Fides: Secure and Scalable Asynchronous DAG Consensus via Trusted Components

Shaokang Xie[†], Dakai Kang[†], Hanzheng Lyu[*],

Jianyu Niu[‡], Mohammad Sadoghi[†],

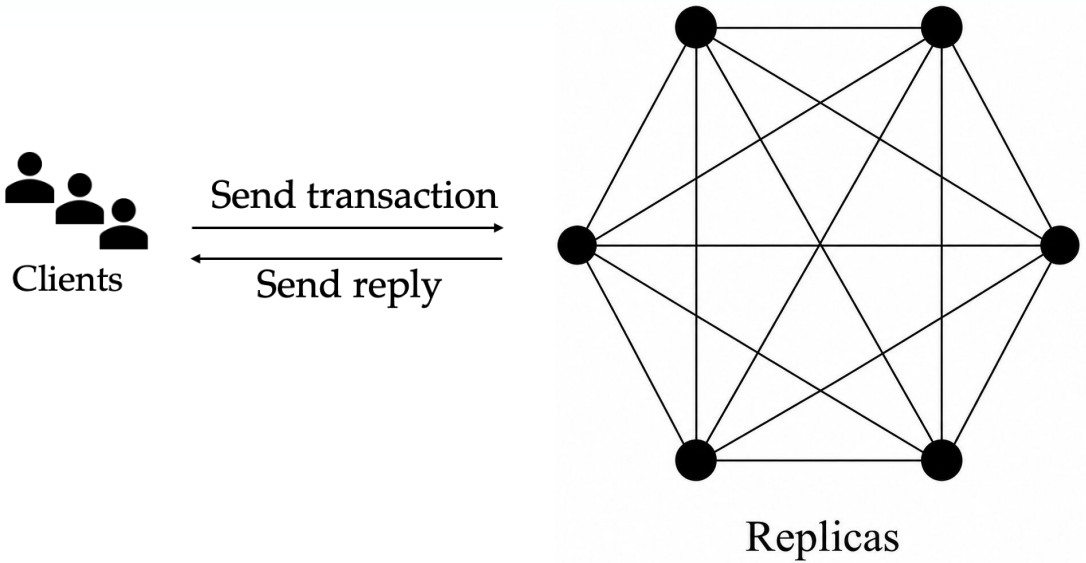
[†] University of California, Davis

[*] University of British Columbia

[‡] City University of Hong Kong

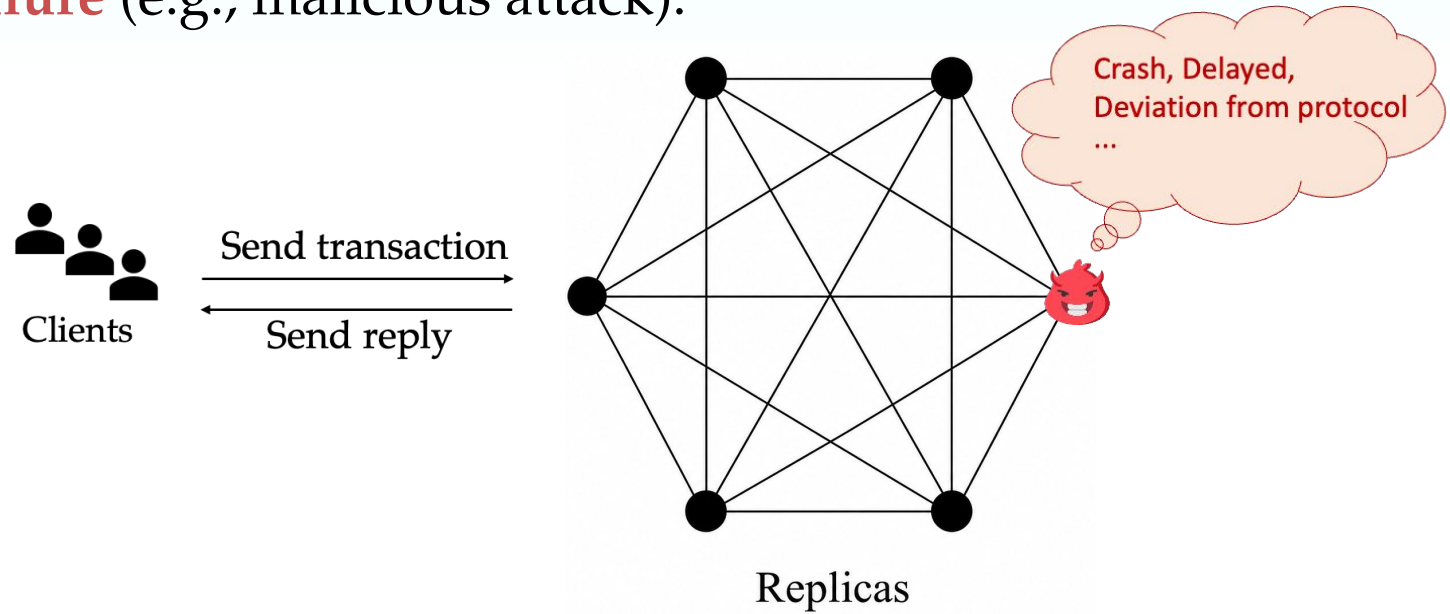
BFT Consensus

Byzantine Fault Tolerant (BFT) Consensus allows a distributed system to reach agreement among replicas despite Byzantine failure (e.g., malicious attack).



