Decentralized Identity
Architecture Highlights
## About the layers

<table>
<thead>
<tr>
<th></th>
<th>Layer Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Application and Service Layer</td>
<td>All the higher level Decentralized services and applications based on identity, enabling the first wave of serverless apps.</td>
</tr>
<tr>
<td>5</td>
<td>User Agent</td>
<td>The presentation layer which manages the user’s secret keys and allows them to be used to access private data.</td>
</tr>
<tr>
<td>4</td>
<td>Directory Services</td>
<td>Provides discovery of identifiers based on public information that users want to be searchable.</td>
</tr>
<tr>
<td>3</td>
<td>Identity Hub</td>
<td>Stores PII and personal content, manages the message queue conveying requests for actions to a user, synchronizes across hubs and notifies apps.</td>
</tr>
<tr>
<td>2</td>
<td>Cross-blockchain layer</td>
<td>Allows other layers to use a single interface to manage identifiers on all the underlying blockchains.</td>
</tr>
<tr>
<td>1</td>
<td>Blockchain layer</td>
<td>Guarantees unique identifiers and stores a base document describing how the owner of an identifier authenticates and how she and others get to the associated Identity Hub (Layer 3) and services.</td>
</tr>
</tbody>
</table>
## What does Decentralized Identity Bring?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Give individuals complete control over their digital identifiers</td>
<td>Empower people to create their own secure digital identifiers (DIDs) and fully control the personal information they present and receive without depending on or being profiled by corporations or governments.</td>
</tr>
<tr>
<td>Provide identifiers and personal data stores that outlive the people who use them</td>
<td>Provide future-proof identities and data stores that will not be affected by changing corporate business goals, the viability of technology companies or changes in government.</td>
</tr>
<tr>
<td>Provide long term availability and provable integrity</td>
<td>Eliminate single points of failure and mitigate targeted attacks through multiparty redundancy and decentralized consensus.</td>
</tr>
<tr>
<td>Provide superior privacy and GDPR compliance</td>
<td>Empower individuals to fully control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.</td>
</tr>
<tr>
<td>Provide increased security for parties relying on identifiers and data</td>
<td>Provide sufficient security for relying parties to depend on DID Documents for their required level of assurance.</td>
</tr>
<tr>
<td>Provide search</td>
<td>Offer a directory/search engine allowing entities to authenticate and interact with other entities using phone numbers, email, etc.</td>
</tr>
</tbody>
</table>

**Enable next-generation personal apps that cross all boundaries**
The DID and DDO – The base of the system

DDO: Minimal, stable, PII-free information needed to authenticate the owner and point to her identity system services

Request
resolve('did:btcr:xyz123def')

Response
{
  "id": "did:btcr:xyz123def",
  "publicKey": [
    {...},
    {...},
  ],
  "service": [
    {
      "type": "HubService",
      "endpoint": "https://foo123"
    },
    {
      "type": "DirectoryService",
      "endpoint": "https://bar456"
    },
    {
      "proof": {...}
    }
  ]
}

User Agents, Services, SDKs

Universal Resolver REST API

Request For DDO

DDO ID Definition

DDO:  Minimal, stable, PII-free information needed to authenticate the owner and point to her identity system services.

DDO

- Minimal, stable, PII-free information
- Needed to authenticate the owner
- Points to her identity system services

The DID and DDO – The base of the system

User Agents, Services, SDKs

Universal Resolver REST API

Request orchestrator

DDO ID Definition

DDO

- Minimal, stable, PII-free information
- Needed to authenticate the owner
- Points to her identity system services

DID/DDO Cache

Request for DDO

Response

PII and personal data
lives here

Public searchable
info released by user
lives here

DID and DDO Drivers

- btcr
- uPort
- sov
- aspen

Blockchains

- bitcoin
- etherium
- sovrin
- aspen

9/19/2018
By default the hub only has visibility onto metadata, permissions, and public information. As a DID in its own right it can be granted further visibility,

* With unencrypted searchable metadata tags
The Directory

Applications, Services, SDKs

Freeform query
Response
Notify

Decentralized Directory

Indexed Directory Store

DID delta aggregator
(new and changed)

DDO retriever
Profile retriever

Trust Score
(DID Attestations and identity protection)

Supplementary Info
(Hub crawling and join with web info)

Self registration
Chain notification
Universal Resolver

Resolve
Get
Notify
Notify
Notify
Notify

Hub
AI on signals
Crawlers