Dissecting the Performance of Chained-BFT

Fangyu Gai, Ali Farahbakhsh, Jianyu Niu, Chen Feng, Ivan Beschastnikh

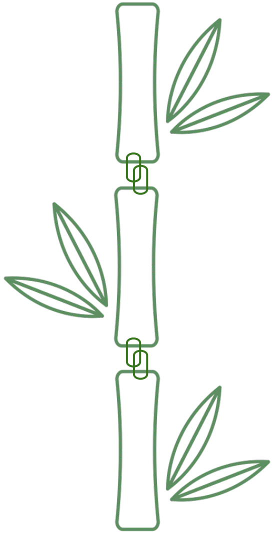
THE UNIVERSITY OF BRITISH COLUMBIA

Blockchain @UBC

Hao Duan

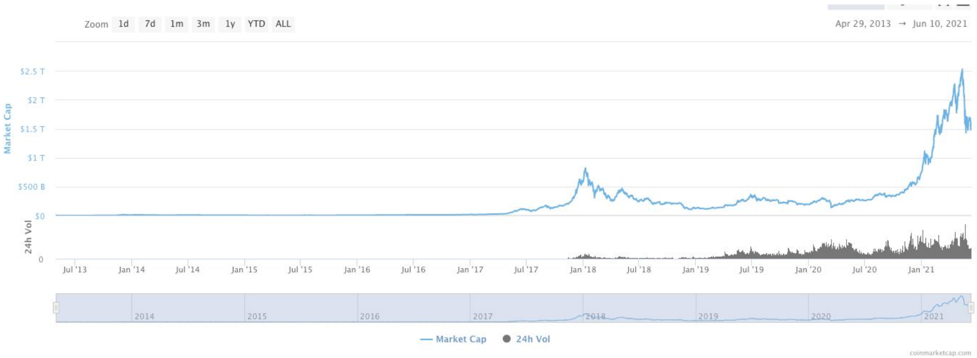
趣链科技 HYPERCHAIN

https://github.com/gitferry/bamboo



Why do we care about BFT SMR?

- Cryptocurrency hype
- Enterprise blockchain is a trend
  - Financial services
  - Health care
  - Data provenance
  - Blockchain-as-a-service



