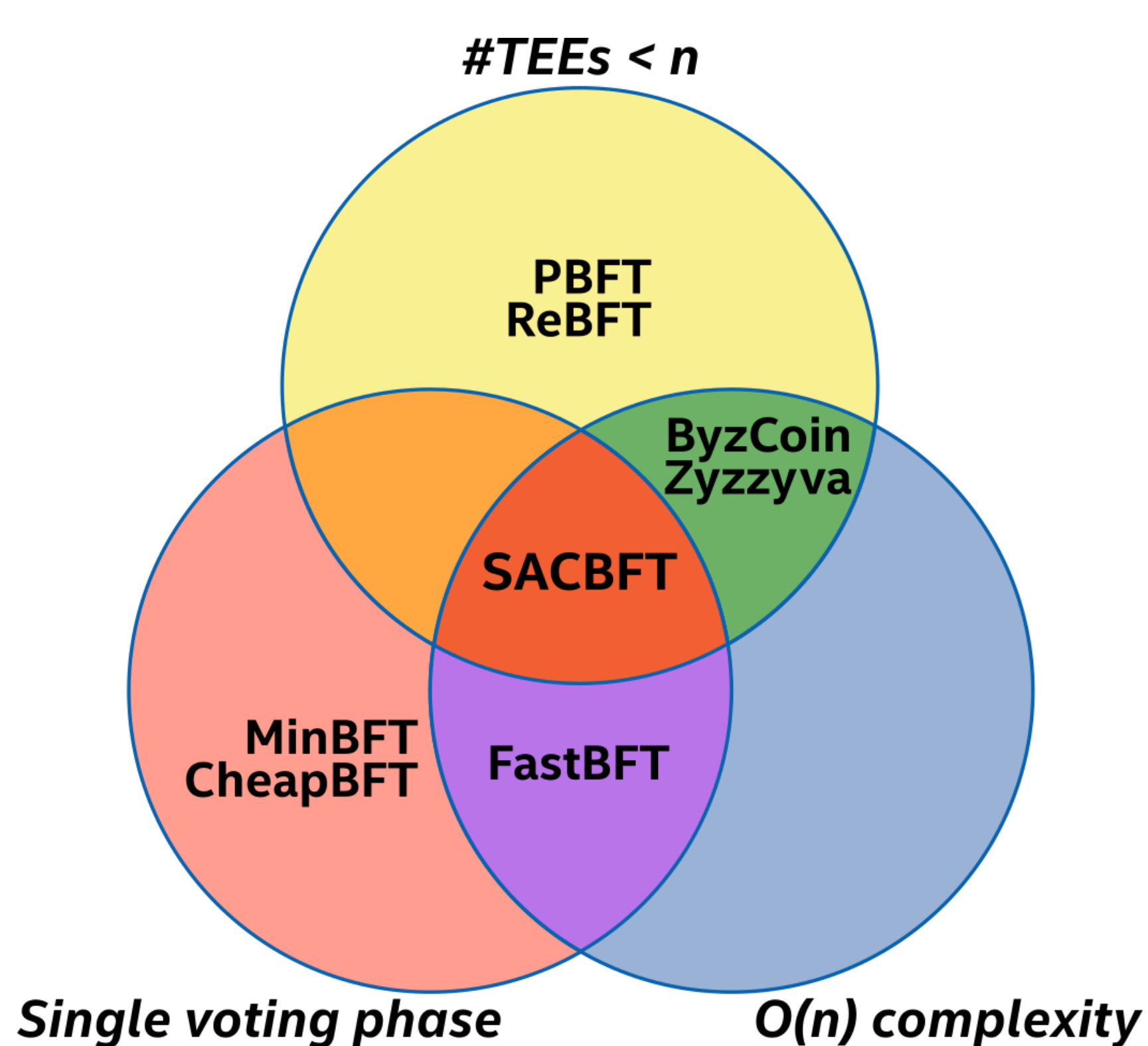


# SACBFT: Single Active Counter Byzantine Fault Tolerance

## SACBFT Transformation:

- Single active trusted counter:
  - not all replicas may have TEEs: e.g. for autonomous systems and internet-of-things applications.
  - allows gradual phase-out of TEE models over time.
- Single voting phase:
  - each request is bound to a monotonic counter value; hence the primary cannot equivocate.
  - eliminates the need for multiple voting phases.
- $O(n)$  communication complexity:
  - most TEE-based BFT protocols are incompatible with signature aggregation, because TEE state varies between replicas.
  - a single trusted counter does not need synchronization, so all replicas always sign the same thing.

