PITHIA

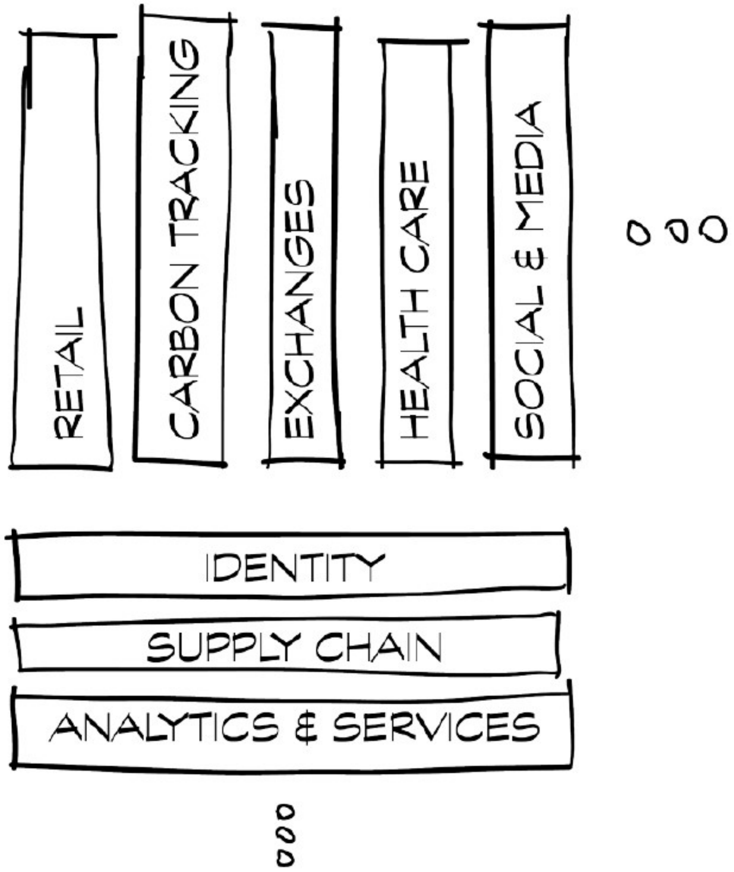
Self-Sovereign Identity Solutions on RChain

RChain Developers Conference

April 16, 2018

Ed Eykholt
Founder and Managing Director
Pithia

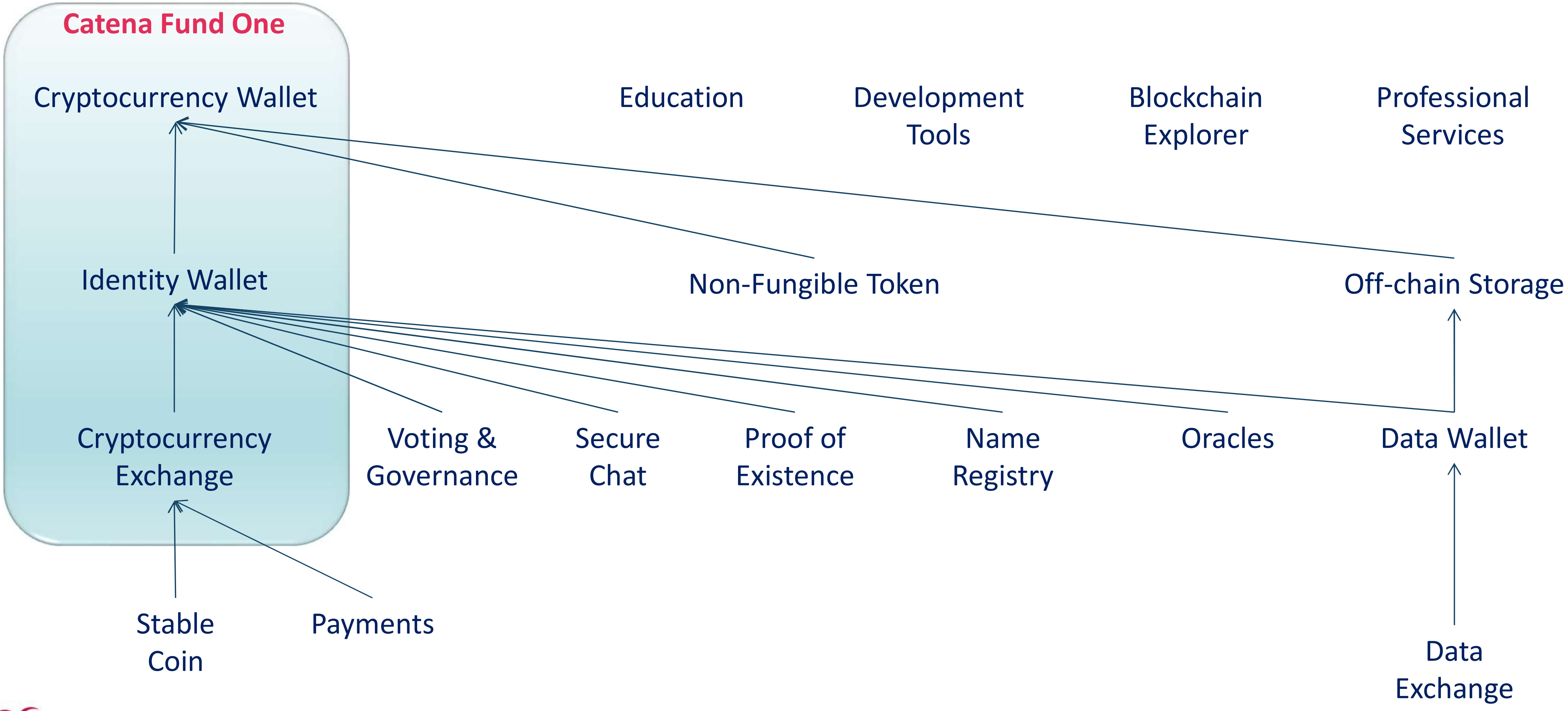
BLOCKCHAIN ADOPTION: COMPLETE PENETRATION



EACH VERTICAL MARKET BUILDS ON ONE BLOCKCHAIN

HORIZONTAL MARKETS MAY SUPPORT MULTIPLE BLOCKCHAINS

RChain Ecosystem:
Enabling Features and their Dependencies



Catena Fund One

Cryptocurrency Wallet

Education

Development Tools

Blockchain Explorer

Professional Services

Identity Wallet

Non-Fungible Token

Off-chain Storage

Cryptocurrency Exchange

Voting & Governance

Secure Chat

Proof of Existence

Name Registry

Oracles

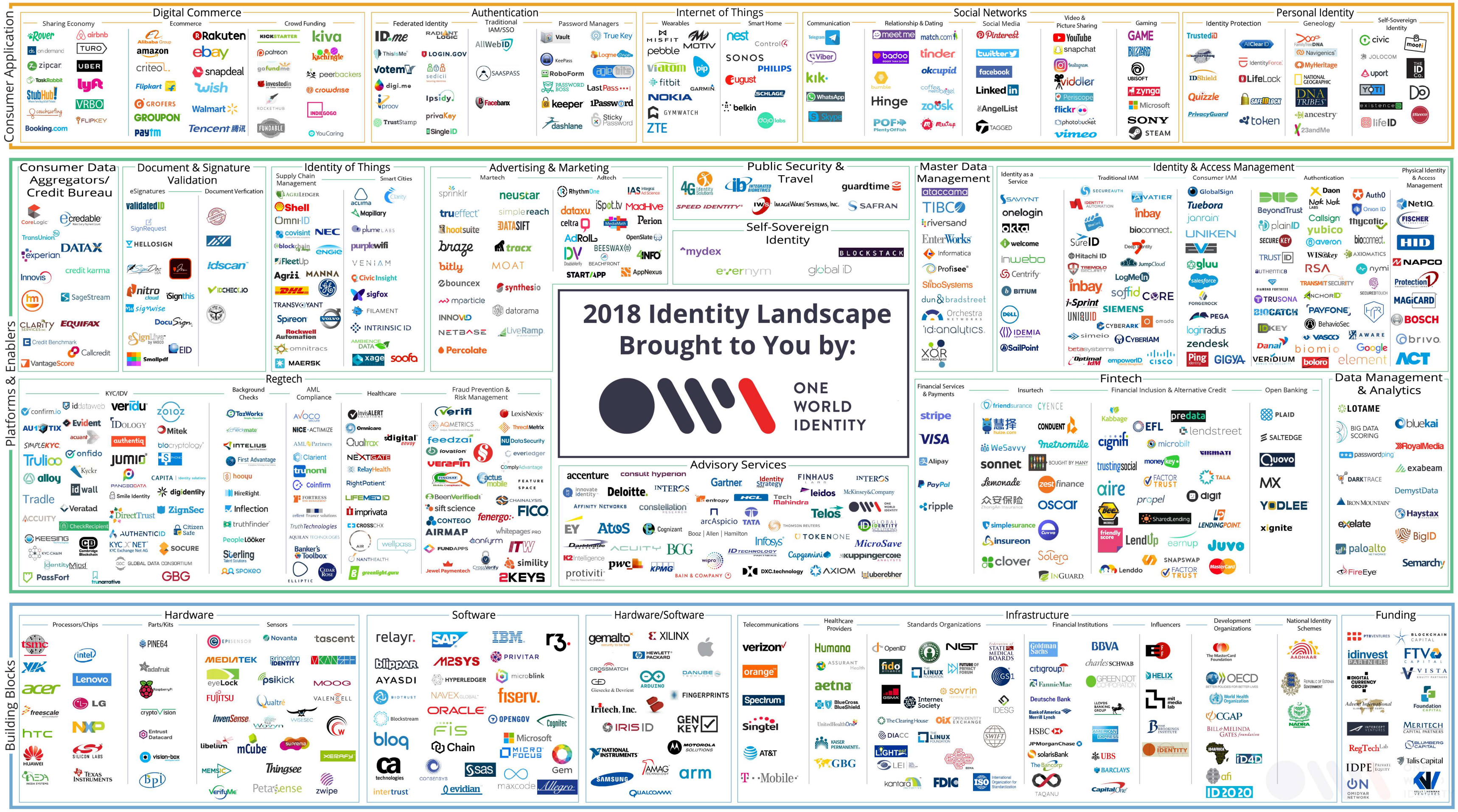
Data Wallet

Stable Coin

Payments

Data Exchange

Many companies are focused on identity



Problems

- Popular authentication mechanisms used today are broken
  - Passwords, email, cell phone number, SSN, mother's maiden name, birthdate...
  - OAuth typically relies on you trusting large, centralized parties
  - Identities are easy to correlate, impersonate, attack
- Practices lead to loss of privacy, assets
- Systemic friction to productivity of enterprises
  - onboarding new customers
  - verifying credentials
  - resetting password
  - dealing with fraud
- GDPR compliance
- Opportunity to better address certain populations
  - Refugees / Homeless / Children / Guardianship

The hidden costs of our dysfunctional Internet identity infrastructure are staggering.

