Analysis and Evaluation of Blockchain-based Self-Sovereign Identity Systems

Martin Schäffner, November 18th, 2019, Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

Introduction

- Introduction to Self-Sovereign Identity
- Problem Statement
- Approach

Components of Self-Sovereign Identity

- RQ1: Which components comprise the architecture for self-sovereign identity?
- RQ2: What is the applicability of the integrated components?

Selected DID Methods

Analysis of DID Methods

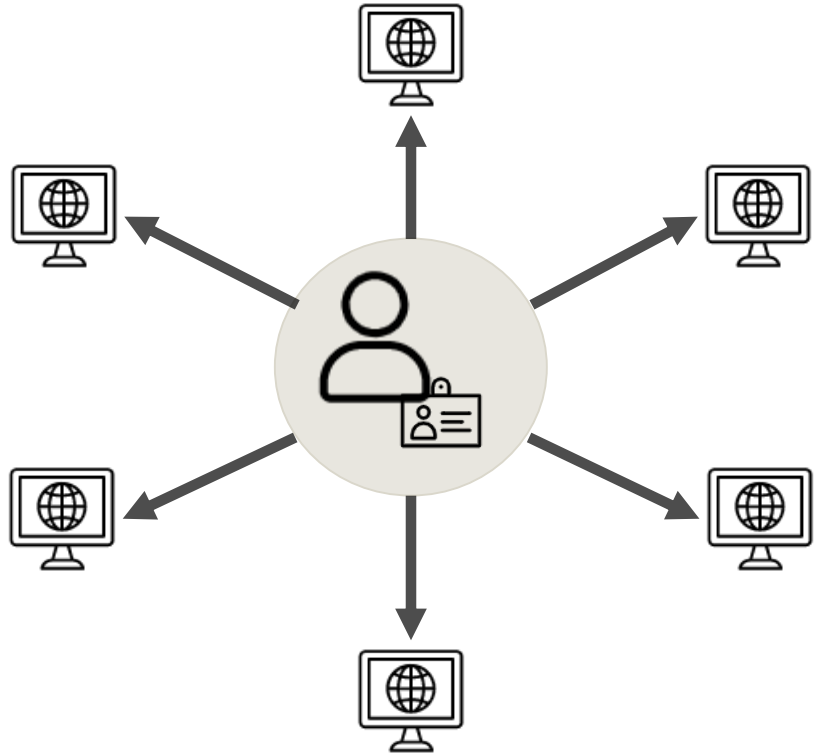
- RQ3: Which criteria can be used to analyze DID methods and their systems?
- RQ4: How do the DID methods and their systems differ based on the criteria?

Evaluation of DID Methods

Introduction to Self-Sovereign Identity (SSI)

Def.: An identity concept for the internet, where users have full control over their online identity and how and with whom their personal data is shared and used.

- User administrates identity by himself
- No need for identity provider
- Decentralized identity ecosystem
- Private data is kept off the ledger
- Sharing of data requires explicit consent
- Attestation of claims and credentials



Goal:
Align the digital identity closer to the analog one with decentralized identifiers and credentials

Icon Source: The Noun Project

Problem Statement

Conventional identity formats come with multiple issues...

- Users have **no full control** over their identifiers
- Trust in the internet is **hierarchical**

Decentralized Identifiers (DIDs) as new representations of identities…

- Users have **sole control** over their identifiers
- Trust in the internet is **decentralized**

Problem:

- How are **DIDs** integrated in the SSI ecosystem?
- Which **components** enable SSI and how are they connected?
- Which **solutions** exist that adapt SSI?

Research Approach

Methods of **Grounded Theory** were used for this thesis. (K. Charmaz and L. L. Belgrave., 2007)

Information was gathered from:

- Publications from experts in the field
- Online Meetups
- Academic Literature
- (Technical) Whitepapers
- Format- & DID method specifications
- Online forums

