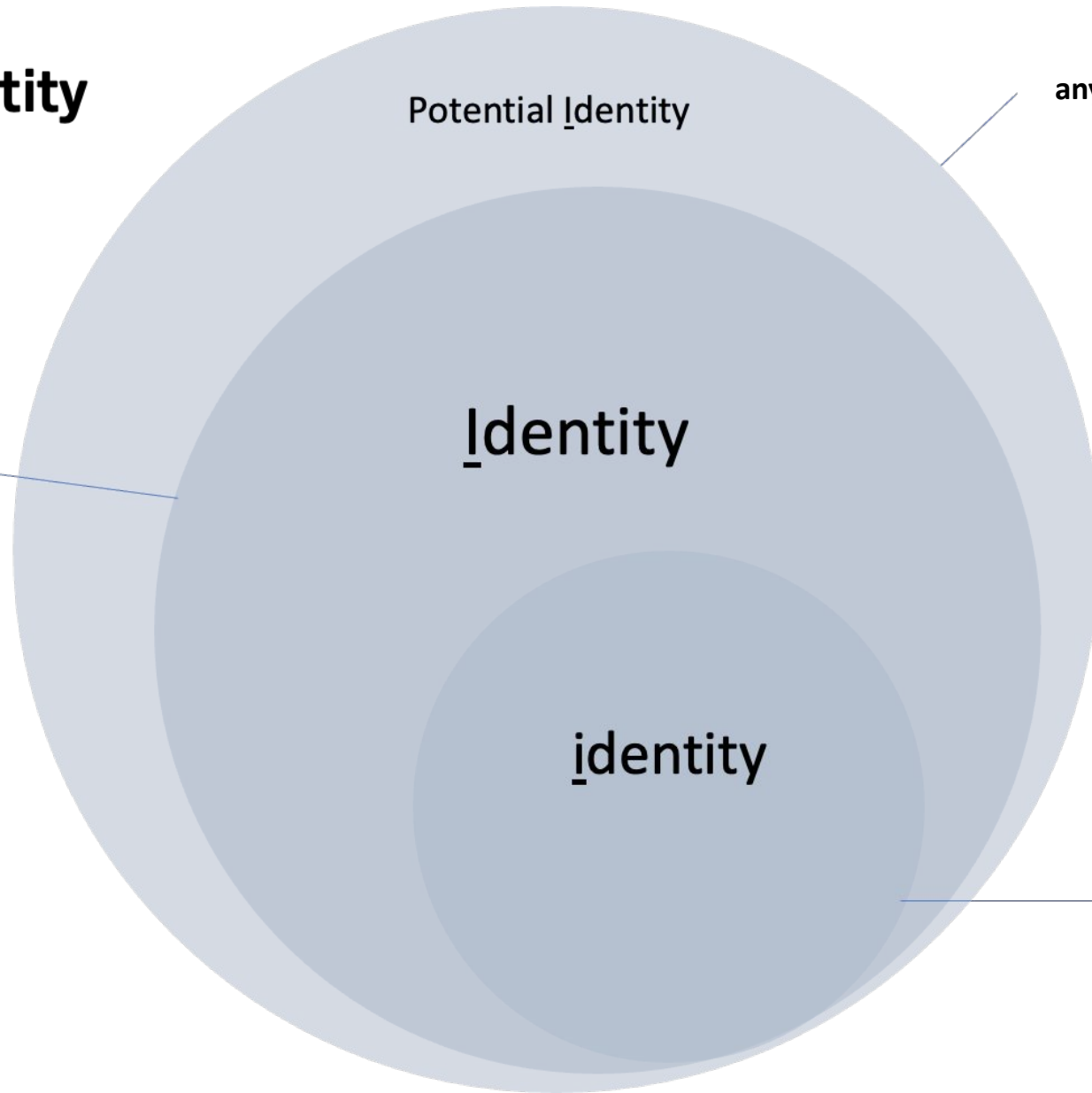


Any given data point can be used to PROVE something about yourself, and therefore, *any data point* can become a constituent of your identity.



The Everything Identity

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



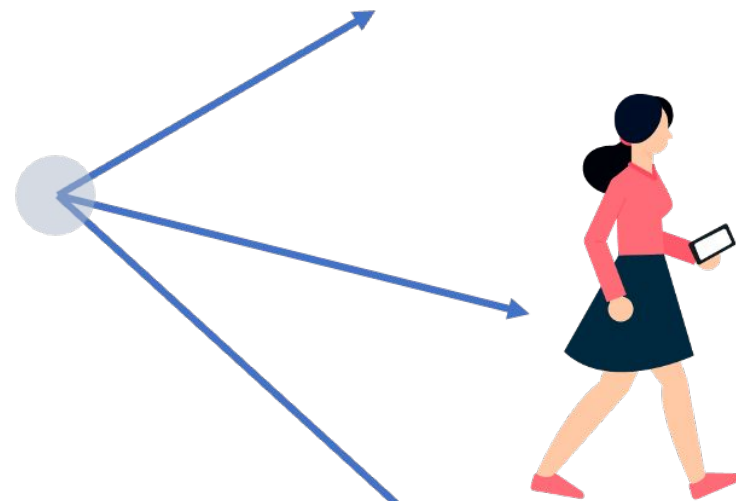
Intity is Everything!

(and anything you want it to be)

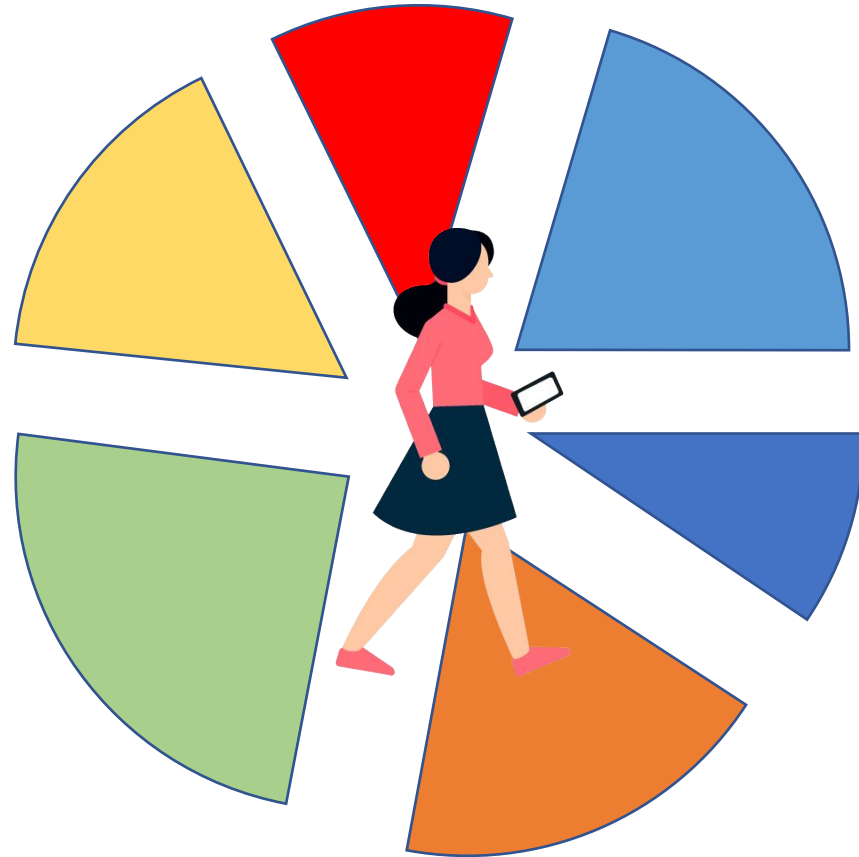
Any data point that refers to a particular data subject.