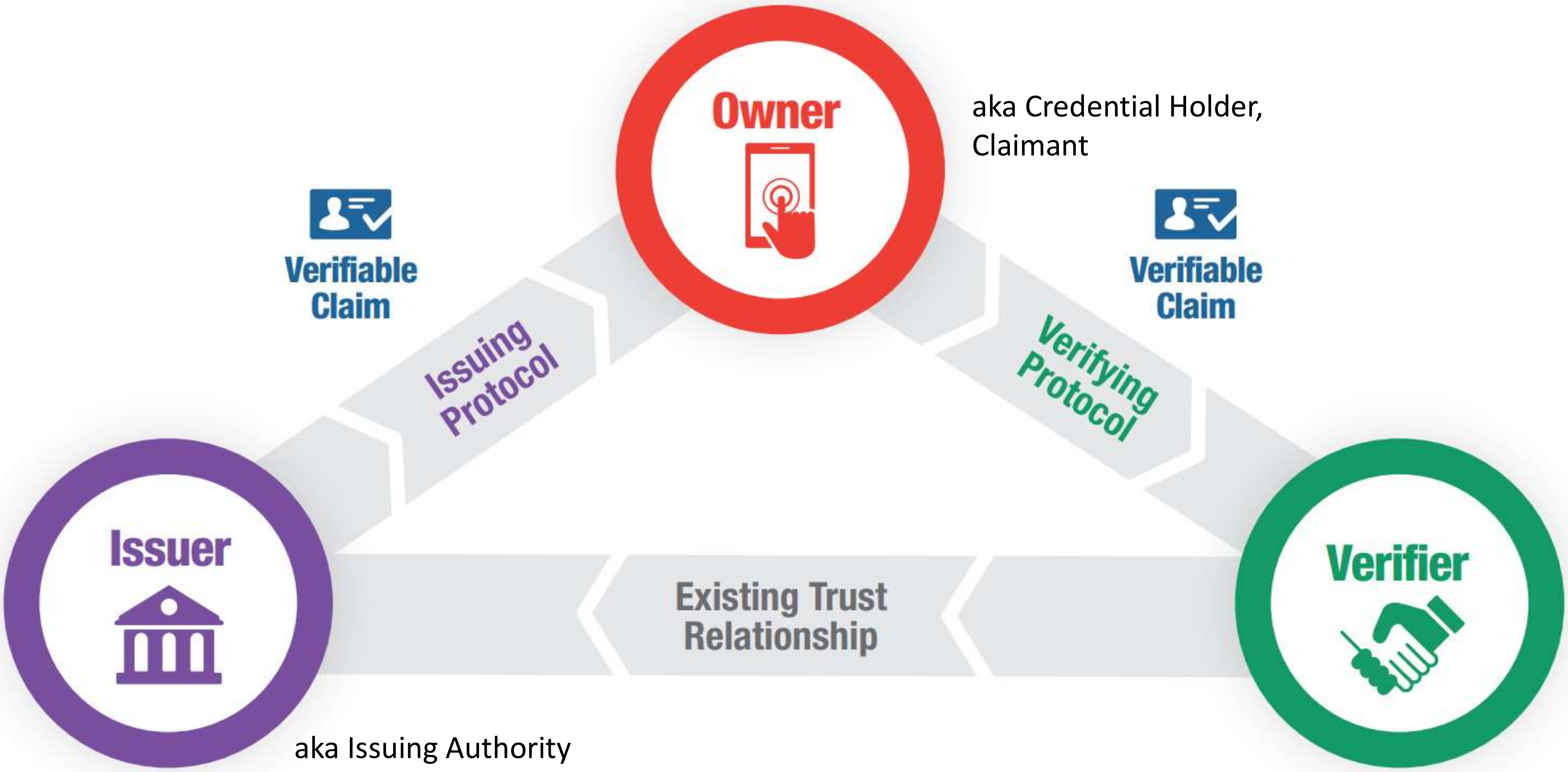
- **The 2017 Hiscox Cyber Readiness Report** estimates that cybercrime and data breaches currently cost the global economy **US $450 billion** per year.
- **The 2016 Cybersecurity Market Report** predicts cybercrime damages will cost the global economy a total of **US $6 trillion** by 2021.
- **The U.S. Public Interest Research Group estimates** consumers will have to directly shell out a collective **US $4.1 billion** to freeze their credit reports and prevent fraudsters from using personal information possibly exposed in the massive data breach at Equifax.[11]
- **IDG estimates that theft of trade secrets** costs every nation from 1 to 3 percent of their gross domestic product (GDP), for a total ranging from **US $749 billion to $2.2 trillion annually.**

From Sovrin Whitepaper

What is Digital Identity?

- Functionally, identity can be the sum of
  - **attributes associated to a person** (age, height, birth date, biometrics, etc),
  - **attributes accumulated over time** (medical information, preferences, communication metadata, etc), and
  - **designated attributes** (telephone number, email, Passport numbers, etc),
- but we can go beyond people and also talk about legal identities, identities of devices or assets, which are often linked to human identity.
- Identifier != Identity

Self Sovereign Identity — a guide to privacy for your digital identity with Blockchain, Alex Preukschat



