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
Byzantine Fault Tolerance

> \( \frac{2}{3} \)
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

A B C D
E F F' F' G G'
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
Conclusion

Twins

• A pragmatic approach to BFT testing, the first of its kind
• Needs a community effort

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