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

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



Decentralization



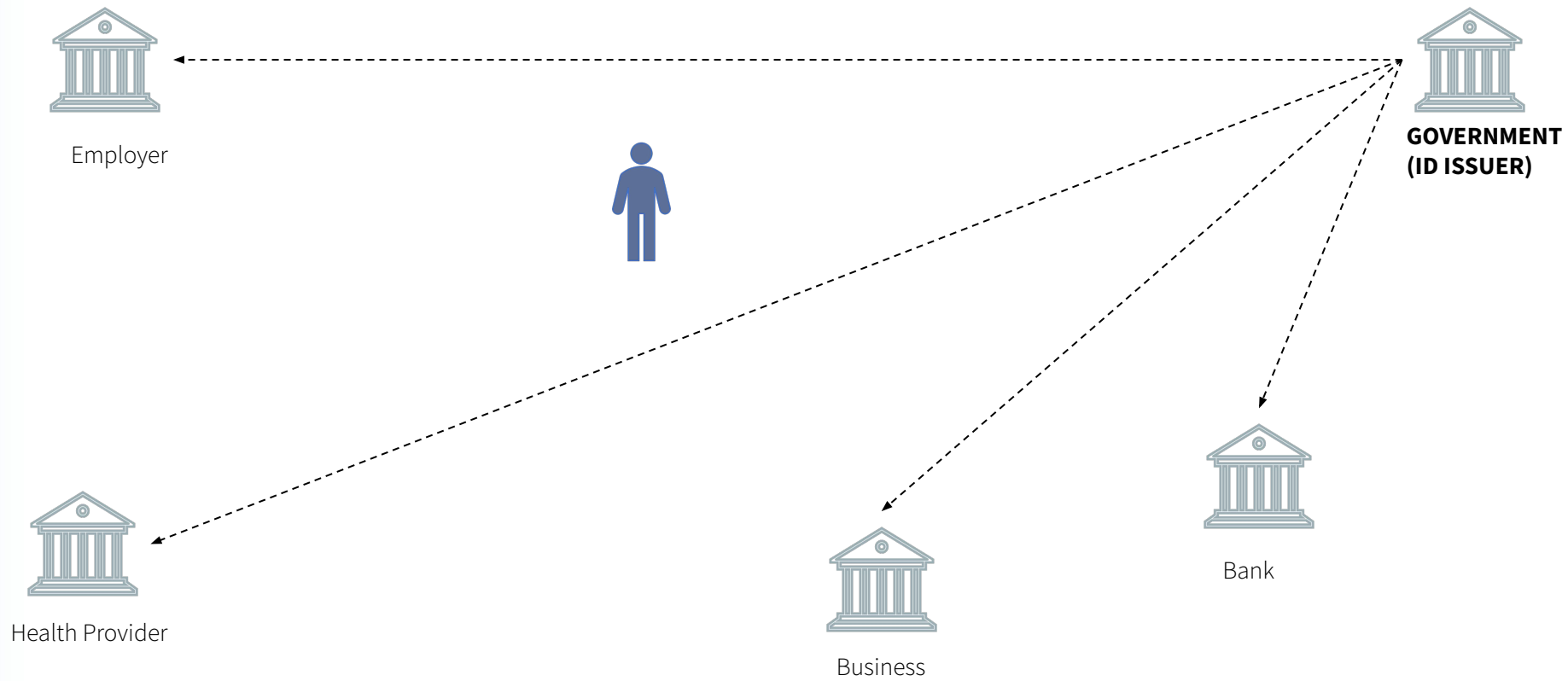
A set of data that refers to a particular data subject

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

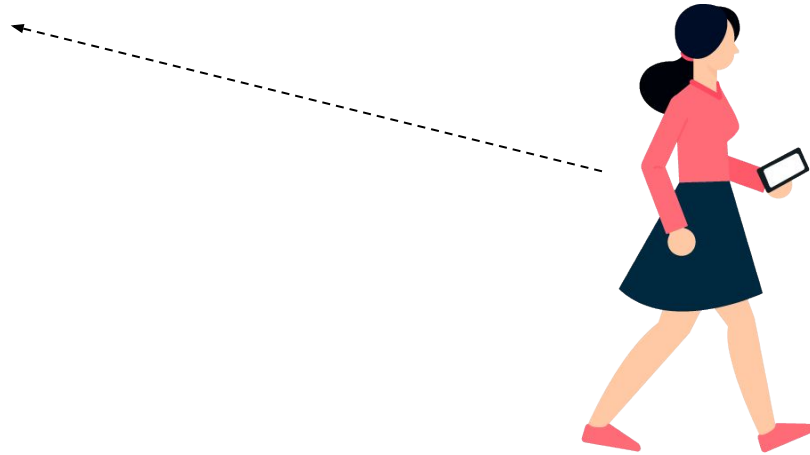
To gain efficiency and trust, entities must integrate systems, which is difficult, costly, and compromises privacy

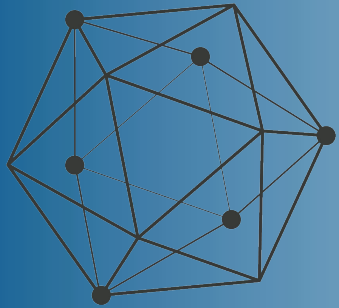


A digital model of the analog world



Government





Trust: Then and now



HYPERLEDGER
FOUNDATION

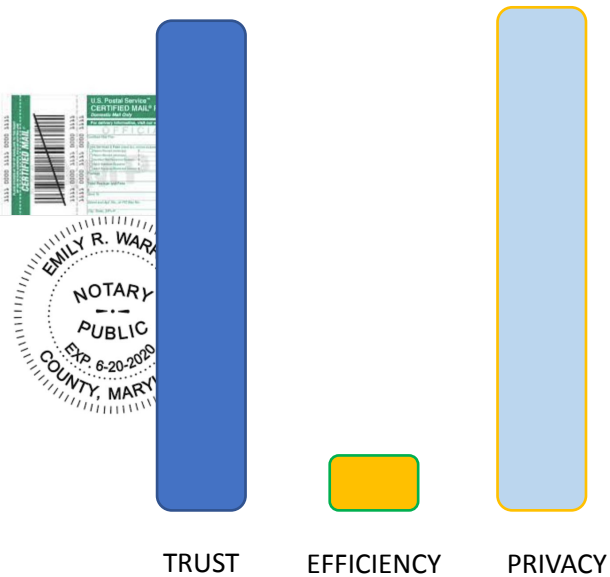
Indicio

The goal of decentralized identity

Analog functionality with digital efficiency

Analog World

3200 BC ~ 1964



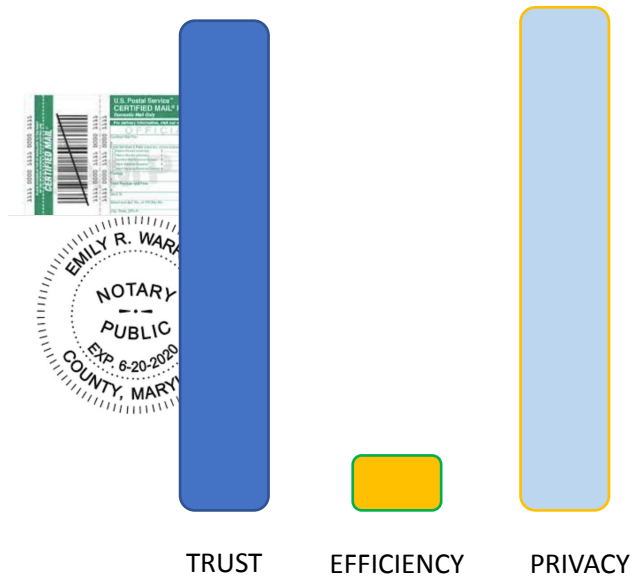
Physical documents sent, shown, signed, notarized, sealed...

