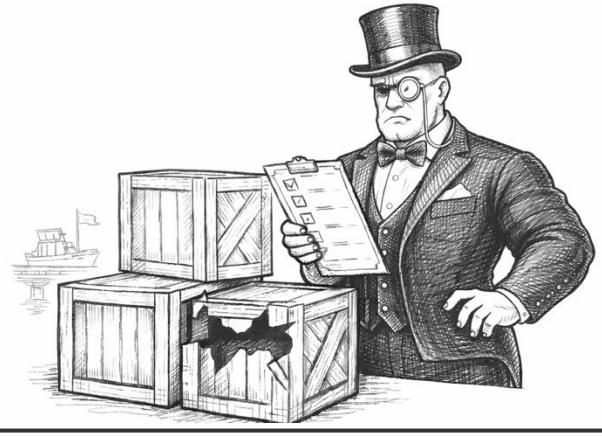
HarborMaster: Rollback Detection for Trusted Distributed Computing

Shubham Mishra
Alexander Thomas
Nurzhan Abdrassilov
Natacha Crooks
John Kubiatowicz

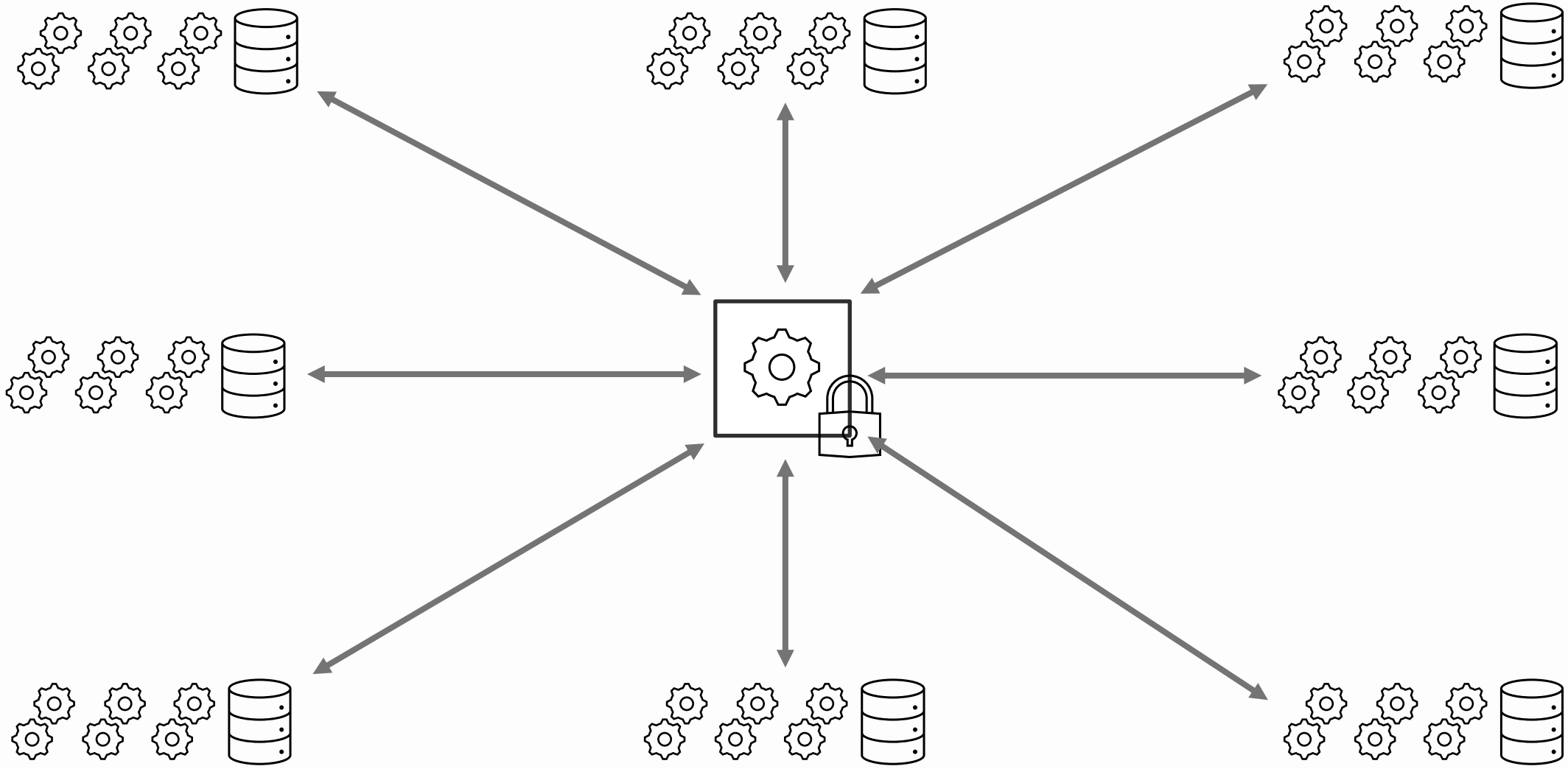


Context: Trusted Execution Environments

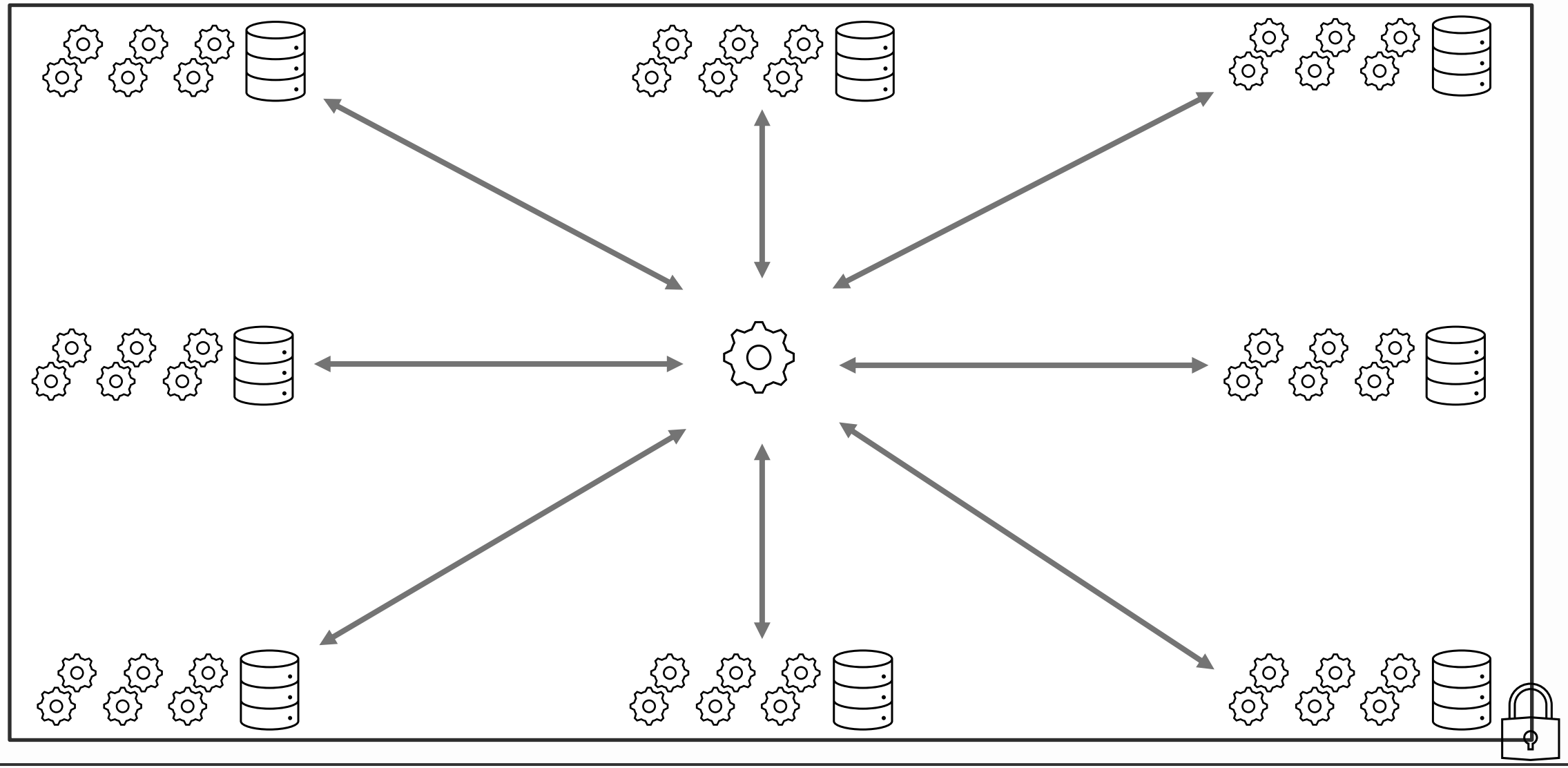
Execution integrity

Confidentiality

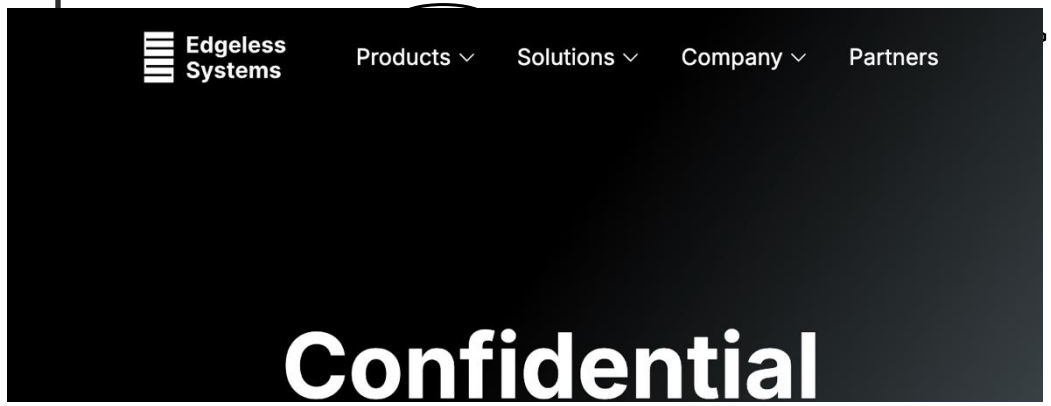
The Evolution of TCB

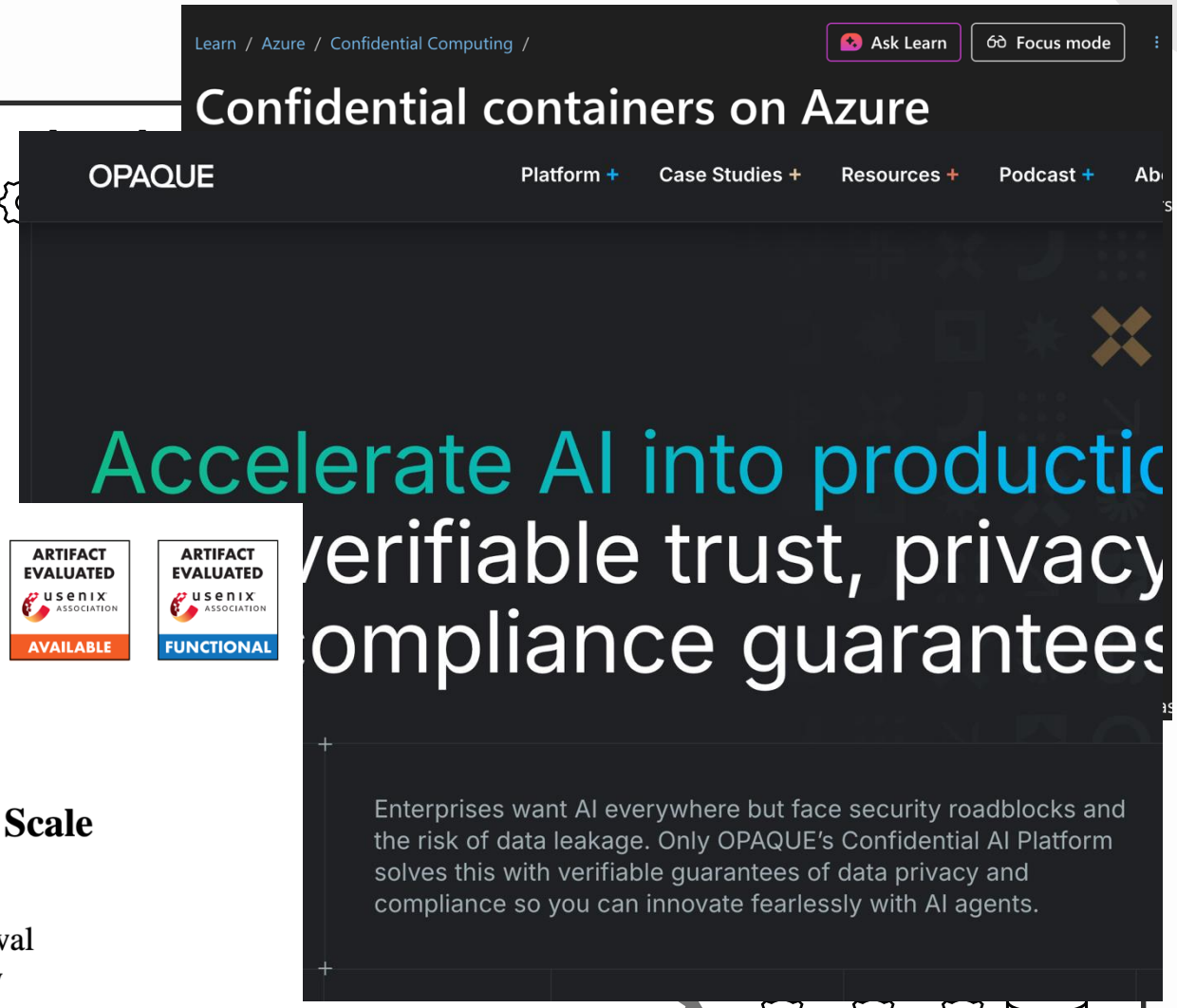


