SCAN

(Source Code Attestation Network)

Vinod Panicker

Distinguished Member Technical Staff

17-12-2017

Vinod Panicker

About me

Expert in open source ,automation, AI and crowd Sourcing platforms with 18+ years of experience in software development.

Co-Creator

- **Openconnect Virtual Env (OVE):** Environment Provisioning Solution.
- **Openconnect :** Inner sourcing platform.
- **Cyber Scraper :** Digital Asset Management for Maintenance projects
- **Wipro UT, WiproCodeChecker And few more..**

Specializations

- **Mentoring open source Projects, Expertise in code partitioning ,open source licensing and open source research .**

Patents

Granted:
Cyber Scraper : System and method for automating identification and download of web assets or web artefacts.

Filed :
269089:Method and system for generation of reusable design patterns
275183:Source Code Auditor with a customized Rules Builder

Open Source is here to stay…

- 65 % companies contributing to open source *
- 59 % doing so to gain a competitive edge….

So is there a lack of TRUST ???

*Open Source Survey, https://www.blackducksoftware.com/2016-future-of-open-source

Open Source Code Management Systems

Monitor and alert when new threats are reported

Fully discover all open source in your code

Set and enforce open source policies

Map components to known vulnerabilities

Identify license and component quality risks

Seamless integration into your DevOps environment

SCAN

Source Code Attestation Network (SCAN) is a proposed code attestation network to self-attest open source code. SCAN makes use of Decentralized Digital Identity to determine the provenance of source code.

SCAN is a public permissioned Blockchain network that can help in the validation of verifiable claims with respect to origin, license and usage of source code.

SCAN will help in determining source code provenance in a transparent manner.

SCAN: Features

Distributed Ledger as world view of open source code

Represents Source code as Source code Unit (SCU)

Store Hub -Registry DID/DDO/Proofs

Trust Anchor Model (Issuer, Verifier , Prover)