The goal of decentralized identity

Analog functionality with digital efficiency

Analog World

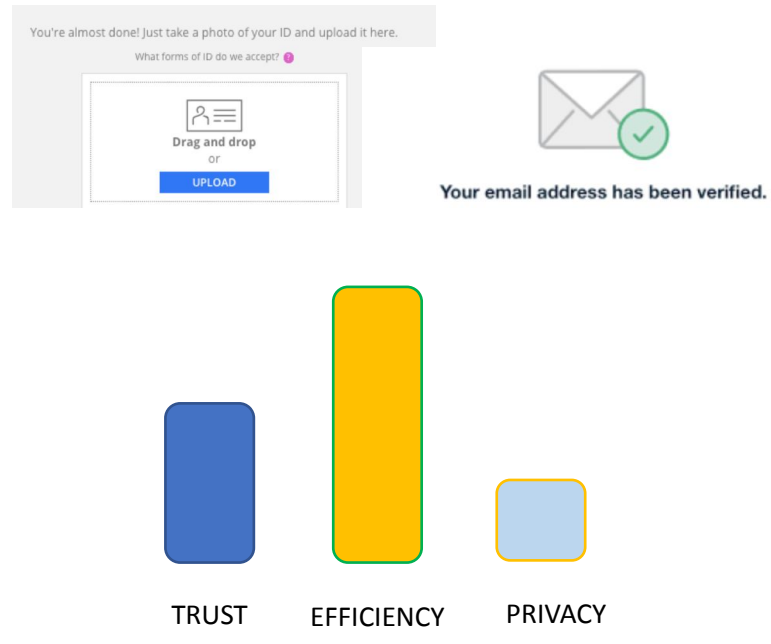
3200 BC ~ 1964



Physical documents sent, shown, signed, notarized, sealed...

Hybrid World

~1964 - 2020



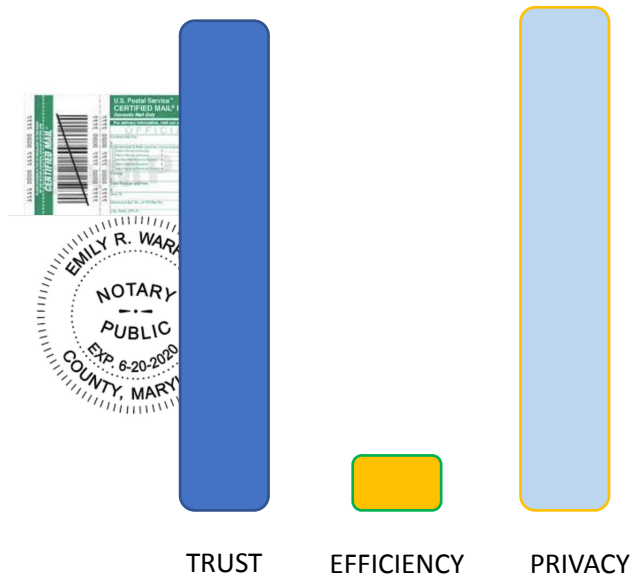
Duplicate and/or digitized documents sent electronically

The goal of decentralized identity

Analog functionality with digital efficiency

Analog World

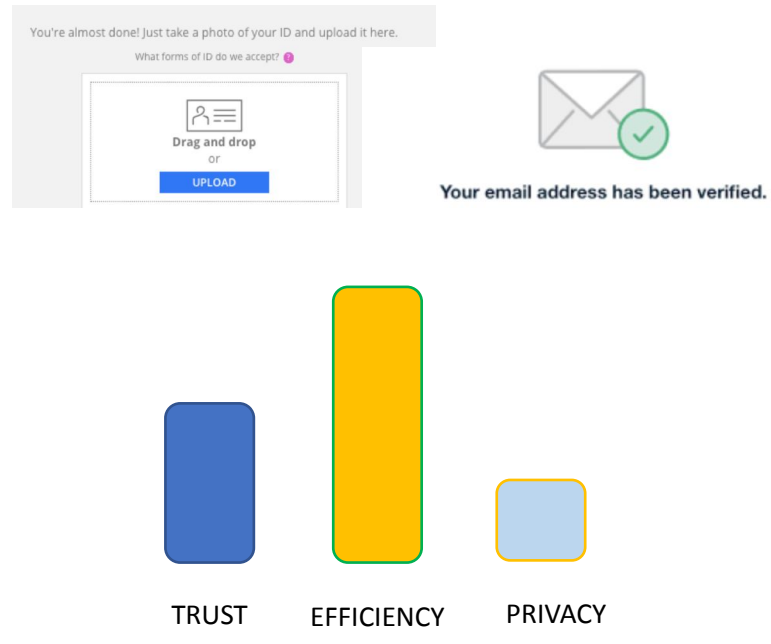
3200 BC ~ 1964



Physical documents sent, shown, signed, notarized, sealed...

Hybrid World

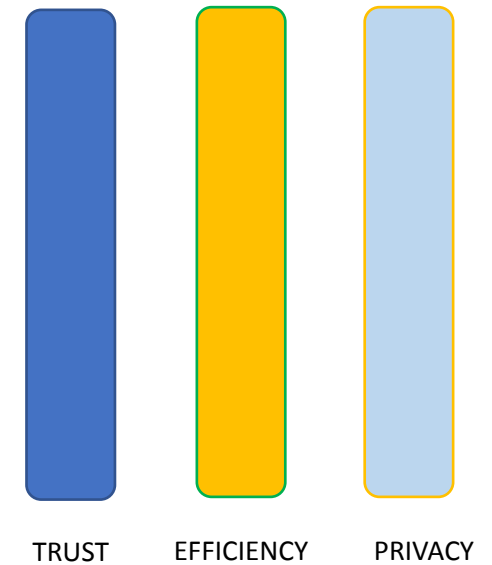
~1964 - 2020



Duplicate and/or digitized documents sent electronically

Decentralized World

~2020 ---



Verification of digital document authenticity and integrity is possible!

Why does it work in “analog” life?

