

Twins

BFT Systems Made Robust

Alberto Sonnino

Acknowledgements

Diem / Facebook Novi

Research

- Shehar Bano
- Alberto Sonnino
- Dahlia Malki

Engineering

- Andrey Chursin
- Dmitri Perelman
- Zekun Li
- Avery Ching

A set of nodes



Byzantine Fault Tolerance



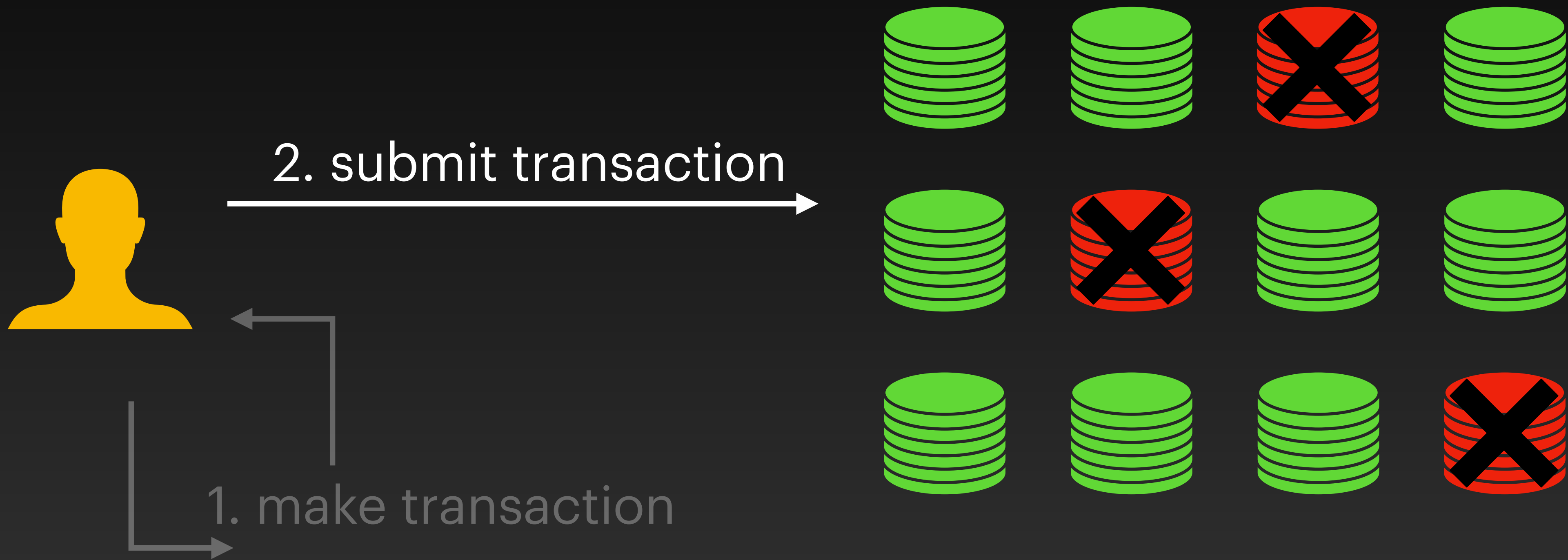