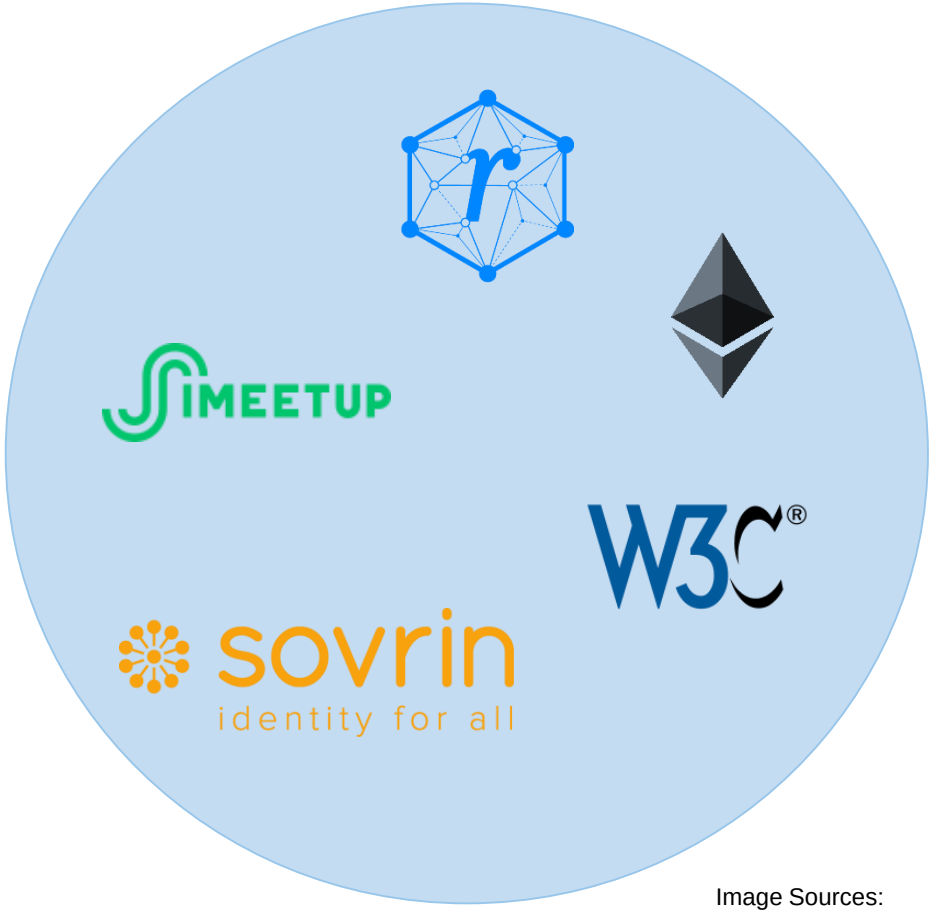
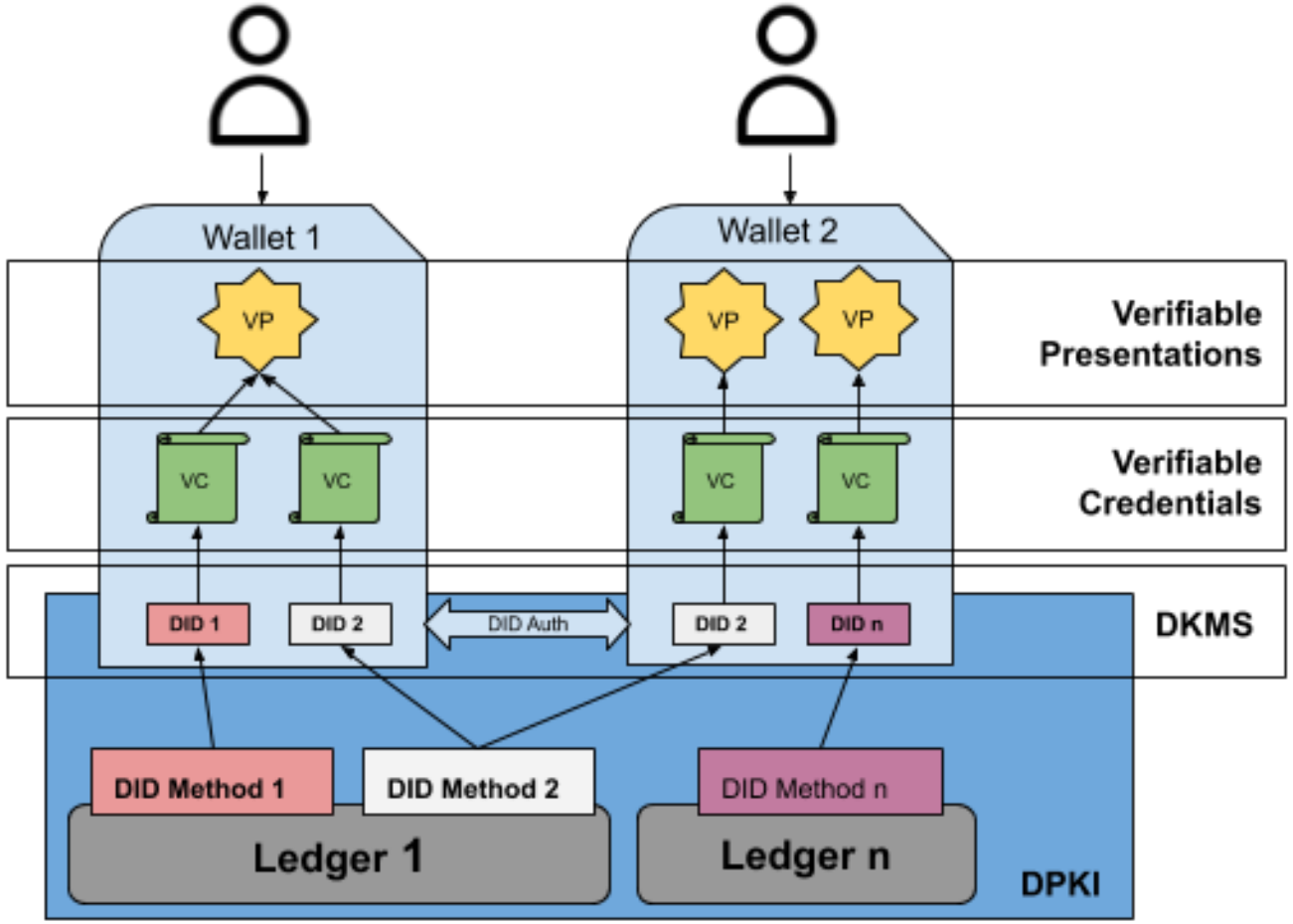


Image Sources:
SSI Meetup, RWOT, Ethereum, W3C, Sovrin

RQ1: Which components comprise the architecture for Self-Sovereign Identity?

- **Web of Trust** between actors
- **Wallets** unite the four layers
- **Verifiable Presentations** to share data in a privacy-preserving manner
- **Verifiable Credentials** to attest personal information
- **DKMS** to manage keys and communication
- **DID Methods** to create and manage DIDs on a ledger to establish **DPKI**

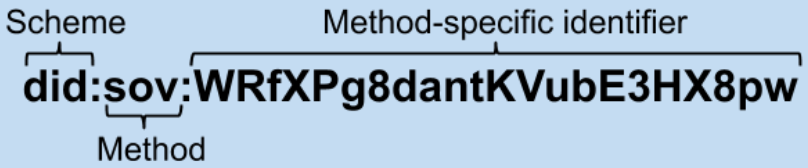


Icon Source: The Noun Project

RQ2: What is the applicability of the integrated components?

Decentralized Identifiers (DIDs)

- Backed with a key pair
- Standard for the SSI ecosystem

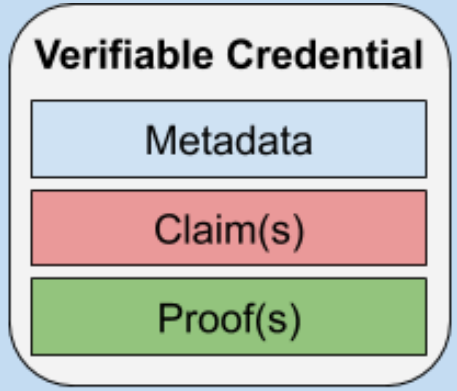


- **DID Document** (DDO) contains further information
- **DID Resolution** to get the DDO from a DID
- **DID Methods** define how to create, manage, and resolve DIDs on a specific ledger

→ Leads to Decentralized Public Key Infrastructure

Verifiable Credentials (VC)

