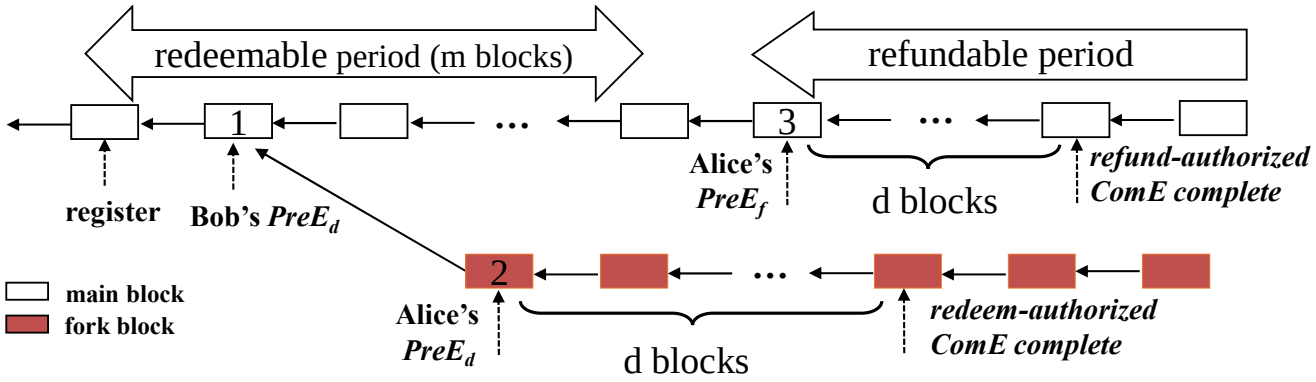
An Efficient Atomic Cross-Chain Commitment Resisting Fork Fraud

Fuqi JIN, Wenquan LI, Lanju KONG, Qingzhong LI

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2275-2

Problems & Ideas

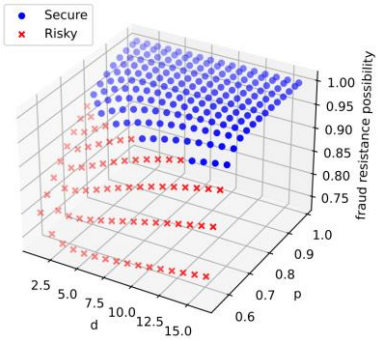
- Problems of conventional atomic cross-chain commitment approaches:
  - The atomic cross-chain commitment cannot achieve high efficiency in terms of storage, transaction fees and so on.
  - The atomic cross-chain commitment is suffering from the security risk of fork fraud.
- Ideas: Leverage the sharing of blockheaders in the witness chain to thin the transaction costs and widen the time gap between fraud and honest evidences.

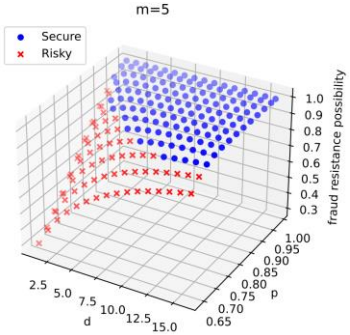


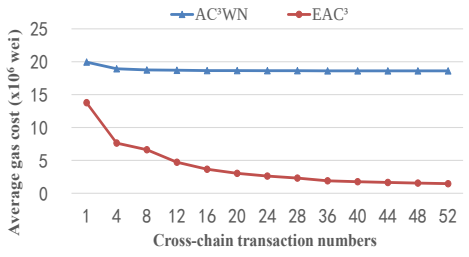
When both redeem-authorized ComE and refund-authorized ComE are in possession, attackers are able to illegally obtain assets on both two chains through fork fraud. Using the redeemable period, the two types of evidence are separated by a time gap and the probability of simultaneous acquisition is suppressed to an acceptable range.

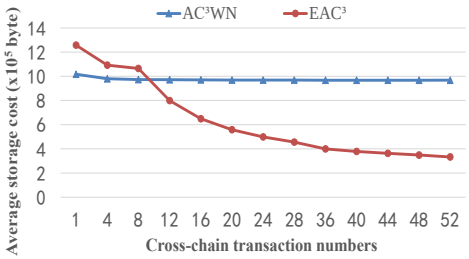
Main Contributions

- Contributions:
  - We propose a new atomic cross-chain commitment protocol EAC^3. This protocol is equipped with strong fork fraud resistance to ensure the atomicity of cross-chain transactions;
  - EAC^3 significantly decreases the cross-chain storage overhead and transaction fees, eliminating the decline of network throughput faced with high-frequency cross-chain transactions;
  - Through experiments, we prove that when cross-chain transactions occur frequently, EAC^3 can reduce the gas cost by about 90% and the storage cost by about 60%. Furthermore, security experiments are also conducted confirming the security of this protocol.









The left two images show that EAC^3 can keep a high resistance in the face of fork fraud. The right two images respectively shows the lower costs of EAC^3 in terms of both transaction fees and storage.