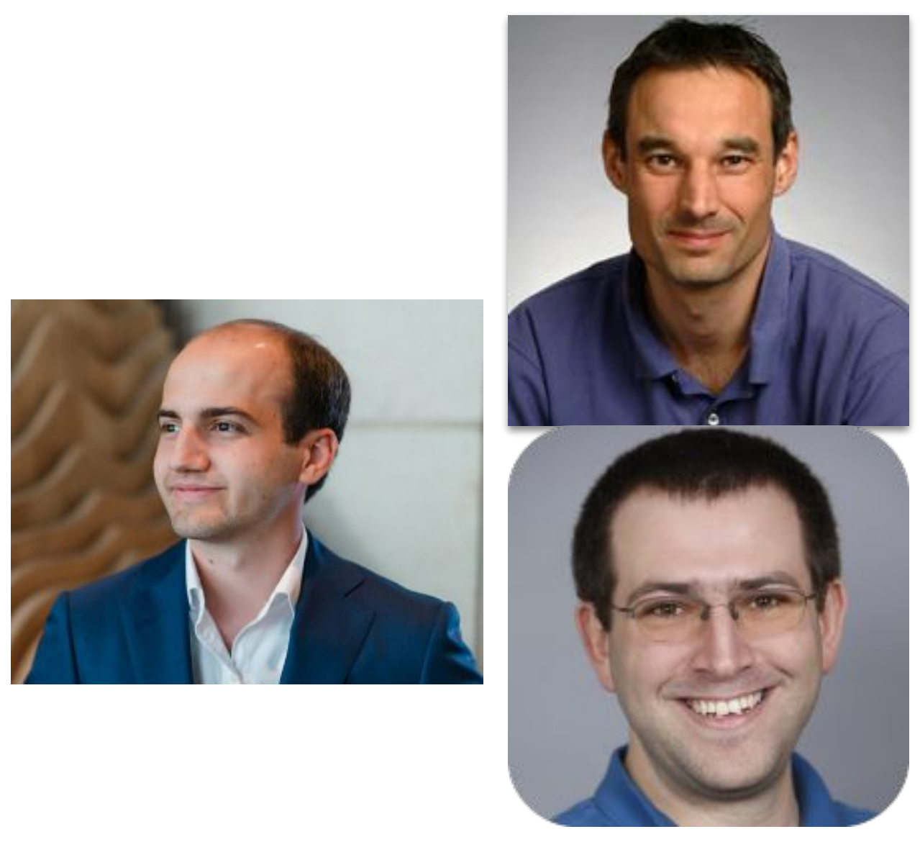
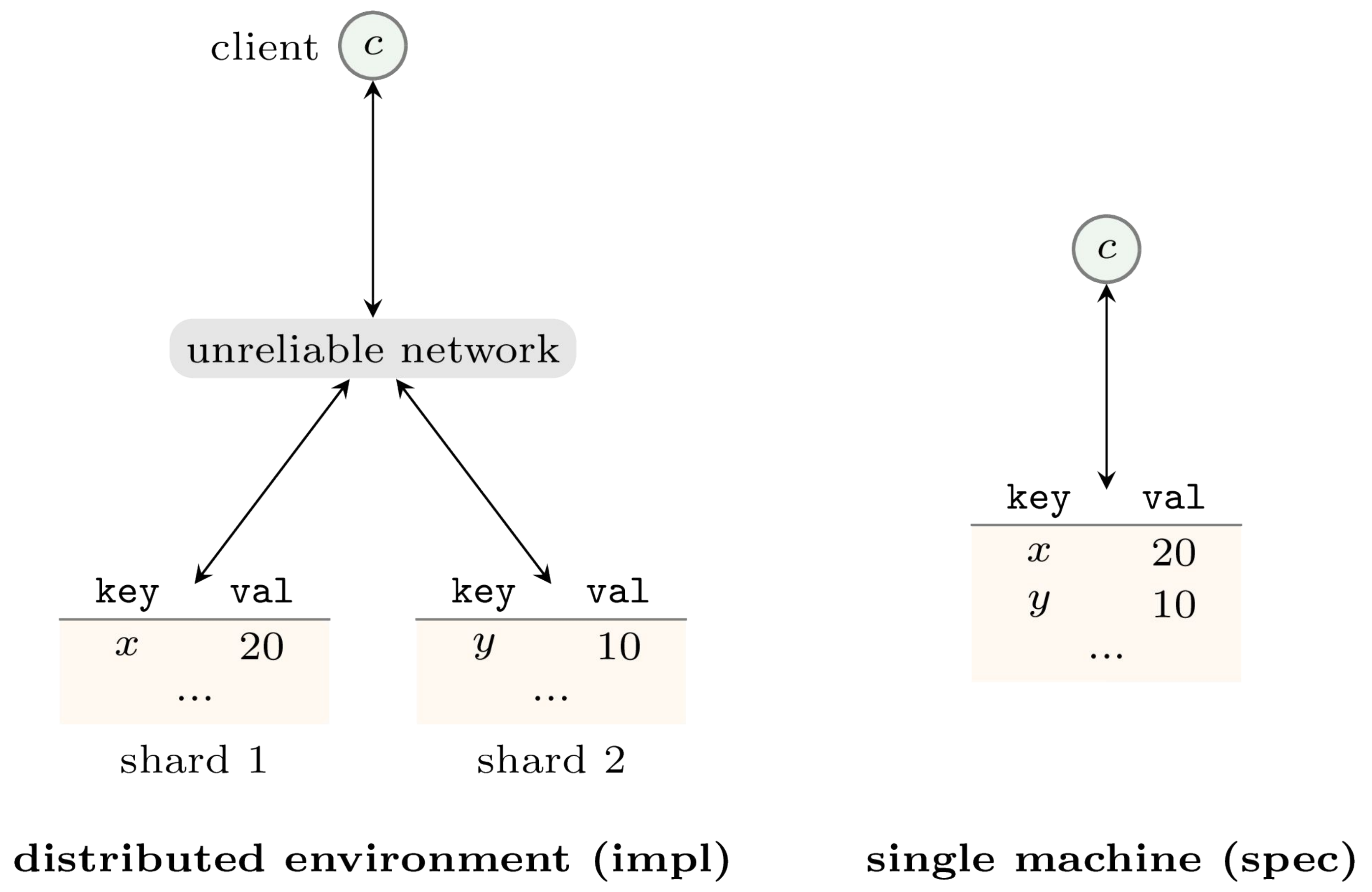
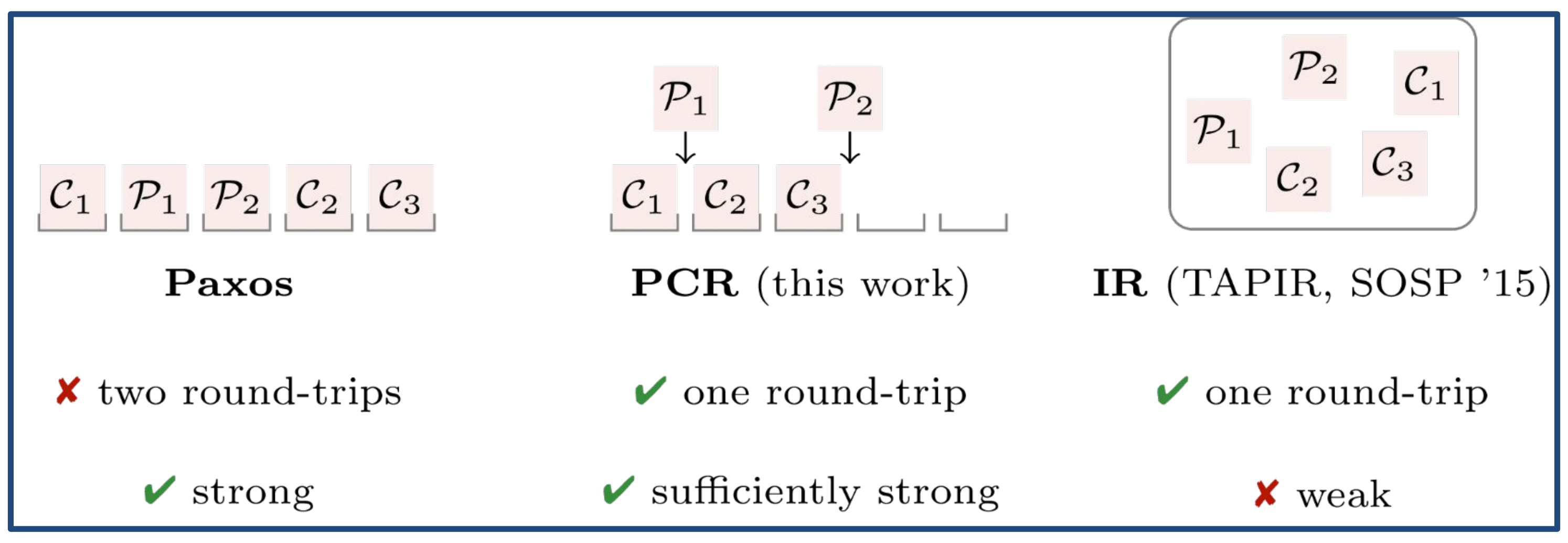
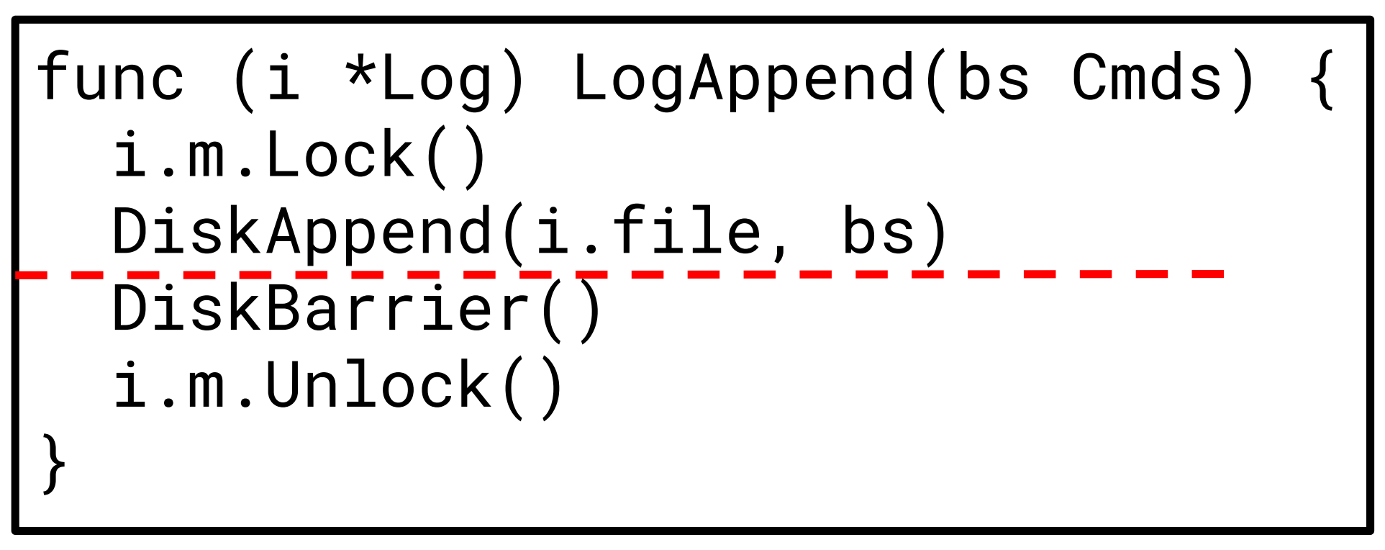
The Phlox Framework for Verifying a High-Performance Distributed Database



Joseph Tassarotti (NYU), Nickolai Zeldovich (MIT), Frans Kaashoek (MIT)




$\mathcal{C}_1$ $\mathcal{P}_1$ $\mathcal{P}_2$ $\mathcal{C}_2$ $\mathcal{C}_3$
Paxos
✘ two round-trips
✔ strong
$\mathcal{P}_1$ $\mathcal{P}_2$
$\mathcal{C}_1$ $\mathcal{C}_2$ $\mathcal{C}_3$
PCR (this work)
✔ one round-trip
✔ sufficiently strong
$\mathcal{P}_2$ $\mathcal{C}_1$ $\mathcal{P}_1$ $\mathcal{C}_2$ $\mathcal{C}_3$
IR (TAPIR, SOSP '15)
✔ one round-trip
✘ weak



```
func (i *Log) LogAppend(bs Cmds) {
  i.m.Lock()
  DiskAppend(i.file, bs)
  DiskBarrier()
  i.m.Unlock()
}
```

Challenges:

- Distributed databases are the foundation of many important systems
- Highly non-deterministic (re-ordering, crashes, message drops) with future-dependent linearization points
- Optimizations involve operating over inconsistent data

Scientific Impact:

- Generalized prophecy variable technique will be usable for verifying other future-dependent data structures
- Verified distributed transaction system could be used as a library for other verified systems

Solutions:

Enhanced Prophecy Variables

- Previously showed how to use prophecy variables in separation logic to verify vMVCC, a single-node high-performance transaction system.
- New Phlox framework extends prophecy variables to support (1) cross-node prophecies, and (2) prophecies about distributed non-determinism (crash, message re-ordering, etc.)

Partially Consistent Replication (PCR)

- New protocol for distributed transactions. Avoids 2 round-trip latency of 2PC over Paxos but still provides strong ordering guarantees on transaction commits.
- Proof (WIP) uses prophecies about transaction effects/ordering across nodes to reason about linearization points.

Broader Impacts on Society

- Reducing bugs in distributed transaction systems is important because they can cause major outages and data loss.
- Verifying correctness of optimizations needed for high-performance is important since these are often complex sources of bugs.

Broader Impacts on Education

- Developing new course material and tutorials on applying separation logic to verify systems. (WIP)
- Tutorial on extending separation logic verification frameworks to reason about different effects (e.g. crashes, distributed execution, etc.) (WIP)

Broadening Participation

- Organized New England Systems Verification Day, bringing together academic and industry practitioners in formal methods.
- Undergraduate / MEng research projects on separation logic and systems verification

The NSF Formal Methods in the Field PI Meeting (2024 FMitF PI Meeting)
November 12-13, 2024 | The University of Iowa | Iowa City, Iowa