- Standard for the SSI ecosystem
- Attested to DIDs
- Cryptographically verifiable
- Roles:
  - Issuer
  - Holder
  - Verifier
- Allow derivation of VPs
- Support any type of claim or credential



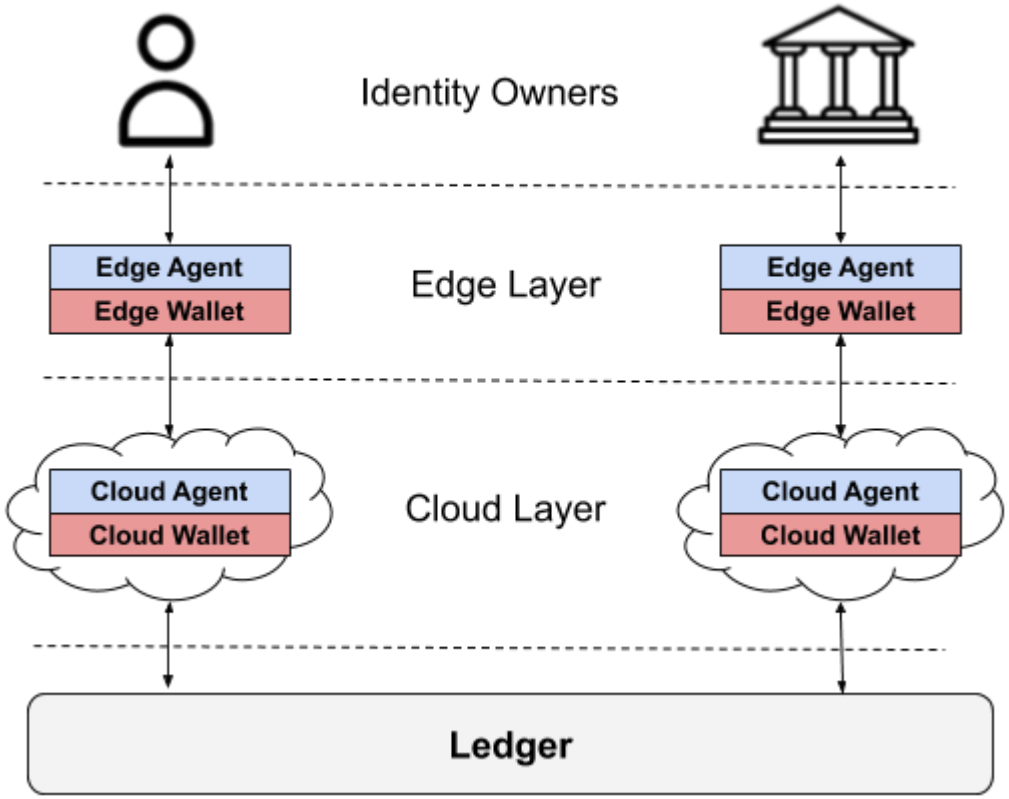
→ Enables to trustfully attest and share personal information

RQ2: What is the applicability of the integrated components?

Decentralized Key Management System

- Allows management of keys and communication
  - Key rotation
  - Key revocation
- Multiple DIDs in one wallet
- Should improve interoperability between DIDs
- Agent layer for user‘s devices
- Cloud layer for availability and communication and to manage multiple wallets

→ Missing Wallet specification
→ No standard processes defined yet
→ Lack of interoperability



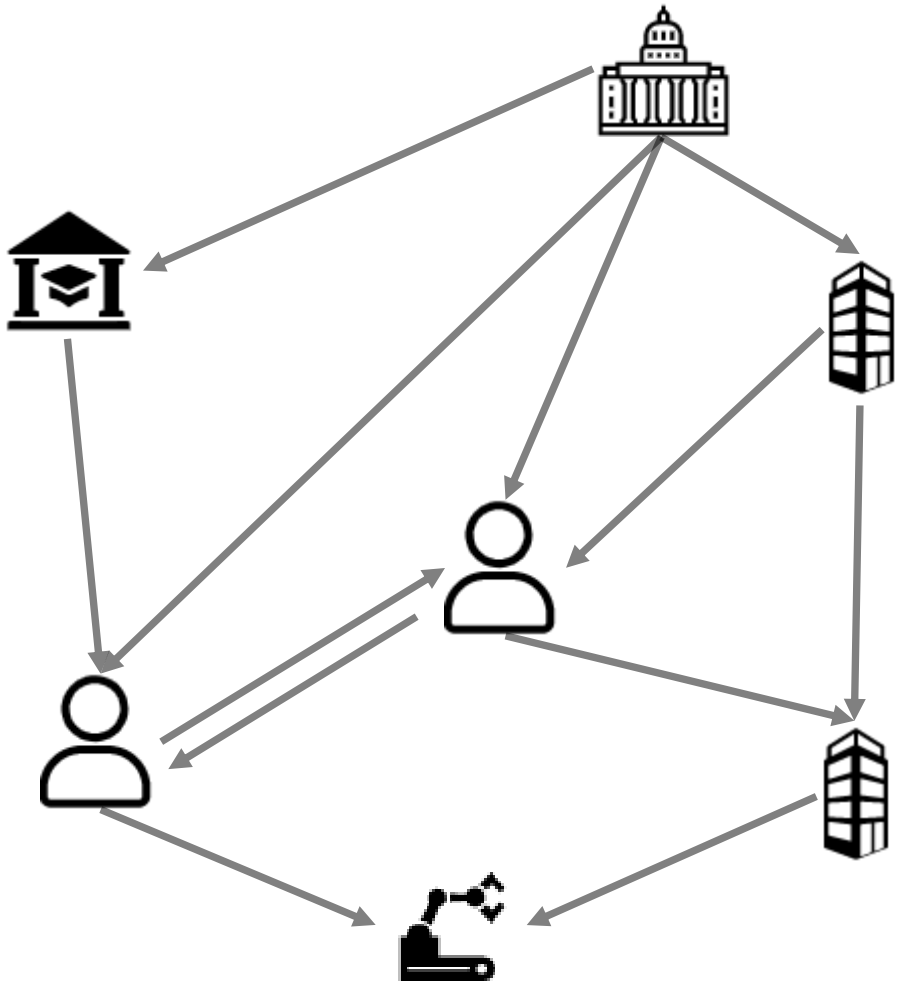
Icon Source: The Noun Project

RQ2: What is the applicability of the integrated components?