aka Credential Holder, Claimant

aka Issuing Authority

aka Relying Party

Image courtesy of Sovrin

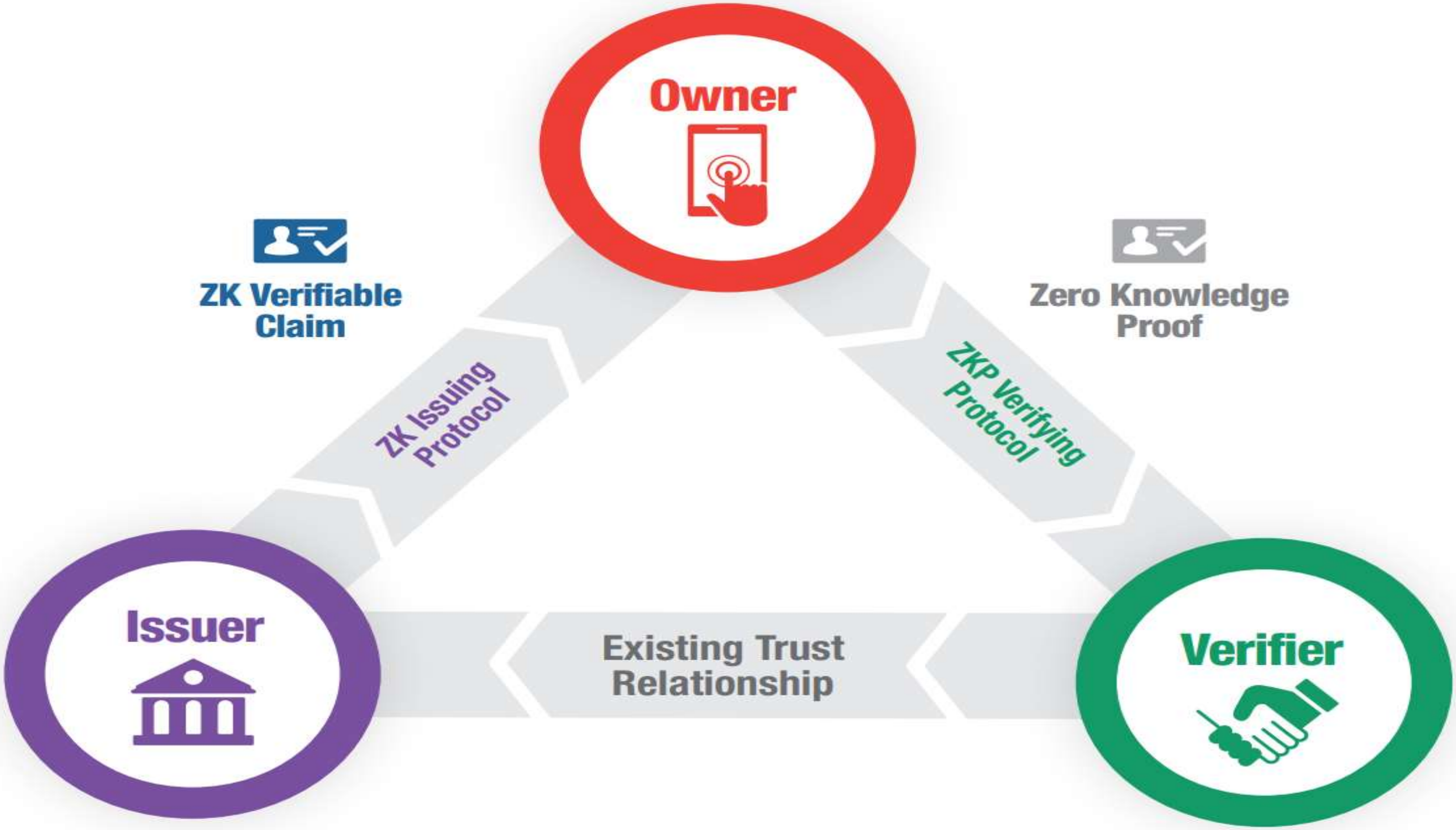


Image courtesy of Sovrin

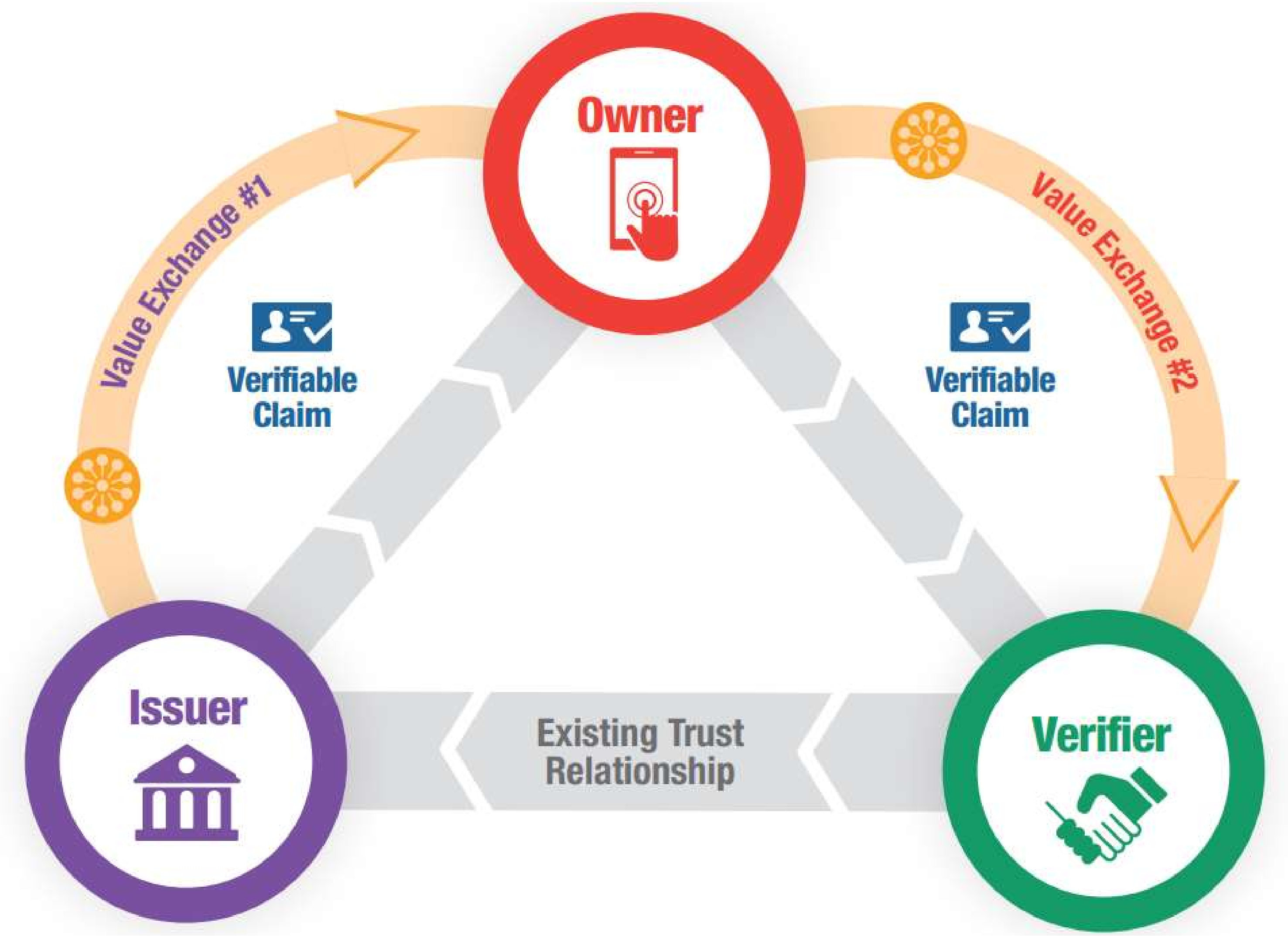


Image courtesy of Sovrin

Identity Ecosystem

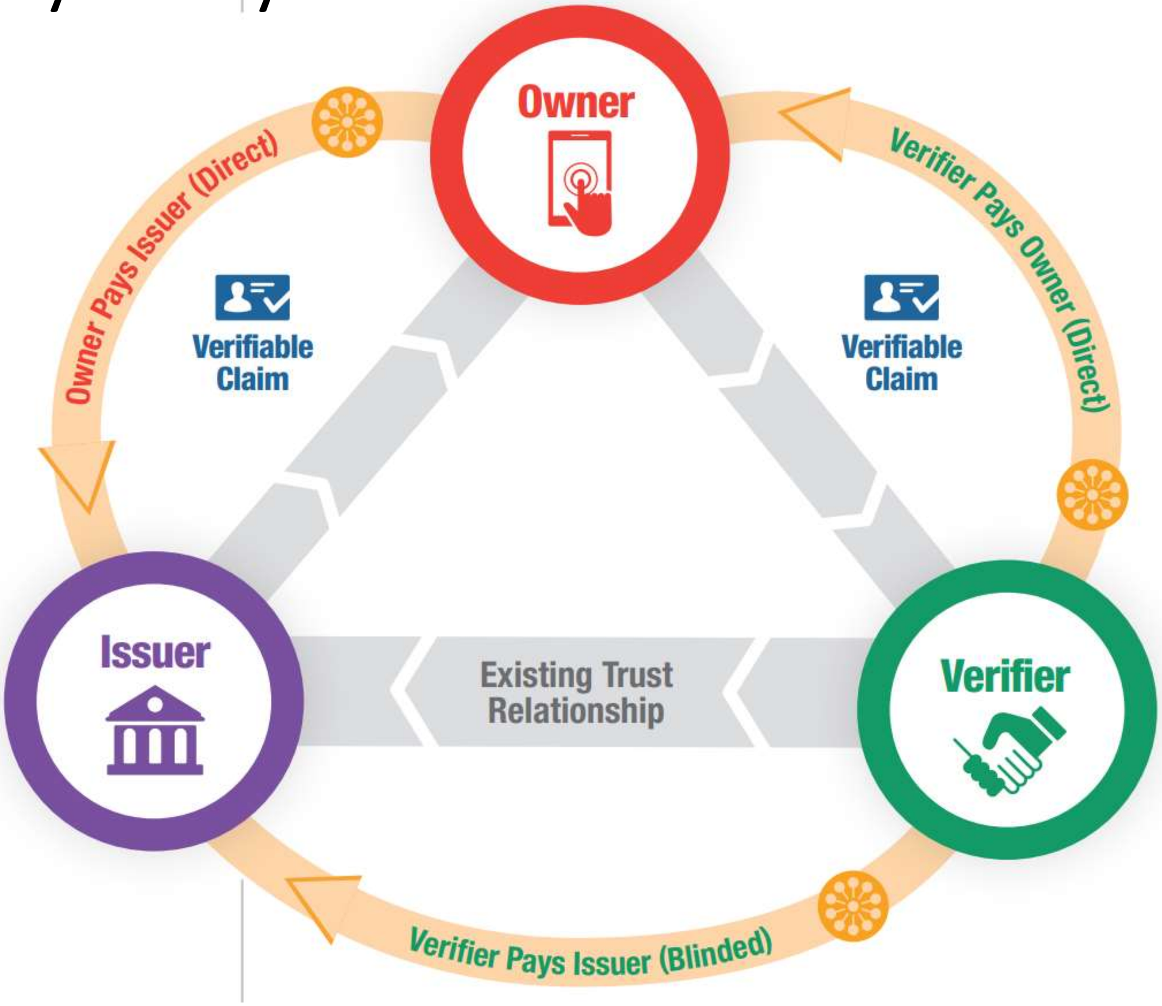

Owner
Verifiable Claim
Verifiable Claim
Owner Pays Issuer (Direct)
Verifier Pays Owner (Direct)
Issuer
Existing Trust Relationship
Verifier
Verifier Pays Issuer (Blinded)