Self Attestation of Source Code

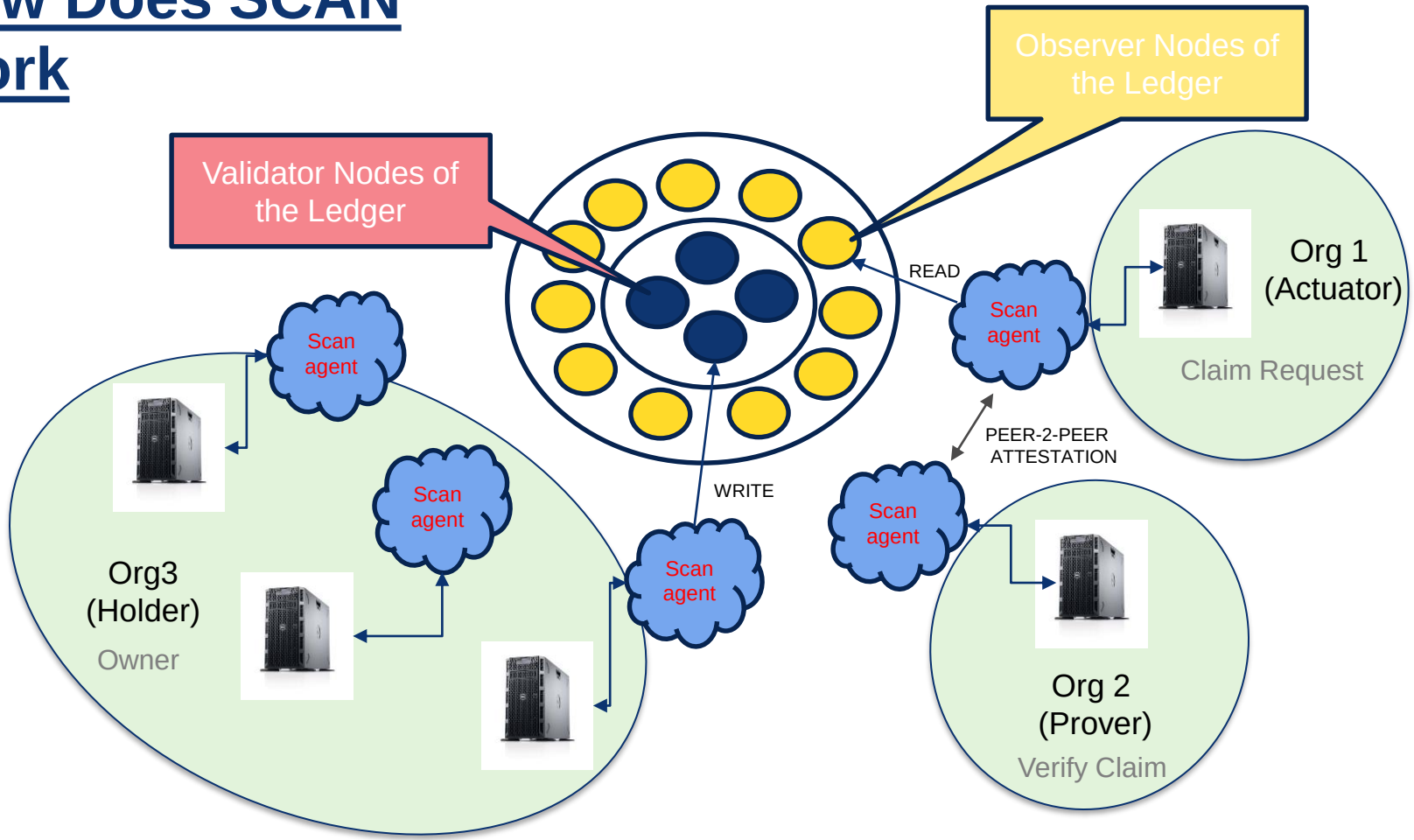
Peer 2 Peer Attestation

ZKP (Zero Knowledge Proofs)