Web of Trust

- Adopted and extended PGP by Phil Zimmerman
- How can users trust each other?
- Entities are equal
- Attestation and Verification of personal information
- Trust anchors required
- DID Auth to authenticate
- Users have to know the DID of others

→ Not yet fully used
→ No prevention of Sybil-attacks



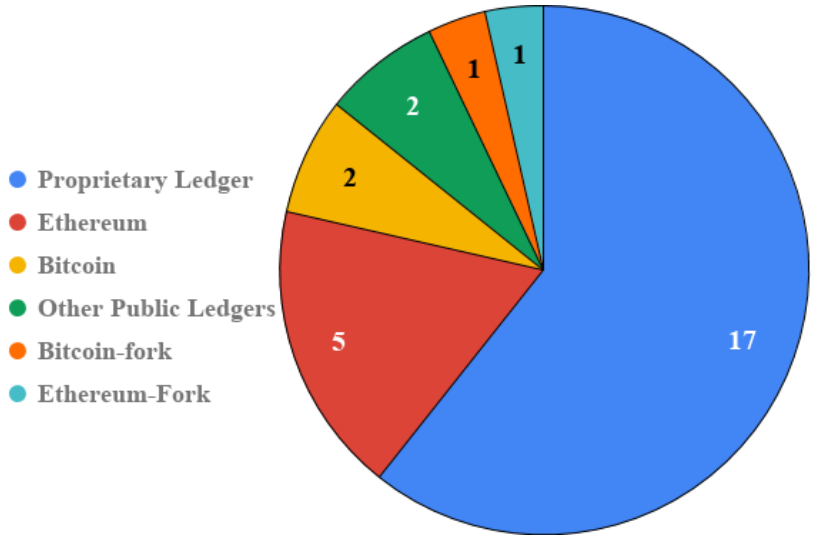
Icon Source: The Noun Project

Already existing DID Methods

DID Method Registry as source for registered SSI systems:

- 28 registered DID methods in total*
- Most of them are proprietary ledgers

  → specially to enable SSI



Selection criteria:

- Progress in development
- Available documentation
- Potential relevance to users
- Different adoptions of SSI on a specific ledger
- Interesting use cases

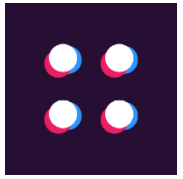
* as of August 2nd, 2019 Source: W3C

Selected DID Methods

BTCR

- SSI on Bitcoin
- Use of OP_RETURN & TxRef

Bitcoin



Blockstack

- Naming System on a Bitcoin-Fork
- ID to access dApps

Bitcoin-fork

uPort

- Smart contract to manage DIDs
- Extensive SDK for SSI

ERC725

- Smart Contract represents the identity

SelfKey

- Smart contract to manage DIDs
- DID gives access to financial marketplace

Ethereum

Sovrin

- Full-Stack identity ecosystem
- Public, permissioned

Veres One

- Ledger to enable SSI
- Public, permissionless

Proprietary Ledgers

RQ3: Which criteria can be used to analyze DID methods and their systems?

Defined criteria to emphasize the differences between each DID methods and their systems

Status: Is the DID method and system already released?

Management and Governance: Who manages the DID method and its system? Is there a governance model?

Fee Structure: Which fees occur and how high are they?

System Design: What is the level of integration? What goes on the ledger? What are their functionalities?

Establishment of Trust: What is the level of trust? Is there an additional trust infrastructure?

Icon Source: The Noun Project

RQ4: How do the DID methods and their systems differ based on the criteria?

	Status	Management	Governance Model	Fees
BTCR	✓	Community	✗	Gas costs
Blockstack	✓	Institution	✗	Gas costs
uPort	✓	Community	✗	Gas costs
ERC725	✓	Community	✗	Gas costs
SelfKey	✓	Institution	✗	Gas costs
Veres One	✗	Institution	✓	low
Sovrin	✓	Institution	✓	high

Icon Source: The Noun Project

RQ4: How do the DID methods and their systems differ based on the criteria?

	Additional System?	Integration Level	Ledger Interaction	Credentials	Delegation
BTCR	✗	1st Level	CRUD*	✗	✗
Blockstack	✓	2nd Level	CRUD	✗	✗
uPort	✗	1st Level	CRUD	✓	✓
ERC725	✗	1st Level	CRUD + ERC735	ERC735	✓
SelfKey	✓	1st Level	Create + ERC780	ERC780	✗
Veres One	✗	1st Level	Create, DDO	✗	✗
Sovrin	✗	1st Level	CRUD + Revocation Registries	✓	✓

*CRUD = Create, Read, Update, Delete

Icon Source: The Noun Project

RQ4: How do the DID methods and their systems differ based on the criteria?

Trust Services Criteria from AICPA

	Availability	Security	Processing Integrity	Confidentiality	Privacy	Additional Trust Infrastructure
BTCR	✗	✓	✓	✗	✓	✗
Blockstack	✓	✓	✓	✗	✓	✗
uPort	✓	✓	✓	✓	✓	✗
ERC725	✓	✓	✓	✗	✓	✗
SelfKey	✓	✓	✓	✗	✓	✓
Veres One	N/A	N/A	N/A	N/A	N/A	✓
Sovrin	✓	✓	✓	✓	✓	✓

Icon Source: The Noun Project

Evaluation of DID Methods

Bitcoin Reference

+ SSI is possible
- No credentials
- Requires new address for each DID operation

Blockstack

+ Forked Bitcoin for improved usability
+ 2nd-Level protocol integration
+ Great applicability
- No attestation using Claims or VC

Veres One

+ Concept is promising
+ Governance model available
- Not released yet

Sovrin

+ Full-stack identity system
+ Adoption of Verifiable Credentials
+ Extensive Governance and Trust Frameworks
- Expensive

Evaluation of DID Methods

uPort

+ Extensive documentation
+ Credentials library
+ Delegation, Attribute attestation
+ Great for enterprise use cases

ERC725:

+ Smart Contract as Identity
+ Delegation of responsibilities possible
+ Claims supported
- Smart Contract deployment necessary

SelfKey:

+ Claims supported
- Limited use of DID (create)
- KYC required

Evaluation of the SSI Ecosystem

Overall a promising concept for online identities:

+ Users have control over their identifiers and how information is shared
+ Doesn’t require centralized institutions
+ Lots of standards, e.g. verifiable credentials
+ Already many DID methods available/in development

  → Governance is important for corresponding identity systems

SSI is still in its early stages:

- Lack of interoperability
- DIDs are use-case bound
- Missing Wallet Specification
- Web of Trust not clear if it is sufficient
- How will users get onboarded?

