Implementing a sidechain-based asynchronous DPKI

Ziyuan LI, Huimei WANG, Jian LIU, Ming XIAN

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0564-9

Problems & Ideas

- The MKT accumulator in traditional smart contract PKI is too simple to work well in scenarios with complex requirements.
- Ideas: Sidechain-based asynchronous DPKI
  - Adopting MMR accumulator with asynchronous feature.
  - Adopting sidechain technology to improve execution efficiency.

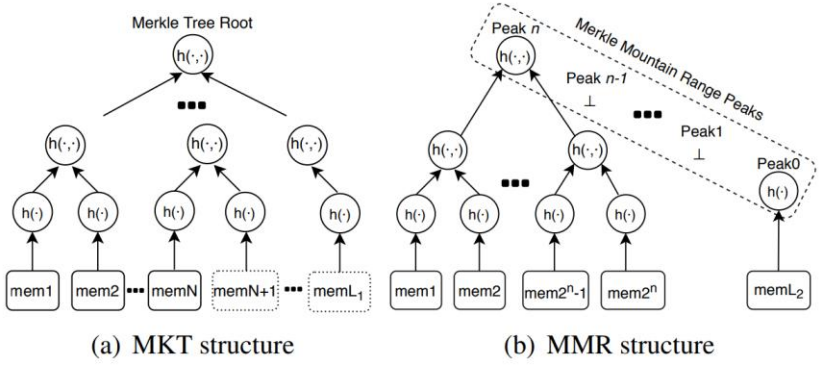

Fig. 1 The data structures of MKT and MMR. (a) shows the filling to L_1, (b) shows a MMR with L_2 members, where $L_2 = 2^n + 1$ (i.e., 10...01 in binary) for intuition. Note the member actually exists in the form of (id, pk).

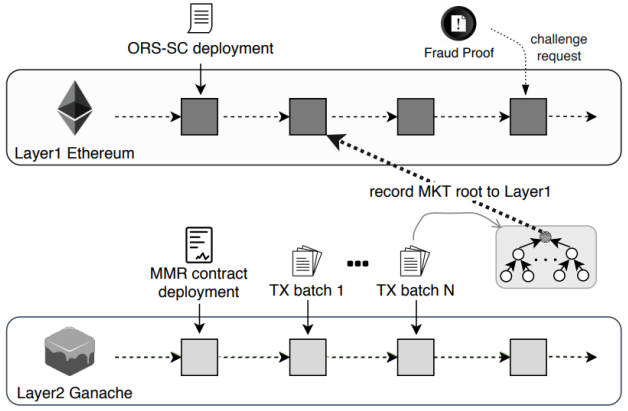

Fig. 2 The ORS-based sidechain architecture. The SC is deployed on Ethereum to account for transactions on the local private blockchain, and allowing any node to issue a challenge.

Main Contributions

- **Time overhead on sidechain and private blockchain (i.e., Ganache).**