Blockchains



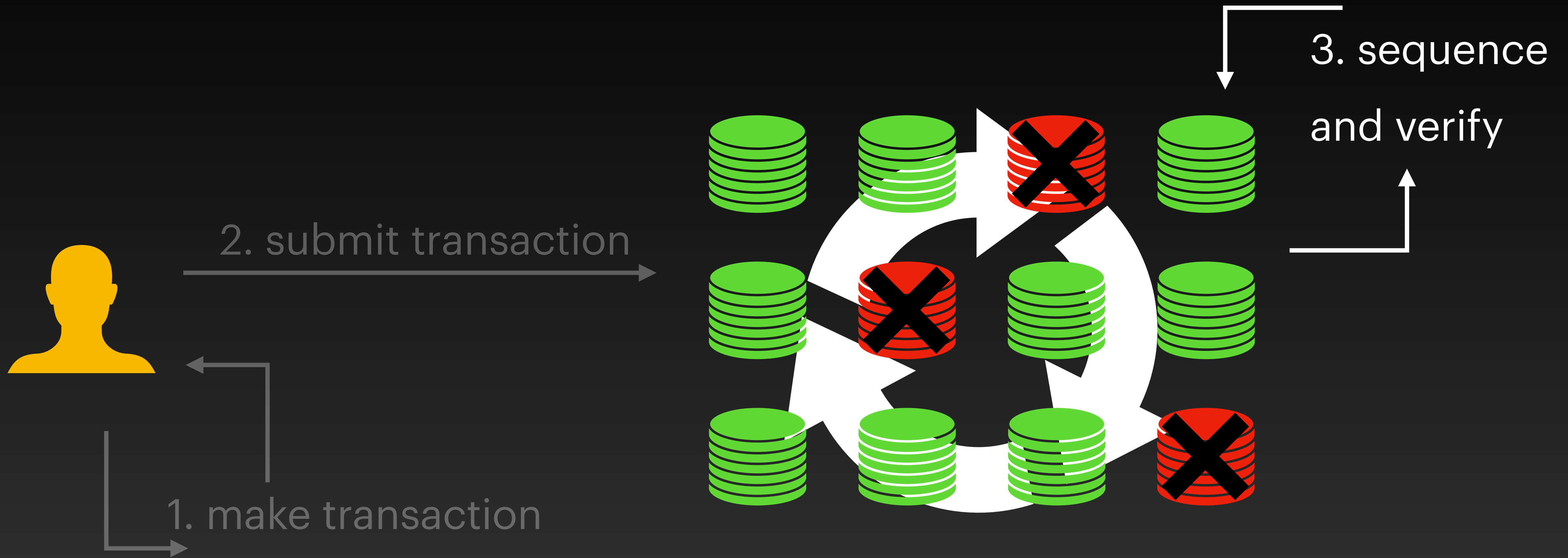
1. make transaction



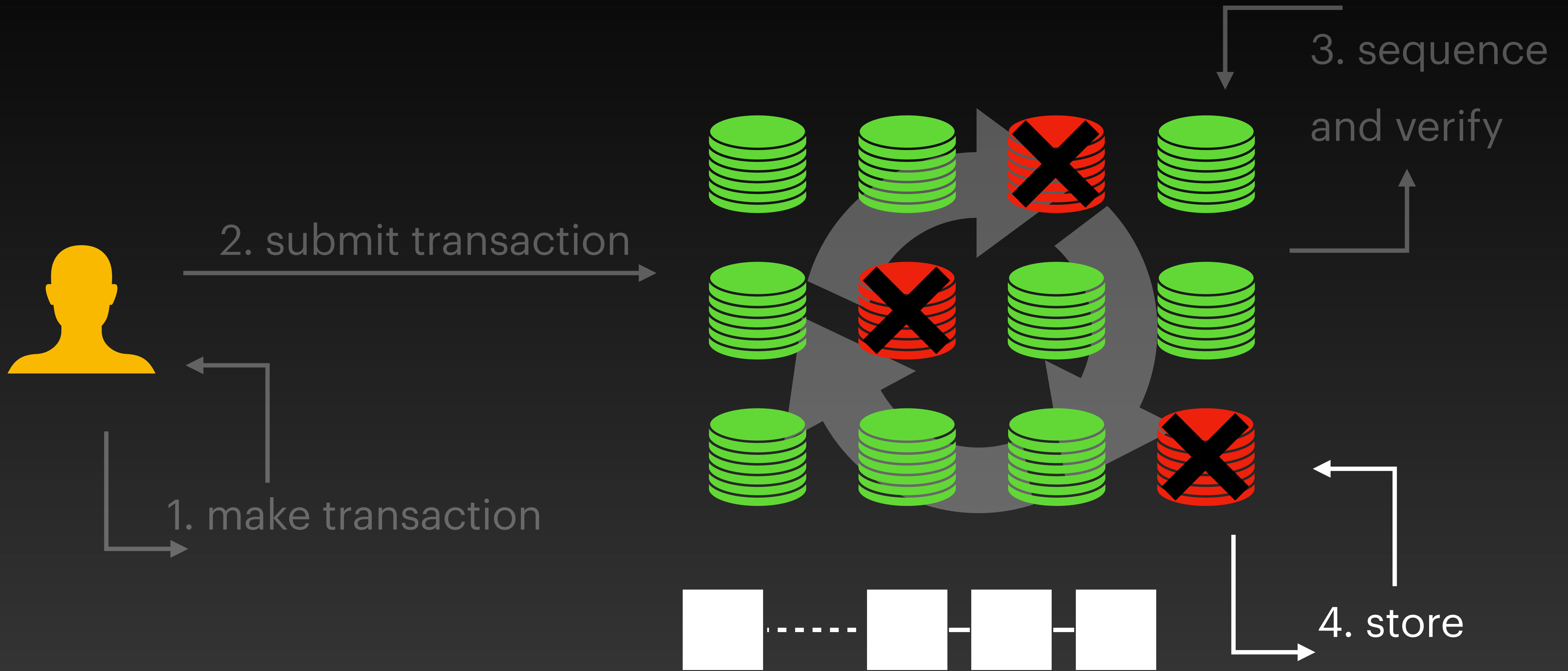
Blockchains



Blockchains



Blockchains



DiemBFT

A Production BFT System

- 10,000 Git commits
- 200 contributors
- Years of development

Byzantine Adversaries

How to write integration/unit tests?