J.P.Morgan

diem

Tendermint

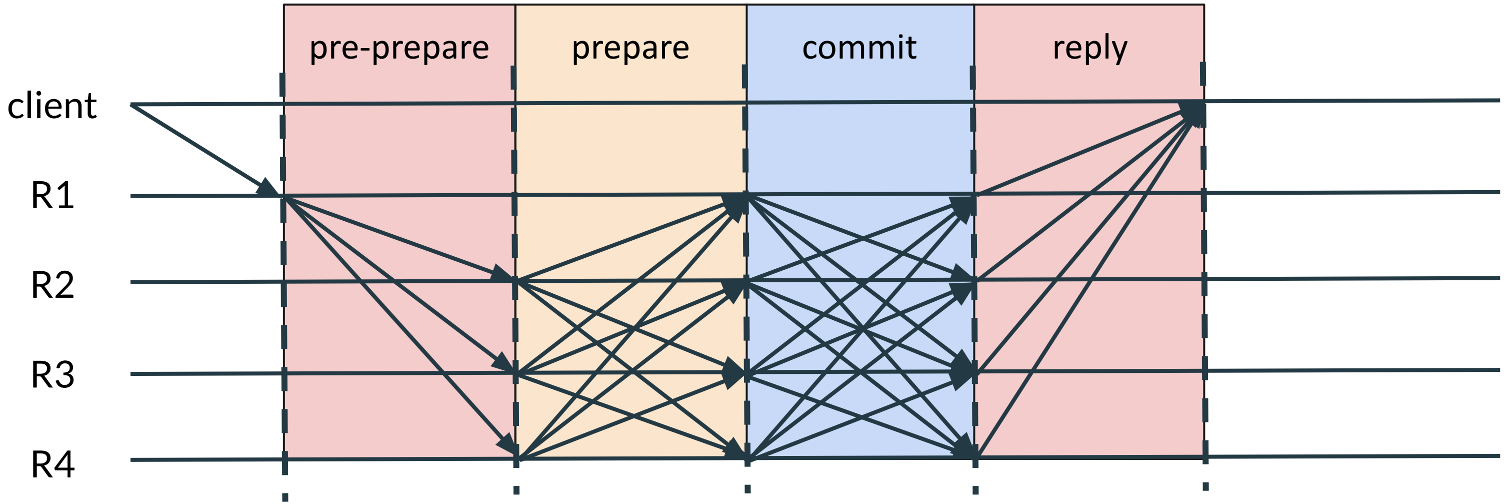
趣链科技 HYPERCHAIN

Microsoft

HYPERLEDGER

ANT GROUP | ANTCHAIN

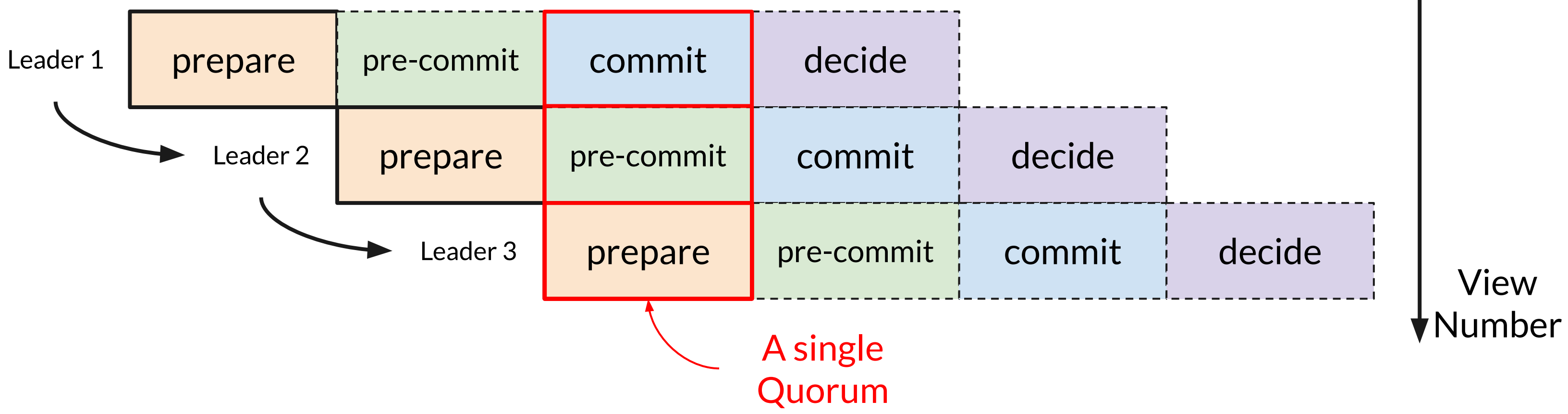
Evolution of BFT SMR: PBFT



*Miguel Castro, Barbara Liskov, **Practical Byzantine Fault Tolerance**, OSDI 1999*

Evolution of BFT SMR: Chained-BFT

HotStuff



Leader 1	prepare	pre-commit	commit	decide		
Leader 2		prepare	pre-commit	commit	decide	
Leader 3			prepare	pre-commit	commit	decide

A single Quorum

View Number

Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan-Gueta, Ittai Abraham,
***HotStuff: BFT Consensus with Linearity and Responsiveness**, PODC 2019*

BFT in the Era of Blockchain: Chained-BFT

Characterization

- Chained structure
- Propose-vote scheme
- A set of safety rules

Chained-BFT family

- HotStuff[1]
- Two-chain HotStuff[1]
- Streamlet[2]
- Casper[3]
- Fast HotStuff[4]
- Strengthened FT[5]
- ……