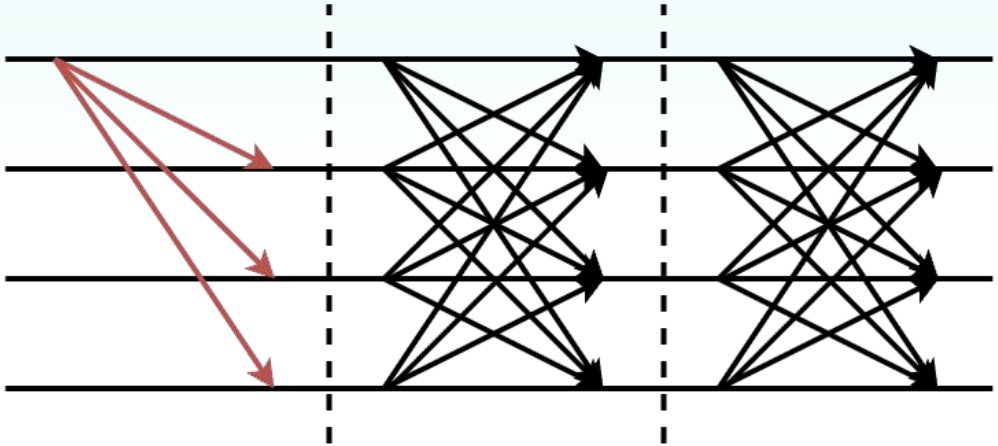
BFT Consensus

Byzantine Fault Tolerant (BFT) Consensus allows a distributed system to reach agreement among replicas despite **Byzantine failure** (e.g., malicious attack).



Leader-based BFT[1]

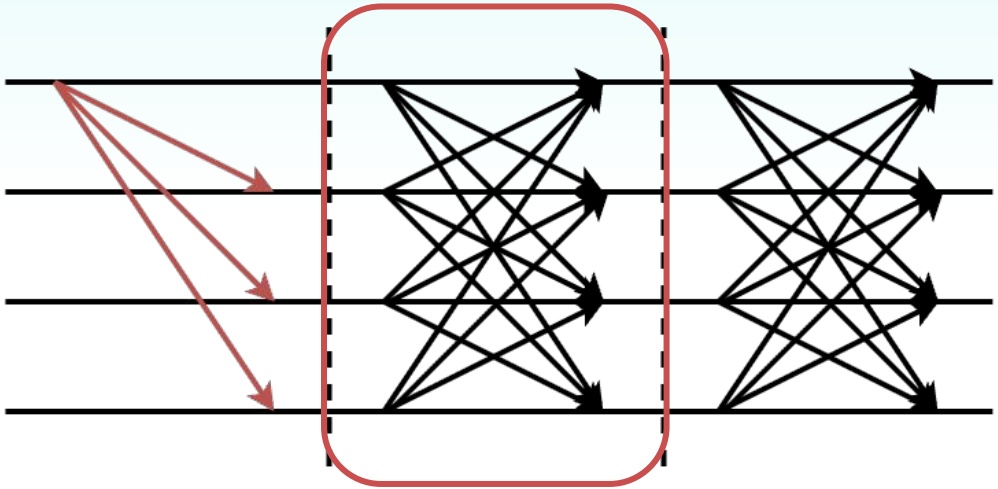
Practical Byzantine Fault Tolerance (**PBFT**) protocol



[1] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In OSDI, 1999.

Leader-based BFT[1]

Practical Byzantine Fault Tolerance (**PBFT**) protocol



Check leader's equivocation

A Byzantine leader may lie.

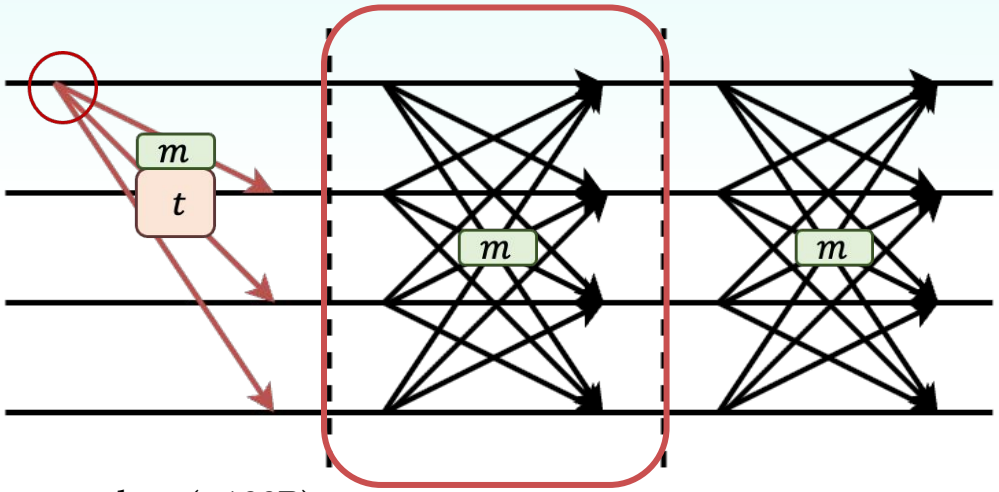
1. **Equivocation Cross-checking:**

   One additional msg phase.

[1] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In OSDI, 1999.

Leader-based BFT[1]

Practical Byzantine Fault Tolerance (**PBFT**) protocol



m: metadata (~100B)
t: payload (~500KB)

size(t) >> size(m)
Load Imbalance!

Check leader's equivocation

A Byzantine leader may lie.

1. **Equivocation Cross-checking:** One additional msg phase.

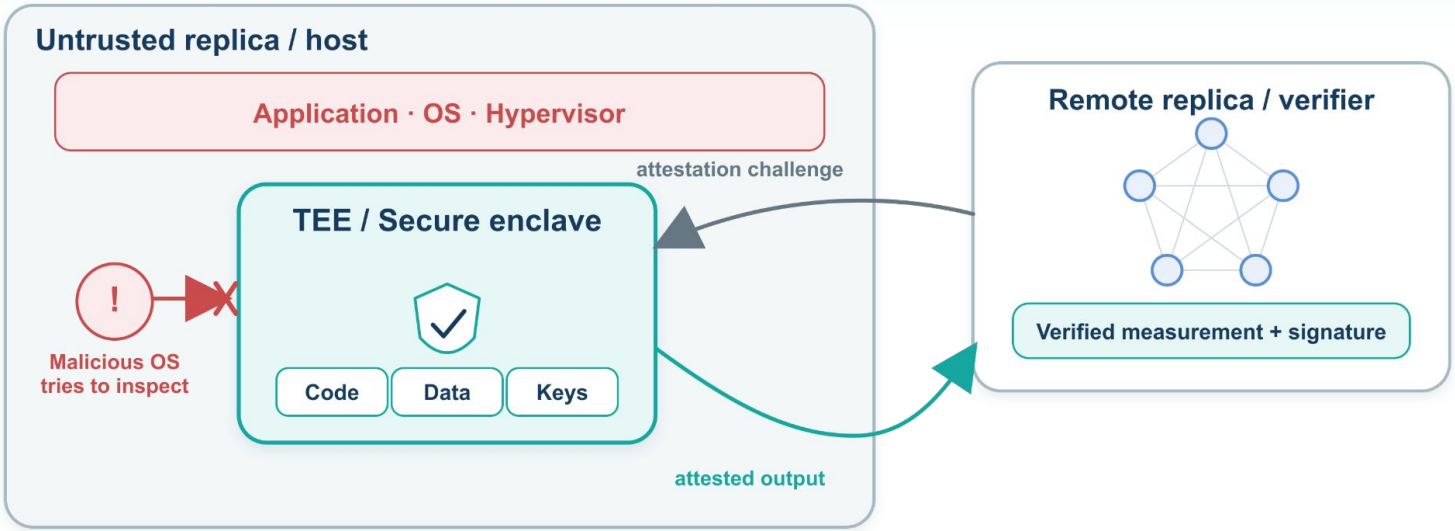
2. **Leader Bottleneck:** leader is too busy while others are idling.

[1] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In OSDI, 1999.

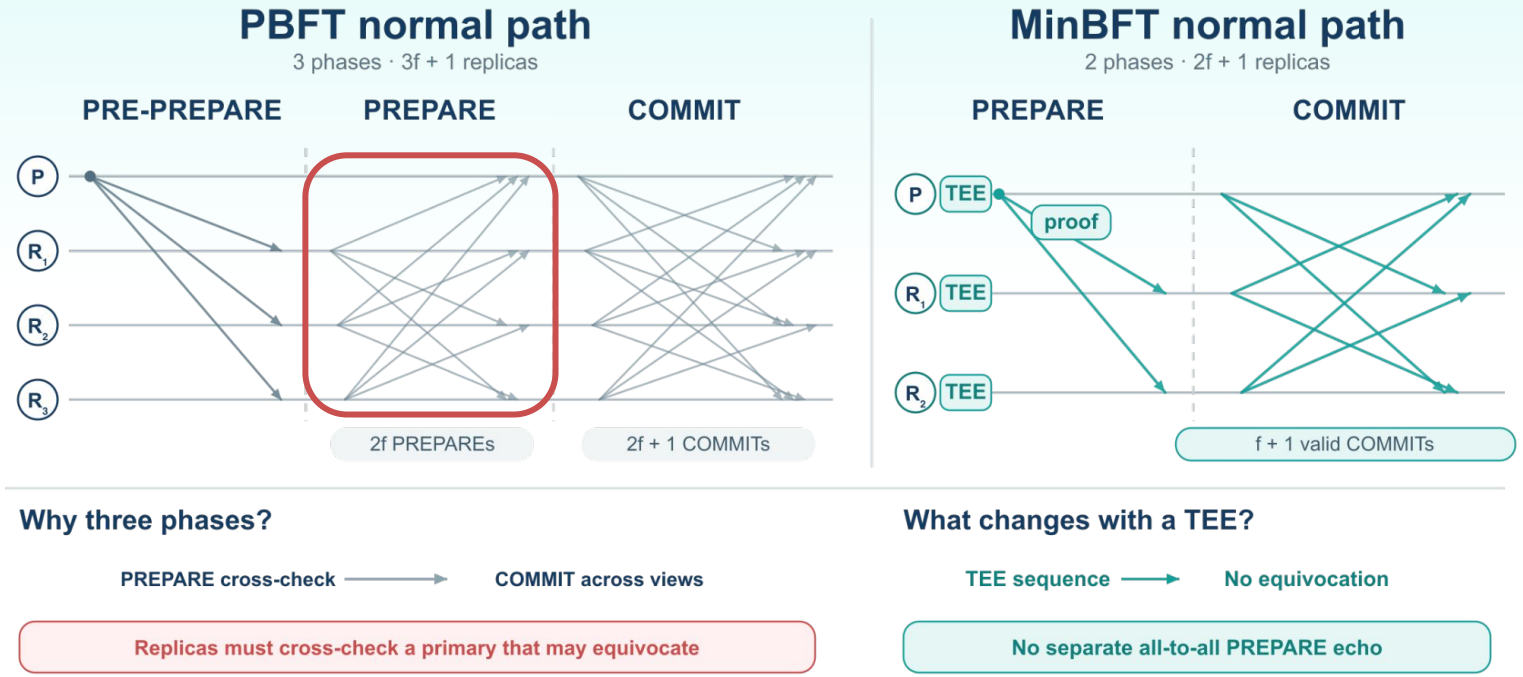
Trusted Execution Environment (TEE)

A TEE creates a small trusted island inside an untrusted replica.

1. **Hardware isolation;** 2. **Remote attestation;** 3. **Verifiable outputs**



TEE addresses 1. Equivocation Cross-checking



TEE brings: 1. One less phase; 2. Higher fault tolerance (f<n/3 -> f<n/2).