Twins is not formal verification

It is a pragmatic (black box) approach

Twins

Multiple copies of the same node



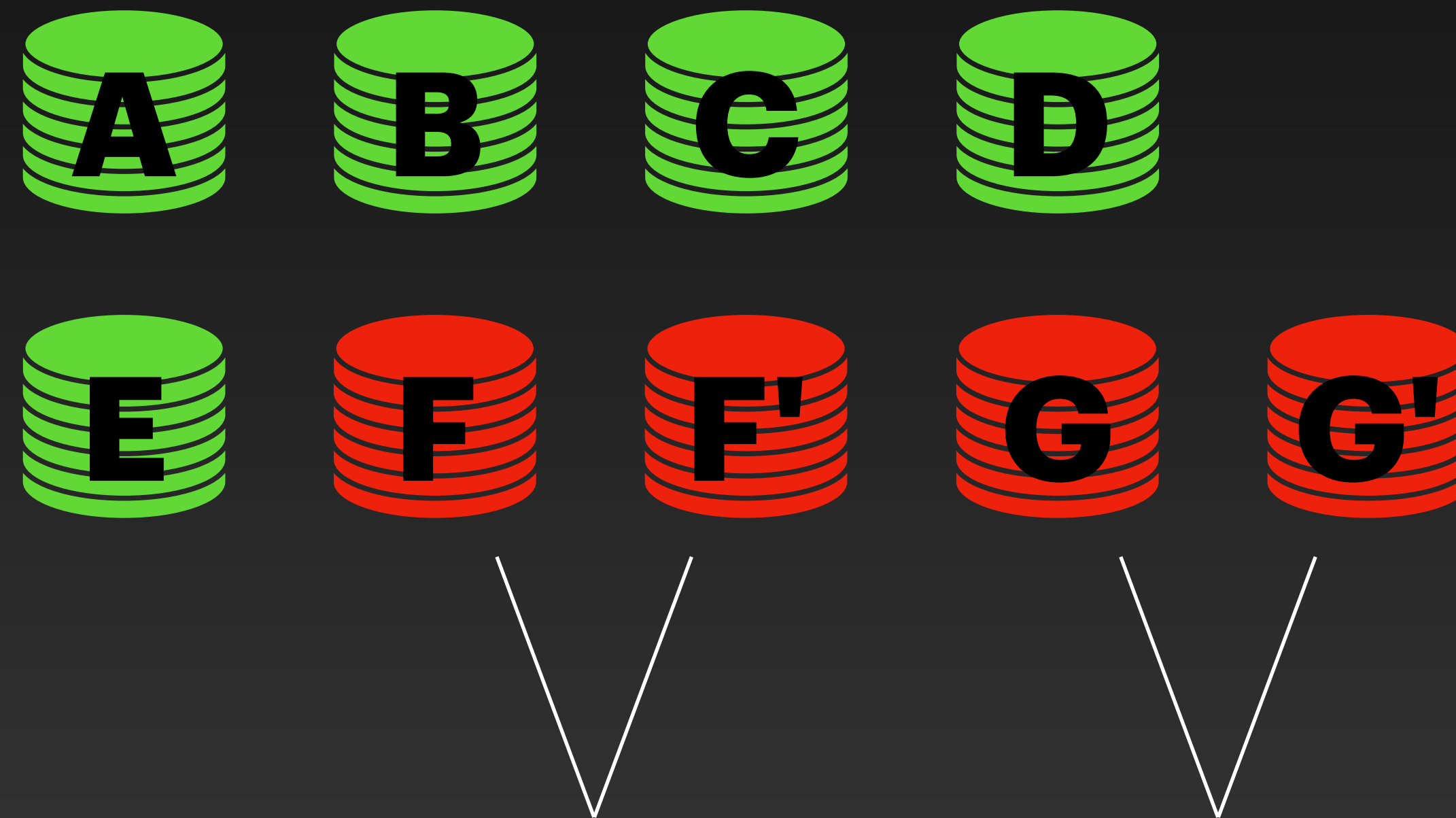
Twins

Multiple copies of the same node



Twins