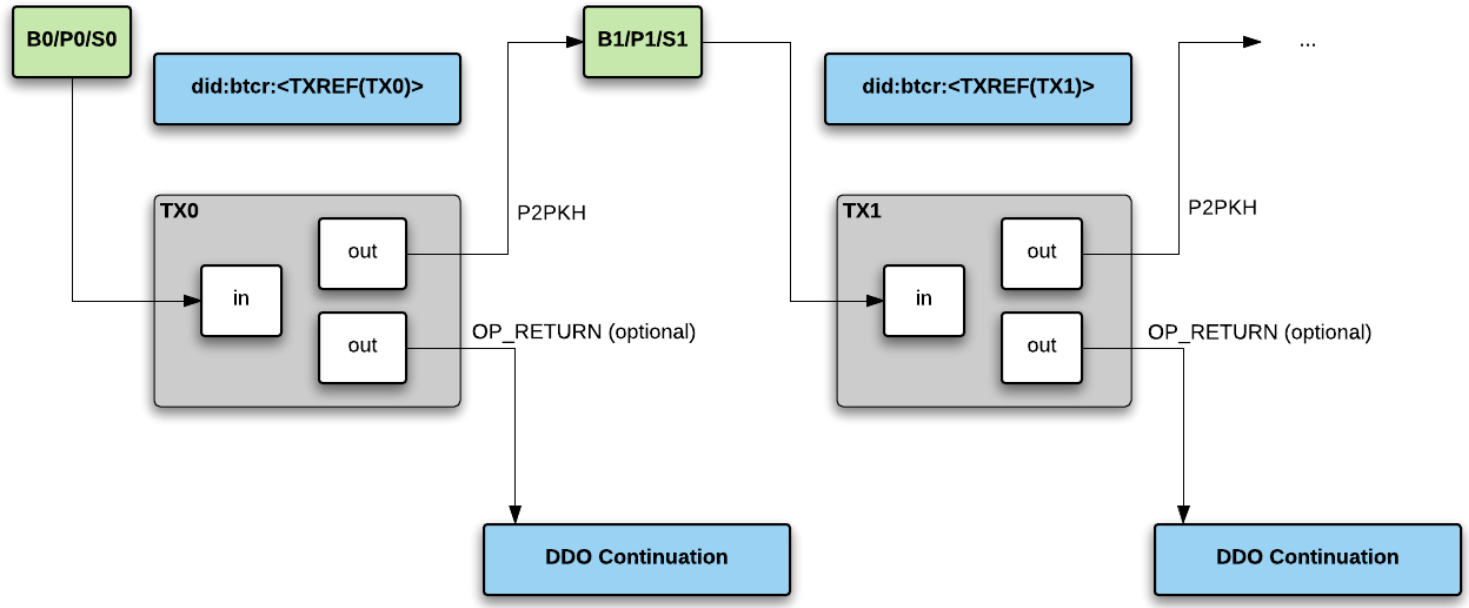
Martin Schäffner

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

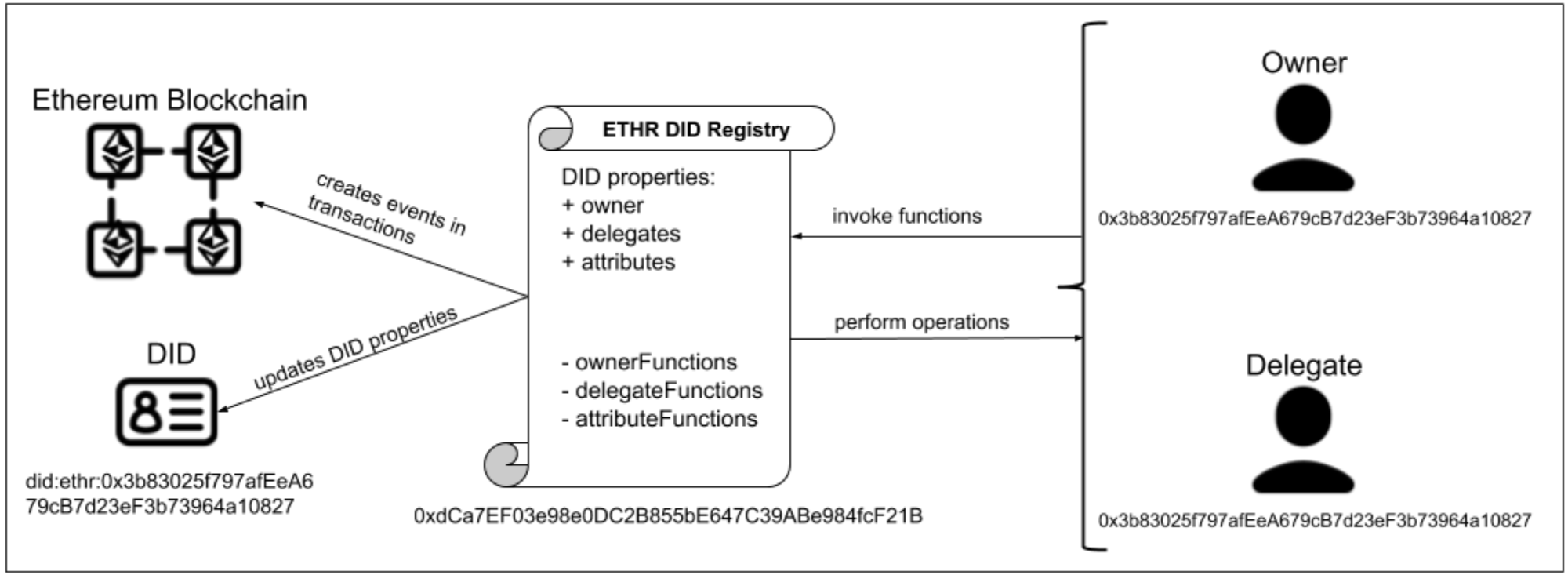
Boltzmannstraße 3
85748 Garching bei München