diem

flow

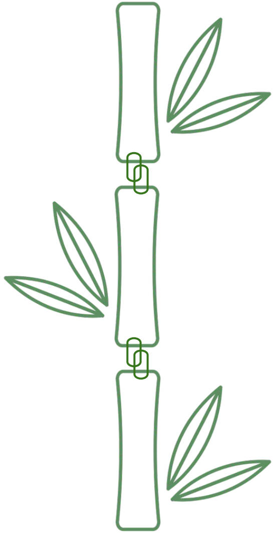
ethereum 2.0

[1] *Maofan Yin et.al. PODC'19*
[2] *Elaine Shi et.al. https://eprint.iacr.org/2020/088.pdf*
[3] *Vitalik Buterin et.al. https://arxiv.org/pdf/1710.09437.pdf*
[4] *Mohammad M. Jalalzai et.al. https://arxiv.org/abs/2010.11454*
[5] *Zhuolun Xiang et.al. https://arxiv.org/abs/2101.03715*

How do cBFT protocols vary in performance?

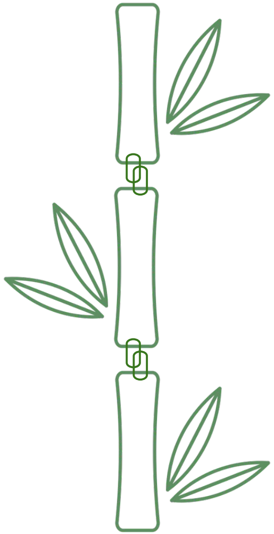
Our approach

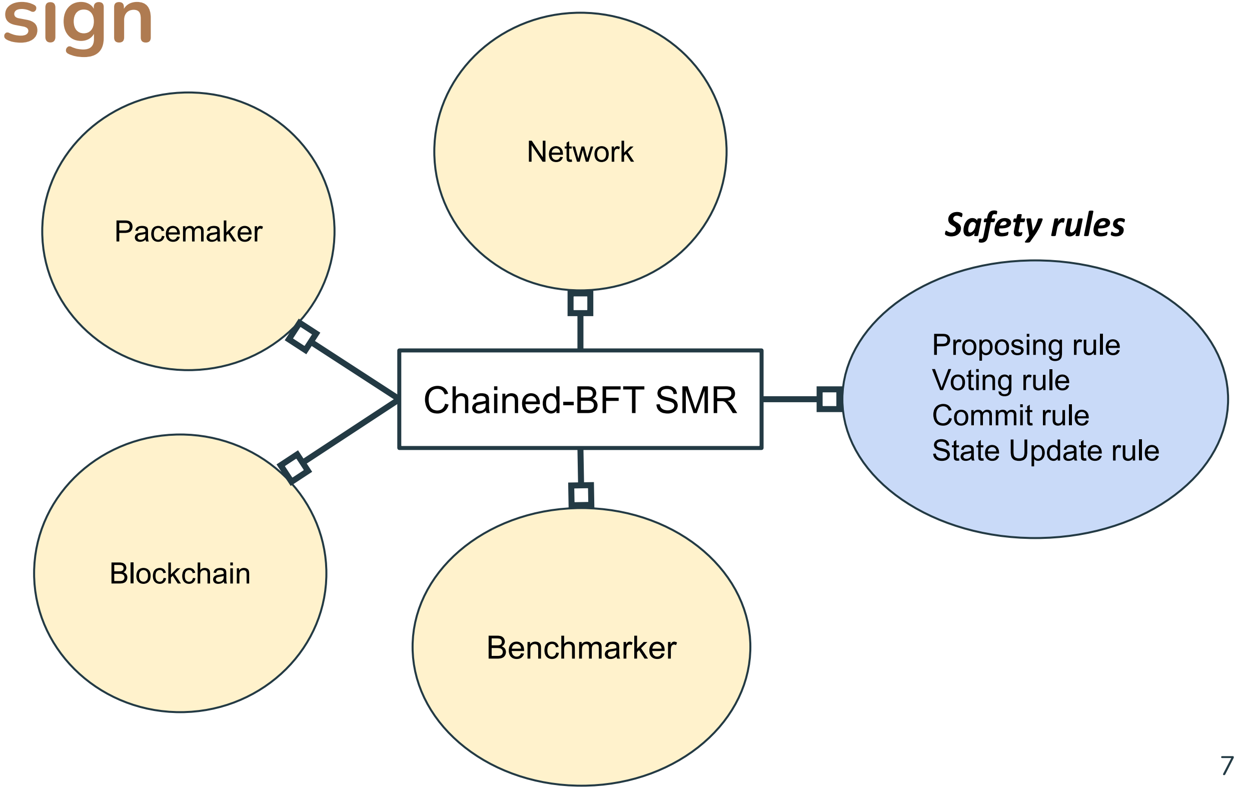
- Abstract the key differences
- Implement common components
- Modeling using the queuing theory