SCAN Services

- Attestation
- Repudiation
- Validation

How Does SCAN Work



SCAN Components

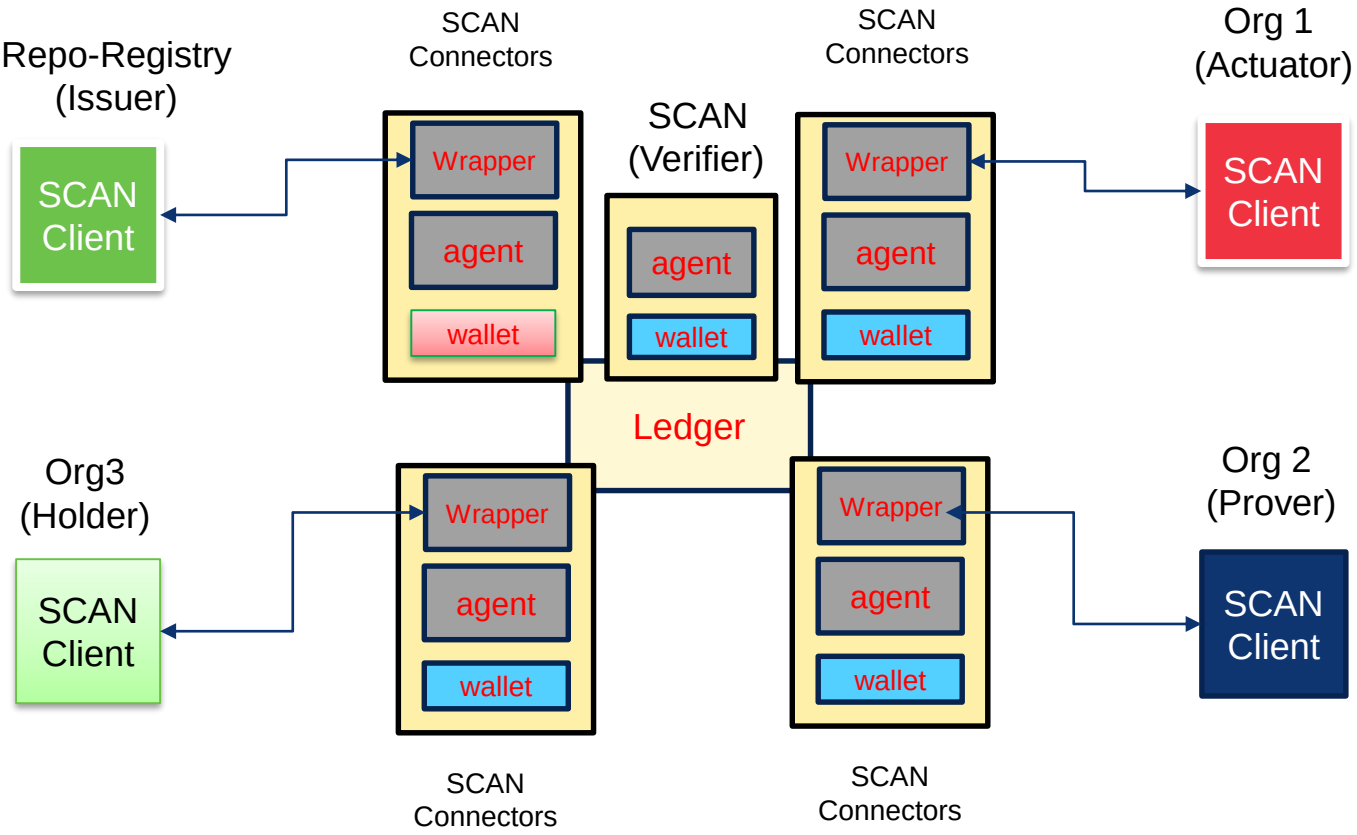
Blockchain Protocol Layer

- Ledger
- Validator Nodes
- Observer Nodes
- Agents

Off-chain Components

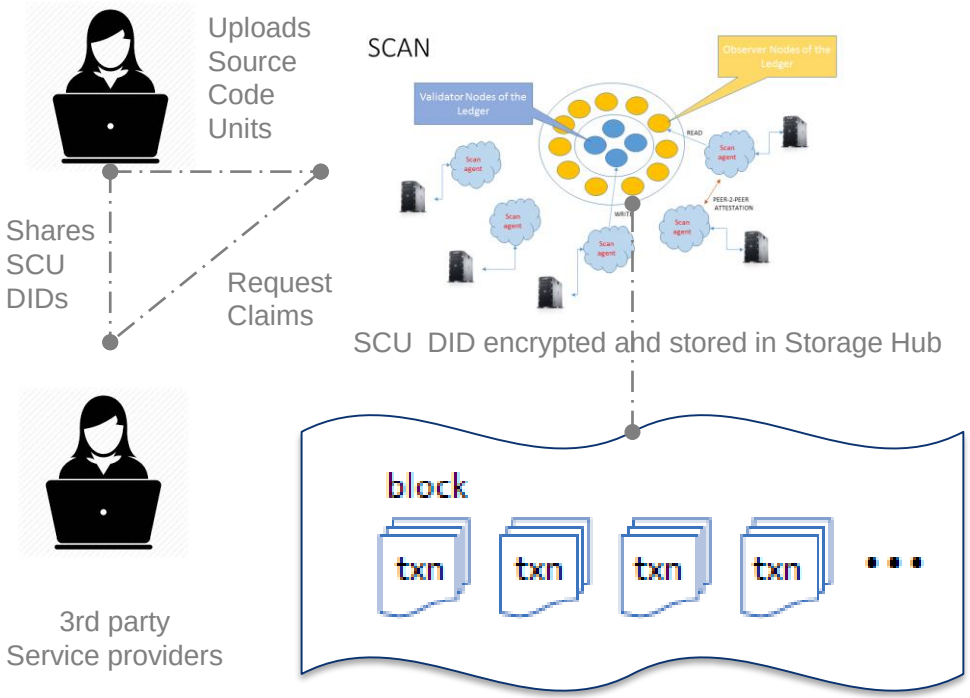
- Source code Parsers (AST)
- DID generators for SCU
- SCU Combiner : Managing Granularity of SCU
- Deduplication Tools
- Audit Tools/System Connectors

TRUST Model


Repo-Registry
(Issuer)
SCAN
Client
SCAN
Connectors
Wrapper
agent
wallet
SCAN
(Verifier)
agent
wallet
SCAN
Connectors
Wrapper
agent
wallet
Org 1
(Actuator)
SCAN
Client
Ledger
Org3
(Holder)
SCAN
Client
Wrapper
agent
wallet
SCAN
Connectors
Wrapper
agent
wallet
SCAN
Connectors
Org 2
(Prover)
SCAN
Client

SCAN Services

Provides proofs of Code Commits, open source Usage , open source License based on verified claims raise against public source code repositories.



SCAN Services Overview:

- Organization uploads SCU -DIDs
- Claims on DID SCU are verified and self-signed by Validator Nodes & Trust Anchors
- Digital, hashed representation SCU
- Encrypted SCU DIDs will be stored in Blockchain
- When SCU Owners provide consent then the SCU proofs are shared with a 3rd party after digital handshake

Consensus (built-in)

- Consensus based on:
  - Proof Of Code Commit (POCC)
    - Based on Public Code Repositories
  - Proof Of open source Usage (POU)
    - Based on Verified claims in SCAN ID Hub as usage proof
  - Proof Of Applied open source License (POAL)
    - Precedence of license made available

Sustaining SCAN

- Community driven governance model
- Rotation of Foundation Members
- Credibility on SCAN
- Trust Anchor (Add more participants)
- Incentives sharing Proofs
- Organize Events, Hack fest to upload public repos
- Open source from day one.

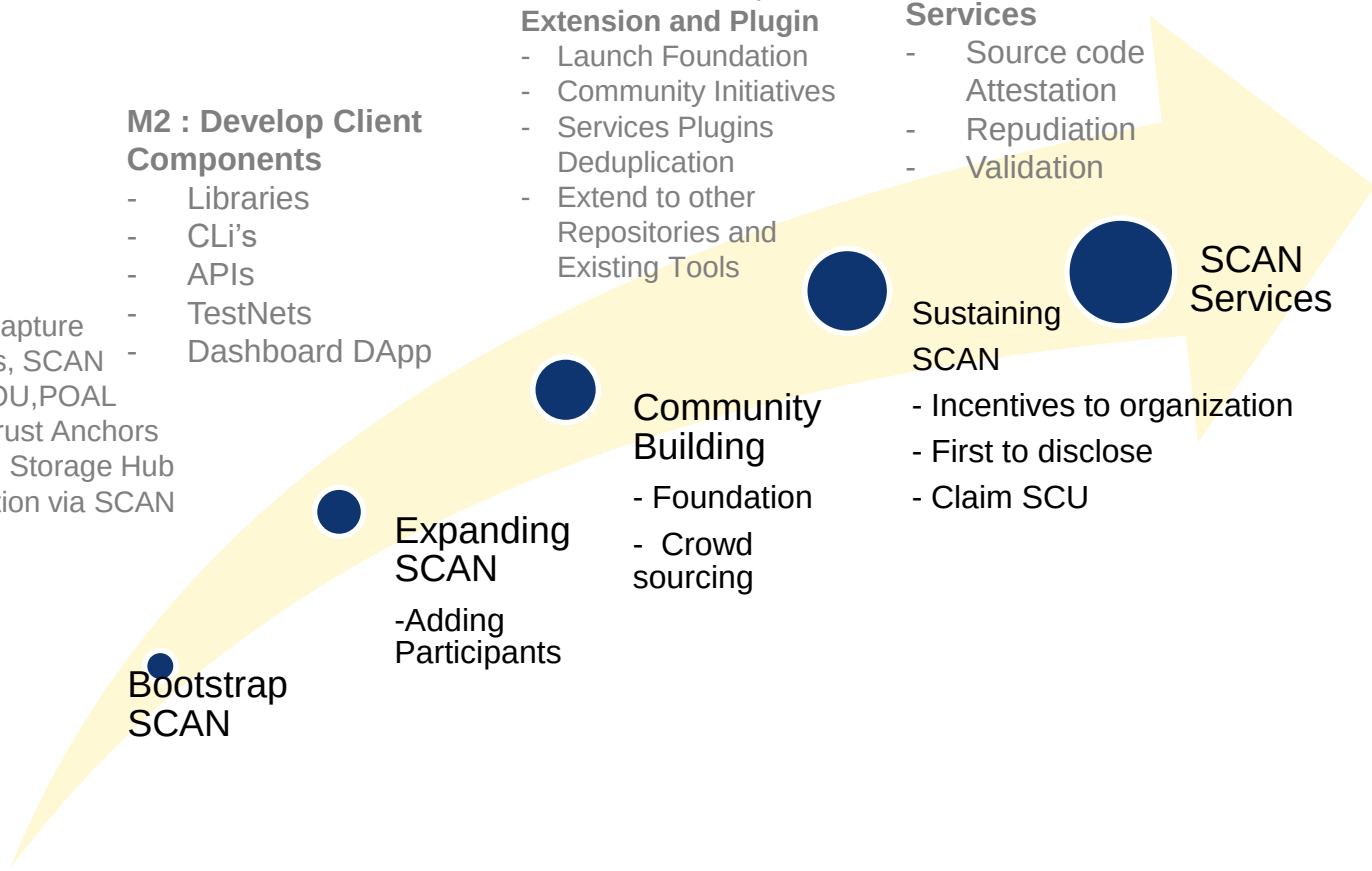
SCAN Roll out

M1 : Prototype
- SCAN metadata capture
- SCAN Connectors, SCAN Agents POCC, POU,POAL
- Self attestation, Trust Anchors
- SCU DID/DDO on Storage Hub
- SCU DID Verification via SCAN

M2 : Develop Client Components
- Libraries
- CLi's
- APIs
- TestNets
- Dashboard DApp

M3 : Foundation , Extension and Plugin
- Launch Foundation
- Community Initiatives
- Services Plugins Deduplication
- Extend to other Repositories and Existing Tools

M4 : Offer SCAN based Services
- Source code Attestation
- Repudiation
- Validation



Summary of Benefits

