TrustChain

A scalable blockchain fabric to build trust

Martijn de Vos

* Distributed Systems
<table>
<thead>
<tr>
<th>Sector-specific Business Logic</th>
<th>Decentralized Market</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logistics, Energy, Finance, Real Estate, Retail, ...</td>
<td>Conditional Payments or Smart Contracts</td>
</tr>
<tr>
<td>Real-time Clearance and Settlement</td>
<td>Internet-of-Money</td>
</tr>
<tr>
<td>Legally valid signatures, electronic business transactions</td>
<td></td>
</tr>
<tr>
<td>Trustworthiness and Reputation</td>
<td>Distributed Temporal Pagerank</td>
</tr>
<tr>
<td>Blockchain Layer</td>
<td>Scalable Consensus</td>
</tr>
<tr>
<td>TrustChain</td>
<td></td>
</tr>
<tr>
<td>Self-Sovereign Identity</td>
<td>IPv8</td>
</tr>
<tr>
<td>Physical Unclonable Functions</td>
<td>Biometric-based Authentication</td>
</tr>
</tbody>
</table>

### Sector-specific Business Logic
Logistics, Energy, Finance, Real Estate, Retail, ...

<table>
<thead>
<tr>
<th>Decentralized Market</th>
<th>Conditional Payments or Smart Contracts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time Clearance and Settlement</td>
<td>Internet-of-Money</td>
</tr>
</tbody>
</table>

| Legally valid signatures, electronic business transactions |

<table>
<thead>
<tr>
<th>Trustworthiness and Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Temporal Pagerank</td>
</tr>
</tbody>
</table>

### Blockchain Layer
TrustChain

### Self-Sovereign Identity
IPv8

| Physical Unclonable Functions | Biometric-based Authentication |

---

Open problems of existing Blockchain solutions

• Scalability (often constant tx/s)
  – Bitcoin Core: ~7 tx/s
  – Ongoing efforts to increase scalability (Lightning network, sharding, off-chain)

• Storage requirements
  – Bitcoin: 149GB as of December 2017
Global Consensus

• Scalability is often limited by requirement for global consensus.
  – Proof-of-work, BFT

• Is global consensus necessary?
  – It is desired if you need scarcity

• What if we can guarantee eventual detection of fraud?
  – Like credit card companies
Transaction Ledgers

• Observation: many blockchain systems are transaction fabrics.
  – Money transfers (Bitcoin, Litecoin)
  – Contract invocations (Ethereum)
  – Attestations (Our ongoing research)
TrustChain

- A scalable blockchain fabric to build trust

Transaction

- Consider a transaction between two users
- Both users sign the transaction
  - Using any secure signing algorithm
Transaction Chaining

• We can chain these transactions together
• Each users keeps track of his own transaction history
Improving Security

• We add an additional pointer to each block
  – Points towards the previous block in the chain of the transaction counterparty
Entangled Chains
Properties of TrustChain

• Entanglement
  – Makes our chain tamperproof

• Eventual detection of a double-spend
  – By gossiping blocks through the network
Advantages

• Higher transaction throughput
  – No (hard) requirement for global consensus
  – However, global consensus improves security

• Less storage required
  – At a minimum, every participant only needs to store their transactions
Research Goals

• Determine how TrustChain can help to accurately store transactions.
  – Bandwidth accounting
  – Attestations
  – Generic asset trading

• Build trust between interacting strangers.
TrustChain

A scalable blockchain fabric to build trust

Martijn de Vos

Distributed Systems