共用数据导向的分布式系统失效注入

高钰, 王栋, 戴千旺, 窦文生, 魏峻
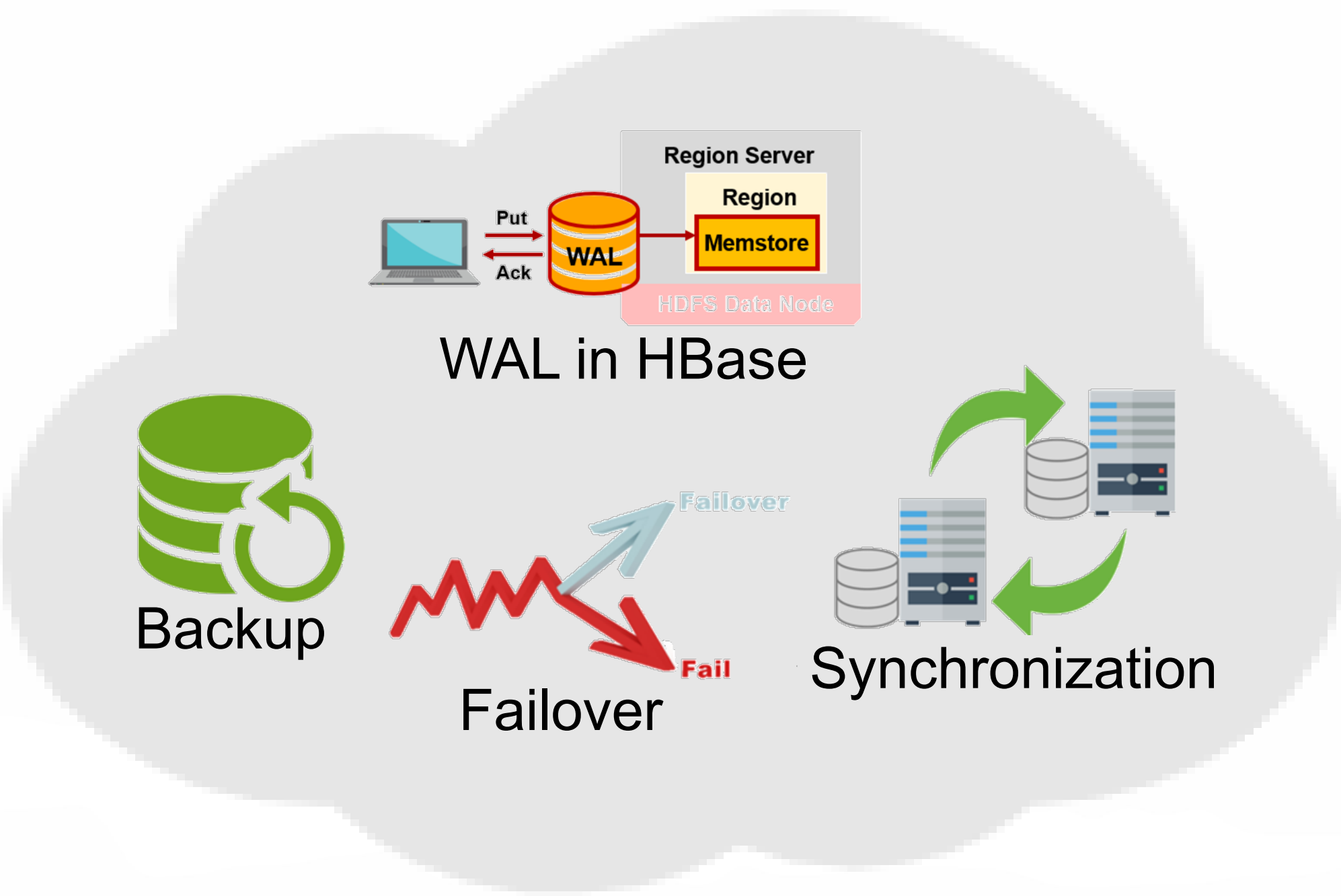
Common Data Guided Crash Injection for Cloud Systems

The 44th ACM/IEEE International Conference on Software Engineering (ICSE Demo'22)
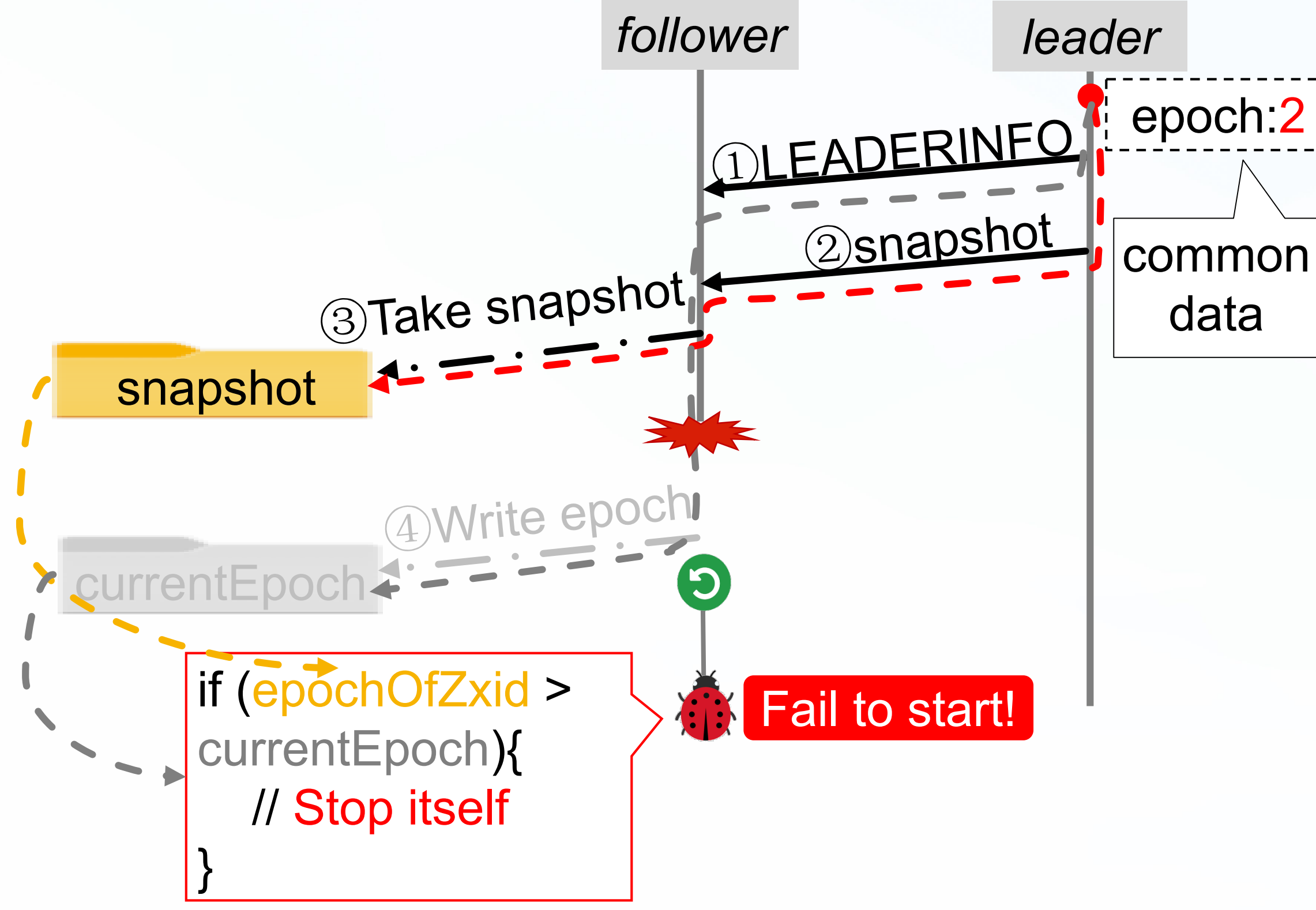
联系方式：高钰, 18810118727，gaoyu15@iscas.ac.cn

Crash Recovery

☐ Crash recovery protocols are designed to combat node crashes.

WAL in HBase

Backup — Failover — Synchronization

◆ Node crashes are inevitable.
◆ Recovery must be a first-class operation of cloud systems.

Crash Recovery Bugs

☐ Crash recovery code can be buggy.


```
if (epochOfZxid >
currentEpoch){
// Stop itself
}
```

Fail to start!
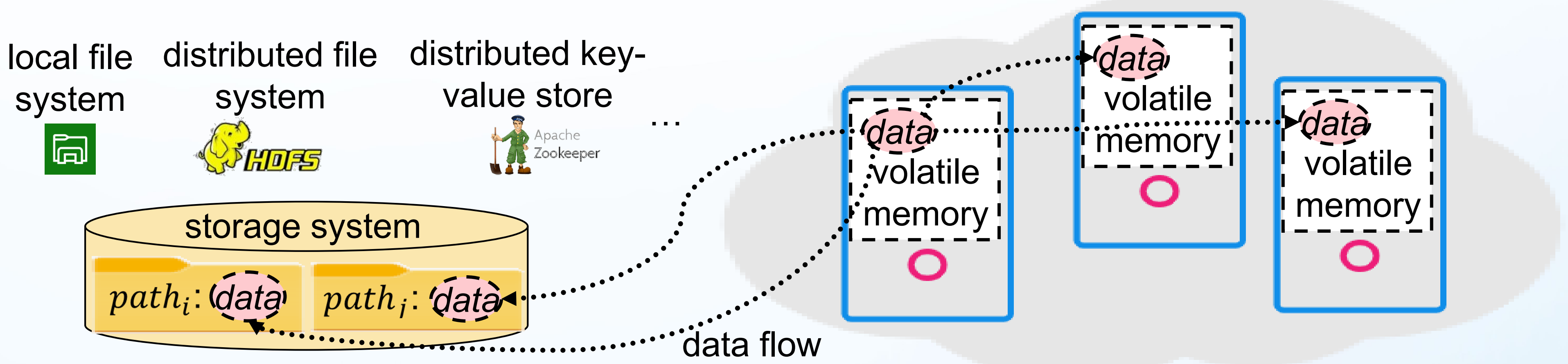
◆ In this real-world bug from ZooKeeper, operation ③ and ④ store common data *epoch* to two different files.
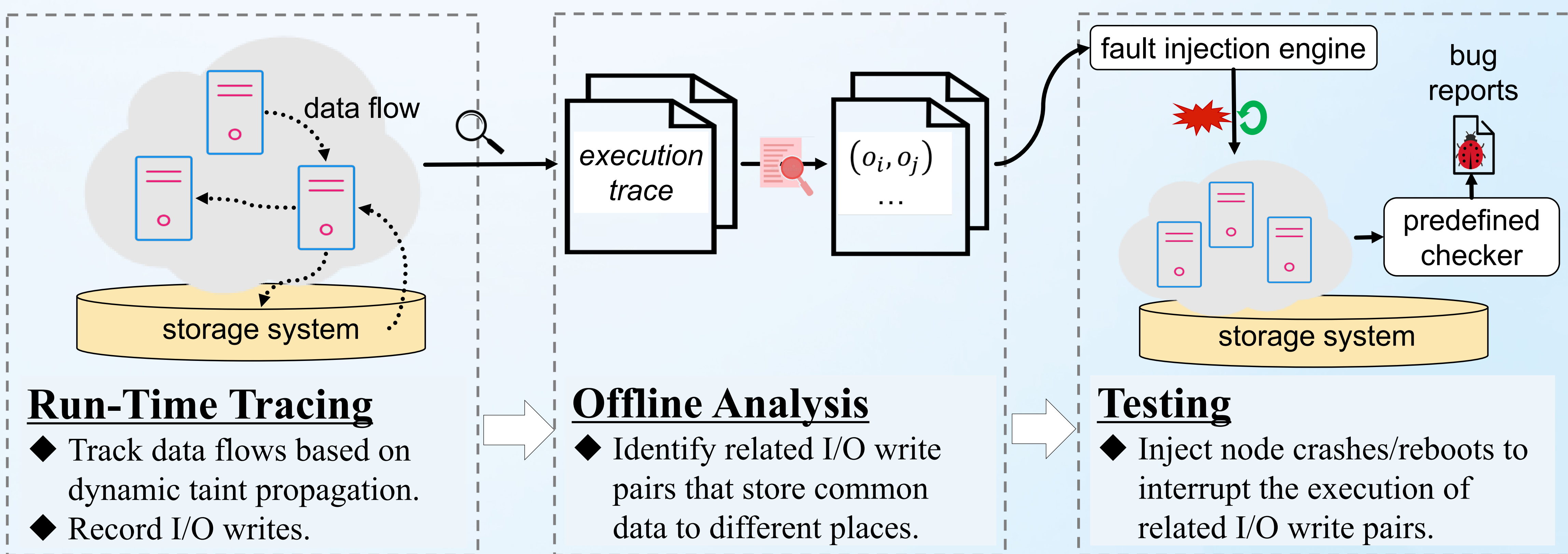
Key Observation

☐ A node can store common data to multiple places.
☐ Node crashes can leave a cloud system in inconsistent states, which are more likely to trigger crash recovery bugs.
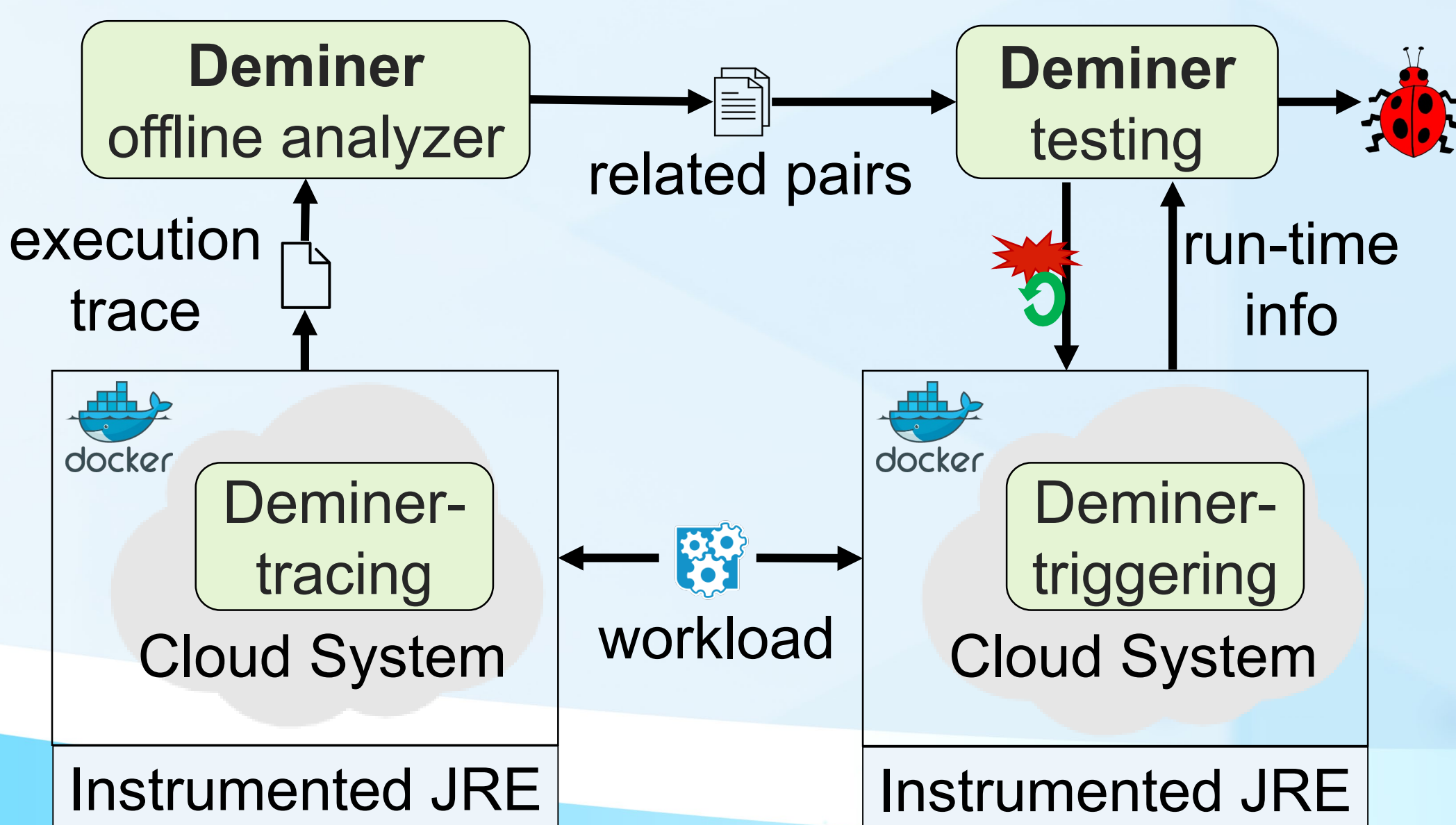

local file system — distributed file system HDFS — distributed key-value store Apache Zookeeper

storage system

$path_i$: $data$ $path_j$: $data$

data flow

$data$ volatile memory

Deminer

☐ Automatically expose crash recovery bugs in cloud systems guided by common data.

data flow → execution trace → (o_i, o_j) … → fault injection engine → bug reports → predefined checker

storage system

Run-Time Tracing
◆ Track data flows based on dynamic taint propagation.
◆ Record I/O writes.

Offline Analysis
◆ Identify related I/O write pairs that store common data to different places.

Testing
◆ Inject node crashes/reboots to interrupt the execution of related I/O write pairs.

Deminer Usage

☐ Deminer is implemented as an easy-to-use command line tool.

Deminer offline analyzer → related pairs → **Deminer** testing → 🐞

execution trace ↑ | run-time info ↓

Deminer-tracing Cloud System ←workload→ Deminer-triggering Cloud System

Instrumented JRE | Instrumented JRE

Deminer Evaluation

☐ Deminer has detected 6 crash recovery bugs on three popular cloud systems.

Apache Zookeeper v3.6.3

APACHE HBASE v2.4.8/v1.7.1

hadoop HDFS v3.3.1

Bug ID	Failure Symptom
hb26370	Misleading error message
hb26391	Data staleness
hb26420	Cluster out of service
zk4283	Node downtime
zk4416	Node downtime
hd16381	Operation failure