The Evolution of TCB



The Evolution of TCB



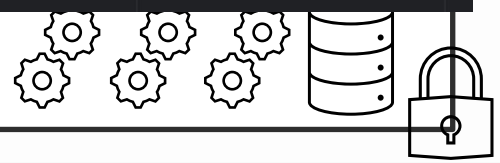


Weave: Efficient and Expressive Oblivious Analytics at Scale

Mahdi Soleimani
Yale University

Grace Jia
Yale University

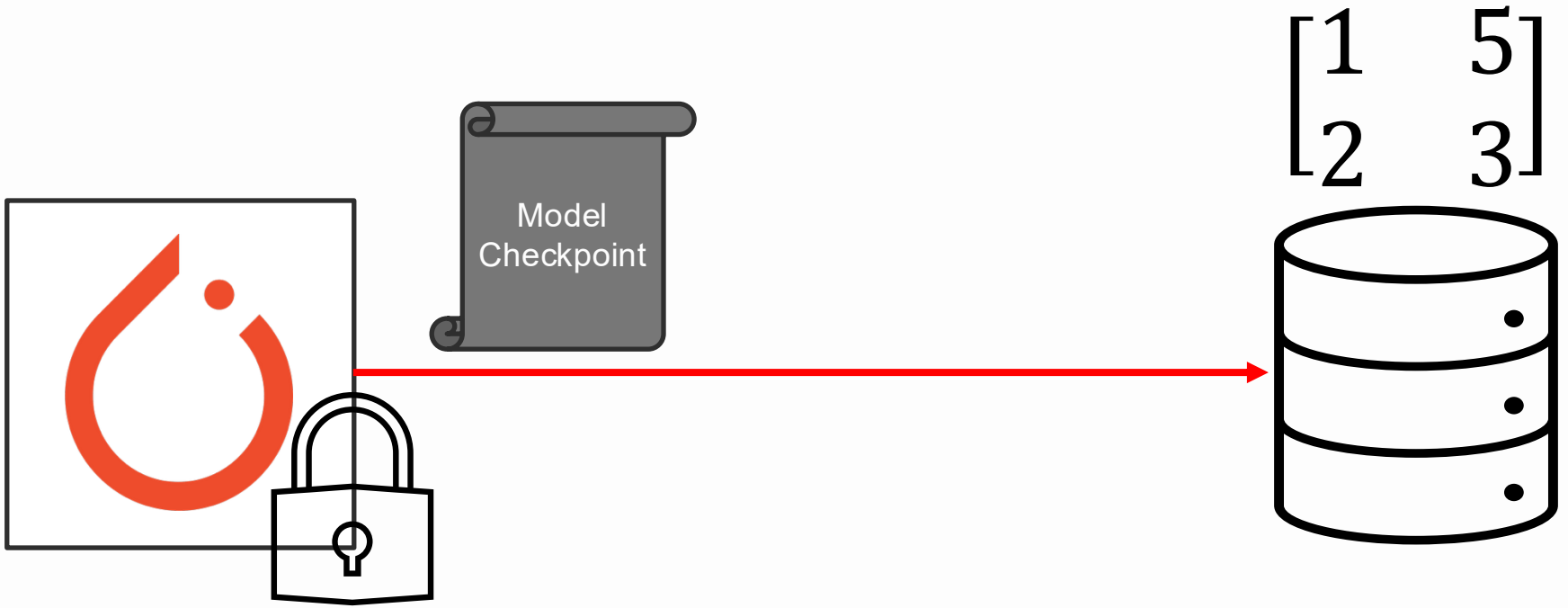
Anurag Khandelwal
Yale University



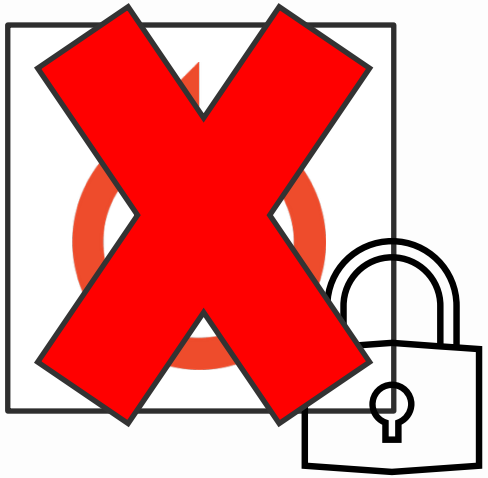
There’s one big problem!

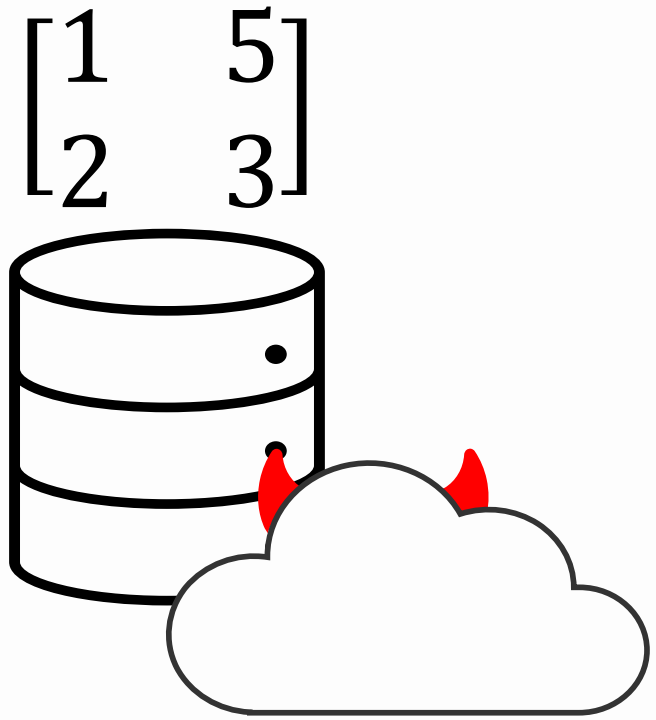
TEEs do not protect persistent storage!