- SCAN has the potential to disintermediate the code audit process.
- Improves developer productivity.
- Decentralized Digital Identity for Source Code
- Disclose only what you must about your code with ZKP’s.
- Enables better collaboration between organizations
- Can put together a world view of open source code giving due credit to original authors and contributors.

.

Thank you…

Vinod Panicker

Distinguished Member Technical Staff -SM

Linkedin/vinodpanicker

Open Source Code Strategy

- Open vs Closed source project execution strategies.
- Break access barriers , dropping costs to gain competitive edge.
- Subscription Models.
- Establish Trust and Credibility.
- Communities based product delivery and support models.

Foundation

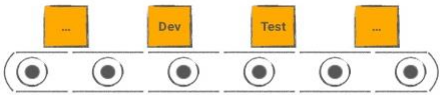
- Community Support
- Governance
- Sustenance
- Not for Profit.

Design Considerations

- Pluggable/Swappable modules.
- API based Access.
- Open source and scales well on commodity hardware.
- Comply with open standards
- Pluggable Block chain components,
- Supports multiple Block chain protocol,
- Common Tool chain for Development, Deployment and Operations for multiple Block chain Frameworks.

On Premise

On Cloud



Automated Nodes & Network Provisioning

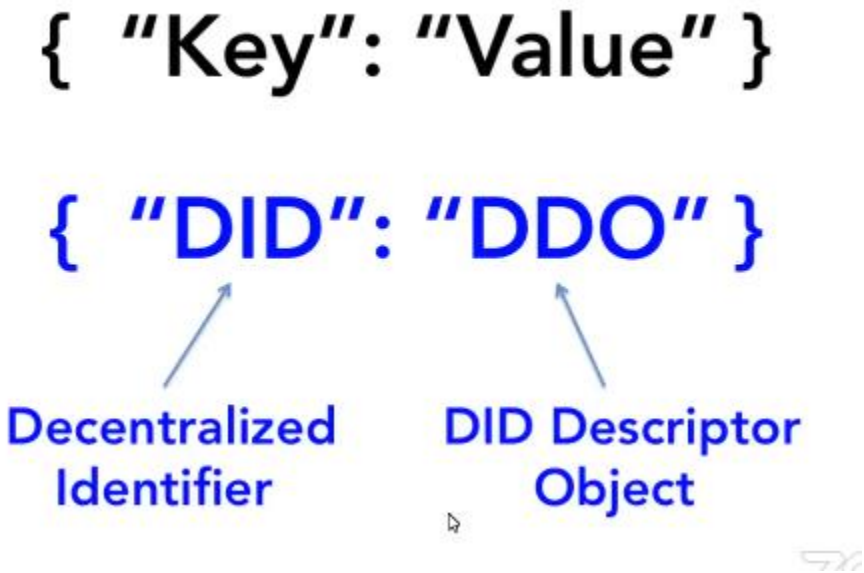
topcoder

Designed for Crowdsourcing

Type of Claims

- Has_Duplicate
- Has_Usage
- Has_Valid_License

SCU -DID


{ "Key": "Value" }
{ "DID": "DDO" }
Decentralized Identifier
DID Descriptor Object

