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

> 2 / 3
Blockchains

1. make transaction
Blockchains

1. make transaction

2. submit transaction
Blockchains

1. make transaction
2. submit transaction
3. sequence and verify
Blockchains

1. make transaction
2. submit transaction
3. sequence and verify
4. store
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)

Partition 1
A B F G E

Partition 2
F' C D G'
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

Partition 1
A  D  C

Partition 2
B  D'  C'
Known Attacks
Expressed at Twins scenarios

- Safety Attack on Zyzzyva (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 Zyzzyva (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
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

A
B
C
D
Implementation
The scenario Executor
Implementation
The scenario Executor

A
B
C
D

network

D'
Implementation
The scenario Executor

![Diagram showing network with nodes A, B, C, D, and D']
Implementation
Putting Everything together

Generator

Executor

Persistent Storage

scenario

logs

More scenarios?

Yes

No

Finished
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

- **Code:** https://github.com/diem/diem