Rollback Attacks



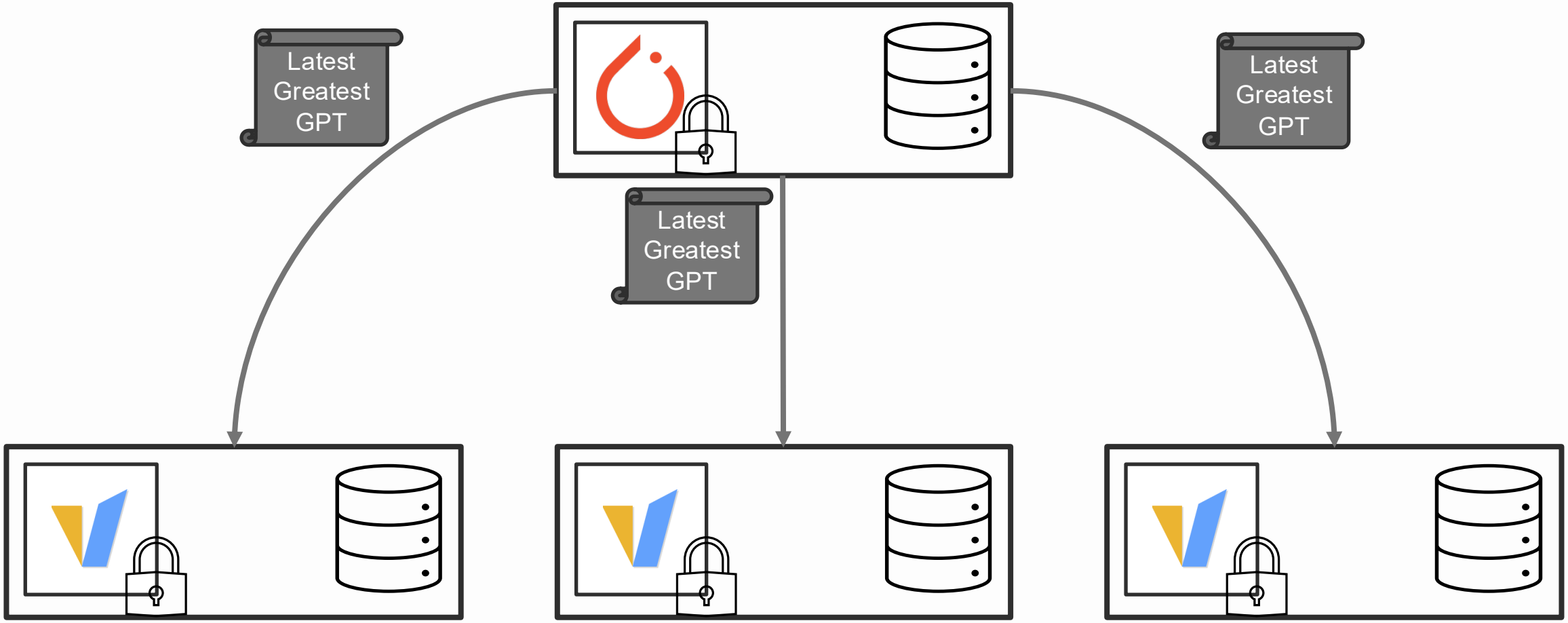
Rollback Attacks



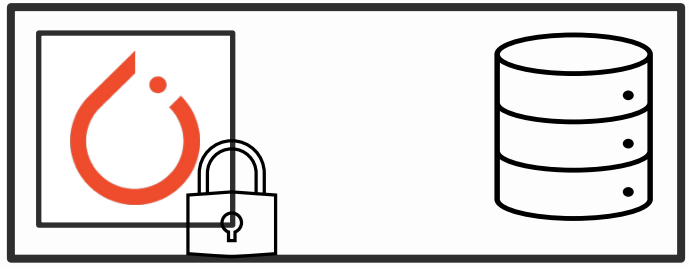


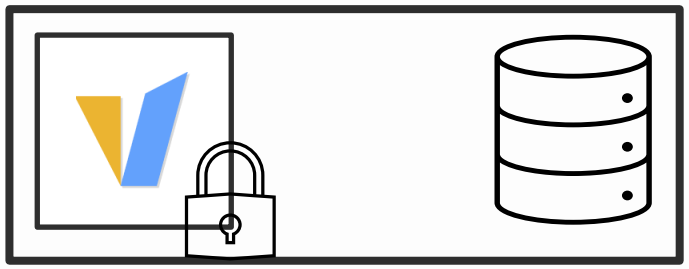
Rollback Attacks

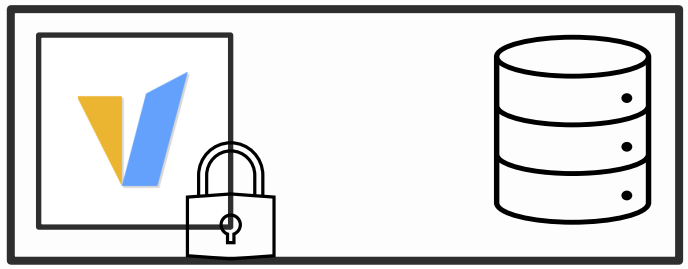
Rollback Attacks

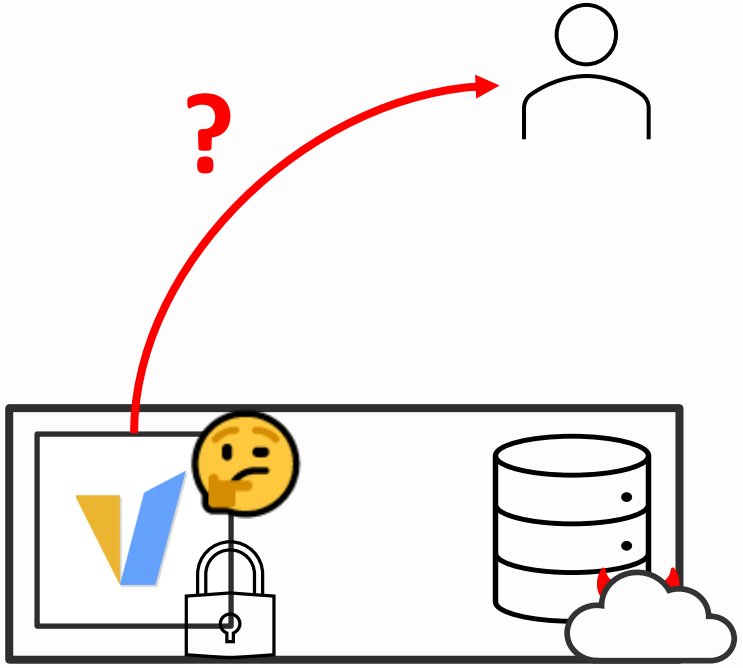


Rollback Attacks





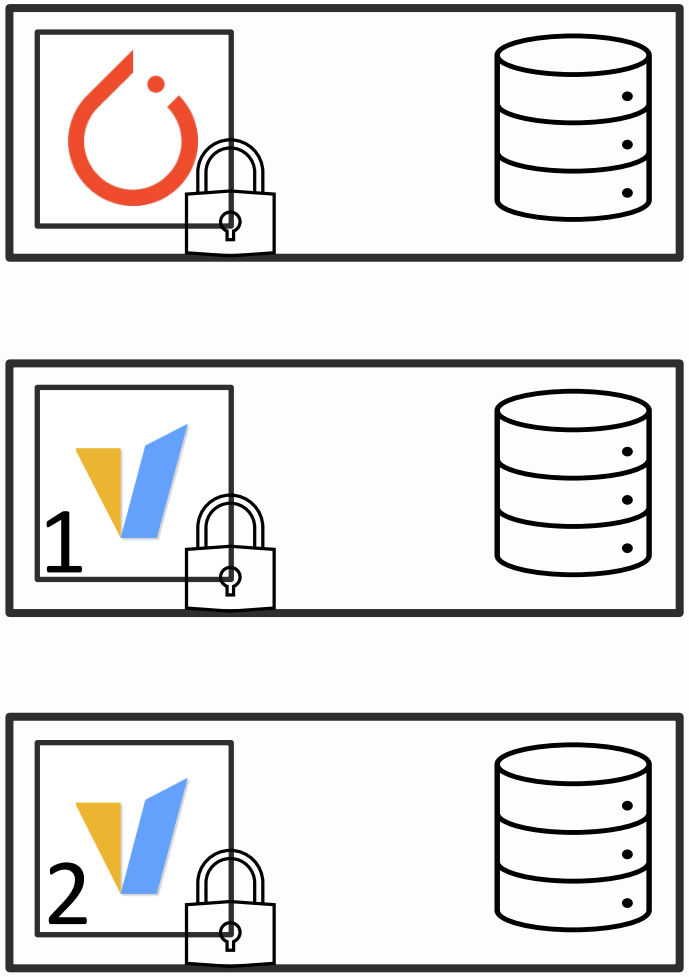


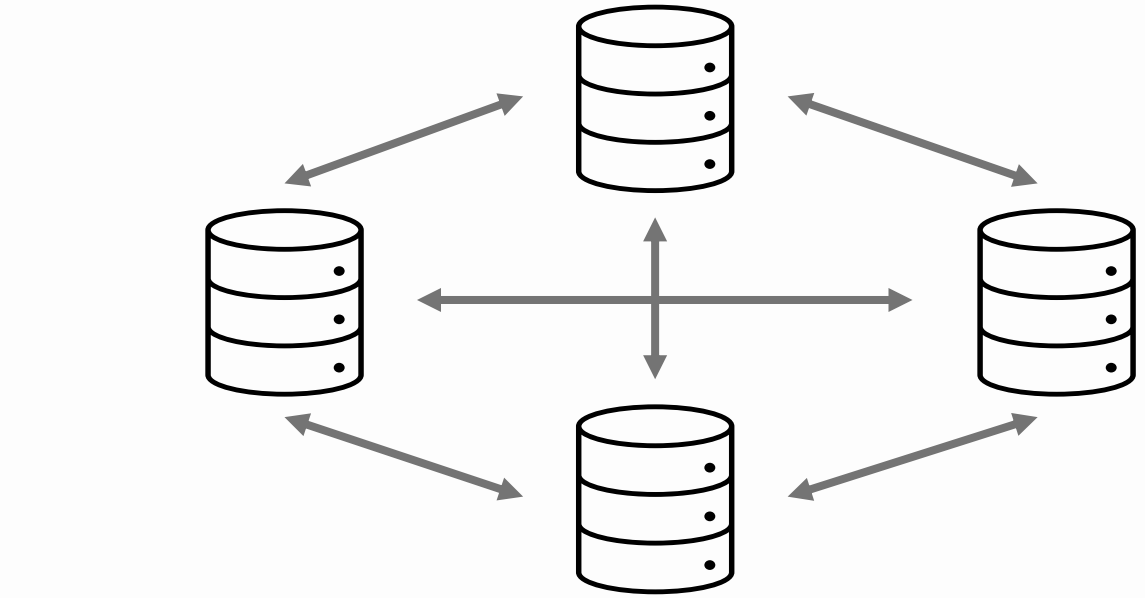


Rollback *Detection*

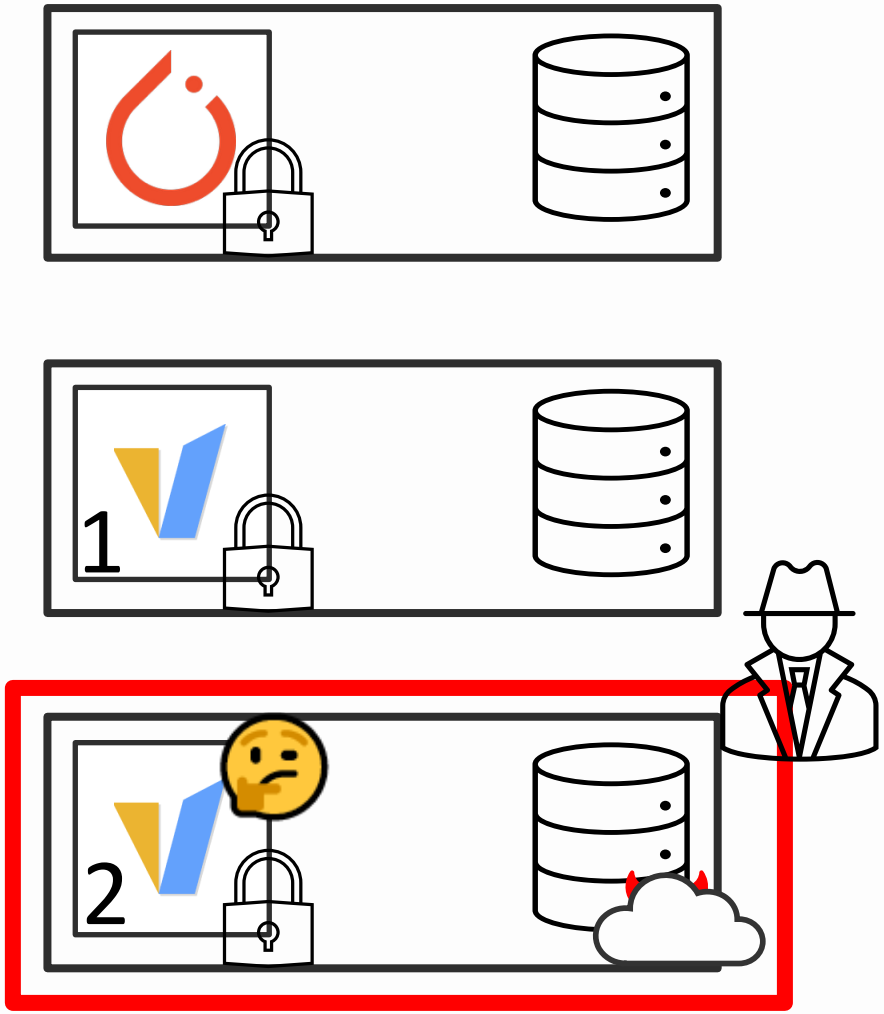
Durable Logging is necessary!

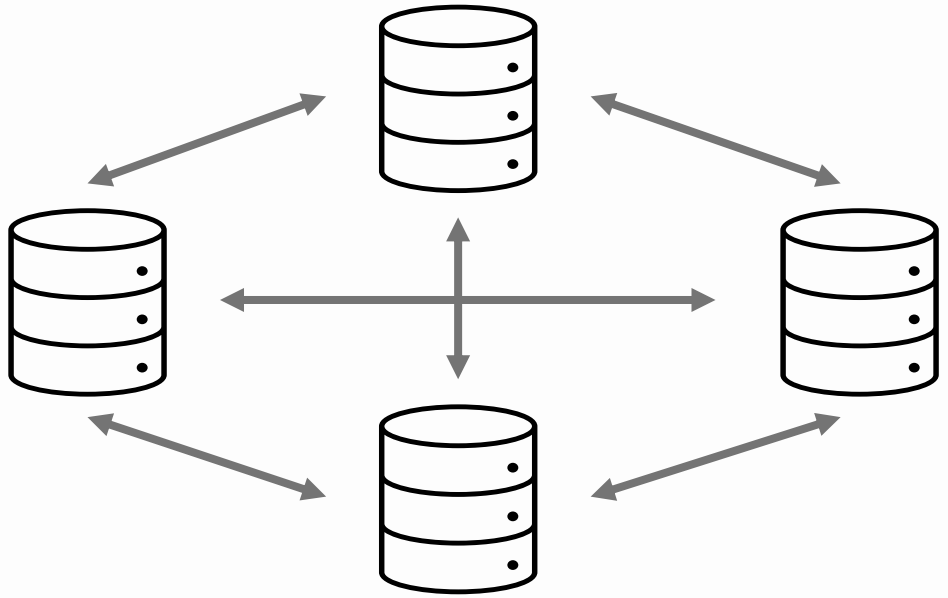
The Single-Log Approach





The Single-Log Approach

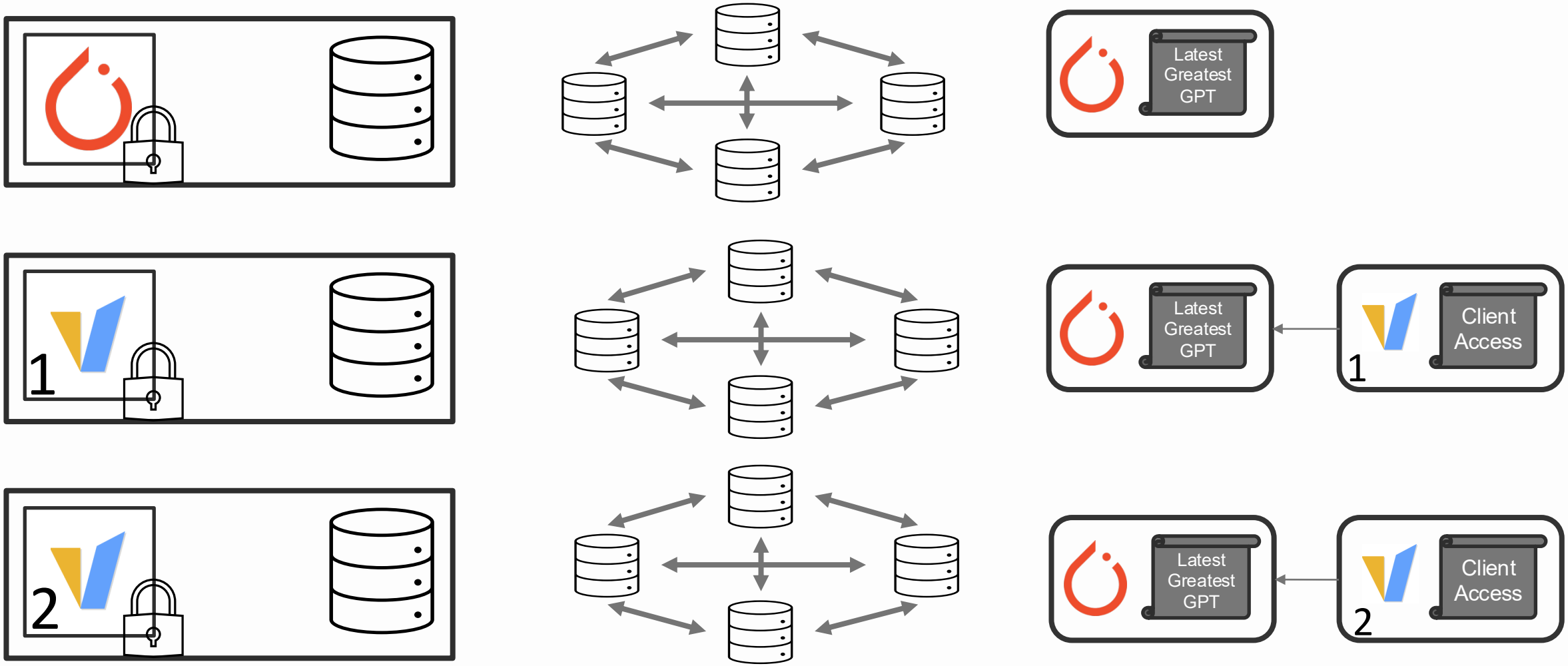




The Single-Log Approach

- One log: easy to audit.
- But very high **coordination overhead.**
- Operations can’t run in parallel, must be serialized.

The Multi-Log Approach



The Multi-Log Approach

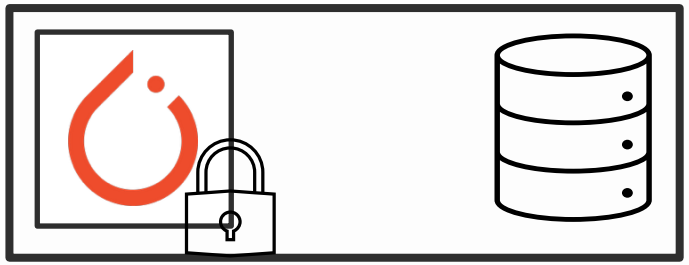
- No Coordination Overhead.
- But prone to high **write amplification**!

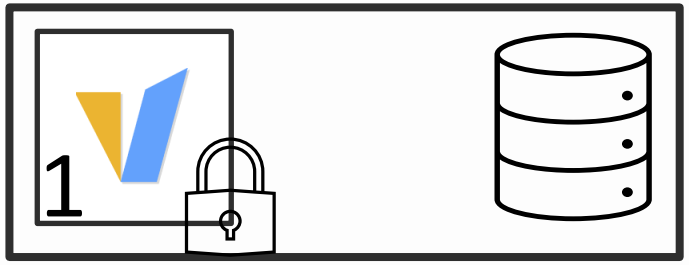
Can we do better?

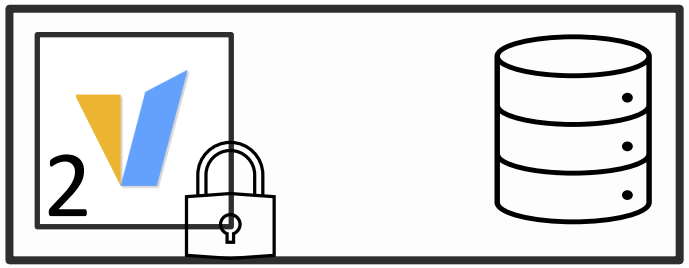
Insight

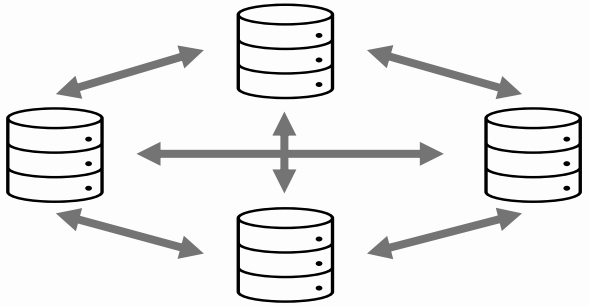
Rollback Attack $\Rightarrow$ Violation of Causality

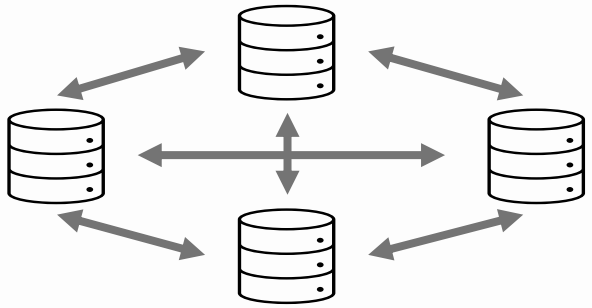
Insight

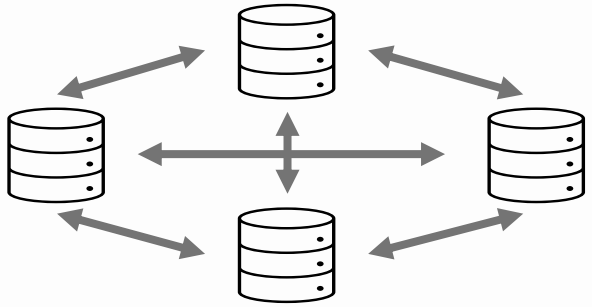




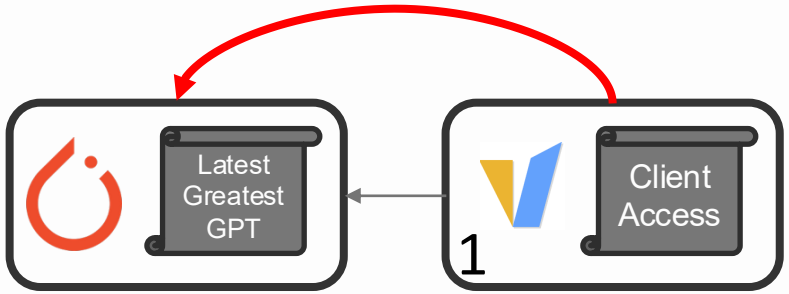




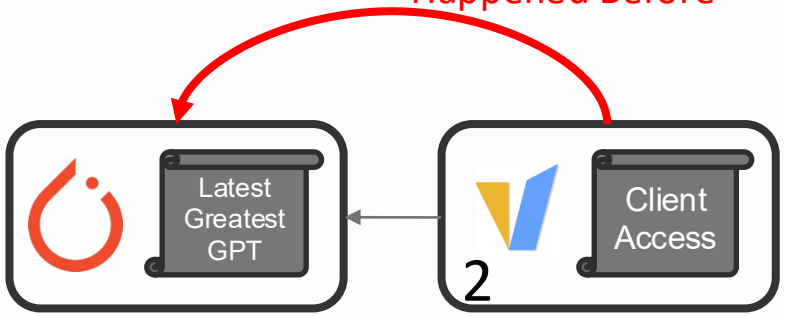




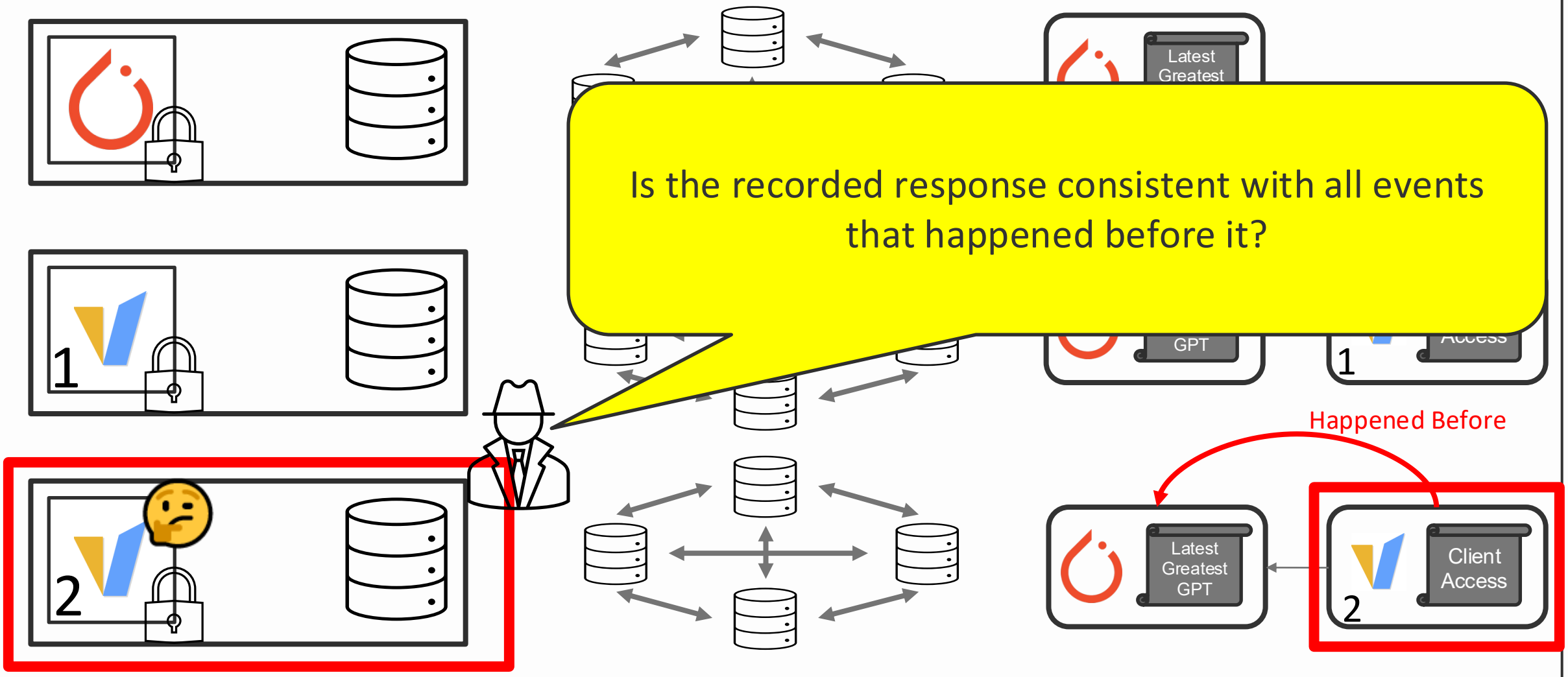
Happened Before



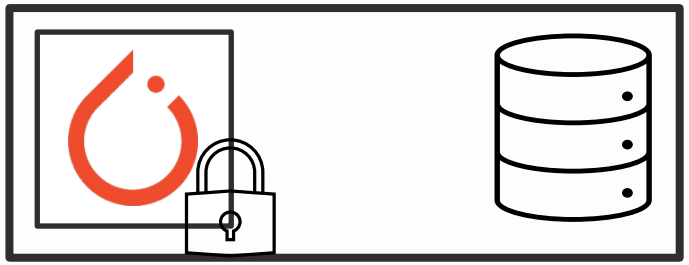
Happened Before

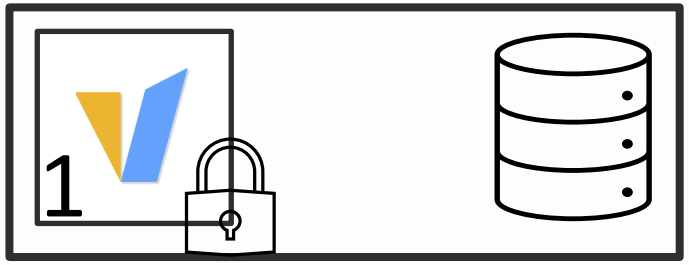


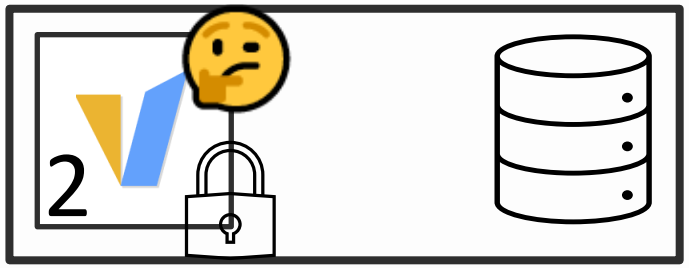
Insight

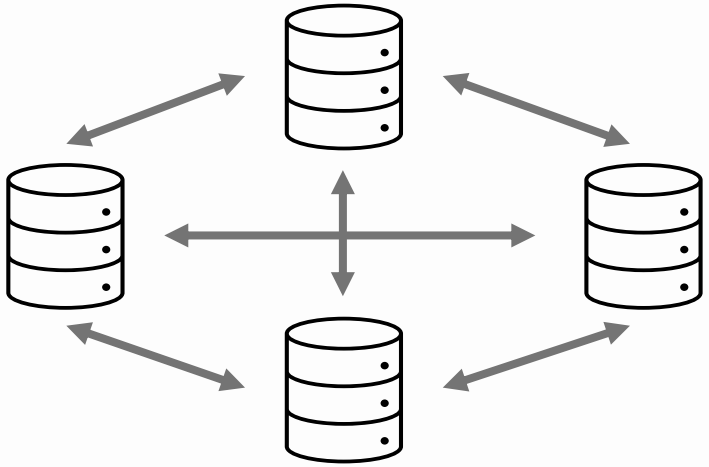

1
2
Is the recorded response consistent with all events that happened before it?
Latest Greatest GPT
Client Access
Happened Before
Latest Greatest GPT
Client Access

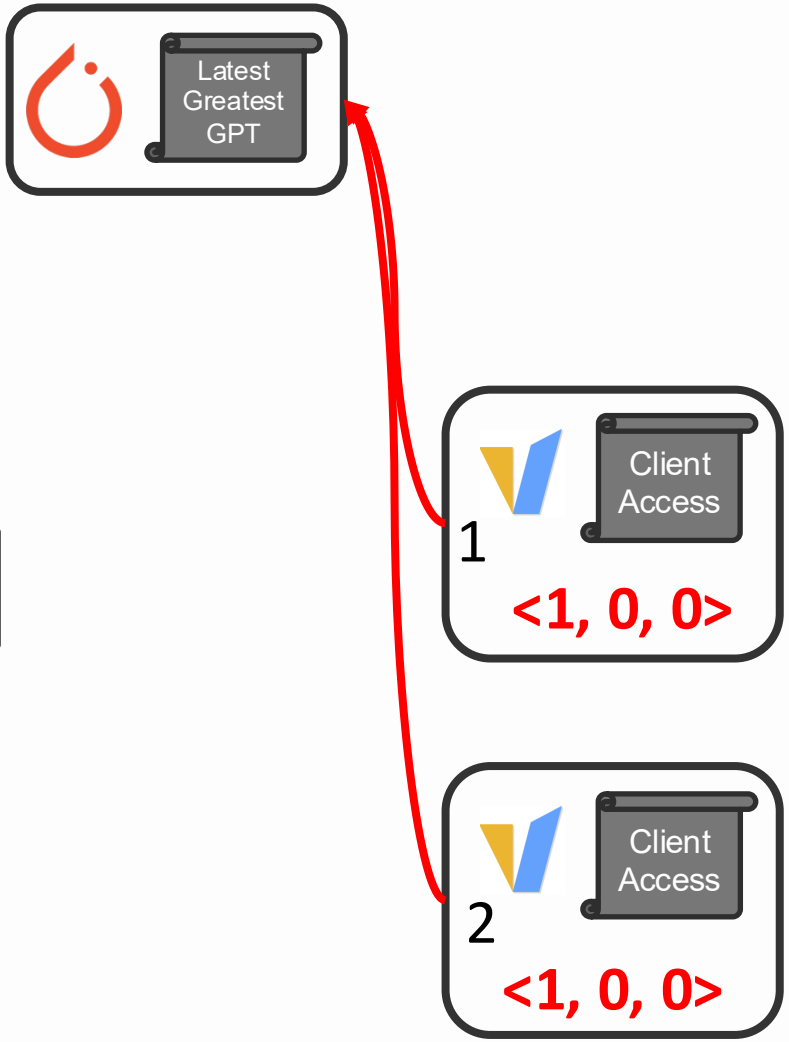
Causal Logging: Vector Clocks



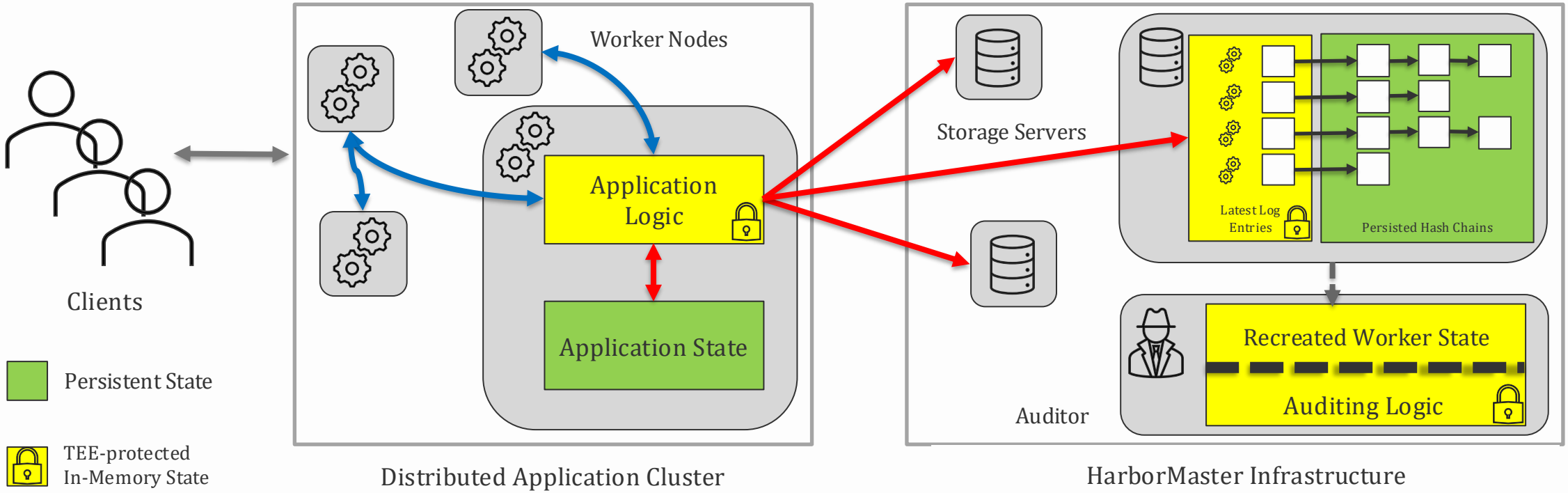








HarborMaster Architecture



Pick your ~~poison~~ antidote!

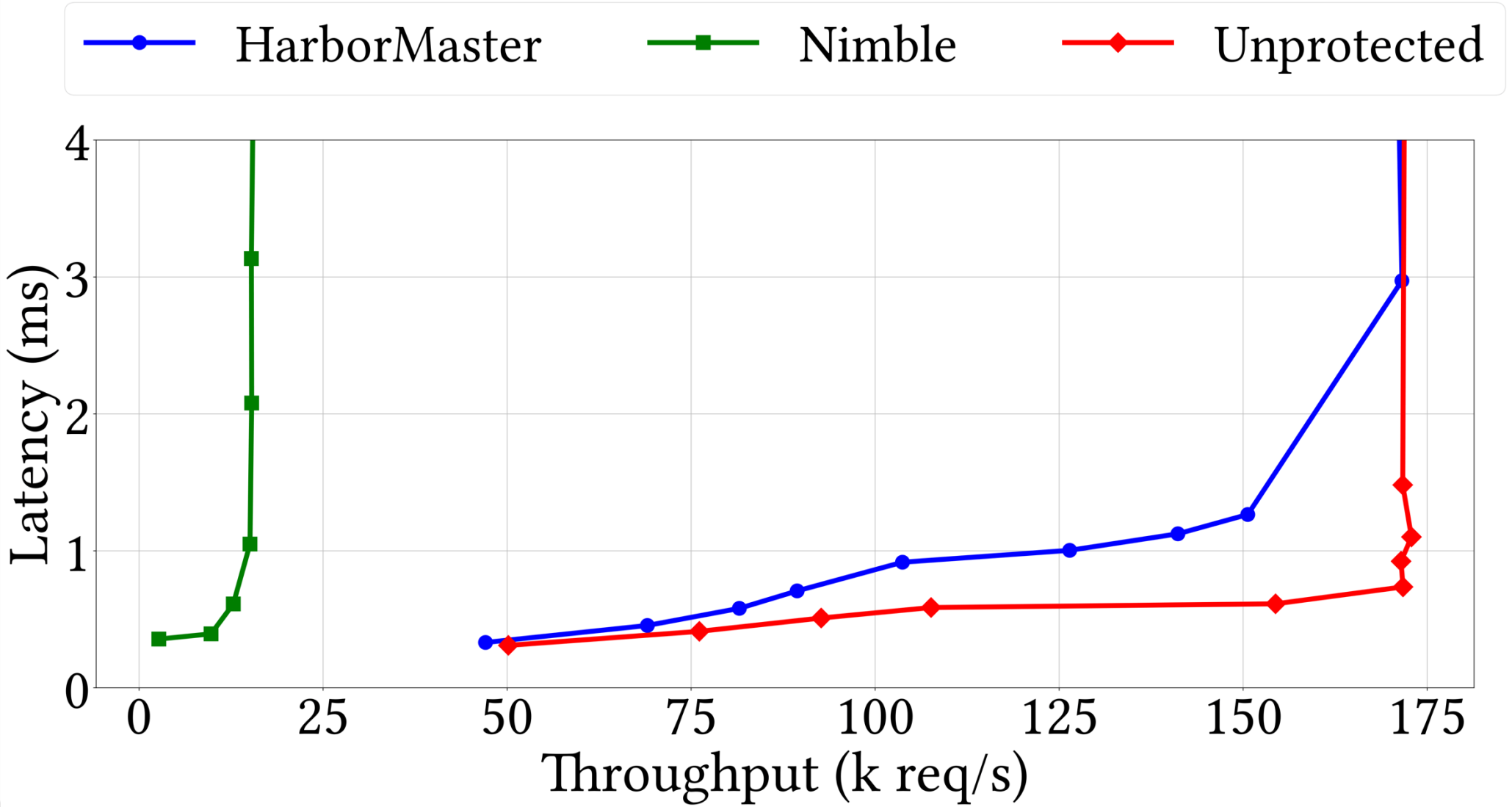
HarborMaster-lite

- Just the logging and auditing infrastructure.
- Suitable for lifting-and-shifting existing applications.

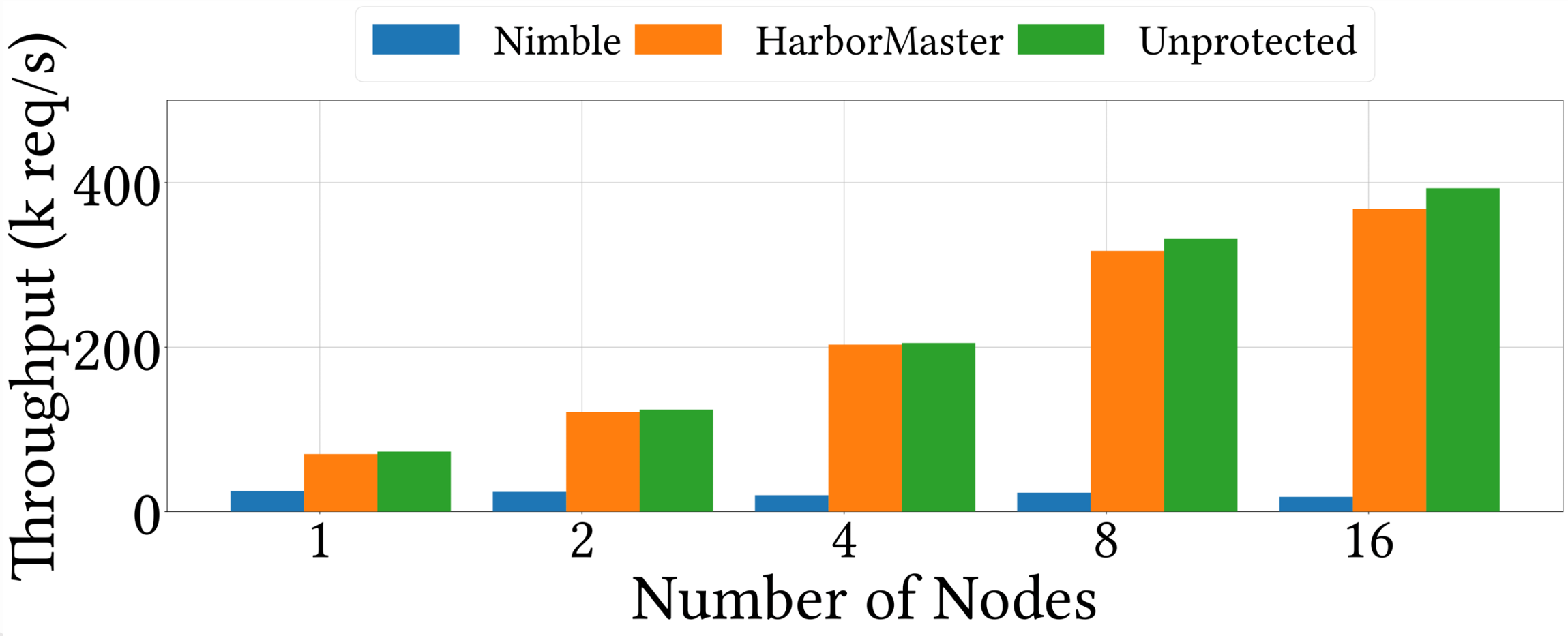
HarborMaster-core

- Also includes an eventually consistent distributed KV store.
- New applications can abstract away the details of causal logging.

Evaluation


HarborMaster
Nimble
Unprotected
Latency (ms)
0
1
2
3
4
0
25
50
75
100
125
150
175
Throughput (k req/s)

Evaluation


Nimble
HarborMaster
Unprotected
Throughput (k req/s)
400
200
0
1
2
4
8
16
Number of Nodes

Thank you!

Rollback Attack ⇒ Violation of Causality

<shubham_mishra@berkeley.edu>

Find me during poster session tomorrow!