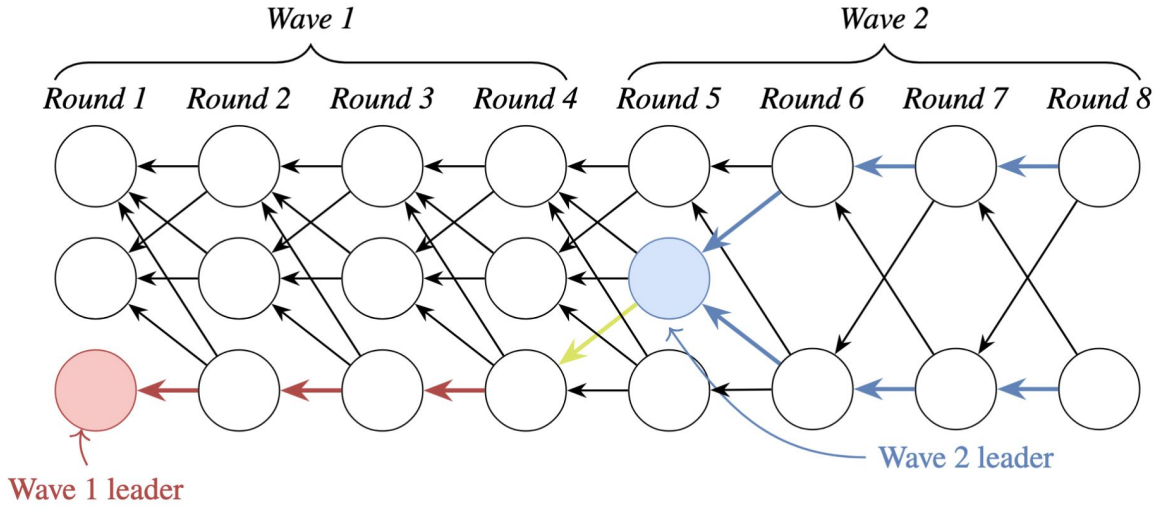
[1] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In OSDI, 1999.
[2] Giuliana Santos Veronese et al. Efficient Byzantine Fault-Tolerance. In IEEE Trans. on Computers, 2013.

DAG-based BFT addresses 2. Leader Bottleneck

Problems of PBFT/MinBFT: All workload is relied on one single leader.

Core Idea:

1. **All replicas propose concurrently and link proposals into a DAG.**
2. **A leader is selected in each *wave* to derive a consistent commit order.**



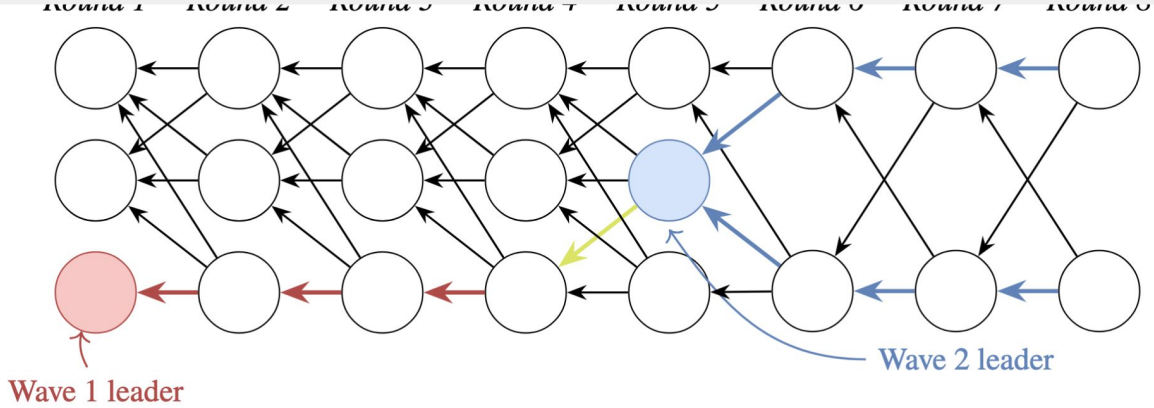
DAG-based BFT addresses 2. Leader Bottleneck

Problems of PBFT/MinBFT: All workload is relied on one single leader.

Core Idea:

1. All replicas propose concurrently and link proposals into a DAG

Can we combine TEE and DAG to scale BFT?