Image courtesy of Sovrin

Self-Sovereign Identity Model

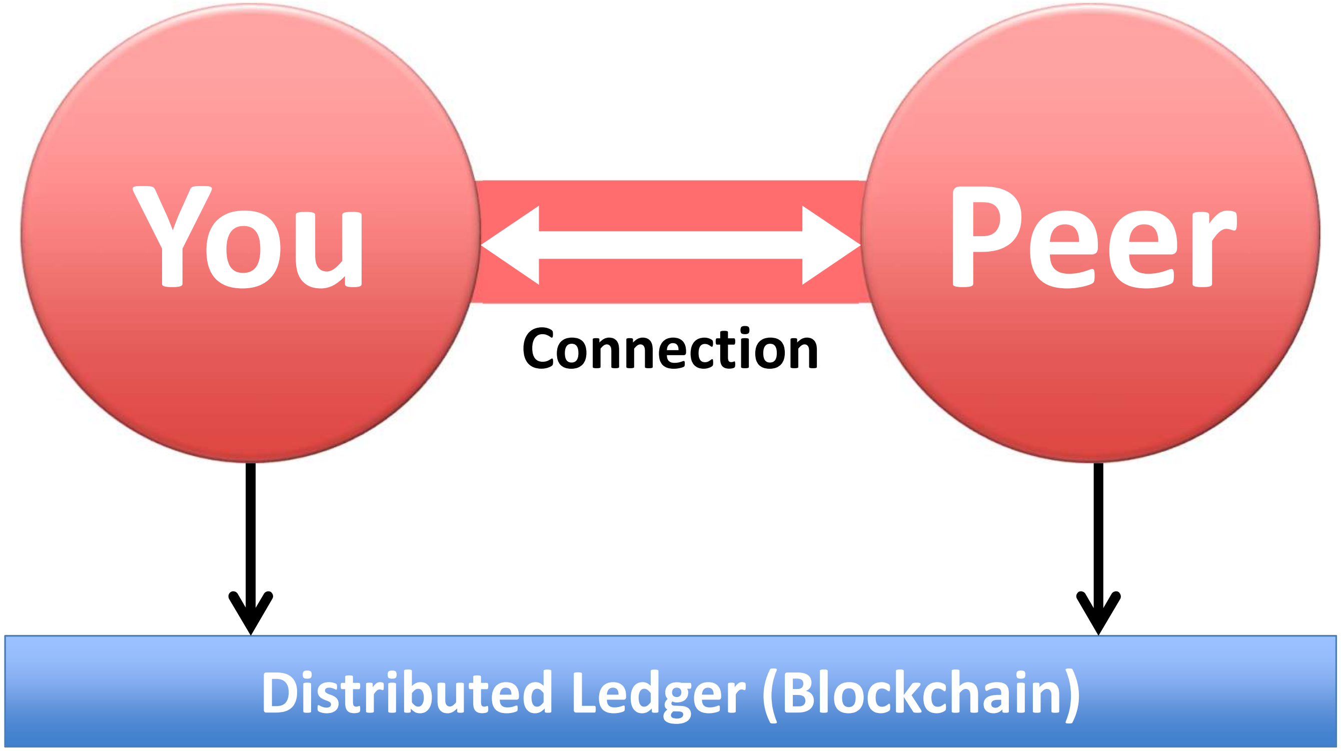


Image courtesy of Sovrin

- You and each peer have multiple **personas**!
- Pairs of personas can form Peer-to-Peer connections
- Symmetrically Encrypted – “a private VPN”

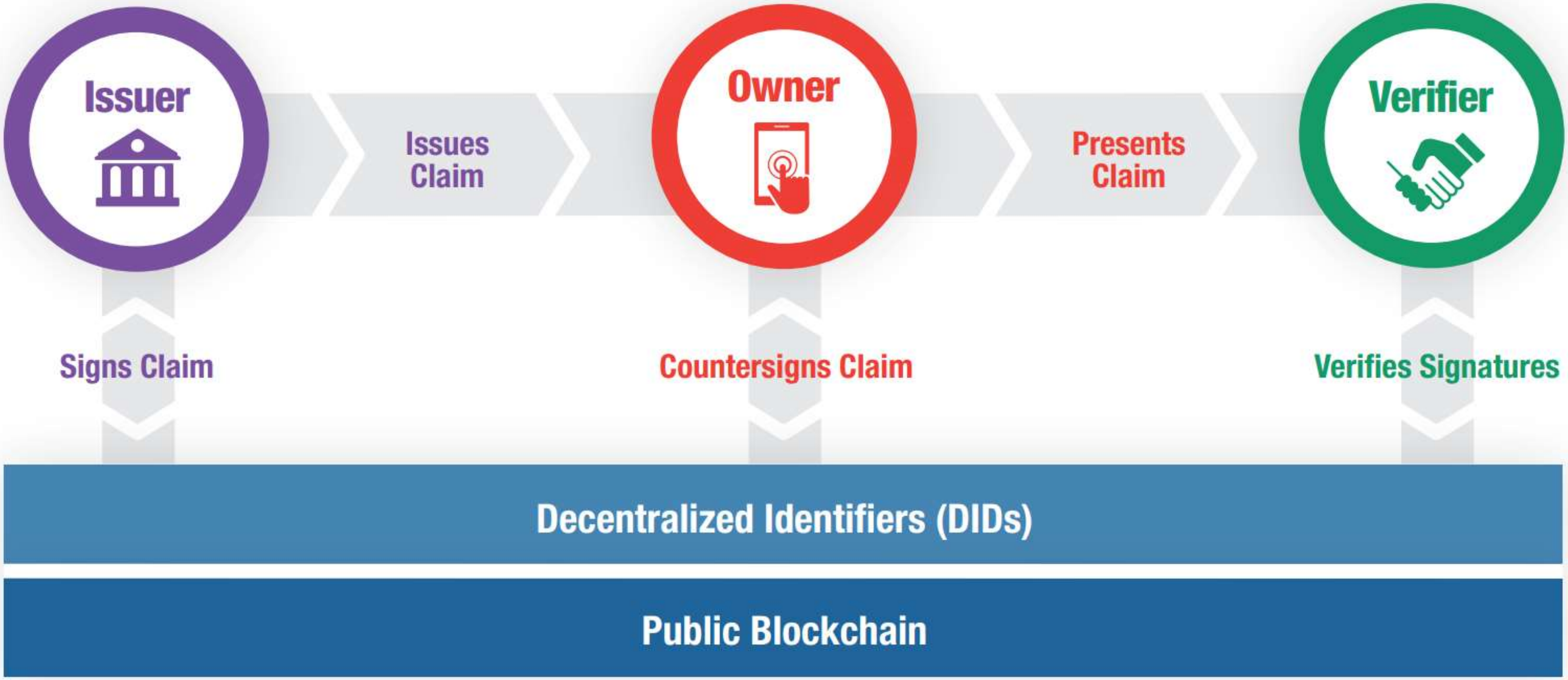


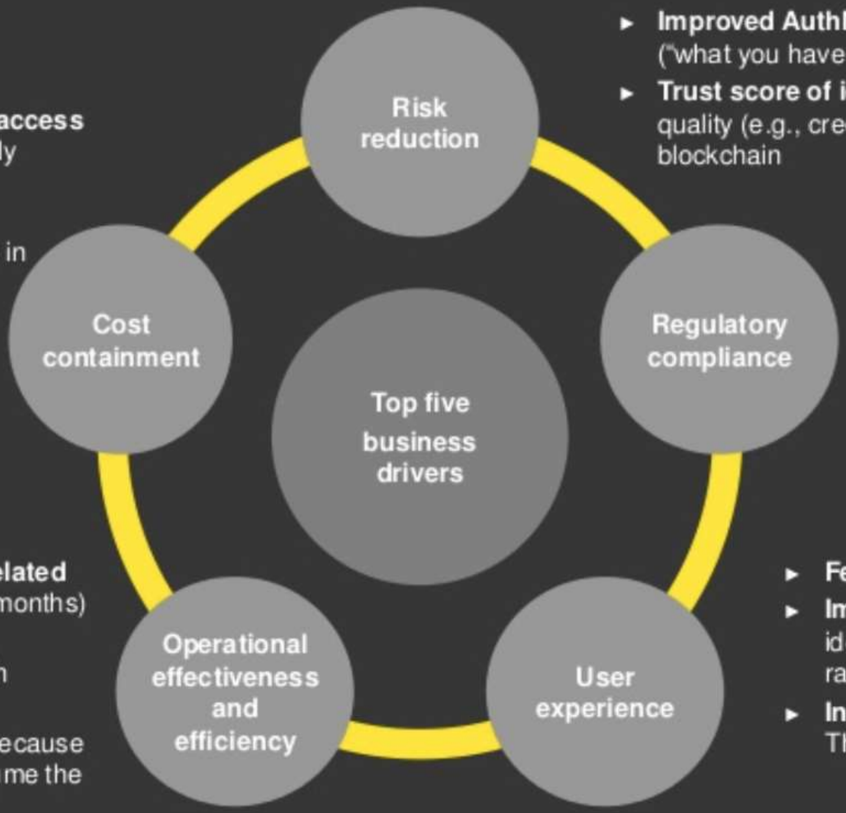
Image courtesy of Sovrin

Typically on-chain:

- DIDs with associated addresses, validity
- Revocations of claims

Business benefits of blockchain-based IAM

- **Reduced time and effort to manage access rights** by reducing the need for centrally managed identity governance and administration solutions.
- **Reduced need to maintain identities** in a directory or identity data warehouse



- **Improved AuthN** and **AuthZ mechanism** ("what you have and are" + "what others know")
- **Trust score of identity ledger** increases with quantity and quality (e.g., credit bureaus, trusted authorities) of peers on blockchain

- **Improved auditability** of identities due to distributed, open nature of identity ledgers

- **Improve service-level agreements related to user onboarding** (days instead of months) for third-party access
- **Utilize payment networks** to establish **identities**
- **Fault tolerance** and **elastic scaling** because each node in the blockchain can consume the self-contained assertion

- **Fewer passwords** to remember
- **Improved digital experience** through unified identity experience and improved app store ratings
- **Interoperability** with Internet of Connected Things

What’s in your wallet?

Cryptocurrency Wallet

- Send, Receive, History
- Accounts, Aliases
- Integrations
  - Blockchain (Tx’s)
  - Explorers (history, details)
  - Exchanges (price, exchange)
  - Fiat Money Services (buy, sell)

Key Management and Signing

- Private Keys
- Sign Tx’s
- Key rotation
- HD
- Storage backup, recovery
- Social backup, recovery
- Integrations
  - Hardware
  - Browsers
  - Browsers Add-Ins
  - Key Management Services

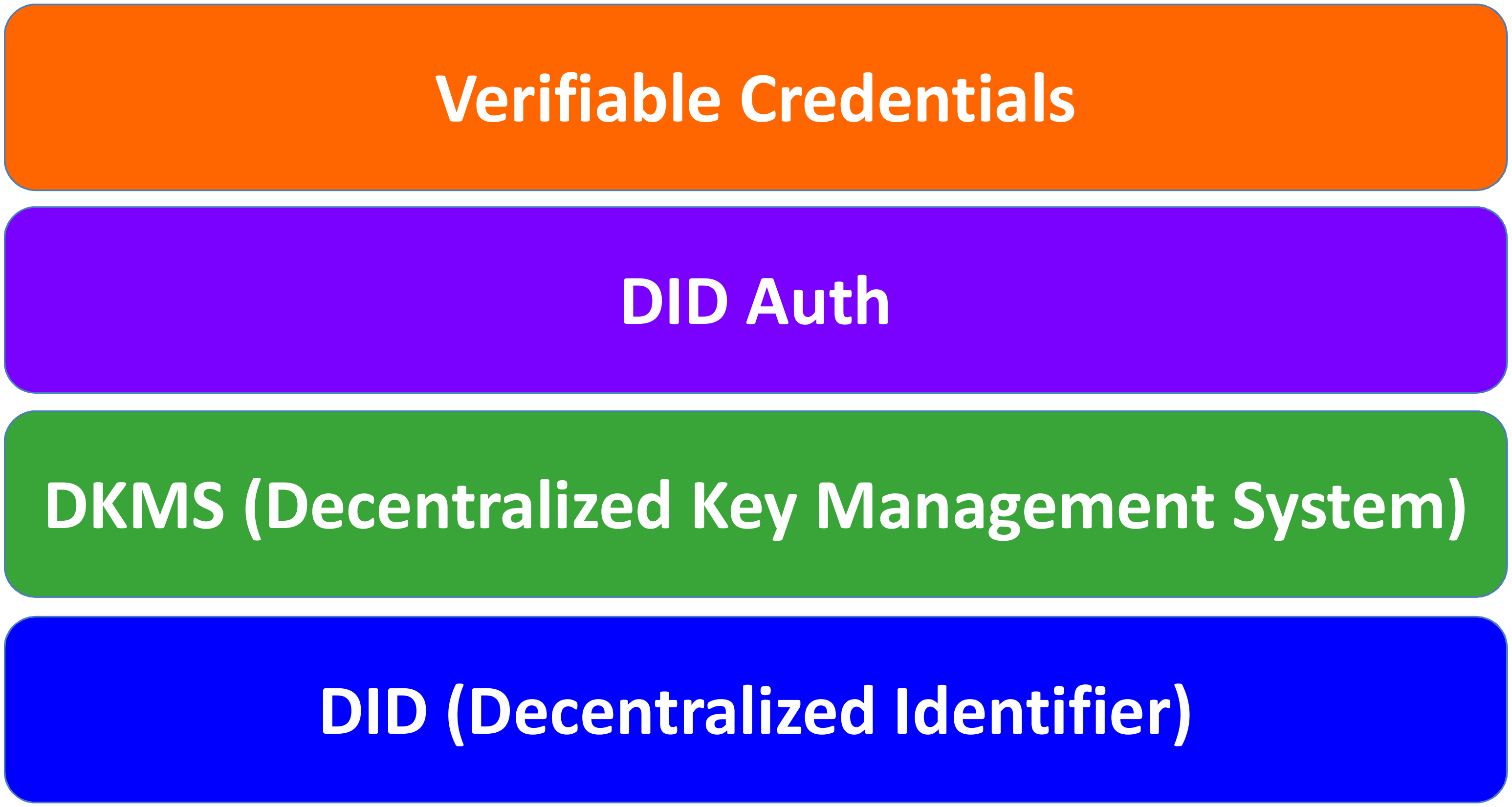
Identity Wallet

- Credentials, Claims, Verification, Revocation
- Personas and connections
- Pass around keys/tokens
- Integrations
  - Blockchain (DIDs, Public Attestations, Revocations)
  - DID Resolvers, DID Auth

Data Wallet / Personal Information Manager / Personal Data Service

- Private data
- Storage backup, recovery
- Integrations
  - Personal Data Exchanges (PDXx)
  - Markets (e.g. opt-in advertising)

Four Emerging Open Standards for SSI


Verifiable Credentials
DID Auth
DKMS (Decentralized Key Management System)
DID (Decentralized Identifier)

to

Image courtesy of Sovrin

Working Group for SSI (sponsored by Pithia)

- Members
  - LifeID, NuID, Sovrin, Trusted Key, Verif-y, Dynas Yunas
- Support interoperability across Identity Wallets, Protocols
  - Track and Contribute to Emerging Standards
    - DIF DID, RWOT DKMS, RWOT DID Auth, W3C Verifiable Claims (Credentials)
  - Support exchange of verifiable claims
    - Zero Knowledge Proofs
    - Claims Exchange Protocol
- For RChain:
  - Identify requirements for core platform
  - Assure design of DID format, implementation of a DID resolver
  - Collaborate on identity protocols, interfaces
  - Create reference implementation smart contracts

Identity App Requirements for RChain Platform

- Multiple ECDSAs

✓secp256k1: used on Bitcoin and Ethereum

□ secp256r1 (aka prime256): native on iPhone and Android

□ Low or zero correlation between DID transactions and Cryptocurrency transactions

– Context: Service creates a DID for User and stores it on blockchain. How is the payment kept anonymous, so the service and the user is not correlated?

– Ability to transfer cryptocurrency and crypto-token anonymously, shielding sender's address.

– Requires Zero Knowledge Proofs at core layer?

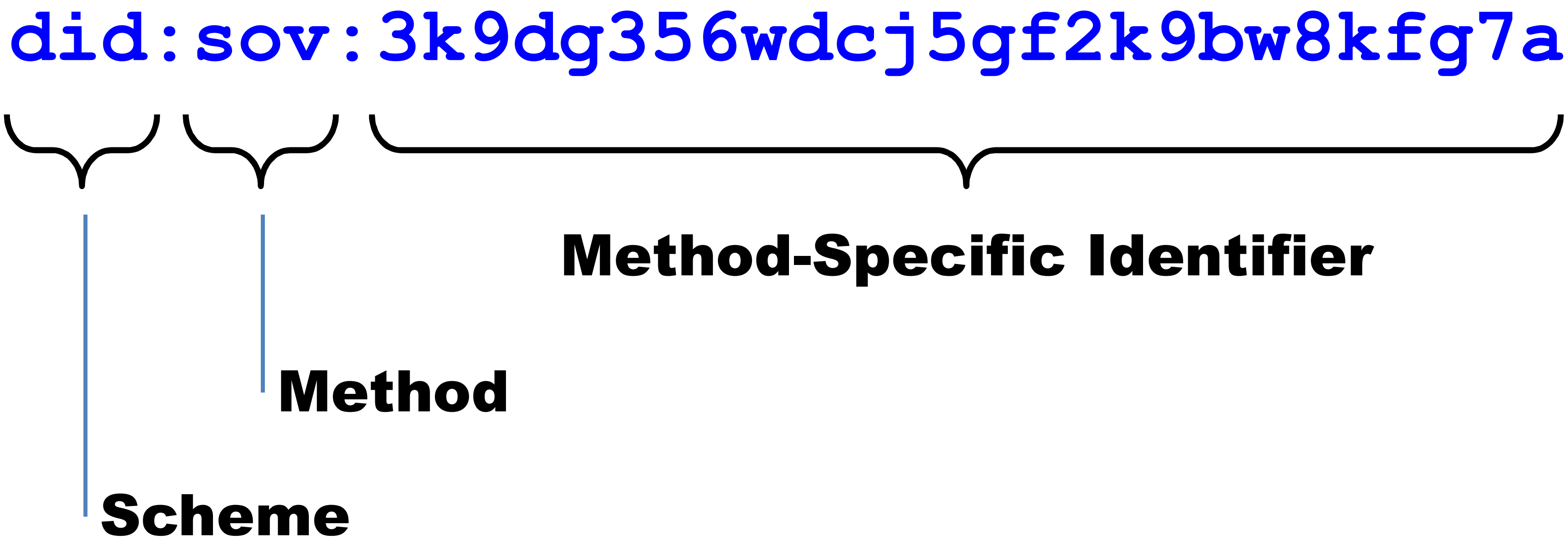
lifeID

Your identity, for life!

Q&A

Decentralized Identifiers (DIDs)

DID Syntax (W3C)



did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

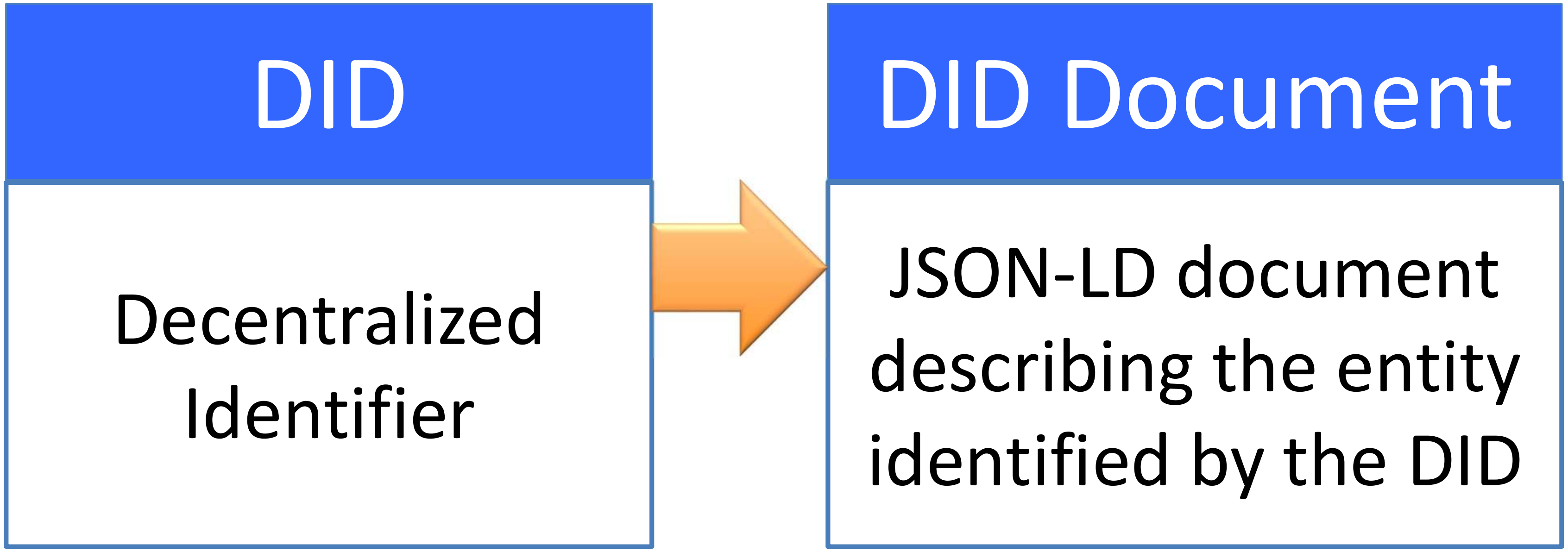
Method-Specific Identifier

Method

Scheme

Image courtesy of Sovrin

{ “Key”: “Value” }



DID

Decentralized Identifier

DID Document

JSON-LD document describing the entity identified by the DID

Image courtesy of Sovrin

The standard elements of a DID doc

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. Set of auth protocols (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)

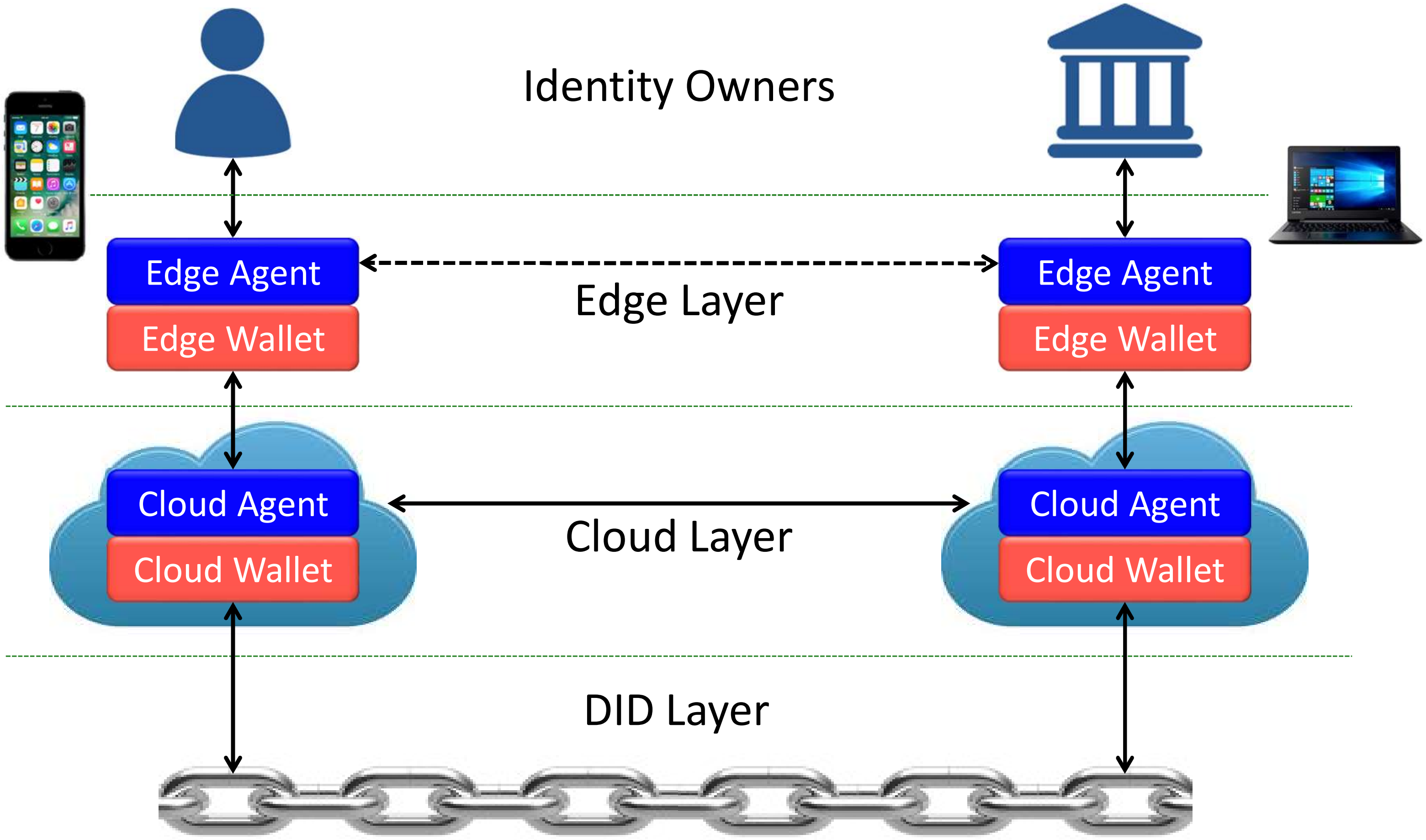
Image courtesy of Sovrin

DKMS
(Decentralized Key Management System)

DKMS

- A proposed open standard for managing the private keys you need for DIDs—including robust, highly usable key recovery
- Key recovery supports both *offline* recovery ("paper wallet") and *social recovery* ("trustee") methods

The decentralized identity “stack”



Identity Owners

Edge Agent

Edge Wallet

Edge Layer

Edge Agent

Edge Wallet

Cloud Agent

Cloud Wallet

Cloud Layer

Cloud Agent

Cloud Wallet

DID Layer

Image courtesy of Sovrin

DID Auth

DID Auth is…

A simple standard way for a DID owner to authenticate by proving control of a private key

The decentralized identity “stack”

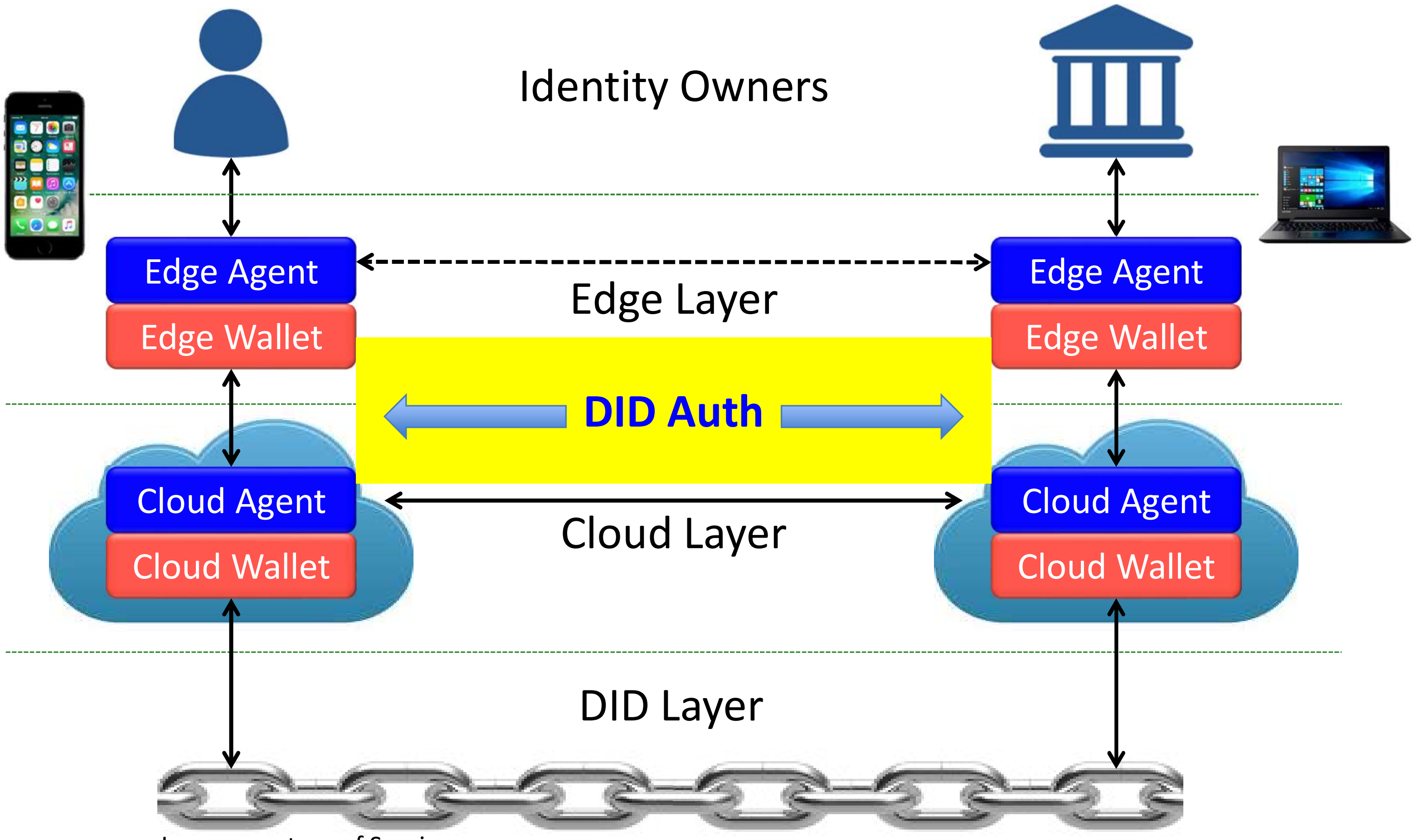
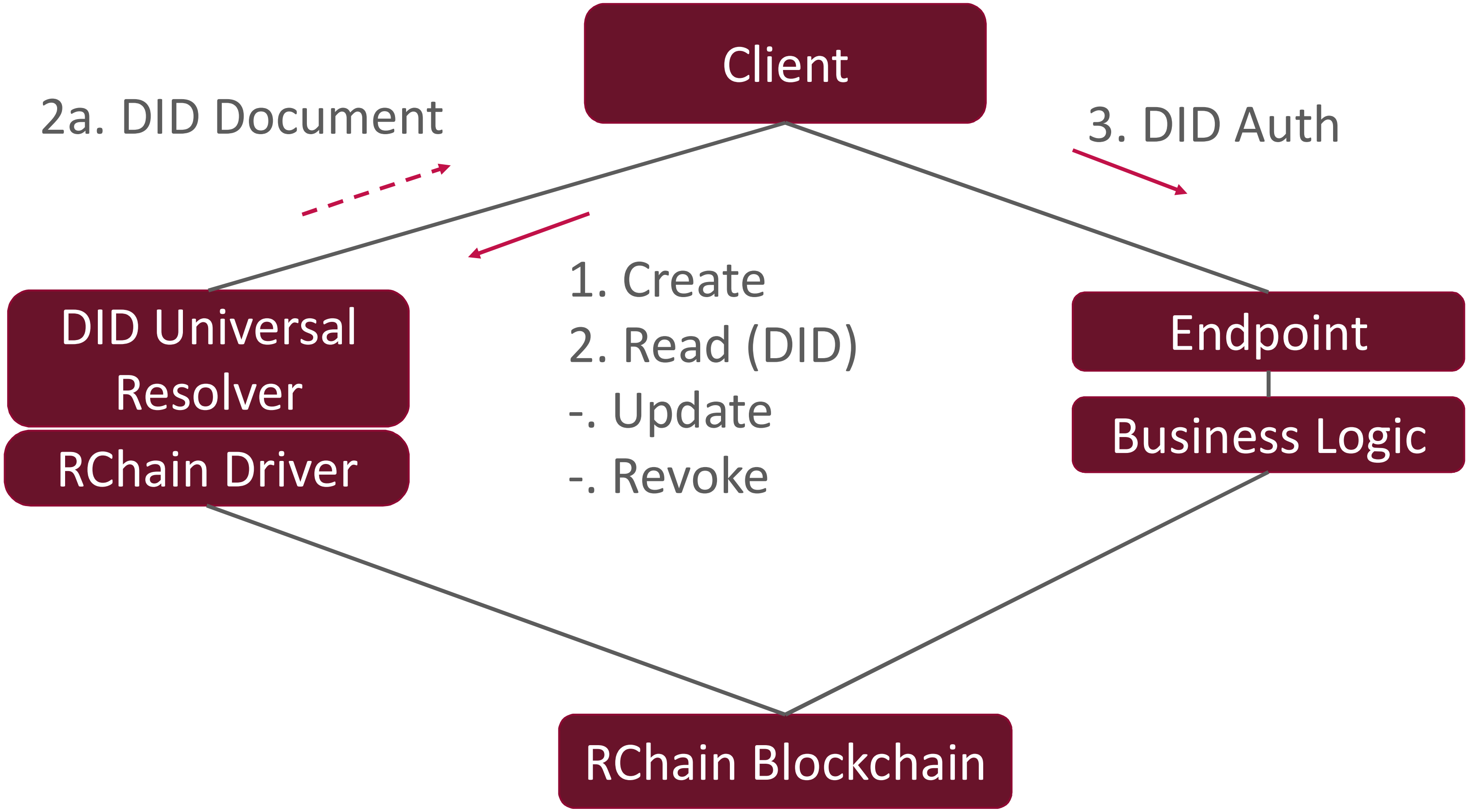


