Secure Credit Reporting on the Blockchain

Amir Goharshady
Ali Behrouz
Krishnendu Chatterjee
Designing a blockchain use-case for the general public

• Find something in the real world that irritates people

• Make sure the problem is due to centralization

• Replace the central authority with a blockchain protocol or smart contract
• Do not revolutionize the concept
• Revolutionize the means (technology)
Credit Reporting is Awful (and has always been so)

You don’t have to spend long preparing a broadcast about credit agencies before you learn **one simple truth**: Everyone, and I mean Everyone, has a horror story. (1991)

If every 20th Frosty that Wendy’s sold turned out to be a cup of warm goat semen, we would want some accountability and we’d want it fast! (2016)
Problems with Credit Reporting

- Errors and Inconsistency
- Identification Problems
- Long Update Intervals
- Endemism
- Data Breaches

- All of these problems are due to centralization and credit reporting agencies
Financial Mechanisms are Here to Stay

• We do not attempt to change how credit reporting works
• We do not attempt to make credit more/less accessible
• We do not attempt to change the basics of who trusts whom
What We Need

- A reliable way to injectively map real-world identities to identities in our system
- An access control mechanism that ensures one can see (parts of) the credit report only if its owner agrees to disclosure [Note that public records such as bankruptcy information should remain public]
- An assurance for the creditor that (s)he has received a correct and complete credit report
- An assurance for the customer that (s)he can prove mistakes/wrongdoing by the creditor and fix the record
Identity Management Protocol

- There are already systems in place for managing identities of banks and financial institutions.
- Hence, institutions can recognize valid signatures by other institutions they trust.
Identity Management Protocol

1. register(public key, fingerprint, pointer1, pointer2)
2. Ask for certification (public key)
3. Challenge (random string)
4. Signature
5. Real-world Proof of Fingerprint
6. certify(public key)
Credit Accounts Protocol
Adding a Credit Account

1) Key Exchange

\[
\begin{align*}
K_i & \quad K'_i \\
(K_c, k_c) & \quad (K'_c, k'_c) \\
(K'_s, k'_s, 1) & \quad (K'_s, k'_s, 2)
\end{align*}
\]
## Adding a Credit Account

### 2) Creating the Contract

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K'_i$</td>
<td>Set at contract initialization, remains constant afterwards.</td>
</tr>
<tr>
<td>$K'_c$</td>
<td>Set at contract initialization, remains constant afterwards.</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>Set at contract initialization. Can be updated but each update needs signatures from both $k'_i$ and $k'_c$.</td>
</tr>
<tr>
<td>Data</td>
<td>Can be updated using $k'<em>i$. Is meant to be encrypted by $K'</em>{s,1}$.</td>
</tr>
<tr>
<td>Signature</td>
<td>Can be input once using $k'_i$, remains constant afterwards.</td>
</tr>
<tr>
<td>Next Account</td>
<td>Can be input once using $k'<em>c$, remains constant afterwards. Is meant to be encrypted by next account's $K'</em>{s,2}$.</td>
</tr>
</tbody>
</table>

### 3) Commitment

- The bank commits by signature
- The customer commits by adding the contract to her credit accounts list
Reading a Credit Report
Public Records Protocol

• Similar to Credit Accounts protocol, except that:
  ▫ The pointers are not encrypted
  ▫ Anyone can add a new record to the list
    • Spam is ignored and is not a big deal, but is also prevented by gas usage
Back to the Guarantees

- Errors and Inconsistency
- Identification Problems
- Long Update Intervals
- Endemism
- Data Breaches
What We Can’t Fix or Don’t Want to Fix

• The possibility that cryptographic systems we use today, might be broken in the future
• Legal problems
• Any type of fraud that originates in the real-world
  • e.g. A person having two real-world identities can get certified for two distinct identities in our approach
• Anything that is part of the financial mechanisms
  • The fact that many people do not have access to credit
  • Unfair decision-making by the banks
Thank you for your time and attention!

• Please be kind to the session chair and ask a question. If you don’t, (s)he has to come up with a fake question, and that’s awkward.

• Feel free to write to me at goharshady@ist.ac.at

• Acknowledgments: