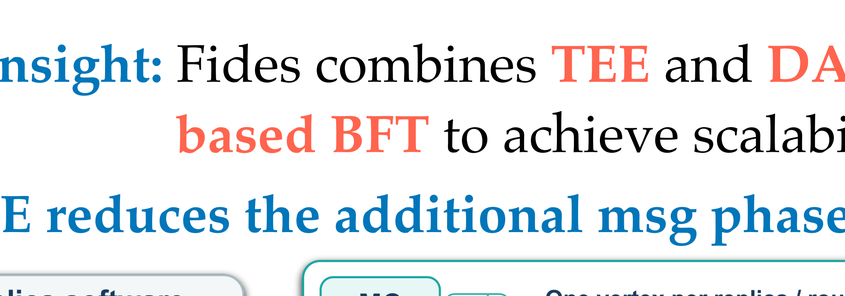
Fides: Secure and Scalable Asynchronous DAG Consensus via Trusted Components

Shaokang Xie†, Dakai Kang†, Hanzheng Lyu*, Jianyu Niu‡, Mohammad Sadoghi†

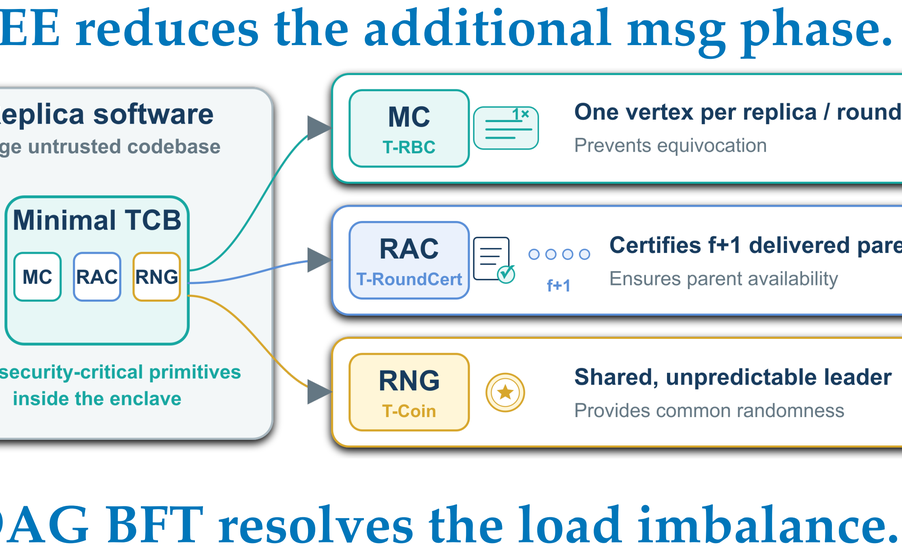
† University of California, Davis, * University of British Columbia, ‡ City University of Hong Kong

Background

- **BFT consensus** allows replicas to reach agreement despite **malicious** replicas (e.g., crash, delay, deviate from protocol).

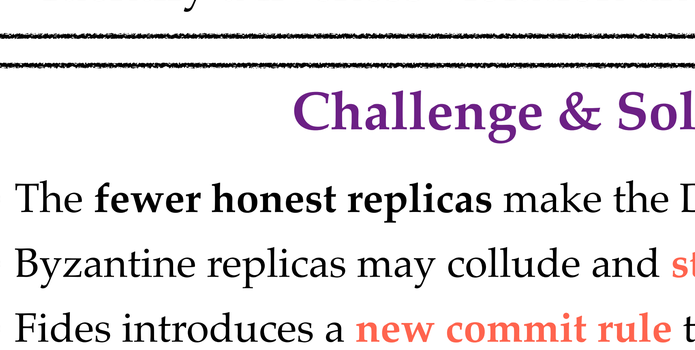


- A **Trusted Execution Environment (TEE)** creates a small trusted island inside an untrusted replica.



Motivations

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



1. Byzantine replicas may lie, so it requires one additional msg phase to coordinate.

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

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

2. One replica handles most of the load, causing load imbalance.

Key Contributions of Fides

The **first DAG-based & TEE-assisted BFT** protocol

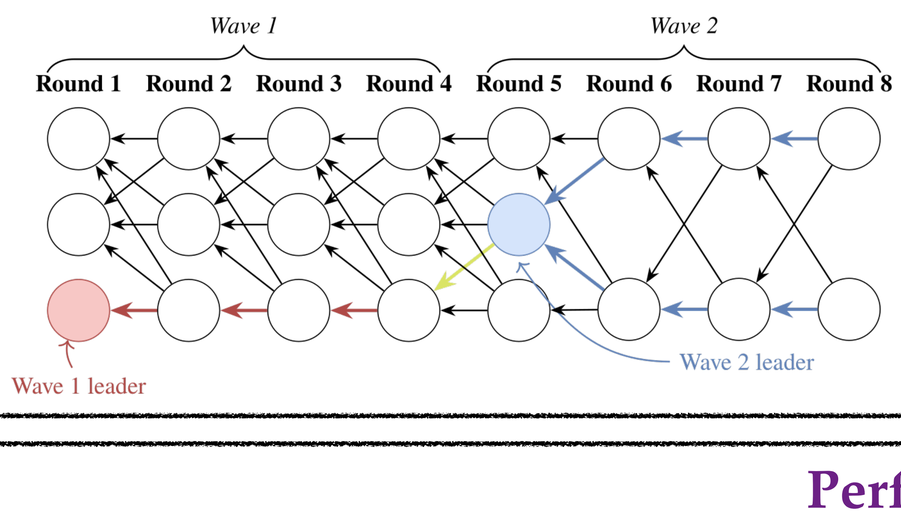
- Tolerates f Byzantine replicas with n=2f+1.
- Scale the system with 3 tiny trusted components.
- Identify a liveness violation and solve it.

Overview of Fides

Key Insight: Fides combines **TEE** and **DAG-based BFT** to achieve scalability.

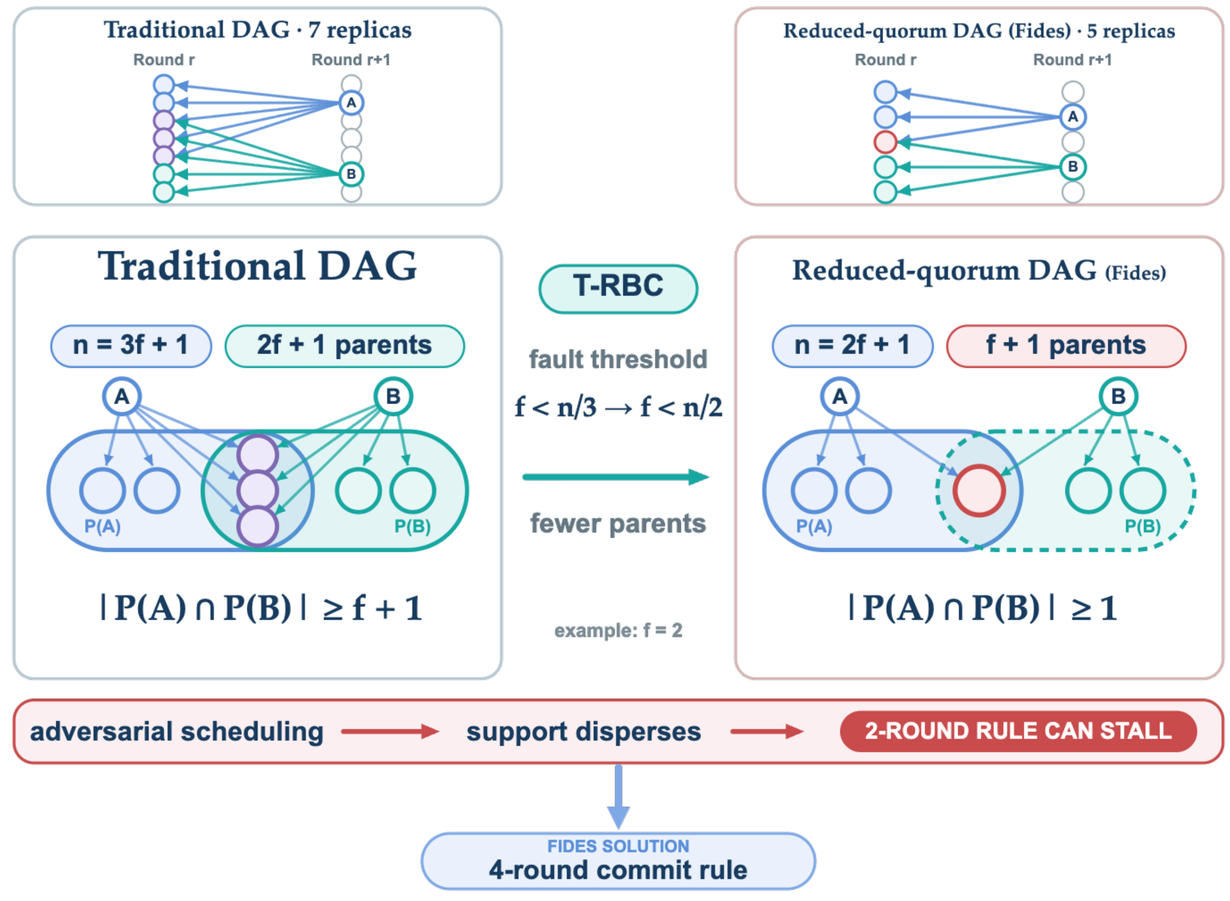
1. TEE reduces the additional msg phase.

2. DAG BFT resolves the load imbalance.

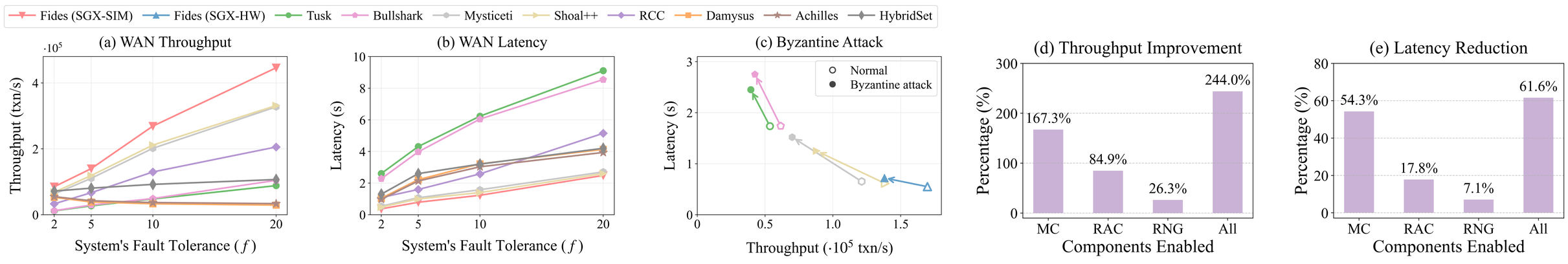


Challenge & Solution

- The **fewer honest replicas** make the DAG **less connected**.
- Byzantine replicas may collude and **stall the whole progress**.
- Fides introduces a **new commit rule** to handle this issue.



Performance Evaluation



- **Scalable:**
  Fides reaches 446K txn/s at (f=20), with 2.48 s WAN latency.
- **Resilient:**
  Fides retains the best performance under Byzantine attack.
- **Complementary gains:**
  All components yield +244% throughput and 61.6% lower latency.

Apache ResilientDB Incubating

ResilientDB open-sourced at https://resilientdb.incubator.apache.org