Open Source Code Management Systems

Monitor and alert when new threats are reported

Set and enforce open source policies

Identify license and component quality risks

Fully discover all open source in your code

Map components to known vulnerabilities

Seamless integration into your DevOps environment

SCU - DDO

The primary elements of a DDO

1. DID (self-describing)
2. List of public keys (for the owner)
3. List of controlling DIDs (for key recovery)
4. List of service endpoints (for interaction)
5. Timestamps (for audit history)
6. Signature (for integrity)

Blockchain Identity

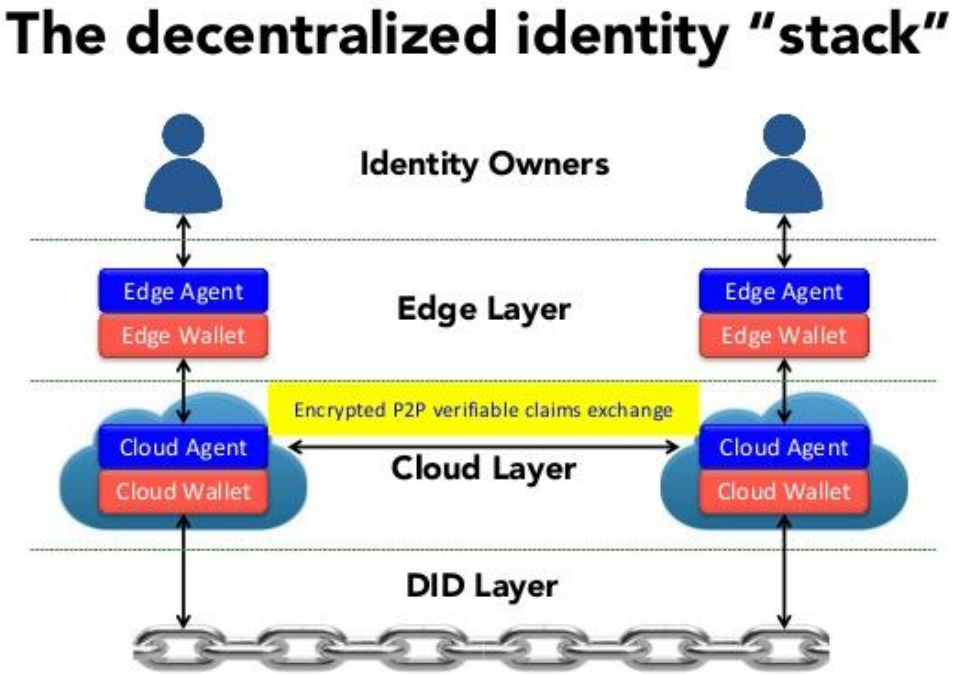
Why is blockchain identity a breakthrough?

- Distributed ledgers (blockchains) are massively secure, scalable, and reliable
- For digital identity, a distributed ledger can solve the "root of trust" problem:

  How can there be a global source of identity that everyone trusts, but isn't owned or controlled by any one company or government?

- Enables truly *self-sovereign* identity

DI Stack


The decentralized identity "stack"
Identity Owners
Edge Agent
Edge Wallet
Edge Layer
Edge Agent
Edge Wallet
Encrypted P2P verifiable claims exchange
Cloud Agent
Cloud Wallet
Cloud Layer
Cloud Agent
Cloud Wallet
DID Layer

Roadmap

M1 : Prototype
- SCAN metadata capture
- SCAN Connectors, SCAN Agents POCC, POU,POAL
- Self attestation, Trust Anchors
- SCU DID/DDO on Storage Hub
- SCU DID Verification via SCAN

M2 : Foundation , Extension and Plugin
- Launch Foundation
- Community Initiatives
- Services Plugins Deduplication
- Extend to other Repositories and Existing Tools

M3 : Develop Client Components
- Libraries
- CLi's
- APIs
- TestNets
- Dashboard DApp

M4 : Offer SCAN based Services
- Source code Attestation
- Repudiation
- Validation

Technologies

- Hyperledger project as base Blockchain framework
- Distributed Apps: Javascripts Framework, ReactJS
- Hybrid Mobile App
- DevOps Tool: Ansible/Docker :