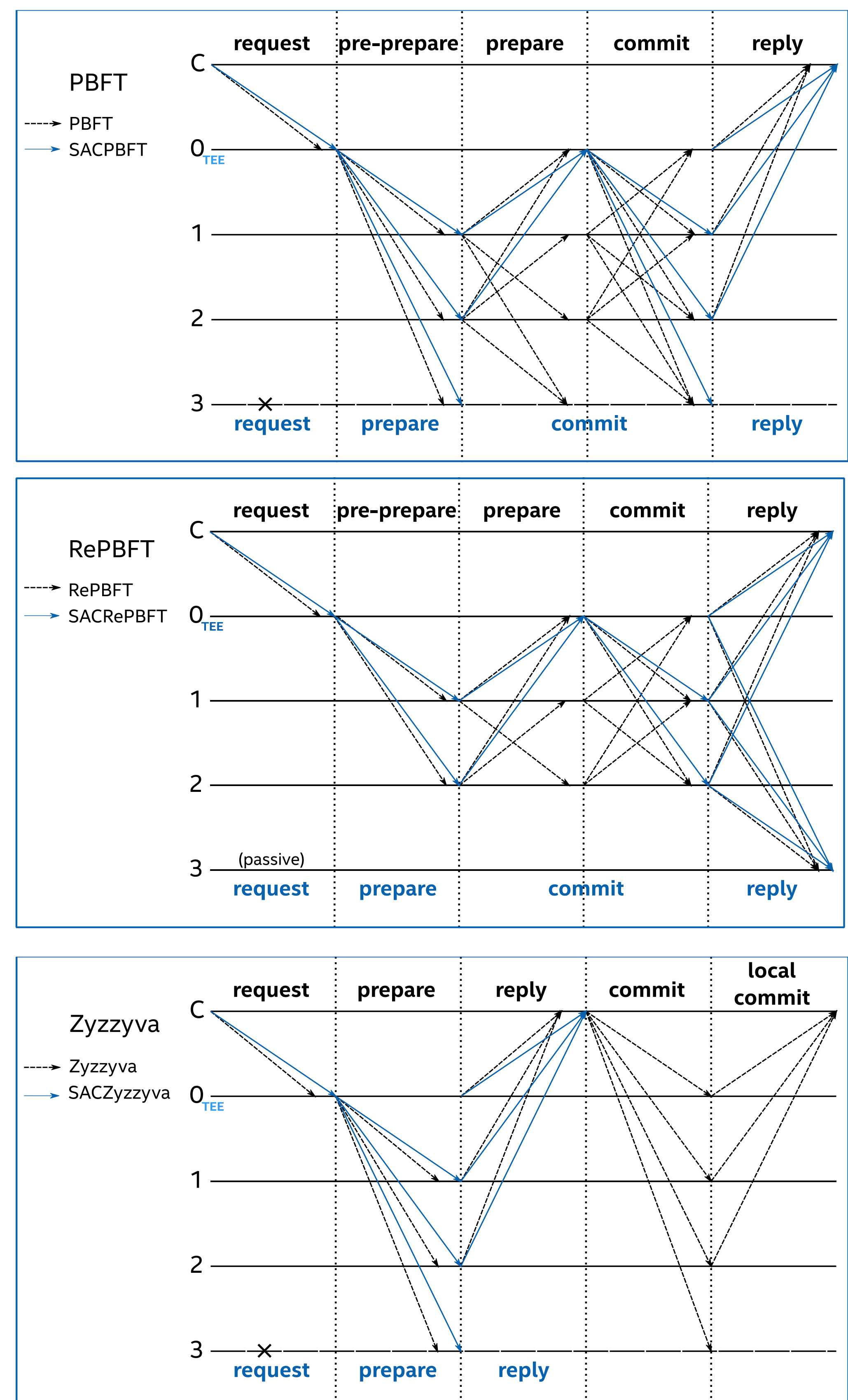


### Protocol property comparison

	Voting Phases	TEEs	Bandwidth	Replicas	Rollback	Tolerates Byz. client
PBFT	2	0	$O(n^2)$	$3f+1$	No	Yes
ReBFT	2	0	$O(n^2)$	$3f+1$	No	Yes
ByzCoin (CoSi)	2	0	$O(n)$	$3f+1$	No	Yes
Zyzzyva	1/2	0	$O(n)$	$3f+1$	Yes	No
MinBFT CheapBFT	1	All	$O(n^2)$	$2f+1$	No	Yes
FastBFT	1	All	$O(n)$	$2f+1$	No	Yes
SACBFT	1	1*	$O(n)$	$3f+1$	No	Yes

\* With fewer than  $f+1$  TEEs, a fallback protocol is required in case all TEE-replicas fail.