- Trusted **issuers** and trusted physical credentials
- Individuals who **hold** the credentials
- Independent **verifiers**



DMV



It works, because I can visually verify where the data came from and whether it's been altered by the presenter



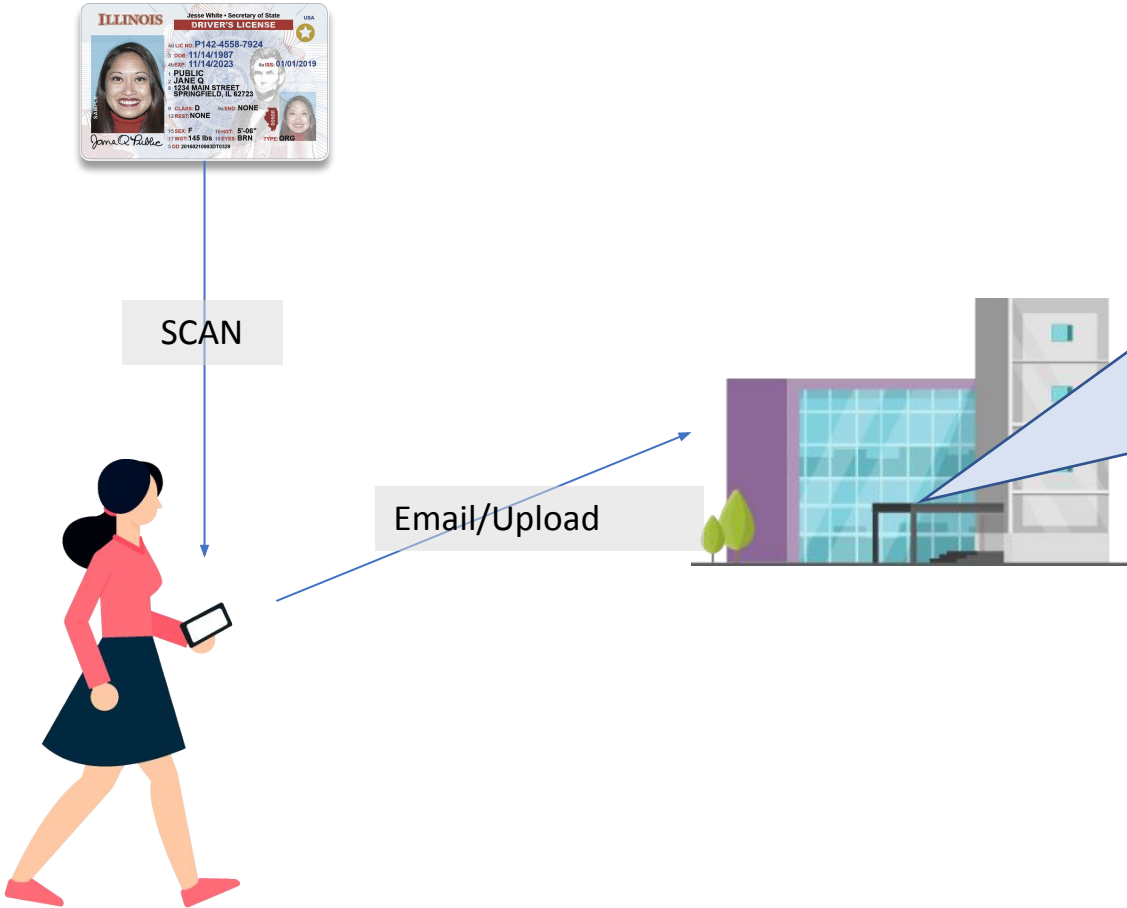
Business



Trust

Placing Trust in Representations and Attestations

Carries Cost and Risk in a Hybrid World



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?

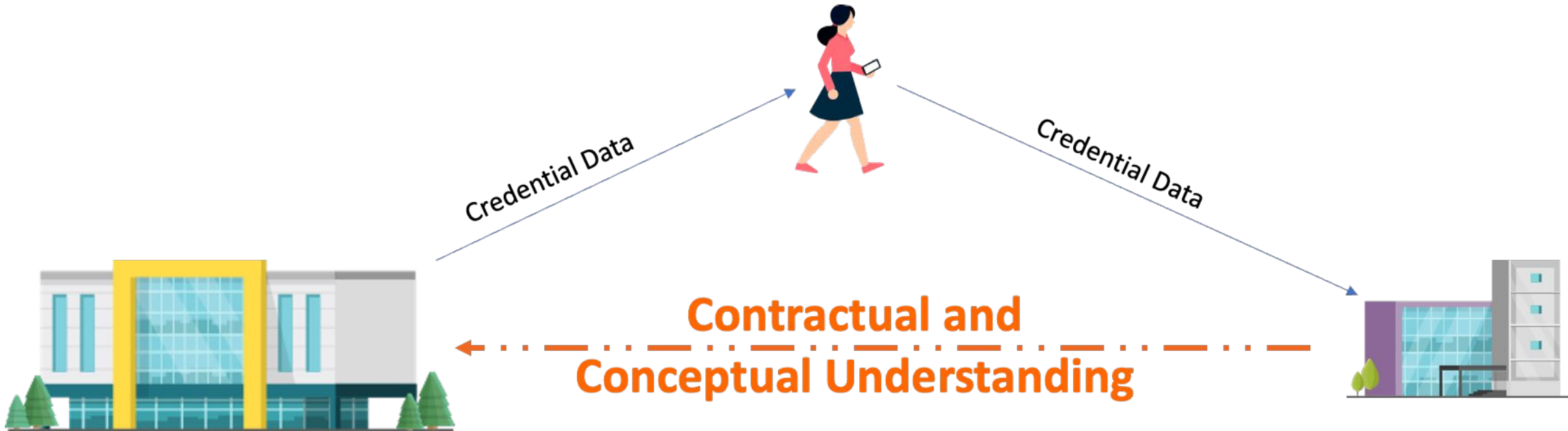
Trust in data comes from three parts:

- 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?*

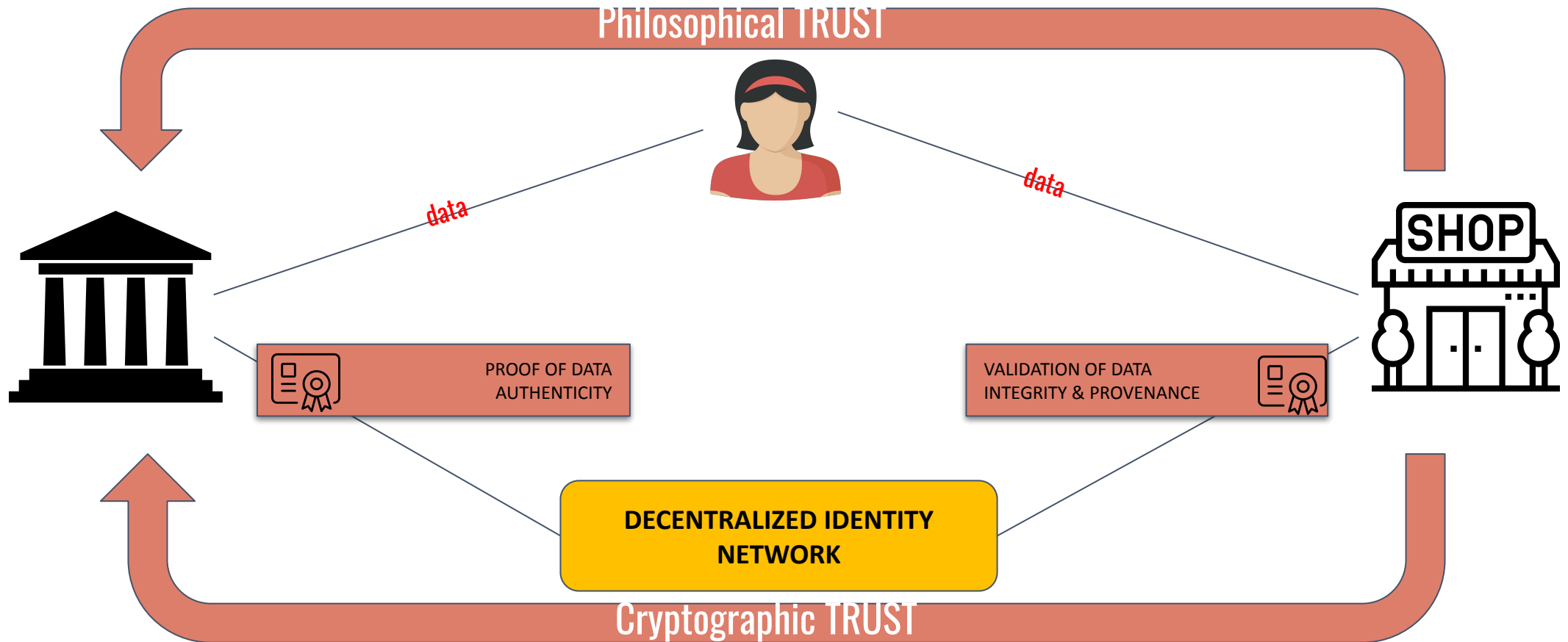
What is trust in data?