Bamboo is a prototype and benchmark framework

Bamboo Design





Pacemaker

Network

Chained-BFT SMR

Blockchain

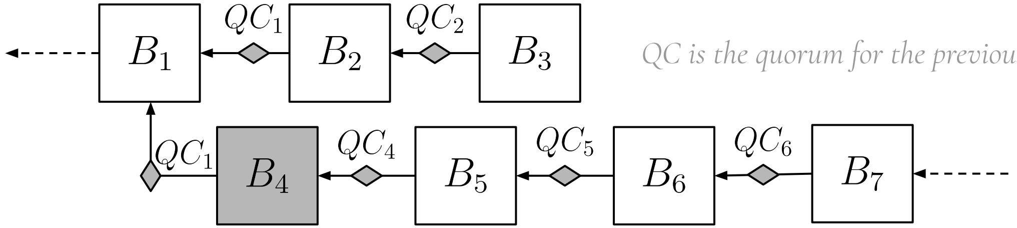
Benchmarker

Safety rules

Proposing rule
Voting rule
Commit rule
State Update rule

CBFT is subject to performance attack*

- *Forking attack* aims to overwrite blocks
- *Silence attack* aims to break the commit rule
- liveness and safety are not violated
- Impact varies on different cBFT protocols



QC is the quorum for the previous block

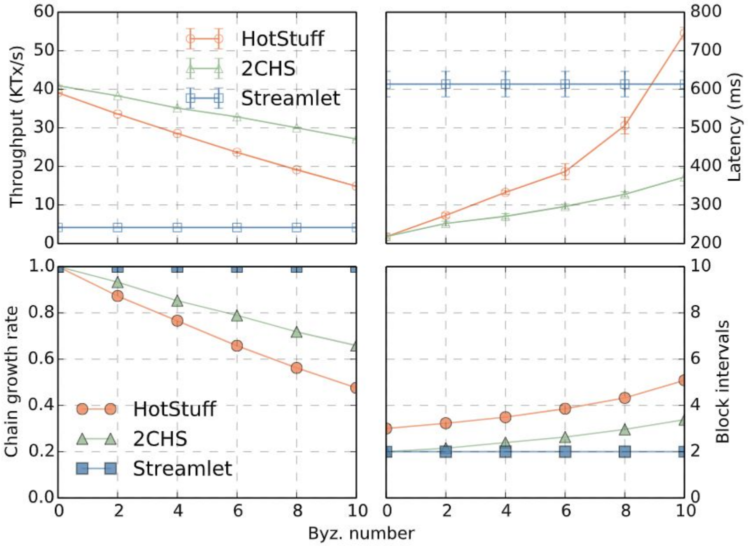
Example of forking attack on chained-HotStuff

We first studied this type of attack in our previous work: **On the Performance of Pipelined HotStuff, INFOCOM 2021*

Bamboo collects many metrics

- **Throughput (tx/s)**
- **Latency (ms)**
- **Chain growth rate**
    - #(main chain)/#(total views)
- **Block intervals**
    - sum(#(view cost by block i))/#(main chain)

Evaluation Results



Protocols under forking attack with 32 fixed nodes

We implemented HotStuff, Two-chain HotStuff, and Streamlet using Bamboo

Insights

- Although Streamlet has the worst performance, it is more tolerate to forking
- HotStuff is more sensitive to forking

Plz see paper for more juicy results :-)

Contribution summary

- Bamboo prototype and benchmarking framework at 4,600 LoC using Golang
- Three prototype implementations using Bamboo, each less than 300 LoC
- Comprehensive evaluations and insightful results
- Performance modeling, validation, and dissection

https://github.com/gitferry/bamboo