Scalable Byzantine Consensus via Hardware-assisted Secret Sharing

Jian Liu, Wenting Li, Ghassan Karame, N. Asokan

Aalto University

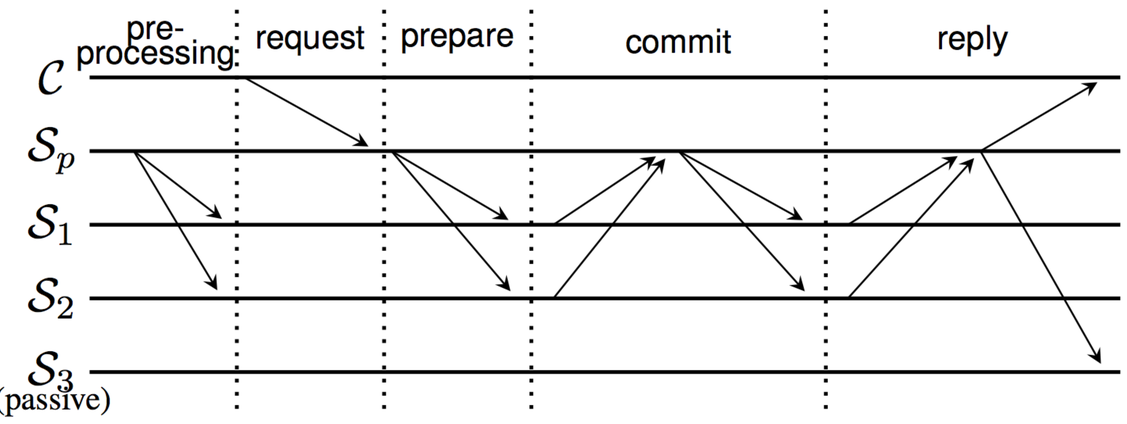
Collaborative Research Institute for Secure Computing

NEC

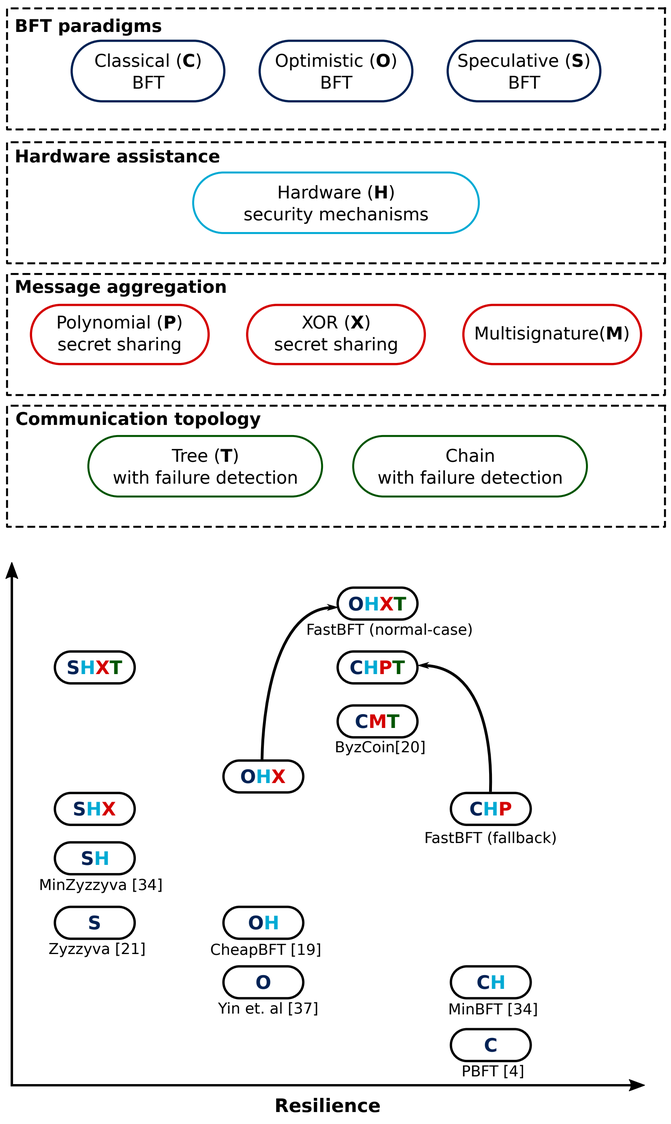
- Blockchain community is trying to add Byzantine fault-tolerant (BFT) protocols into blockchains;
- Existing BFT protocols can only scale to tens of nodes due to their $O(n^2)$ message complexity;
- We propose the fastest and most scalable BFT protocol to-date.

FastBFT Overview:

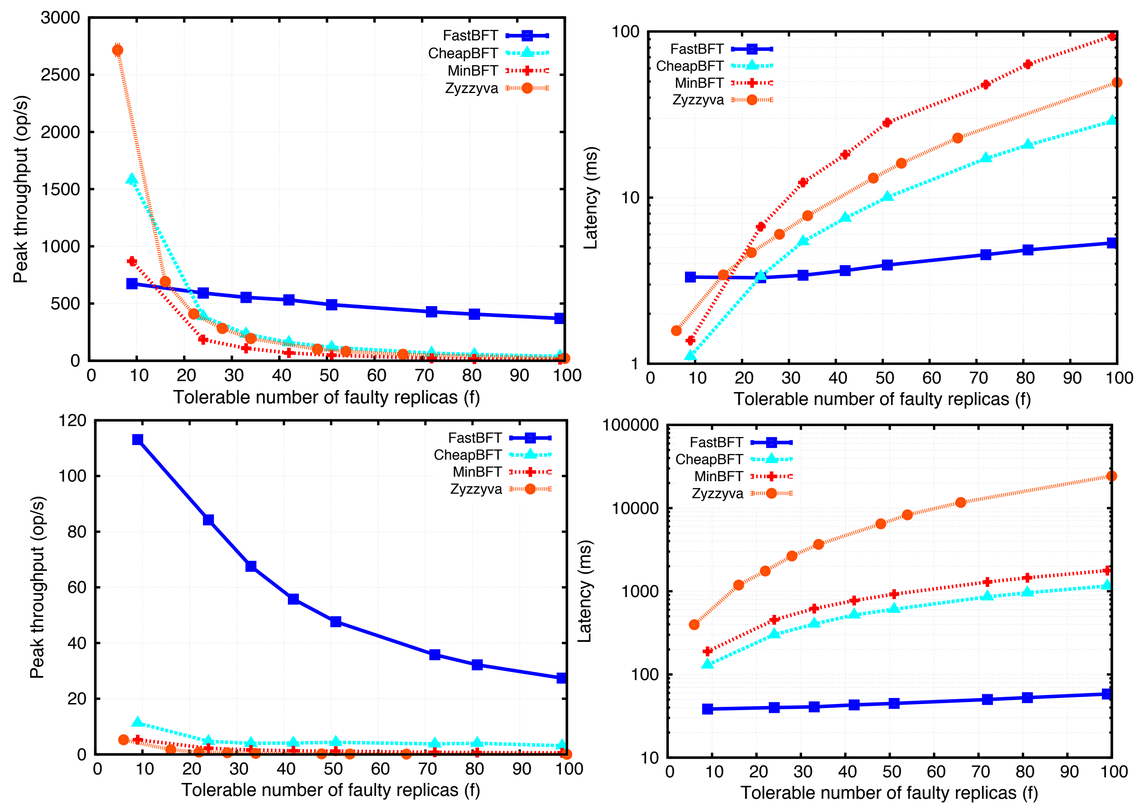
- Using SGX-assisted secret sharing to reduce message complexity to *O(n)* without using any public-key operations;
- Balancing load by arranging nodes in a tree topology;
- Requiring only a subset of nodes to actively run the protocol;
- Using failure detection to avoid frequent view-changes.



A framework that captures various design choices:



https://arxiv.org/abs/1612.04997



Fair Payments

- Fair exchange: exchange digital “items” fairly -- either each player gets the other's item, or neither player does.
- Enabling fairness in existing cryptocurrencies is an essential but insufficiently explored problem.
- Timeout−based schemes do not ensure strong fairness:
  - timeout reached after payee broadcasts his signature but before it is confirmed in blockchain.

Our approach: a new fair payment method that provides strong fairness: payer creates a transaction with some digital money that is spendable when

- payee provides his “item”, or
- payer issues an abort transaction.

https://arxiv.org/abs/1609.07256

Anonymous Payments

- An anonymous payment scheme [1] was built on top of the timeout−based fair exchange.
- We found a flaw: breaks fairness *and* security.

Our approach: fair payment protocol without timeouts

[1] *Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions[C]//International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2016: 43-60.*

Intel CRI for Secure Computing