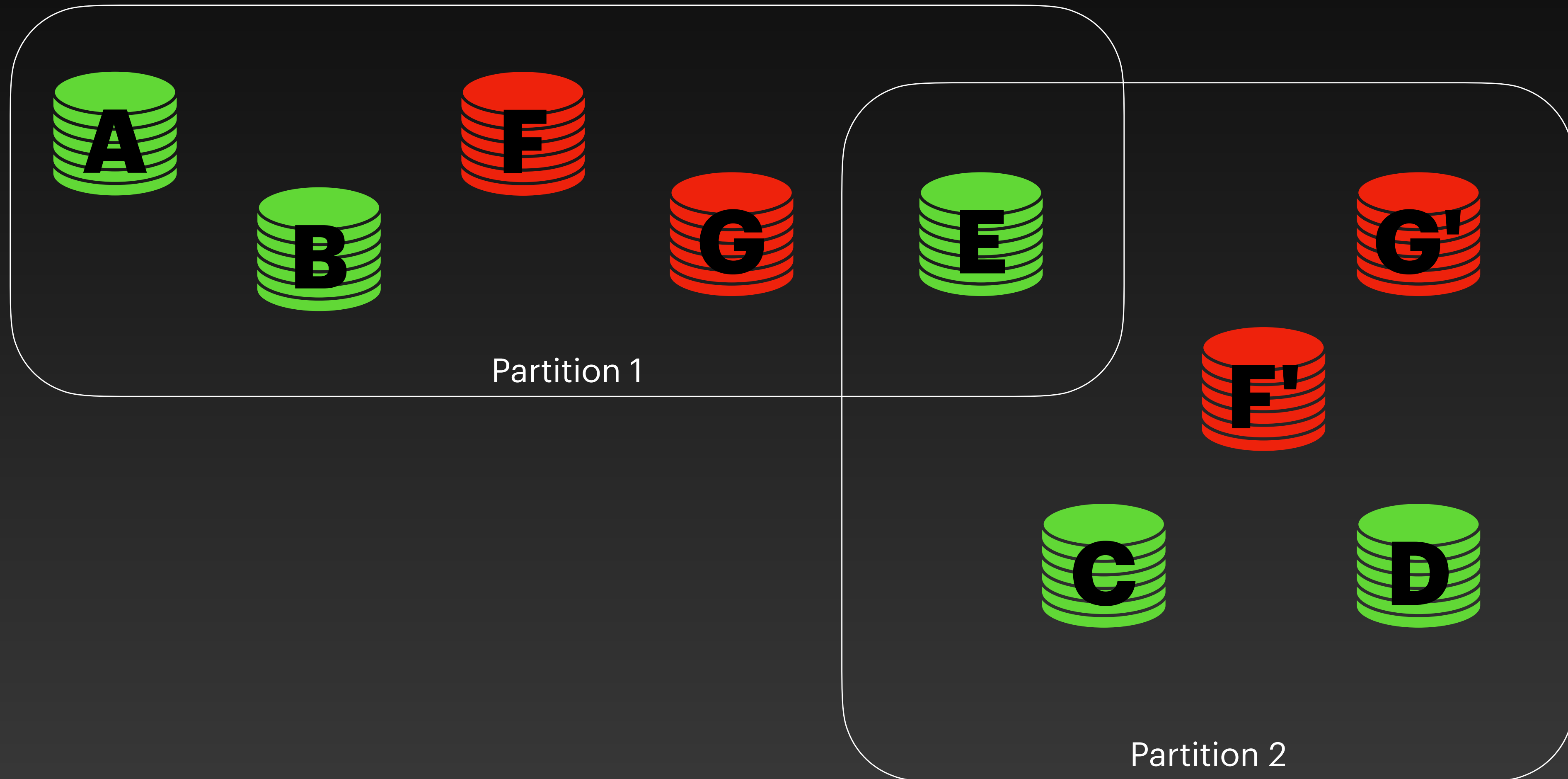
Multiple copies of the same node



Twins have the same cryptographic keys
When leader, they propose a different (random) payload

Twins

Network Partitions (on a round base)



Why does Twins Help?

