Decentralizing Digital Identity: Open Challenges for Distributed Ledgers

Paul Dunphy\textsuperscript{1}, Luke Garatt\textsuperscript{1}, Fabien Petitcolas\textsuperscript{2} 
Innovation Centre 
VASCO Data Security 
\textsuperscript{1}Cambridge UK, 
\textsuperscript{2}Brussels, Belgium
The plan

Setting the Scene
- Quick Identity Primer
- DLT-based identity

Example: Sovrin

A Research Agenda
- Refine understanding of DLT properties needed in identity
- Evaluate deployability in light of PKI challenges
- Evaluate exposure to public permissionless DLTs
- Gather new requirements for user experience

Final Remarks
Identity and Access Management (IAM)
- “enables the right individuals to access the right resources at the right times and for the right reasons”

Ubiquitous 3 party model
- User
- Identity Provider
- Relying Party

User centricity
- “that is, the idea of giving the user full control of transactions involving her identity data” [1]

Applying DLT to digital identity

https://github.com/peacekeeper/blockchain-identity
55% of DLTs track digital identities\(^2\)

Applying DLT in digital identity

55% of DLTs track digital identities\(^2\)


Decentralized Trusted Identity

Self-Sovereign Identity

Example: Sovrin (a.k.a. Hyperledger Indy)

- Ledger is a public permissioned user directory
- Identifiers as decentralized Identifiers (DID)
- Identity is a sequence of claims
- Relies on Idemix anonymous credentials

Sovrin permissioned ledger

DIDs {public keys, end-point addresses}, claim definitions
### Pros
- Supports multiple unlinkable identifiers (e.g., one identifier per interaction)
- Acknowledges need for delegation (Agents)
- Supports Verifiable Claims (an emerging W3C standard)
- No obvious financial cost (to end-users anyway…)

### Cons
- User Experience not (yet?) considered
- Deployability of signing infrastructure
- Silver bullet use case
Refine understanding of DLT properties needed in identity
Evaluate deployability in light of PKI challenges
Support secure delegation of credentials
Evaluate exposure to public permissionless DLTs
Gather new requirements for user experience
Refine vocabulary for DLT-based identity

- Coarse grained vocabulary for DLT-based digital identity
- But which properties of DLT are valuable in digital identity?

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>uPort</td>
<td>Immutability</td>
<td>Transparency</td>
</tr>
<tr>
<td>Sovrin</td>
<td>Decentralisation</td>
<td>Auditability</td>
</tr>
<tr>
<td>ShoCard</td>
<td>Immutability</td>
<td>Auditability</td>
</tr>
</tbody>
</table>

- Action: New ways to conceptually evaluate schemes and map them to usage scenarios
Evaluate exposure to public permissionless DLT

- Public and permissionless DLTs are wedded to proof of work consensus.
  - Energy usage

- Transaction load created and response to congestion

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Authentication</th>
<th>Identifier Creation</th>
<th>Account Recovery</th>
<th>Attribute Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>uPort</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ShoCard</td>
<td>No</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Transaction fees are often abstracted away

- Action: Create models of envisioned user behaviour, transaction load and relevant economic constraints
Evaluate deployability w.r.t. PKI

- Public Key Infrastructure (PKI) adds trust to web browsing

- Credential Lifecycle Challenges
  - Key Management
  - Establishment (e.g. EV certificates)
  - Federation
  - Revocation
    - Certificate Revocation Lists (CRL)
    - OCSP

- Open group PKI rarely used for human identity [4,5]

- Action: Investigate and evaluate operational and technological differences vs. PKI


Gather new user experience requirements

- Identity management is not the user’s primary goal [6]
- Upgrading the user’s workload to achieve already existing outcomes
  - Key management
  - Understand nuances of GDPR
  - No helpdesk to call
  - Account recovery
- **Action:** Redouble efforts to understand how users achieve identity management – as it is

This is an interesting space

Important to work from usage contexts

Let’s do research on:

- Refine understanding of DLT properties needed in identity
- Evaluate deployability in light of PKI challenges
- Support secure delegation of credentials
- Evaluate exposure to public permissionless DLTs
- Gather new requirements for user experience