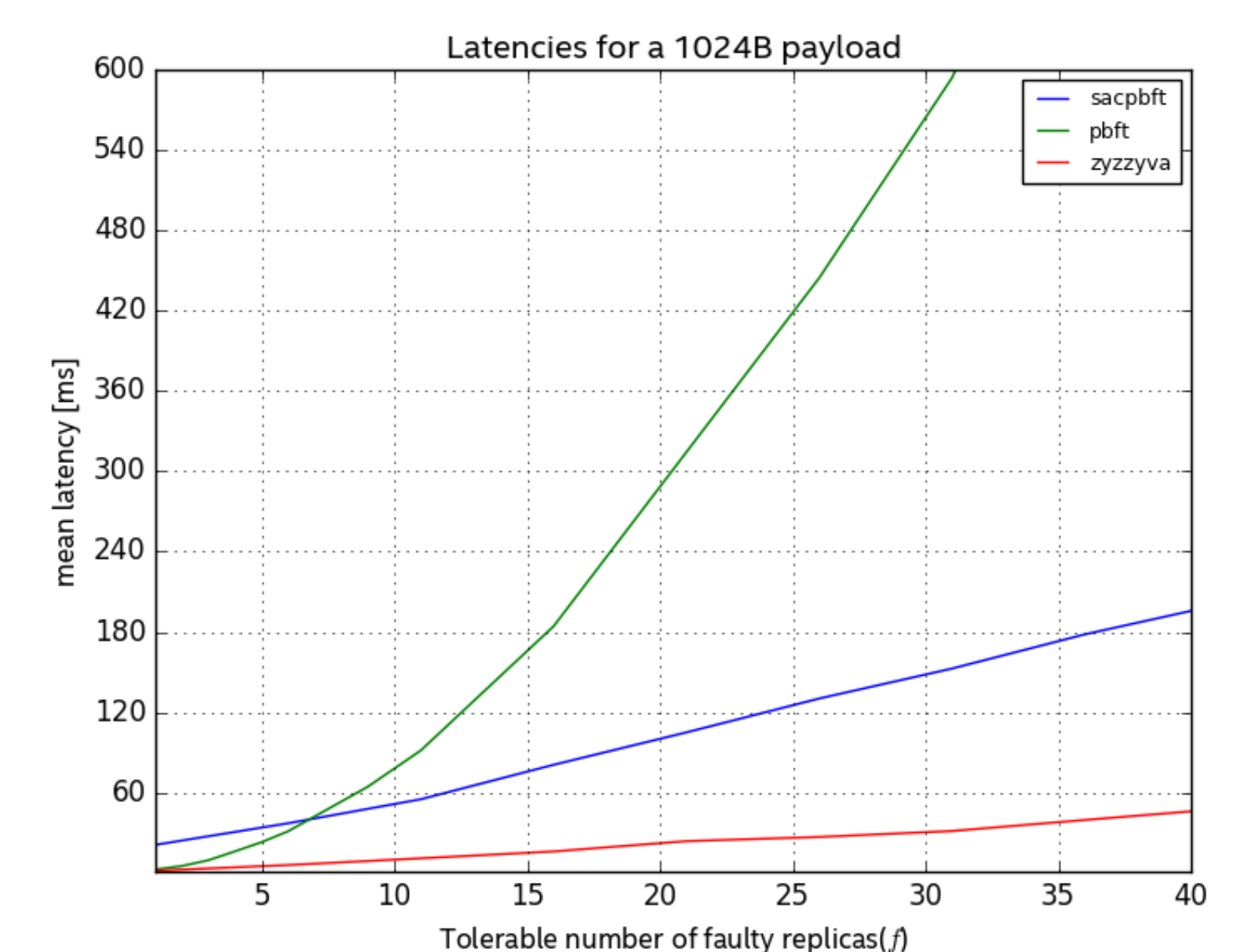
## Application to PBFT, RePBFT and Zyzzyva



## Evaluation

### Test setup:

- 5 physical machines
- No faulty replicas
- 1024B transaction size
- 8Mbit/s per machine



## Future work

- Adapt this approach to the PBFT view-change.
- Minimize public-key operations, e.g. through secret sharing.
- Optimize for IoT scenarios such as self-driving cars.
- Generalize the ordering primitive for use in other settings.