Martin.schaeffner@tum.de

BTCR

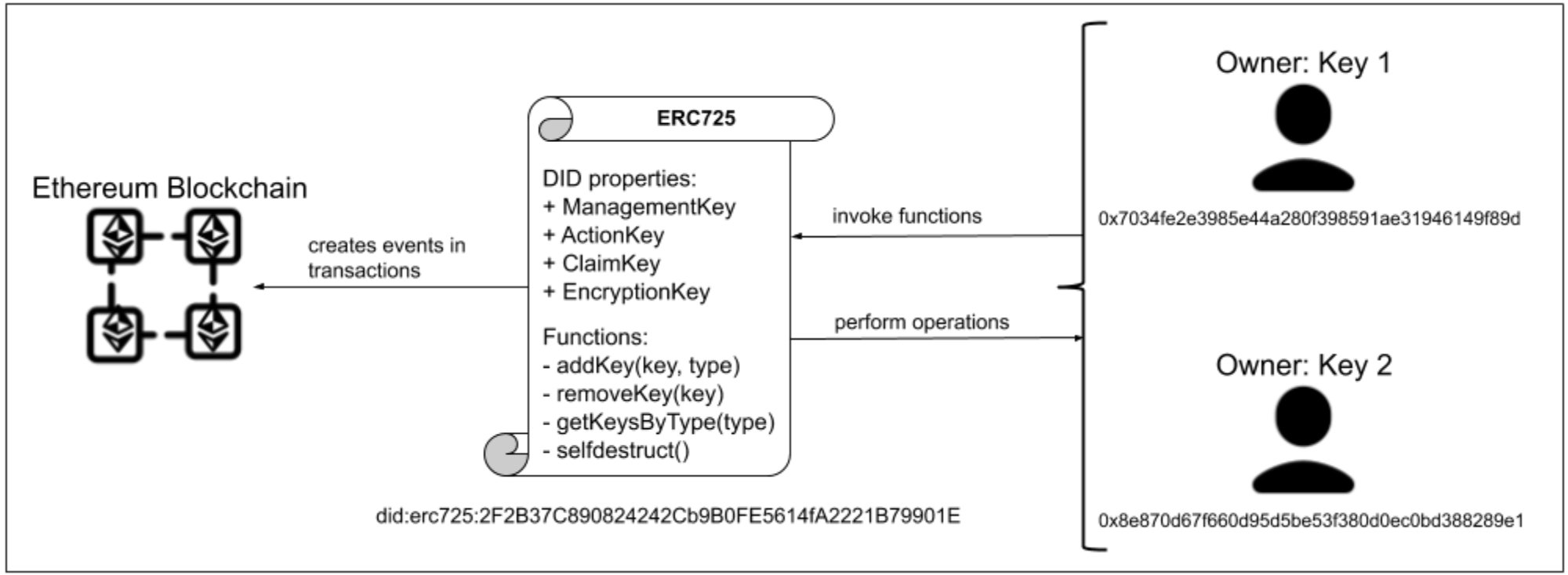

B0/P0/S0
did:btcr:<TXREF(TX0)>
B1/P1/S1
did:btcr:<TXREF(TX1)>
...
TX0
in
out
out
P2PKH
OP_RETURN (optional)
TX1
in
out
out
P2PKH
OP_RETURN (optional)
DDO Continuation
DDO Continuation

ETHR



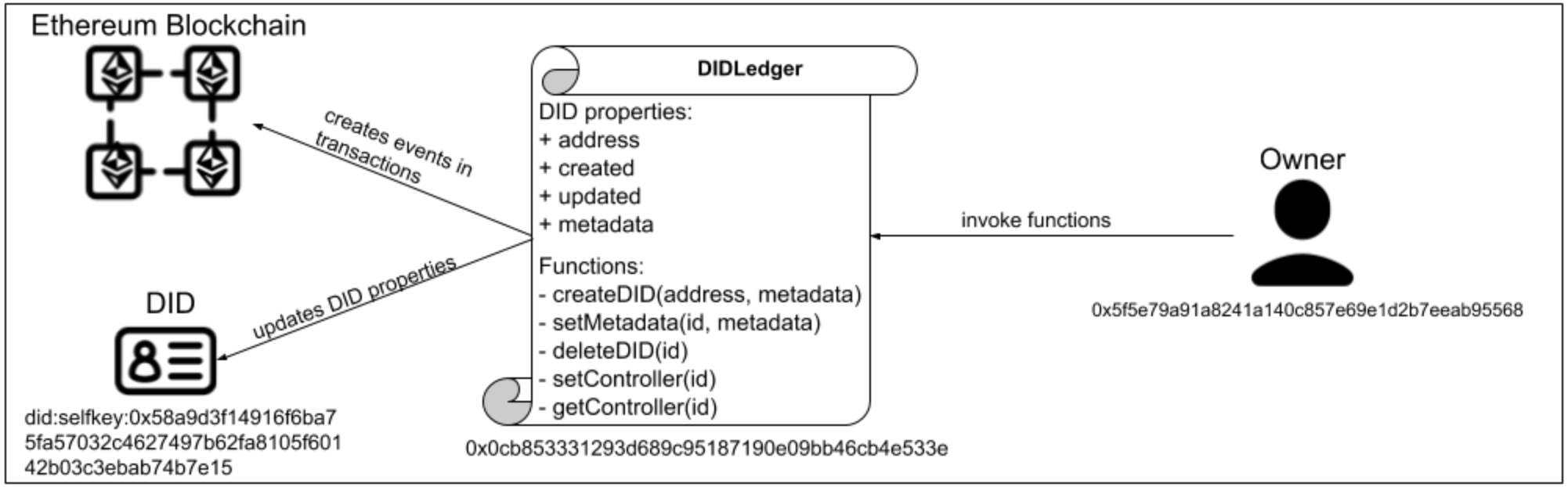
Icon Source: The Noun Project

ERC725



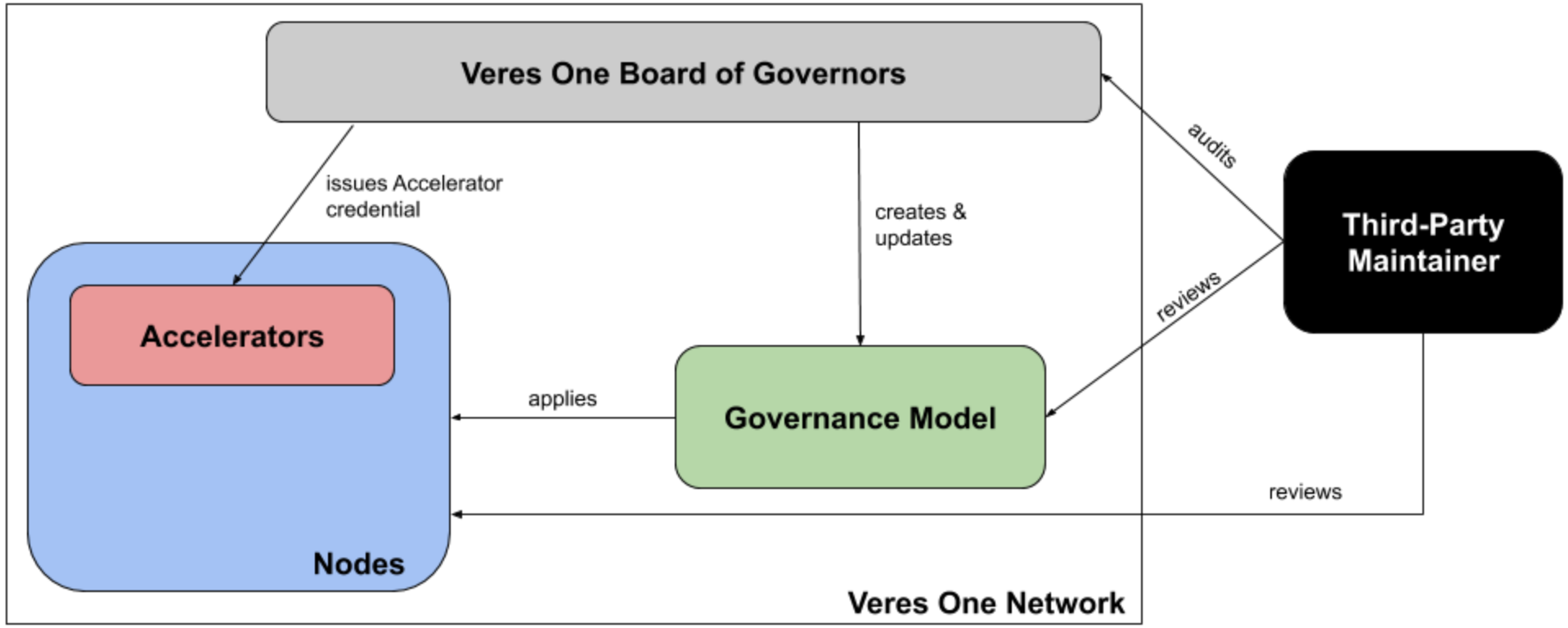
Icon Source: The Noun Project

SelfKey

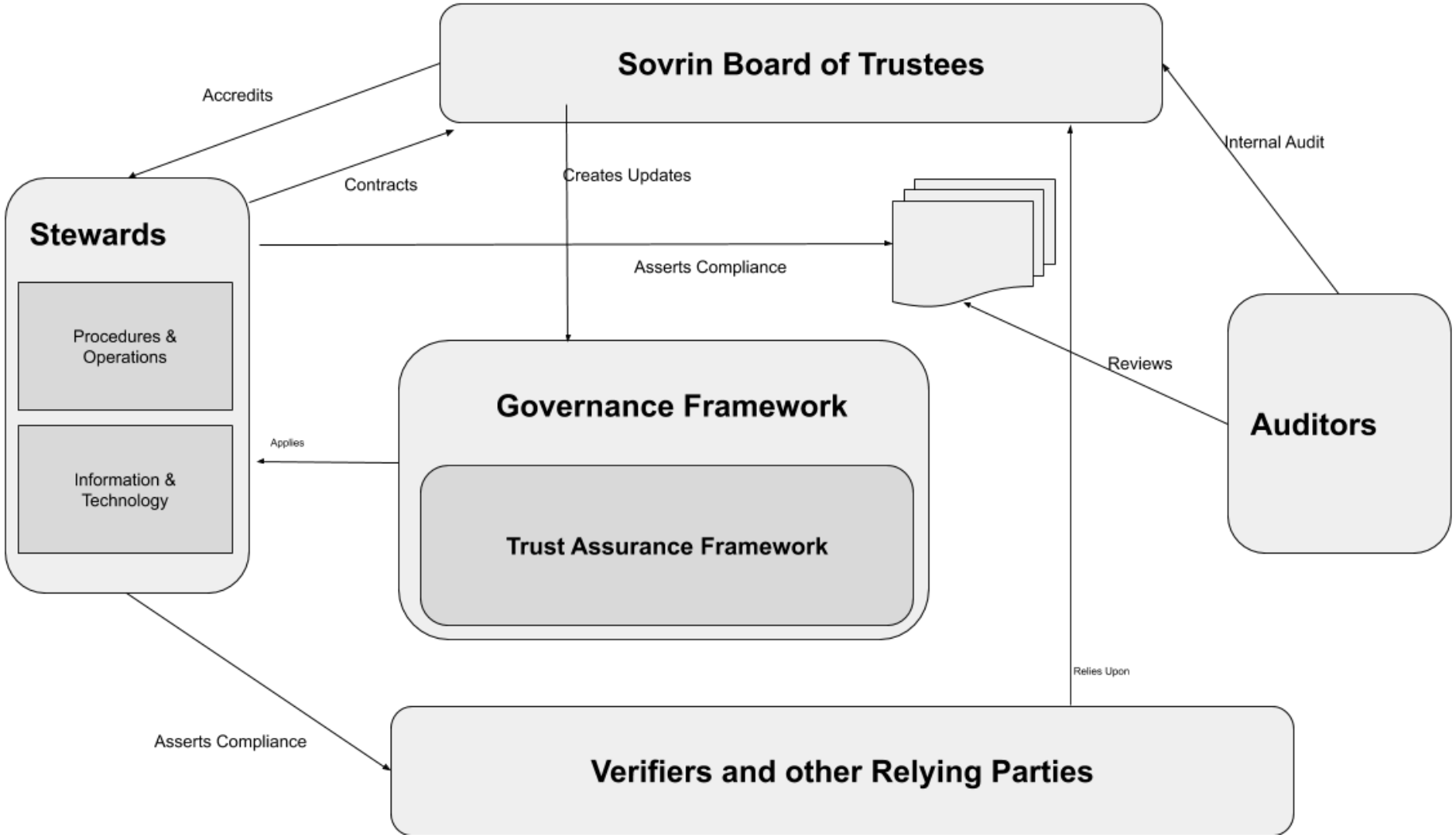


Icon Source: The Noun Project