Image courtesy of Sovrin

Example Interaction with DIDs



The decentralized identity "stack"

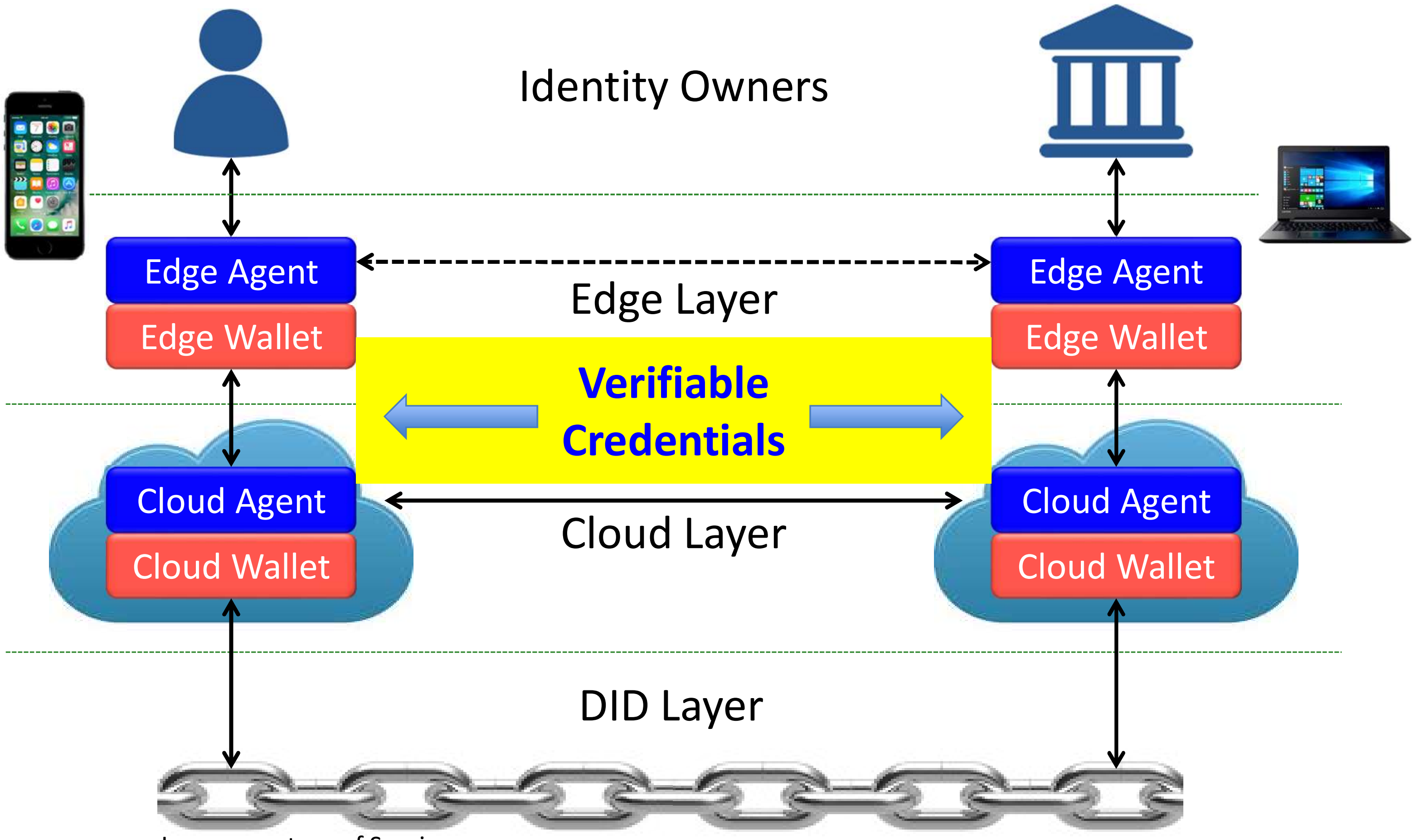


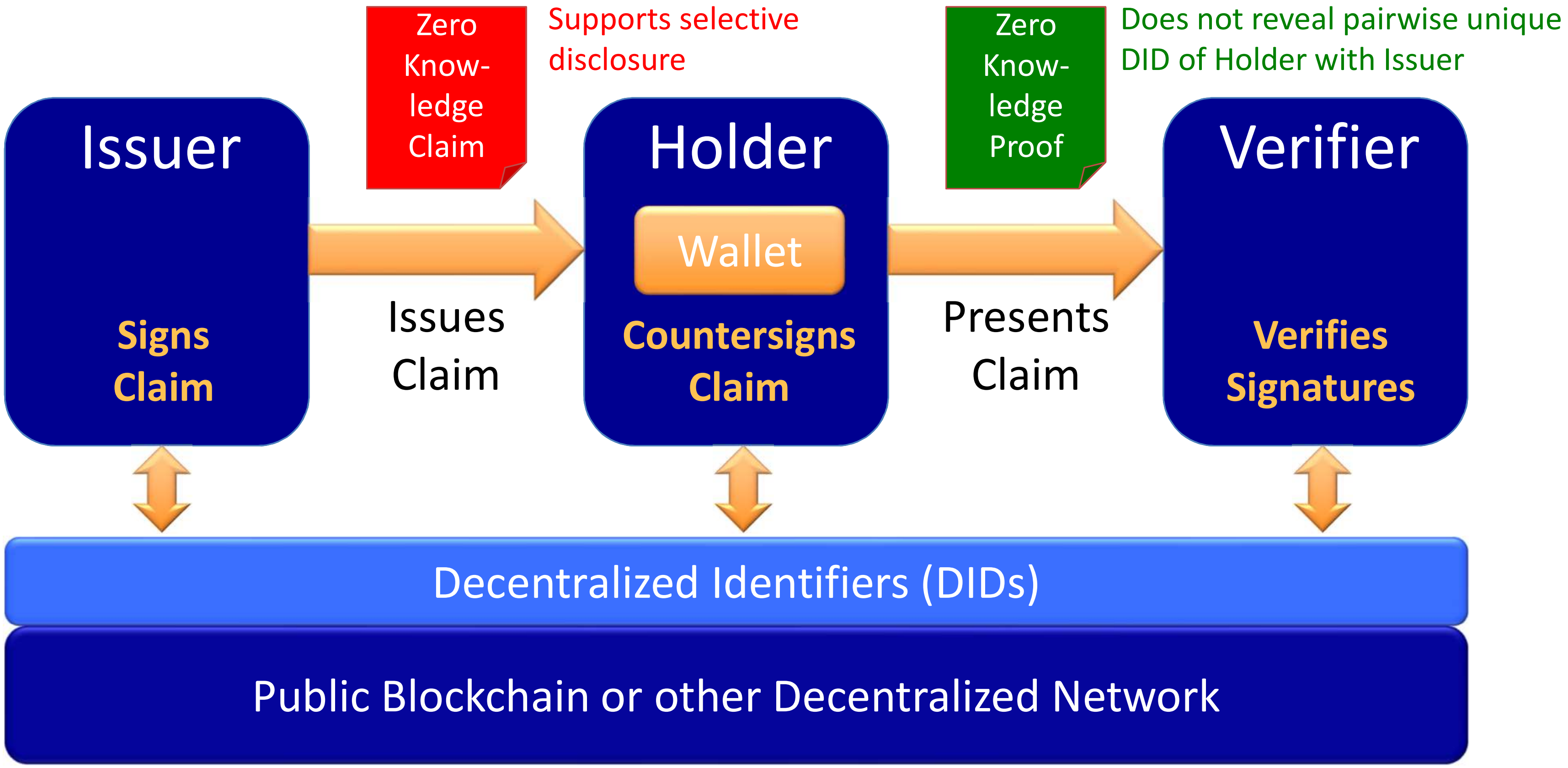
Image courtesy of Sovrin

Verifiable Claims

Verifiable claims are…

The format for interoperable, cryptographically-verifiable digital credentials being defined by the W3C Verifiable Claims Working Group

Sovrin Verifiable Claims Ecosystem



Issuer

Signs Claim

Zero Knowledge Claim

Supports selective disclosure

Issues Claim

Holder

Wallet

Countersigns Claim

Zero Knowledge Proof

Does not reveal pairwise unique DID of Holder with Issuer

Presents Claim

Verifier

Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network

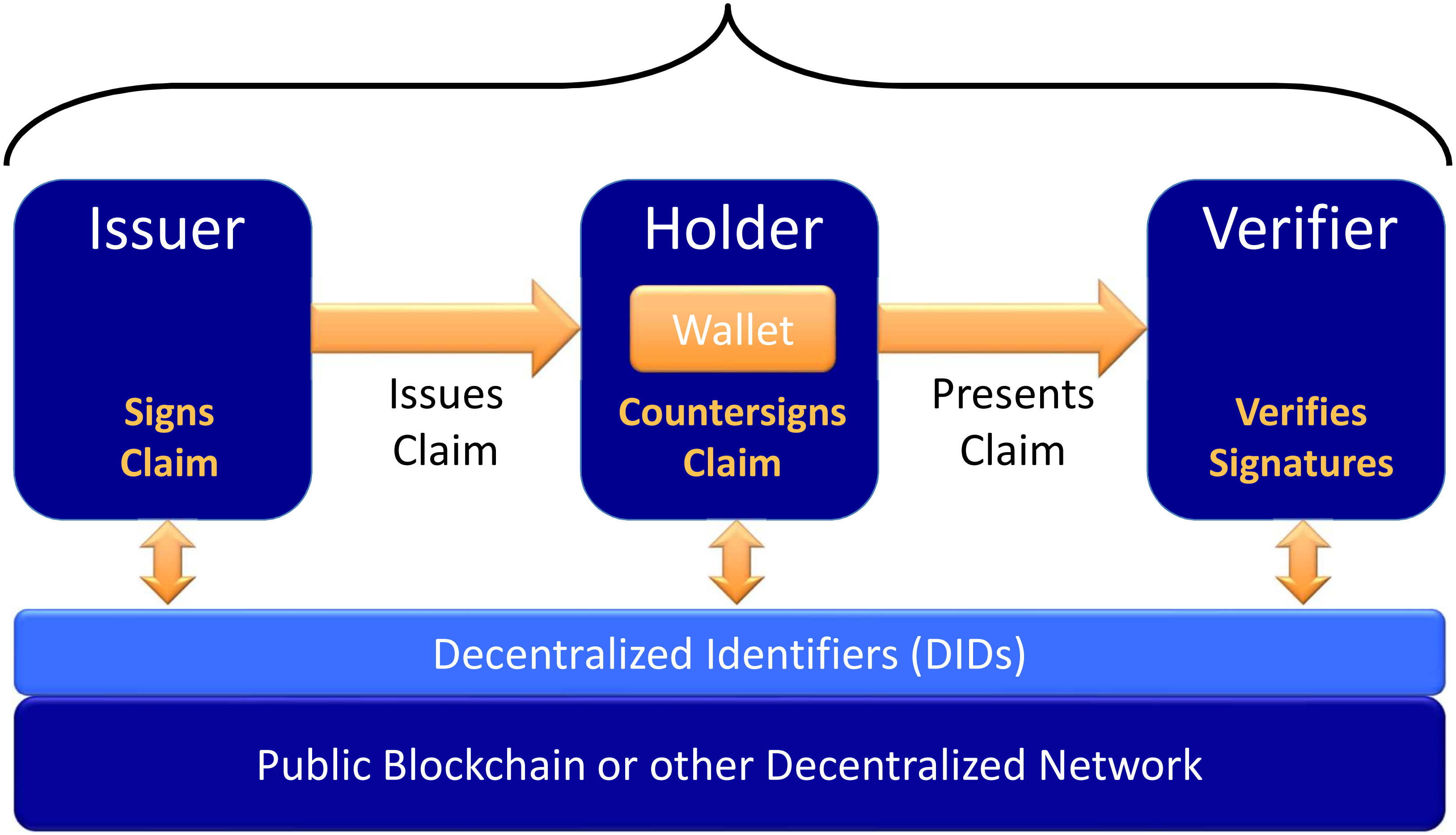
Image courtesy of Sovrin

Trust Frameworks

A trust framework is…

A set of business, legal, and technical rules which members of a community agree to follow in order to achieve trust online

Trust Framework



Issuer

Signs Claim

Issues Claim

Holder

Wallet

Countersigns Claim

Presents Claim

Verifier

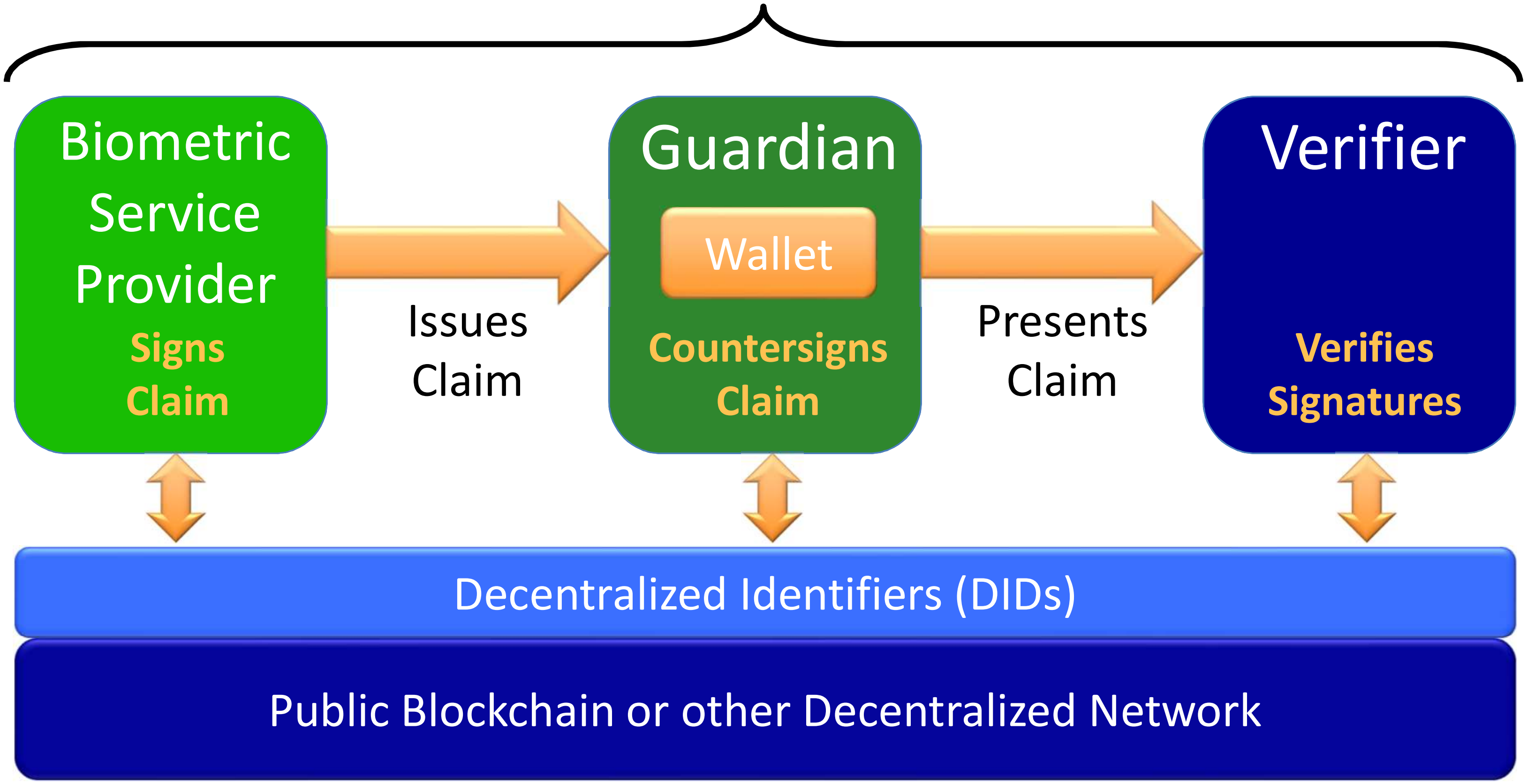
Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network

Image courtesy of Sovrin

Self-Sovereign Biometrics -
Identity for All Trust Framework



Biometric Service Provider

Signs Claim

Issues Claim

Guardian

Wallet

Countersigns Claim

Presents Claim

Verifier

Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network

Image courtesy of Sovrin

PITHIA

Thank You!

Ed Eykholt, Founder and Managing Director

Ed.Eykholt@pithia.com

www.pithia.com

Twitter: @Pithia_funds