It captures notable misbehaviors

Equivocations

Eg. Equivocating proposals

Amnesia

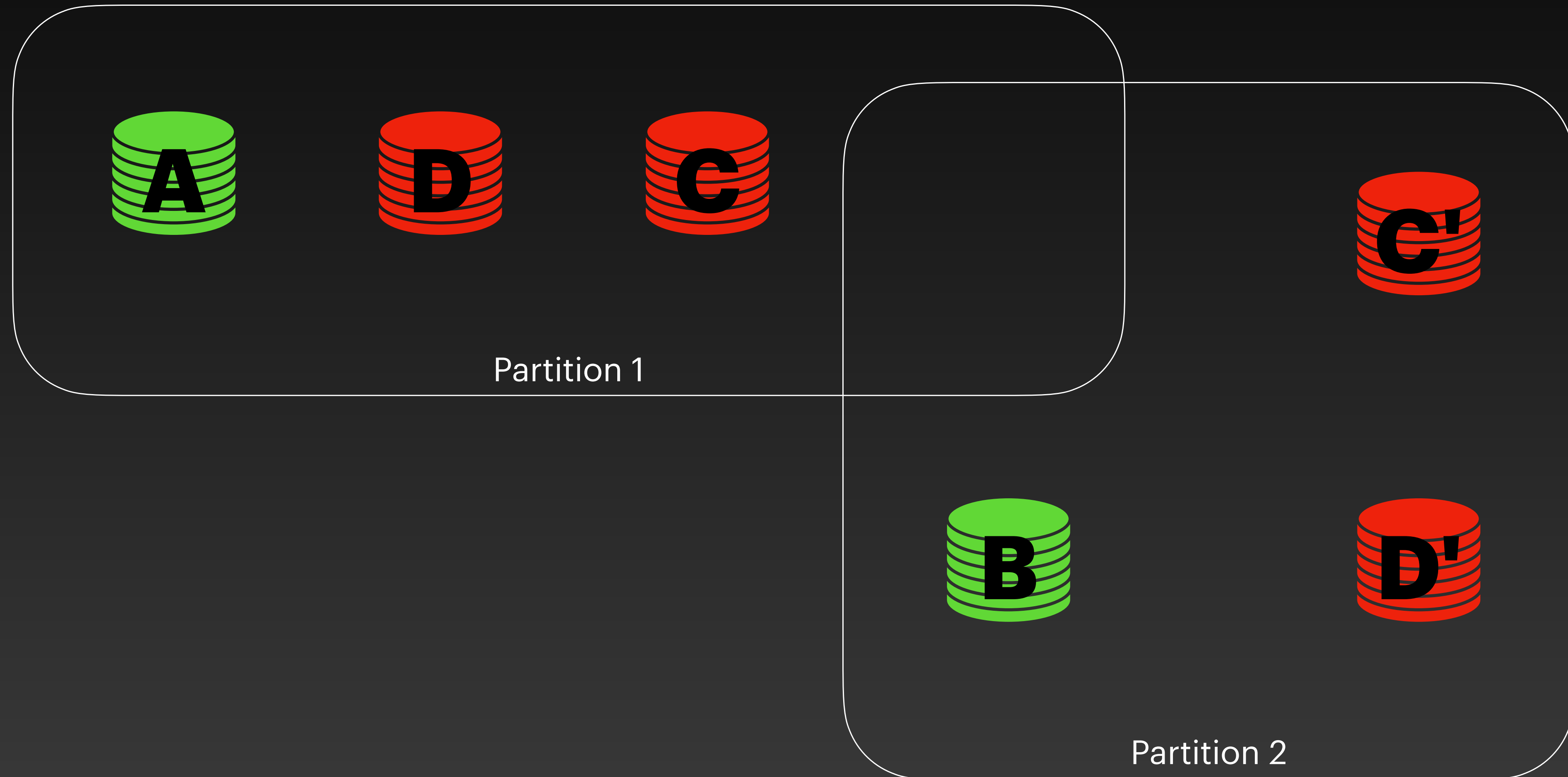
Eg. Forgetting that we already voted in this round