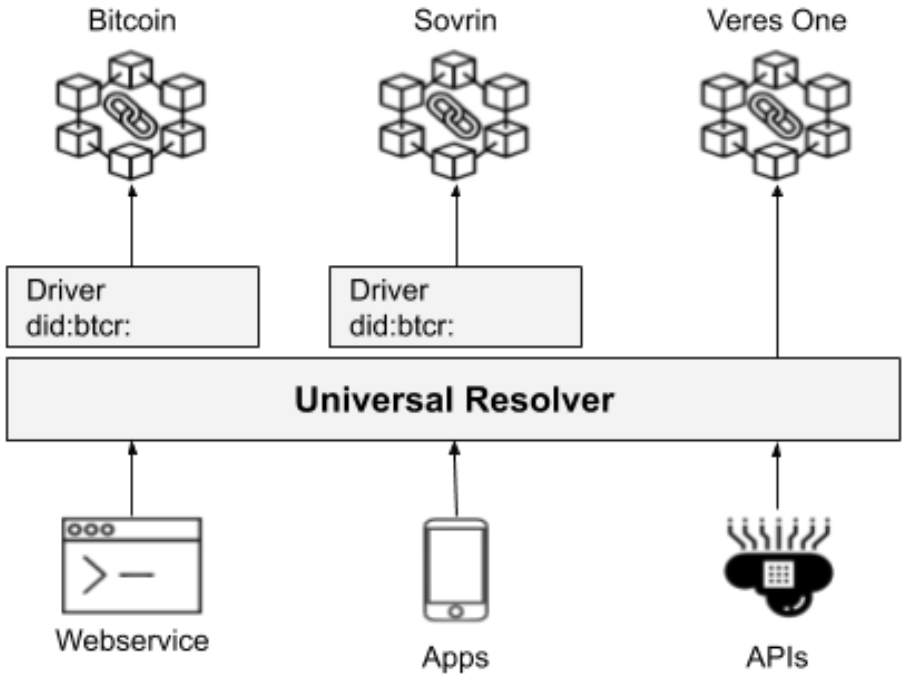
Veres One Trust Framework



Sovrin Trust Framework

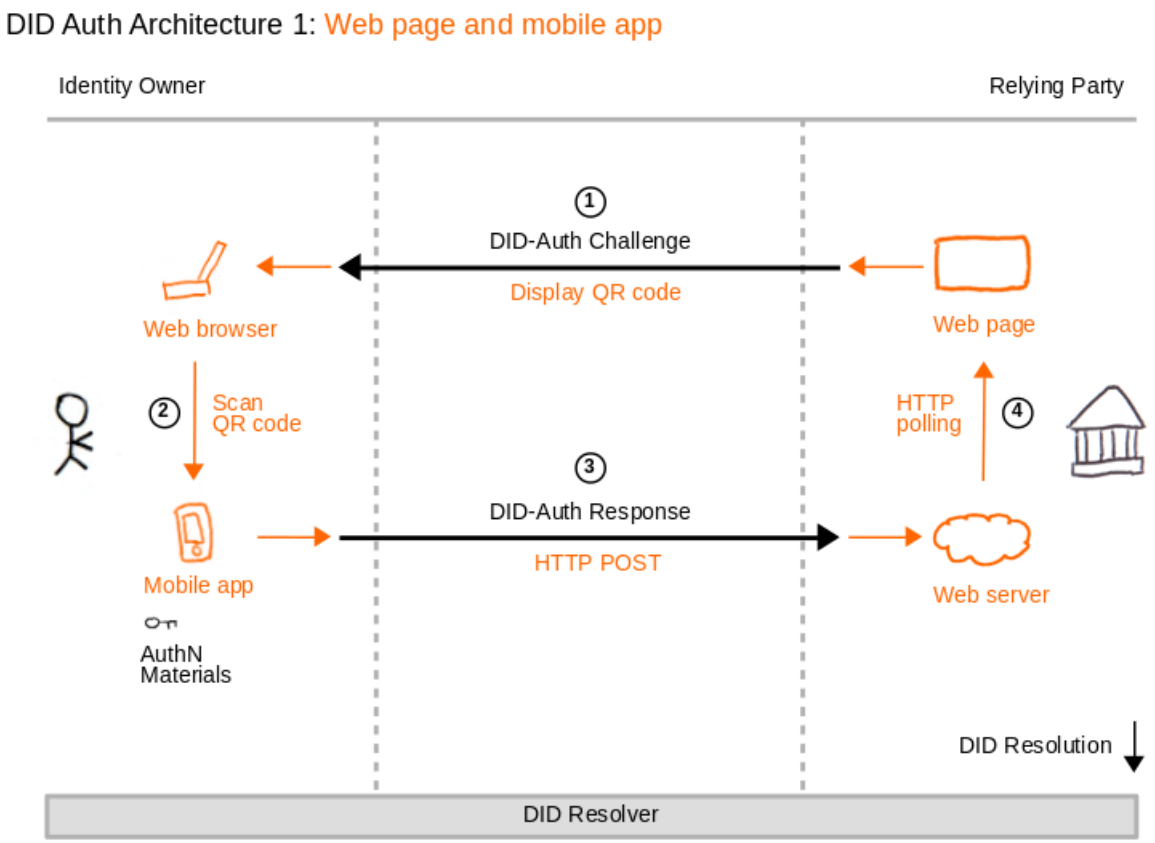


Universal Resolver



Icon Source: The Noun Project

DID Auth



Icon Source: The Noun Project