CompactChain: An Efficient Stateless Chain for UTXO-model Blockchain

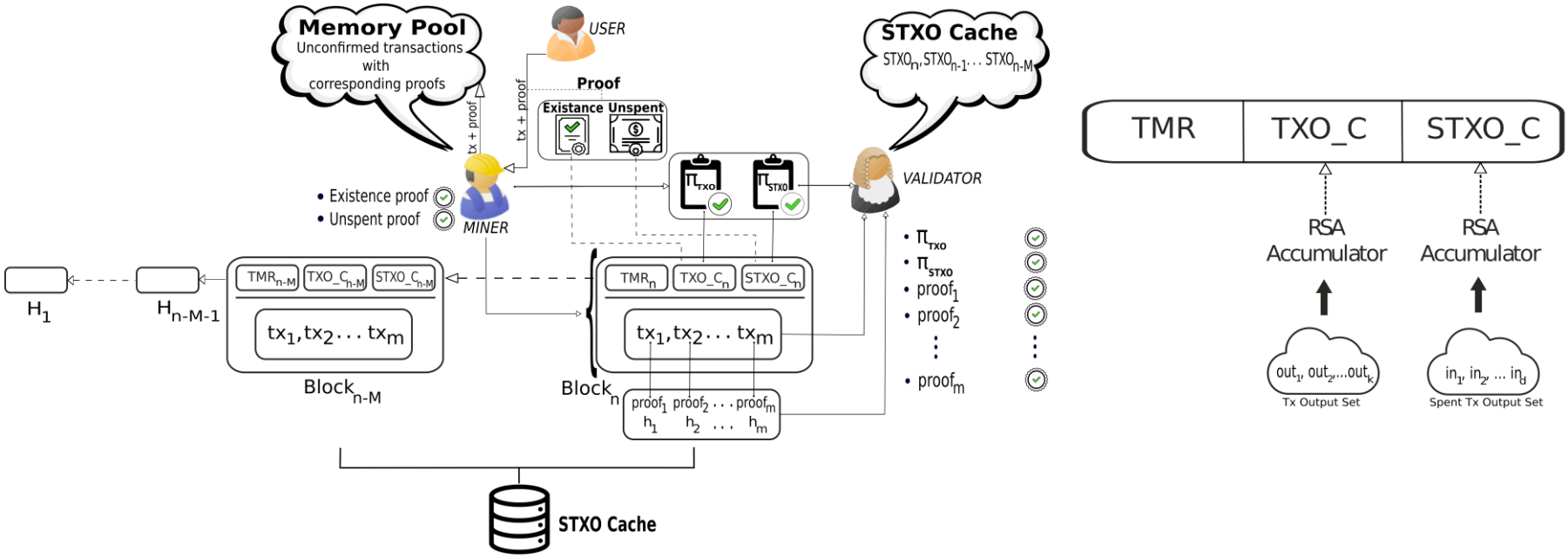
B Swaroopa REDDY, T Uday Kiran REDDY

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2365-9

Problems & Ideas

- Problems of state-of-the art stateless blockchains:
  - Expensive commitment update time (Boneh's Model).
  - Large transaction proof size (Minichain).

Ideas: We use two RSA accumulators to aggregate TXO and STXO sets, this makes the commitment update constant time. In contrast to dynamically updating on single RSA accumulator.



LEFT: CompactChain architecture; RIGHT: Block header composition

Main Contributions

- Contributions:
  - We propose an RSA accumulator for the TXO commitment for a constant sized transaction membership proof in contrast to the ever-growing existence proof size in minichain protocol.
  - We implement CompactChain and compare the performance with Boneh's model and Minichain protocols. Comparing to Boneh, CompactChain has improved the efficiency of commitment update from $O(m^2)$ to $O(m)$. Comparing to Minichain, the transaction proof size has improved from $O(\log_2(m)) + O(\log_2(L)) + O(1)$ to $O(1)$.
  - Through simulation results, we show the performance improvement in network communication latency and TPS compared to Minichain due to reduced transaction proof size.

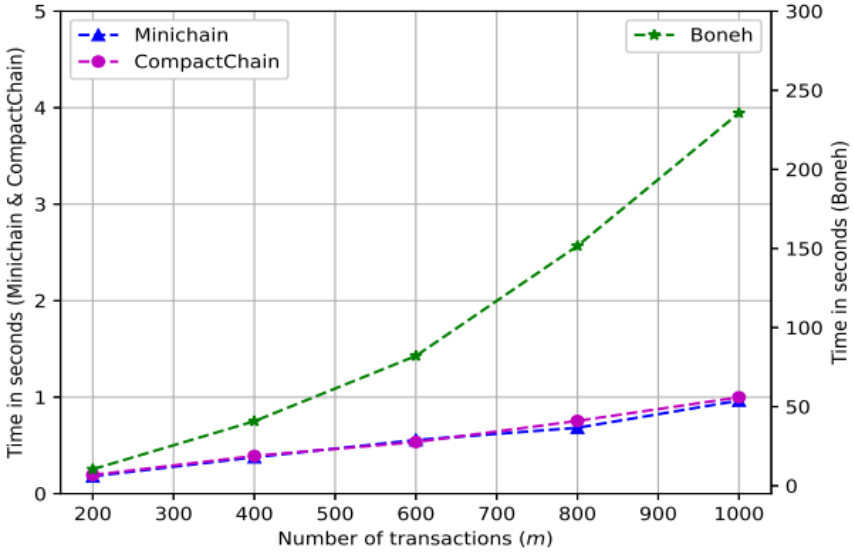


Fig. 3 Performance of the commitments update

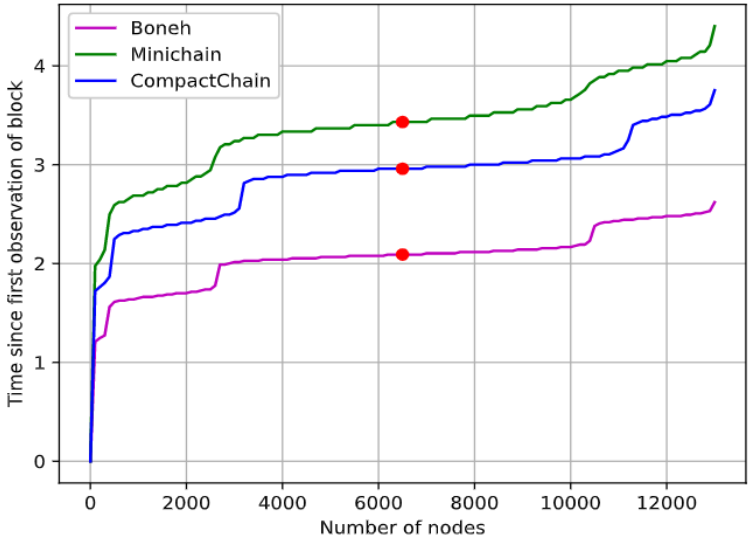


Fig. 9 Performance of propagation latency of a block in the network