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?

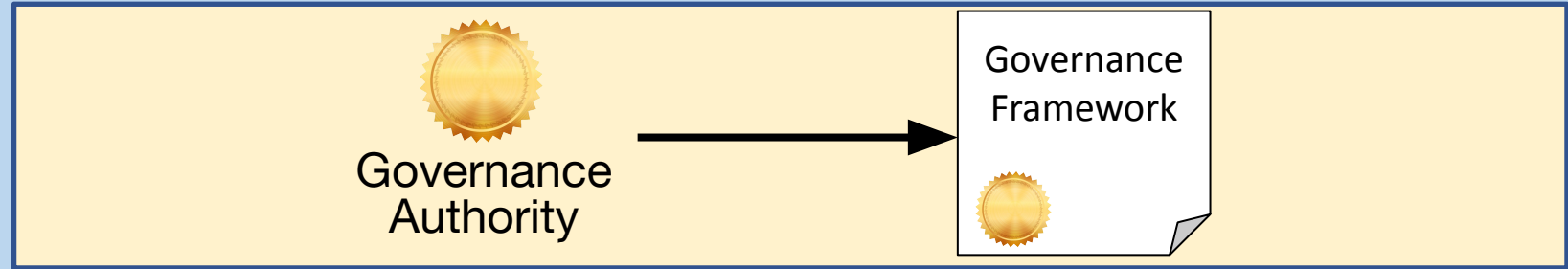


The Trust Model

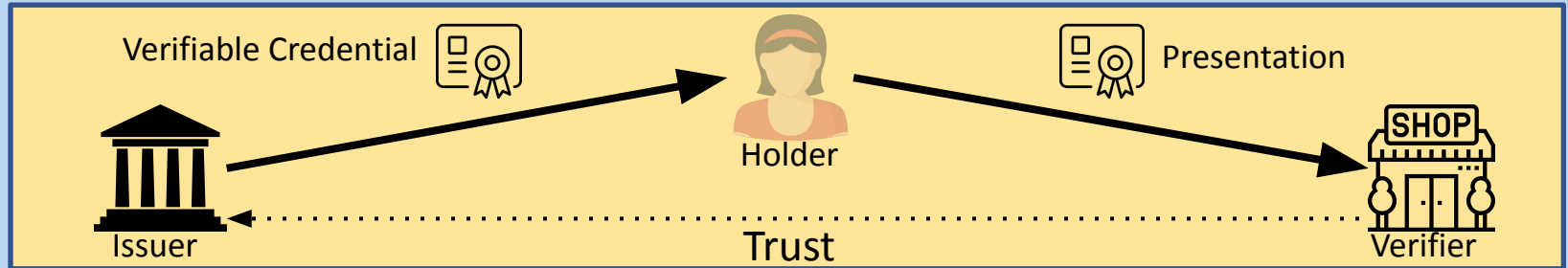


Human Trust

Layer Four:
Governance Framework

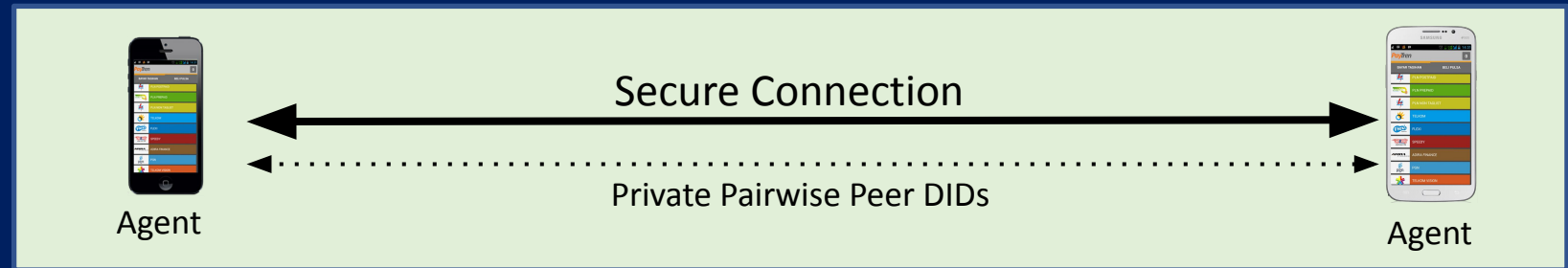


Layer Three:
Credential Exchange

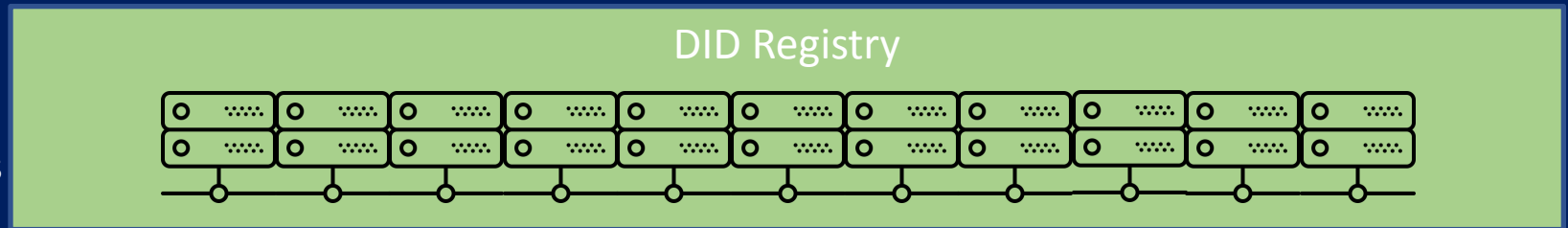


Cryptographic Assurance (Trust)

Layer Two:
Agents/DIDComm

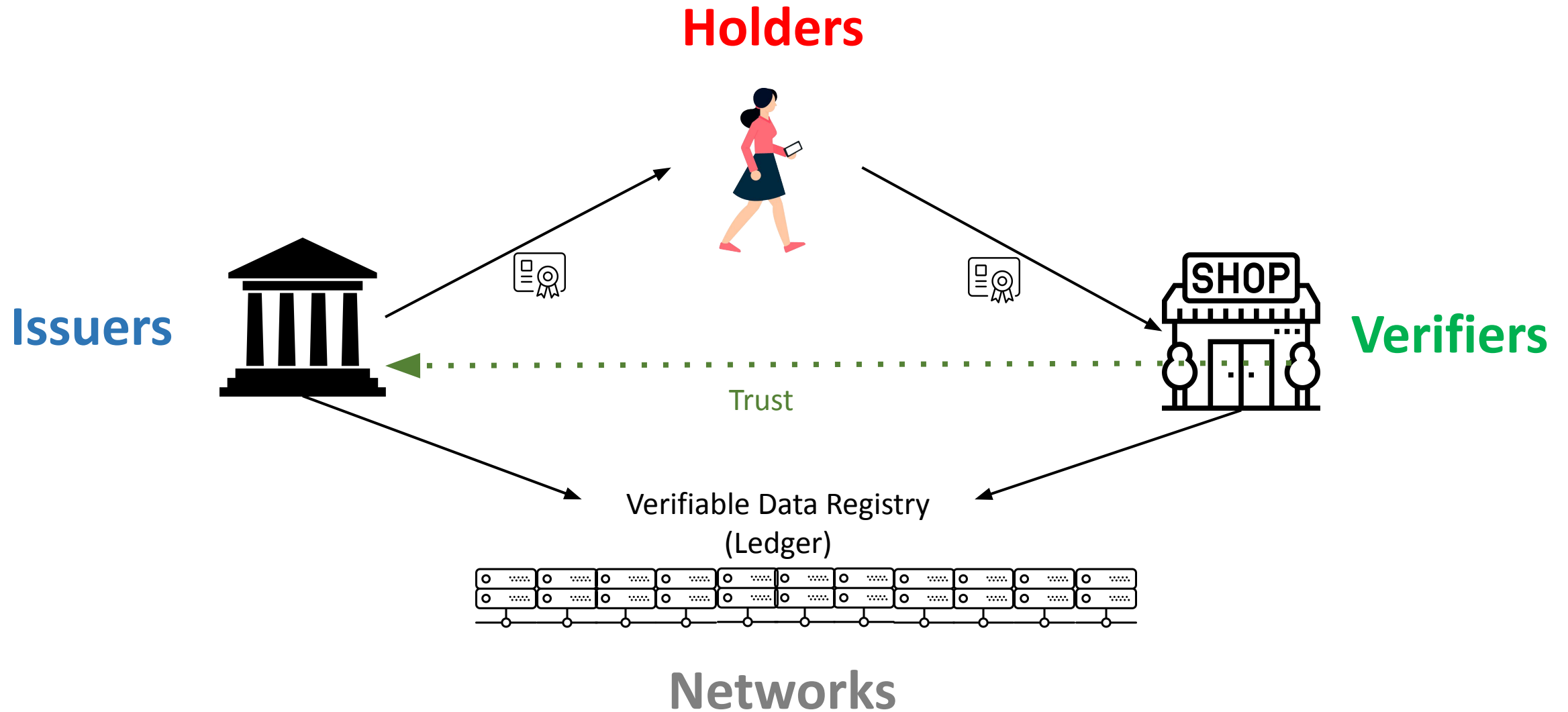


Layer One:
DID Registries



The Verifiable Credential Trust Triangle

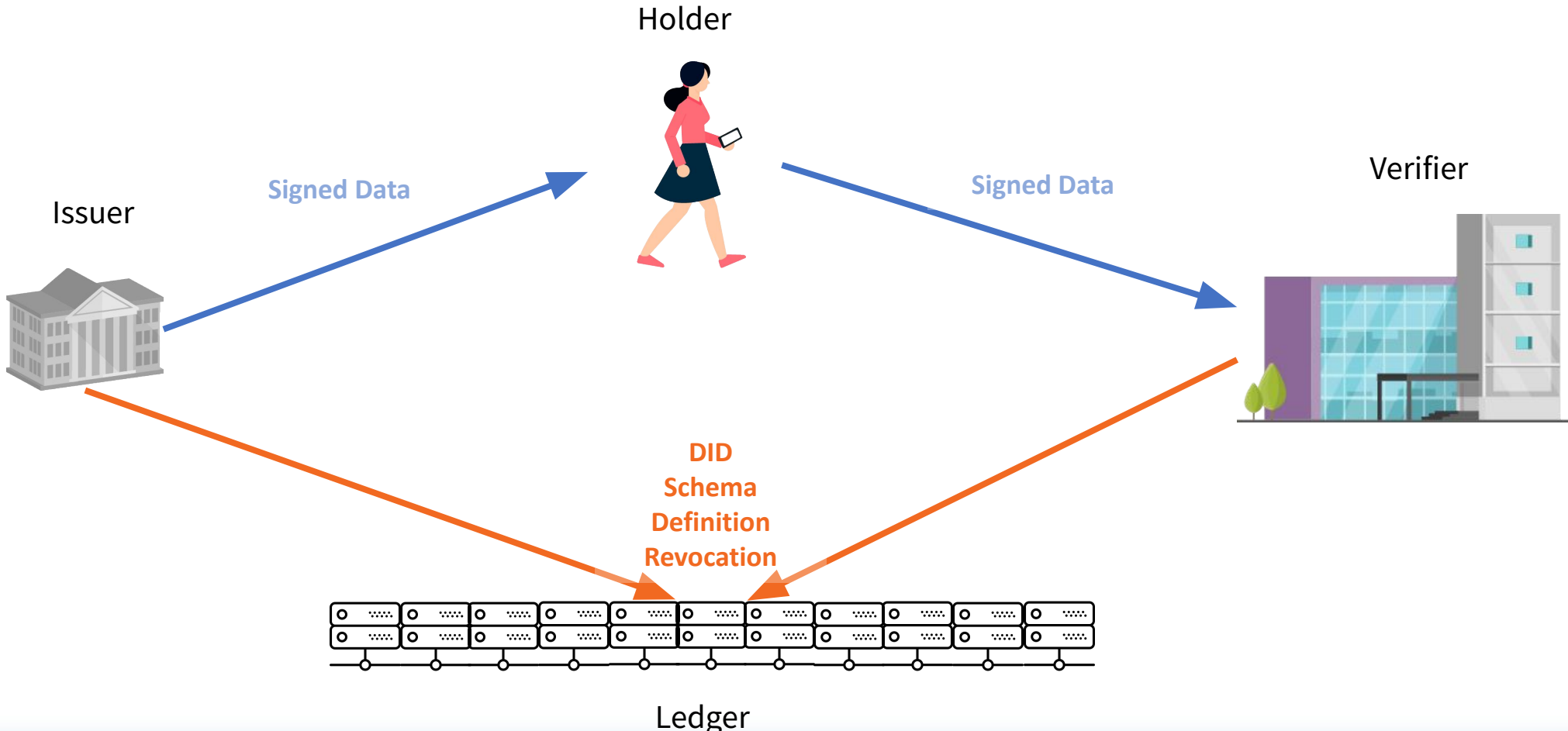
The participants:



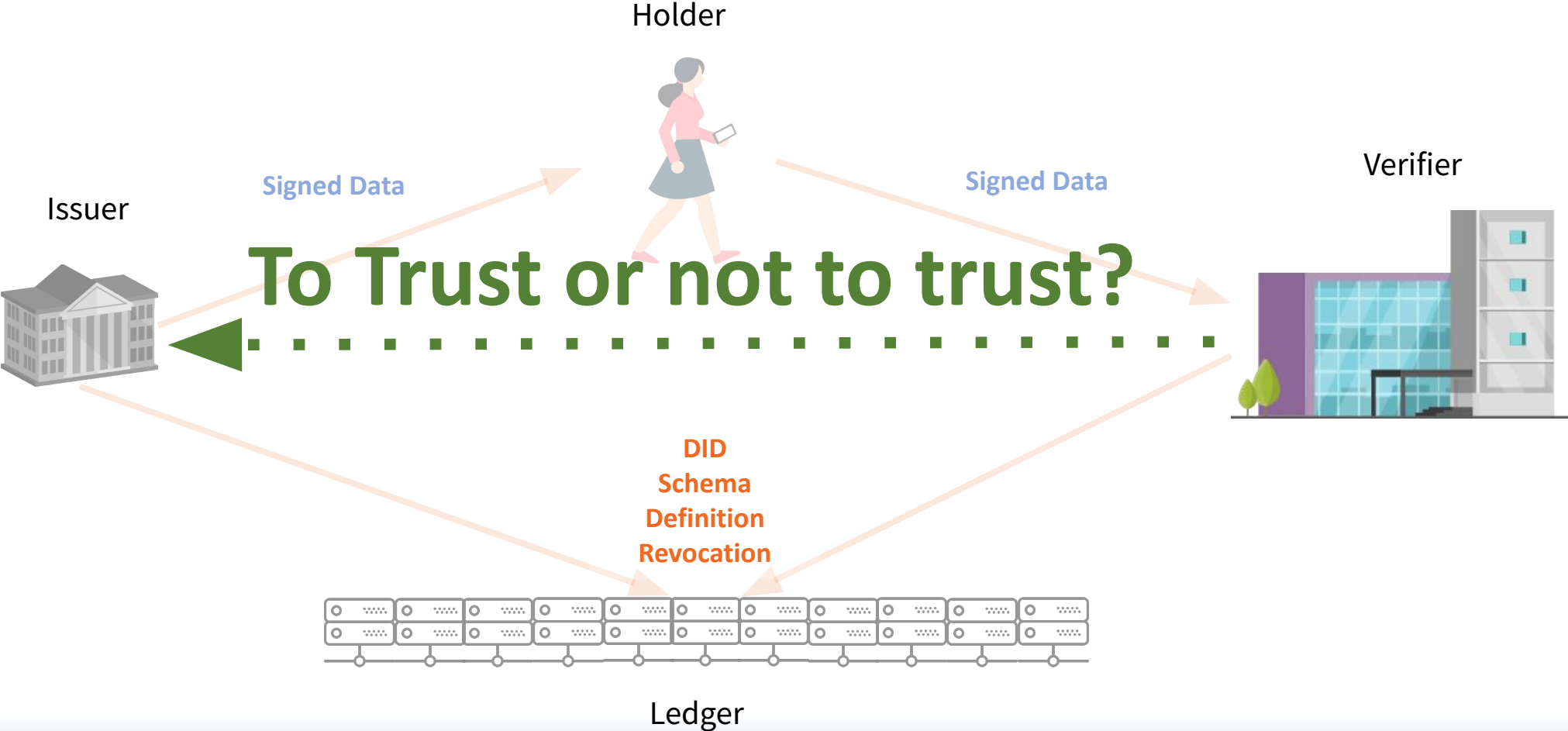
PII (and all Credential Data) stays with data's owner or authorized controller

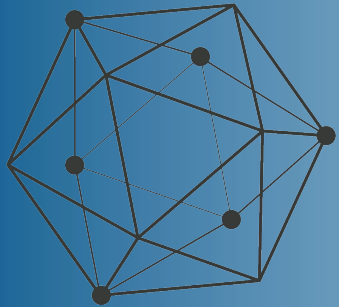
Privacy-by-design and compliance protections

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



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





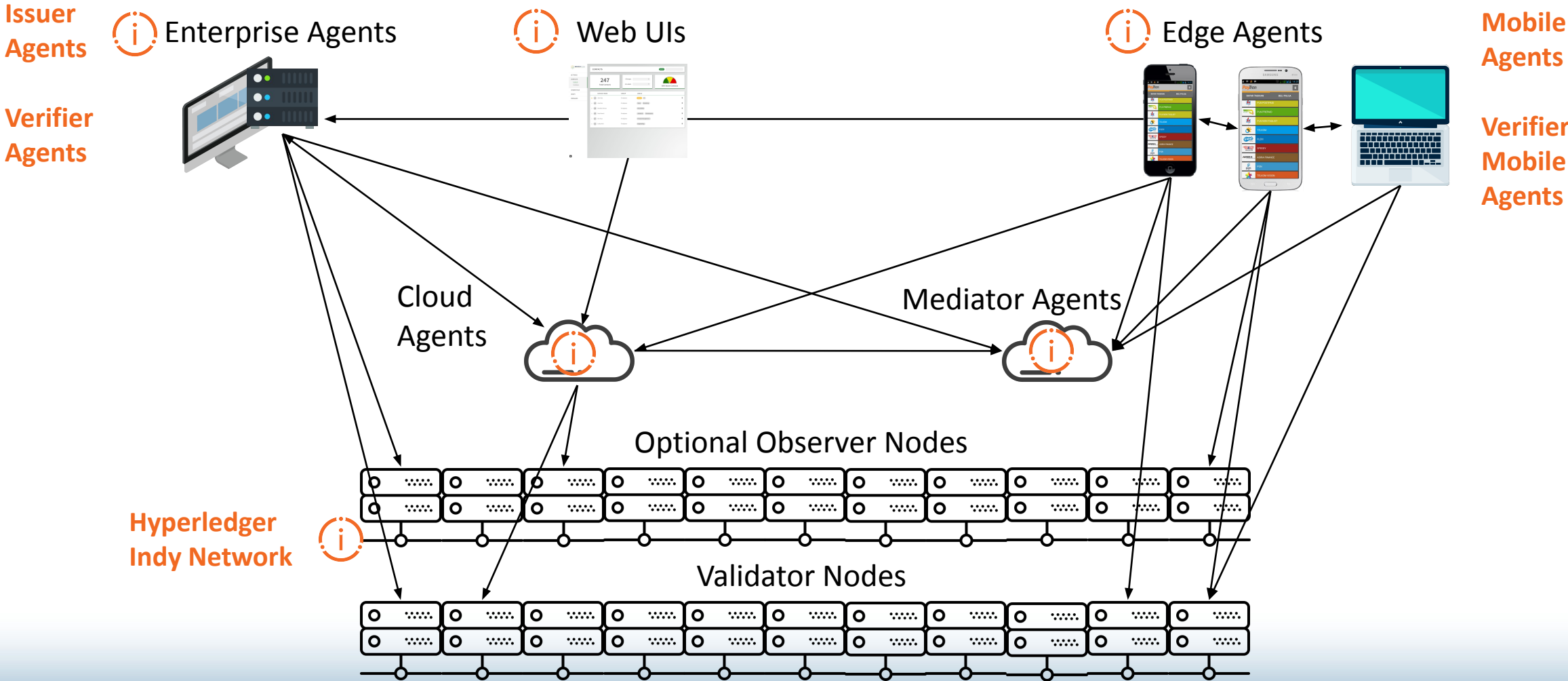
Notes on components roles and conventions