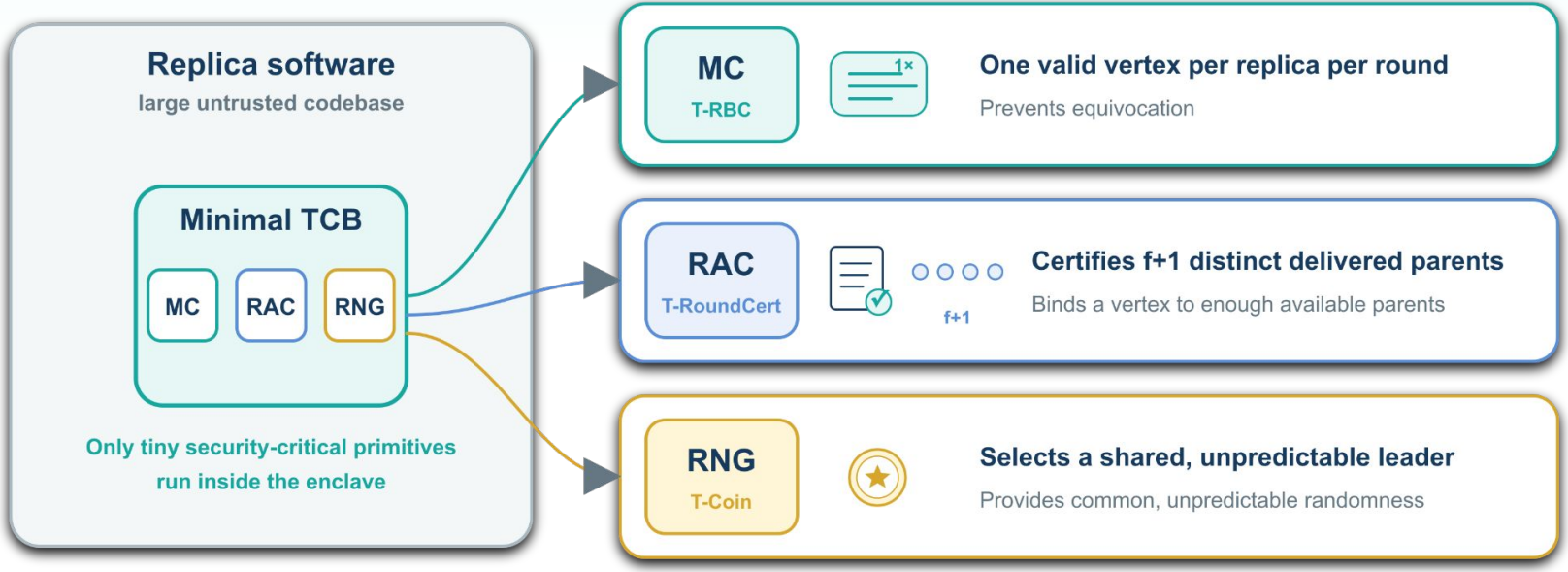


Observation

TEE involves some **crypto overhead**, so we leverage minimal TEE to scale the system (**minimal TCB**): three ***tiny*** (*<1% LOC*) trusted components:

Observation

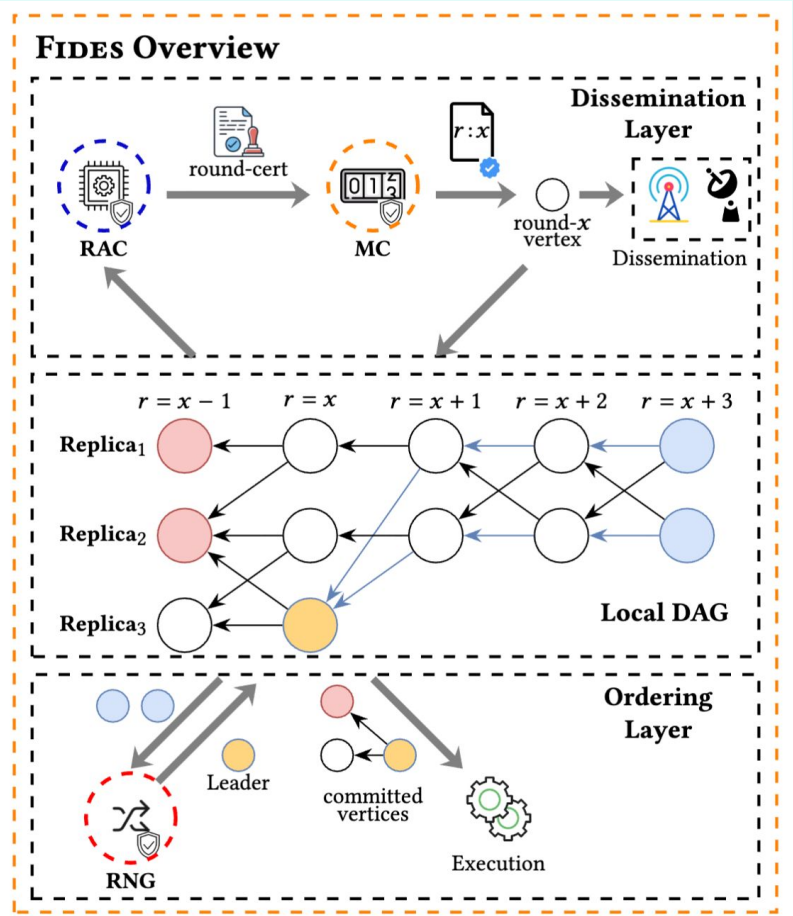
TEE involves some **crypto overhead**, so we leverage minimal TEE to scale the system (**minimal TCB**): three ***tiny*** (*<1% LOC*) trusted components:



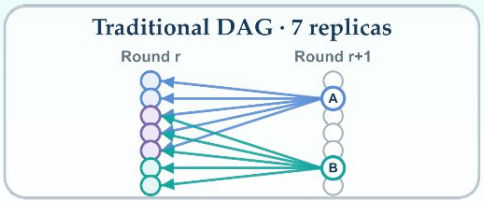
Overview

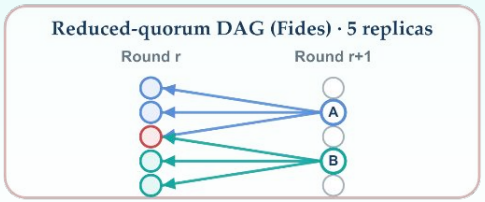
Fides integrates the TEE into the DAG workflow.

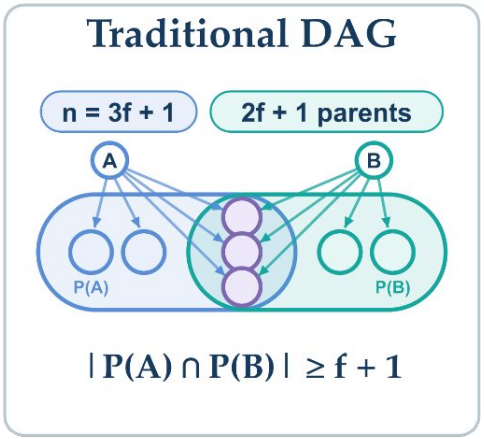
1. **Dissemination:** *RAC* certifies validity of DAG; *MC* ensures replicas can not send conflict msgs.
2. **DAG Construction:** Replicas verify received vertices and link them into their local DAGs.
3. **Ordering:** *RNG* selects a shared leader and commit the transactions.