Losing internal state

Eg. Loose 'locks' guarding voted values

Baseline Case

When $F+1$ nodes are Byzantine



Known Attacks

Expressed at Twins scenarios

- Safety Attack on Zyzyva (Abraham et al)
- Liveness Attack on FAB (Abraham et al)
- Timing Attack on Sync HotStuff (Momose et Al)
- Non-Responsiveness Attack on Linear Leader-Replacement (Yin et Al)

Known Attacks

Expressed at Twins scenarios

- Safety Attack on Zyzyva (Abraham et al)
- Liveness Attack on FAB (Abraham et al)
- Timing Attack on Sync HotStuff (Momose et Al)
- Non-Responsiveness Attack on Linear Leader-Replacement (Yin et Al)

**Found within minutes, with 4-7 nodes
committees**

New Attacks

Expressed at Twins scenarios

- Safety Attack on Fast HotStuff (Jalalzai et al)

New Attacks

Expressed at Twins scenarios

- Safety Attack on Fast HotStuff

Found in 11 rounds, with 4 nodes committee

Implementation

The scenario Generator

1. Produce all possible partitions of nodes
2. Assign each partition to all possible leaders
3. Find all ways in which leader-partition pairs can be arranged in R rounds
4. Filter "trivial" scenarios

Implementation

The scenario Executor



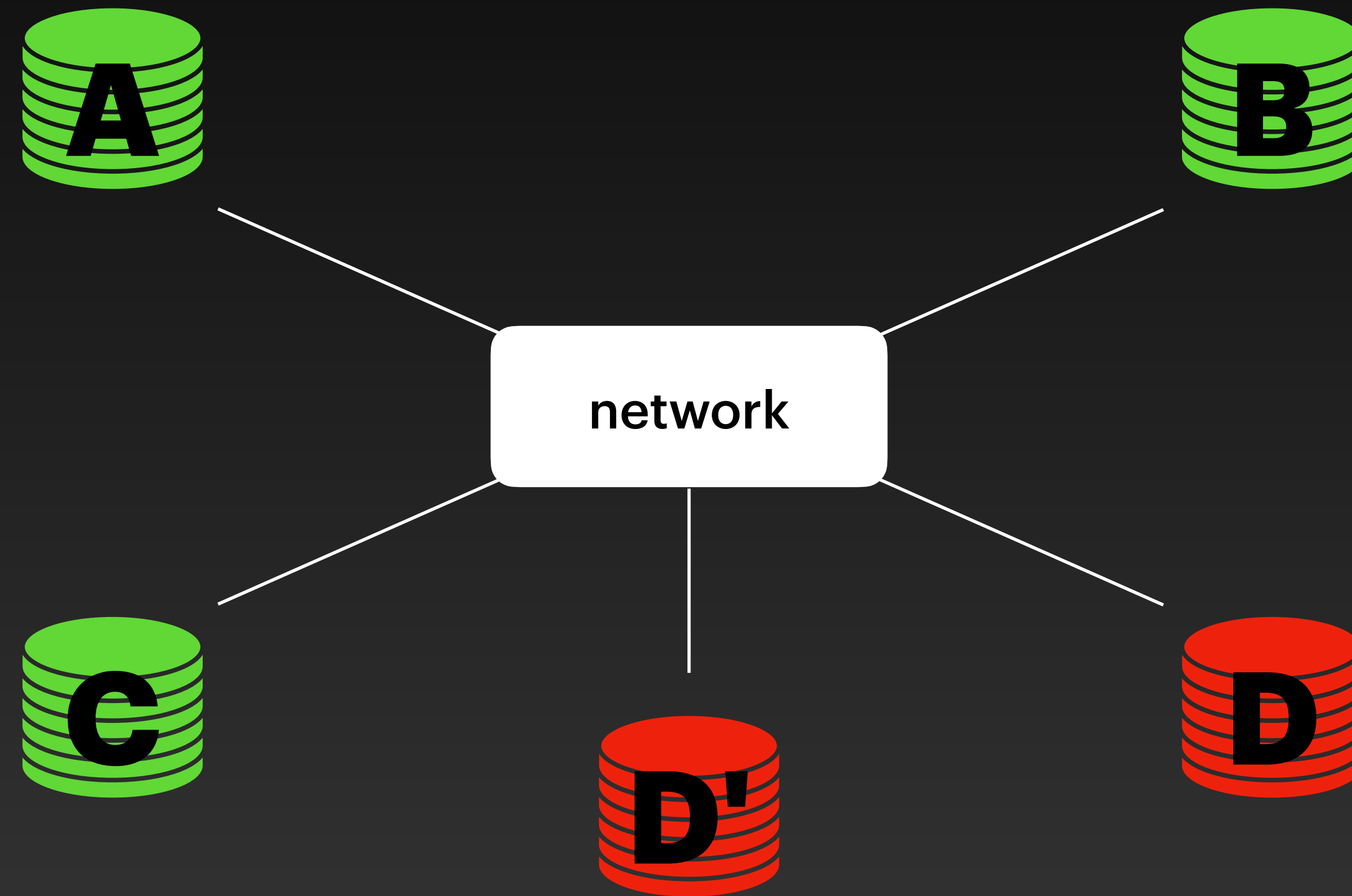
Implementation

The scenario Executor



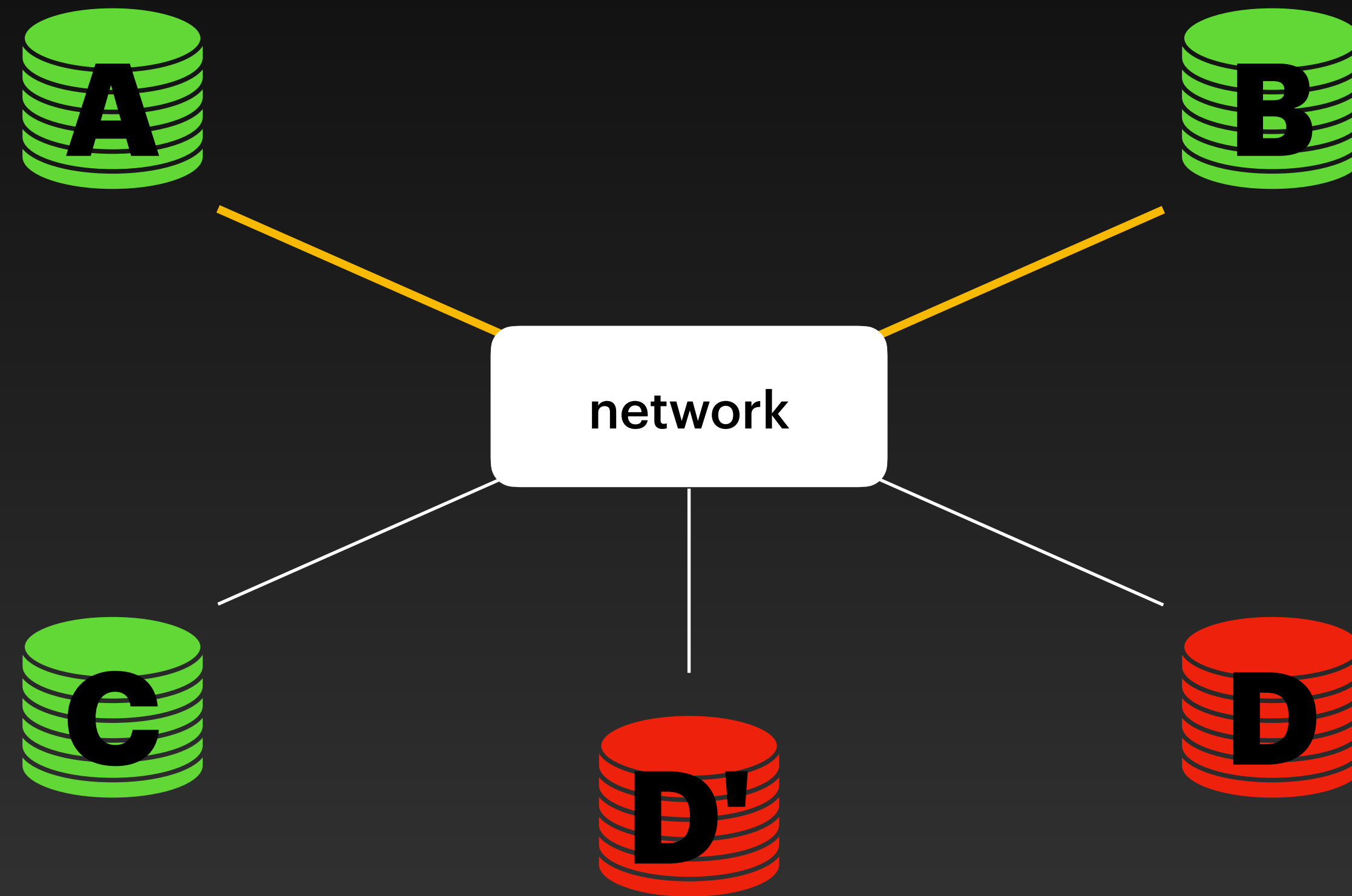
Implementation

The scenario Executor



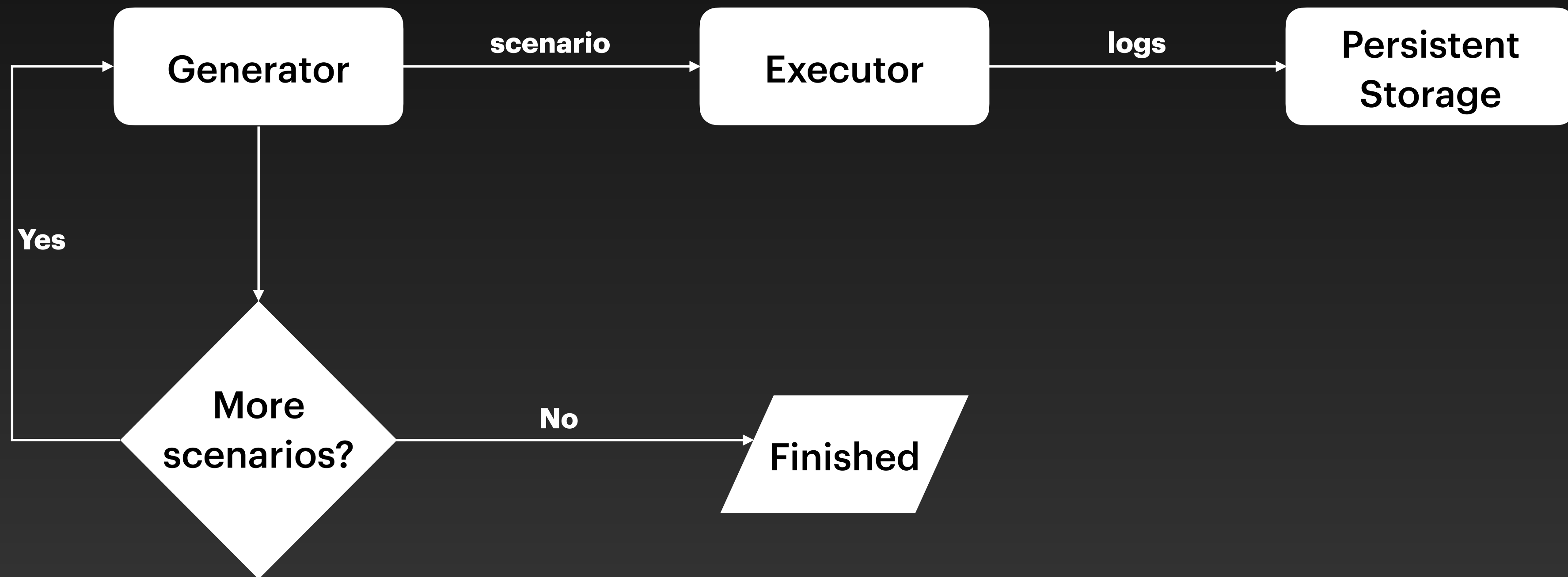
Implementation

The scenario Executor



Implementation

Putting Everything together



Twins runs in production within DiemBFT

What is Missing?

Future Works

- Coverage?
- Deterministic scenarios?
- Guarantees?

Conclusion

Twins

- A pragmatic approach to BFT testing, the first of its kind
- Needs a community effort
 - **Paper:** <https://arxiv.org/abs/2004.10617>
 - **Code:** <https://github.com/diem/diem>