HYPERLEDGER
FOUNDATION

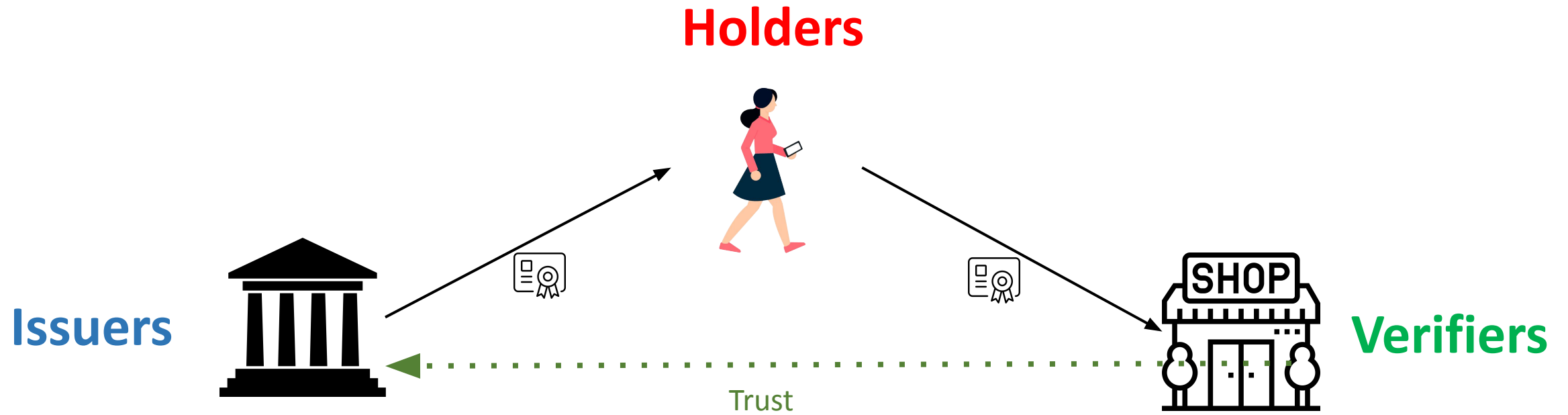
Indicio

Building Blocks

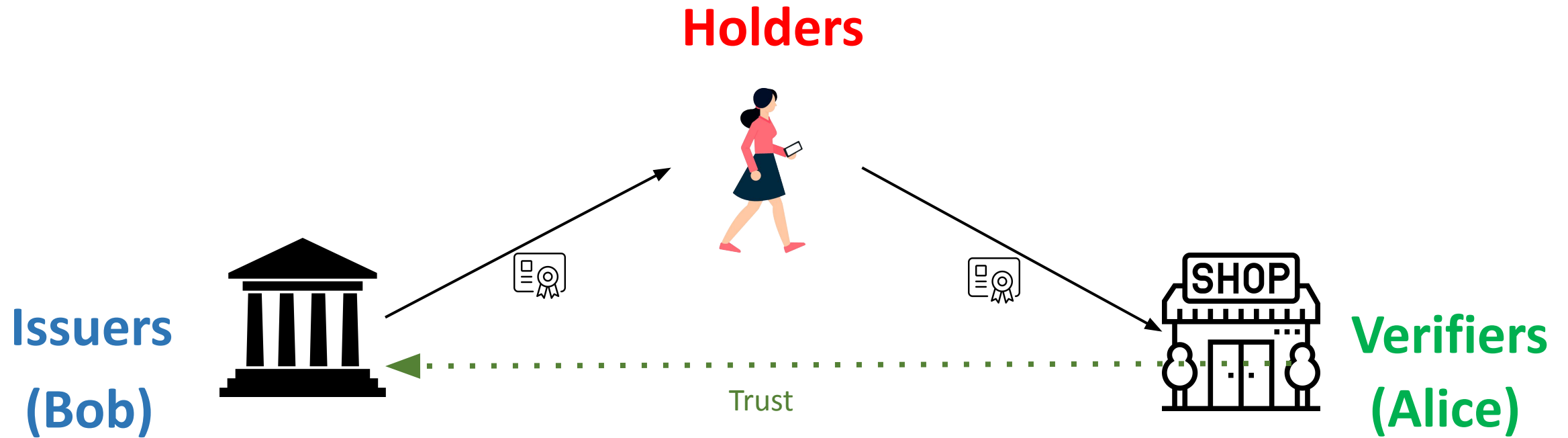


Hyperledger
Indy Network

Roles and Convention

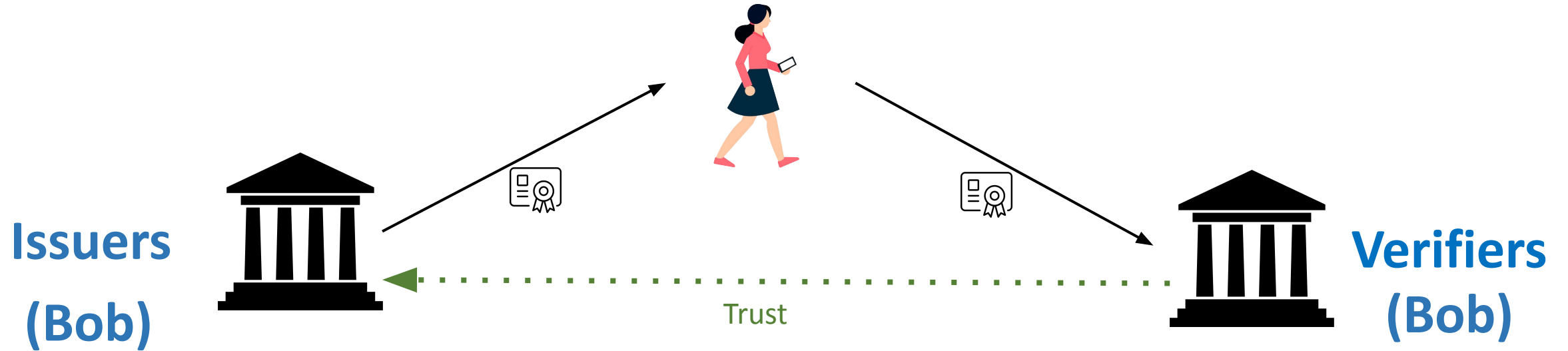


Stories of Bob and Alice



Roles may overlap
Particularly those of *Issuer* and *Verifier*

Holders



Code architecture



Hyperledger Indy Plugins

Hyperledger Indy Node
(Identity Transactions)

Hyperledger Indy Plenum
(Consensus)

Hyperledger Ursa (Cryptography Library)

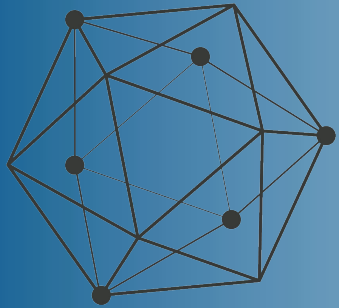
Enterprise, Mobile Apps

Aries Agent

Aries SDK

Indy Resolver





Value



HYPERLEDGER
FOUNDATION

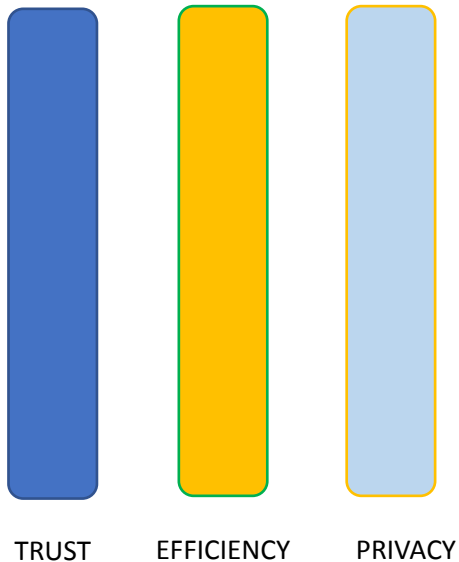
Indicio

Privacy

Protecting individual data through **Privacy by Design**

Decentralized World

~2020 ---



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



- 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: Community Engagement



HYPERLEDGER
FOUNDATION

Indicio