Challenges & Solution







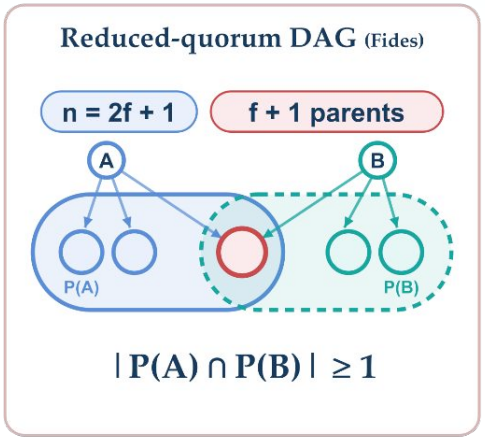
T-RBC

fault threshold

$f < n/3 \rightarrow f < n/2$

fewer parents

example: f = 2



Higher fault tolerance

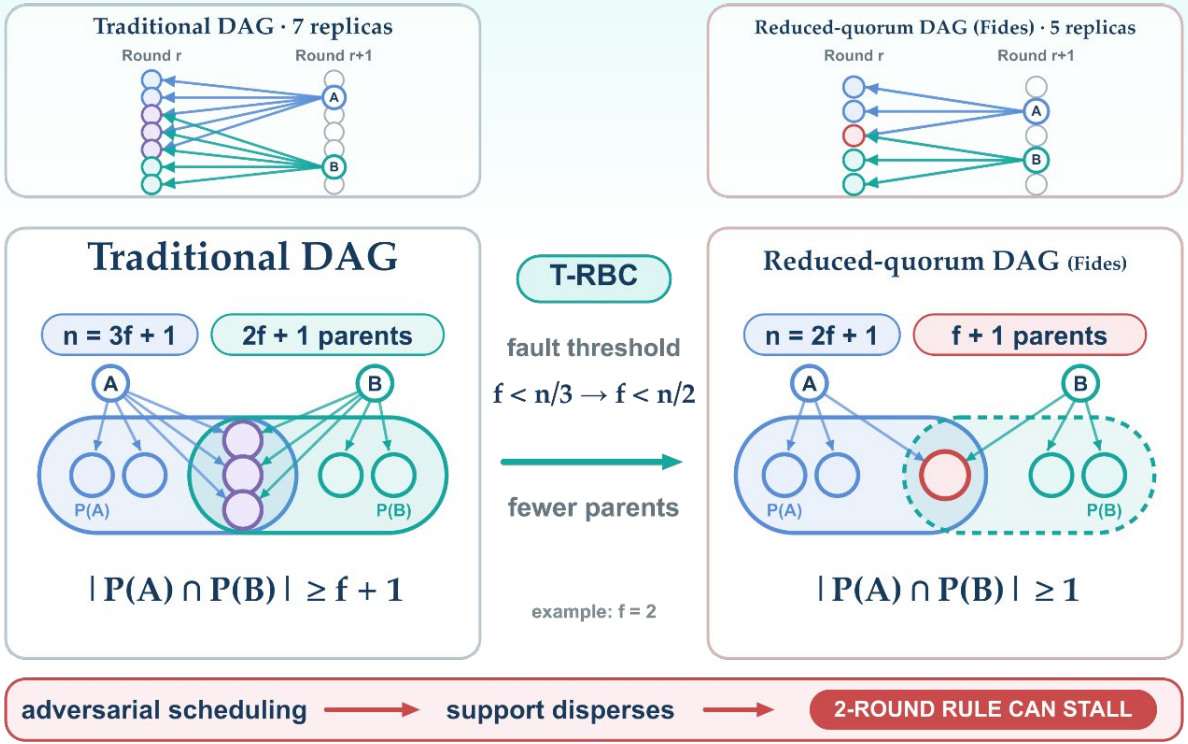
⇩

Less proportion of honest replicas

⇩

Less intersection between references

Challenges & Solution



Higher fault tolerance

⇩

Less proportion of honest replicas

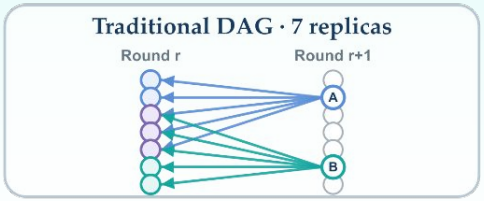
⇩

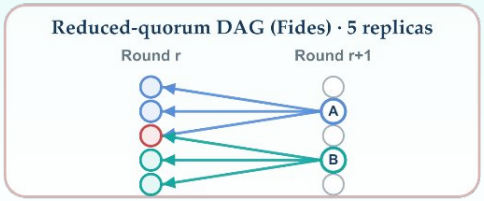
Less intersection between references

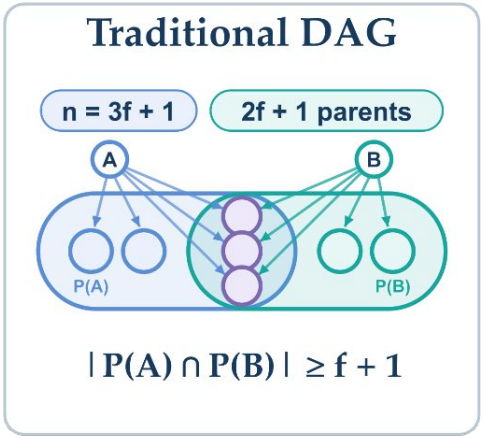
⇩

Weaker DAG connectivity

Challenges & Solution







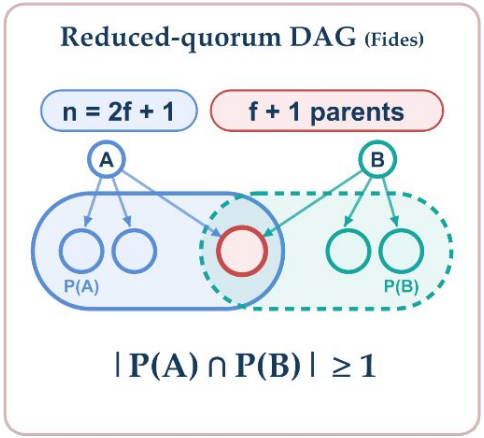
T-RBC

fault threshold

$f < n/3 \rightarrow f < n/2$

fewer parents

example: f = 2



Higher fault tolerance

⇩

Less proportion of honest replicas

⇩

Less intersection between references

⇩

Weaker DAG connectivity

⇩

adversarial scheduling → support disperses → 2-ROUND RULE CAN STALL

FIDES SOLUTION

4-round commit rule

Evaluation Setting

Testbed:

- Alibaba Cloud, g6(t).xlarge
- 4vCPUs and 16GB RAM Ubuntu Linux 22.04
- Deployed both in LAN and WAN
- 50-Byte random KV insertions.

Baseline protocols:

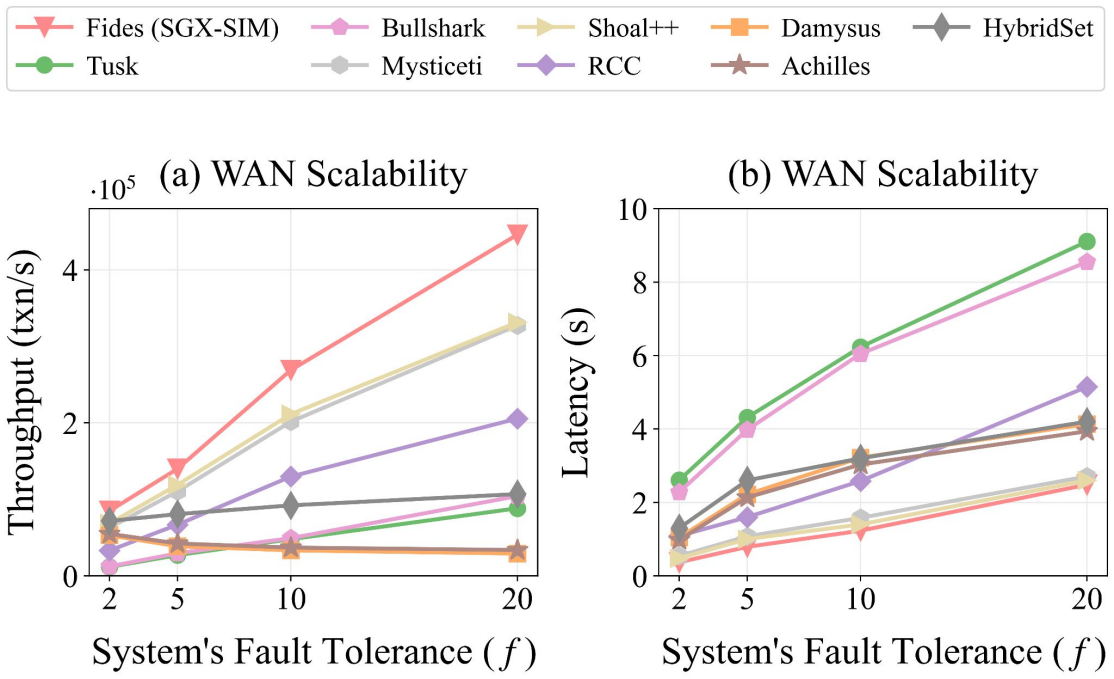
- DAG: Tusk[1], Bullshark[2], Mysticeti[3], Shoal++[4]
- Multi-BFT: RCC[5]
- TEE-BFT: Damysus[6], Achilles[7], HybridSet[8]

Selected Research Questions:

- How does Fides **scale** compared with state-of-the-art BFT protocols?
- How much does each **trusted component** contribute to Fides' performance?
- How **resilient** is Fides under adversarial conditions?

[1] Danezis et al. Narwhal and Tusk: A DAG-Based Mempool and Efficient BFT Consensus, in ACM EuroSys'22.
[2] Spiegelman et al. Bullshark: DAG BFT Protocols Made Practical, in ACM CCS'22.
[3] Babel et al. Mysticeti: Reaching the Latency Limits with Uncertified DAGs, in NDSS'25.
[4] Arun et al. Shoal++: High Throughput DAG BFT Can Be Fast and Robust!, in USENIX NSDI'25.
[5] Gupta et al. RCC: Resilient Concurrent Consensus for High-Throughput Secure Transaction Processing, in IEEE ICDE'21.
[6] Decouchant et al. DAMYSUS: Streamlined BFT Consensus Leveraging Trusted Components, in ACM EuroSys'22.
[7] Niu et al. Achilles: Efficient TEE-Assisted BFT Consensus via Rollback Resilient Recovery, in ACM EuroSys'25.
[8] Zhao et al. Trusted Hardware-Assisted Leaderless Byzantine Fault Tolerance Consensus (HybridSet), in IEEE TDSC'24.

