Scalable Log Auditing on Private Blockchains via Lightweight Log-Fork Prevention

Yuzhe Tang
Syracuse University
Kai Li
Syracuse University
Yibo Wang
Syracuse University
Sencer Burak Somuncuoğlu
Chainalysis

System Model: Monitoring a CT log w Bkc

Untrusted log server [CCS18]

Bitcoin to prevent forks among Monitors [SP17,USS17,NDSI20].

Monitor’s overhead:
- O(1) txs via SPV client
- O(N) log entries
- A CT log of N=2.9 billion Certs (15.8 TB)

Goal: Light Log Monitor Client

Can a browser possibly monitor CT log without TTP (exc. BKC)?
- Preventing forks with O(1) log entries and txs?

The TxChecker Protocol

Step 1: Client log attestation
Step 2: Server log attestation
Step 3: Submitting log query
Step 4: Log auditing based on query results

Evaluation

- System prototyping
  - with FabToken in HyperLedger Fabric
  - Each log update is a FabToken transfer
- Cost evaluation
  - Measure monitors’ costs

<table>
<thead>
<tr>
<th>Security goal</th>
<th>Monitor’s cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent log forks</td>
<td>O(1) log entries</td>
</tr>
<tr>
<td>Catena[SP17], Chainiac[USS17], Ghostor[NDSI20].</td>
<td>✓</td>
</tr>
<tr>
<td>This work</td>
<td>✓</td>
</tr>
</tbody>
</table>

(a) With varying number of clients