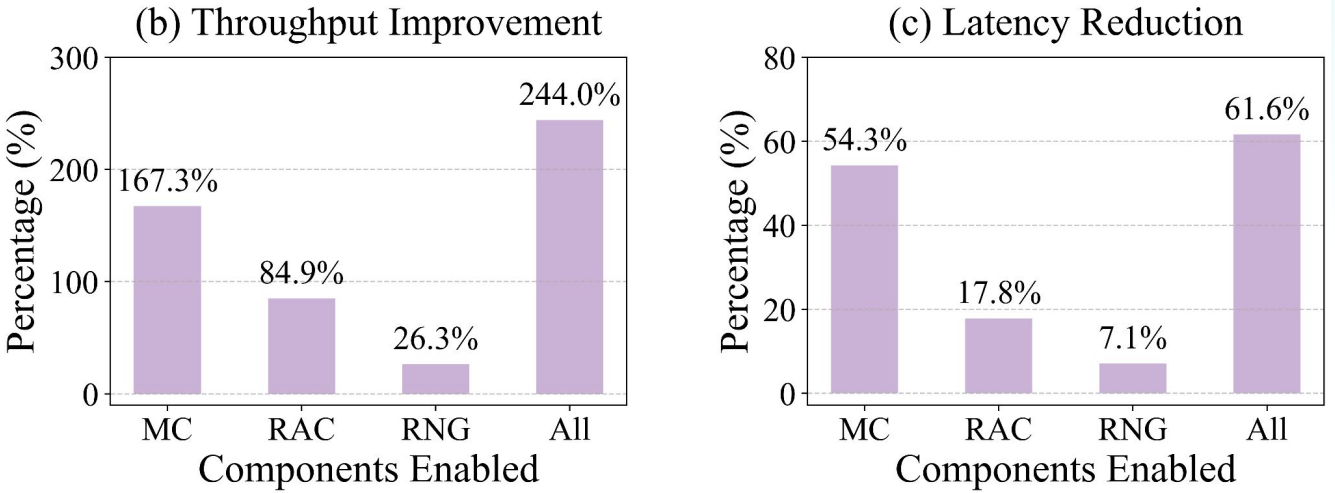
Scalability of Fides and other baselines



- *f* from 2 to 20
- WAN: United States, UAE, Singapore, and Germany

- >4× throughput of Tusk
- ≈35% above the closest DAG baselines

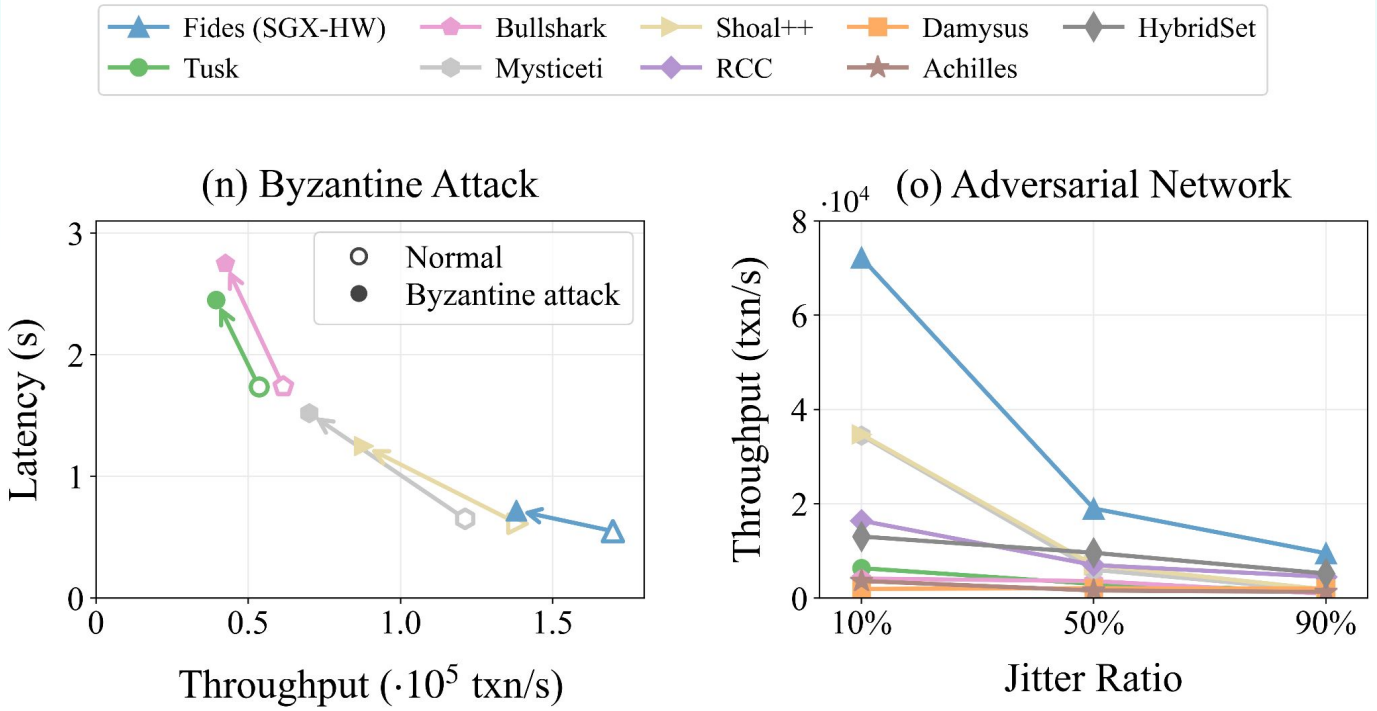
Ablation Study for Trusted Components



- $f = 10$
- MC provides the largest individual gain,

  with RAC and RNG adding further improvements.

Adversarial Experiments



- *f = 10*
- *Byzantine Attack*

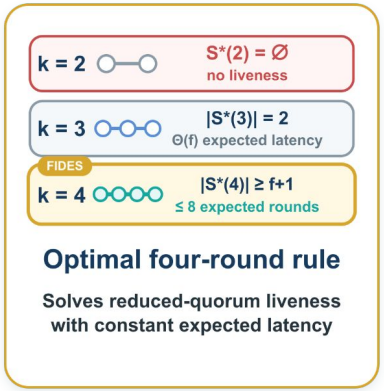
  Selective Delivery
- *Network Jitter*

  10% - 90%

Contributions

Fides: the first **DAG-based & TEE-assisted** BFT protocol

- Tolerates $f<n/2$ Byzantine replicas.
- Scales the system with 3 ***tiny*** trusted components.
- Identifies liveness violation and provides solution.



Code: