Dissecting the Performance of Byzantine Agreement in Blockchain Era

Fangyu Gai, Ph.D. candidate

Blockchain @UBC

THE UNIVERSITY OF BRITISH COLUMBIA

fangyu.gai@ubc.ca

Oct. 2021

Dissecting the Performance of Chained-BFT

Fangyu Gai*, Ali Farahbakhsh*, Jianyu Niu*, Chen Feng*, Ivan Beschastnikh†, Hao Duan‡
University of British Columbia (*Okanagan Campus, †Vancouver Campus), Canada,
Email: *{fangyu.gai, mralifar, jianyu.niu, chen.feng}@ubc.ca, †bestchai@cs.ubc.ca
‡Hangzhou Qulian Technology Co., Ltd., China, Email: duan.hao@hyperchain.cn

BFT in the Era of Blockchain: Chained-BFT

Characterization

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

Chained-BFT family

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

diem

flow

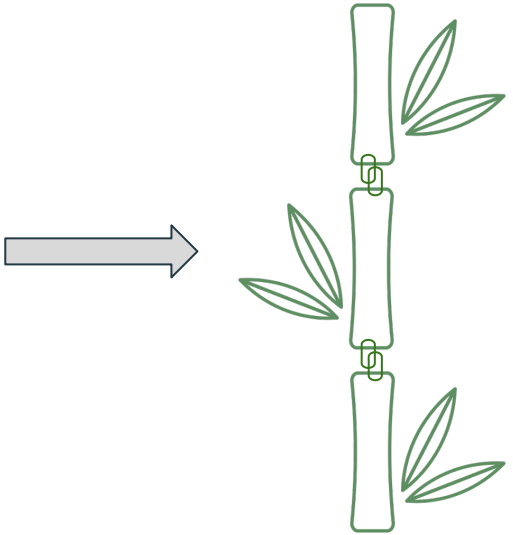
ethereum 2.0

[1]. Maofan Yin et.al. PODC'19
[2]. Elaine Shi et.al. AFT'20
[3]. Zhuolun Xiang et.al. ICDCS'21
[4]. Vitalik Buterin et.al. https://arxiv.org/pdf/1710.09437.pdf
[5]. Mohammad M. Jalalzai et.al. https://arxiv.org/abs/2010.11454

How do CBFT protocols vary in performance?

Our approach

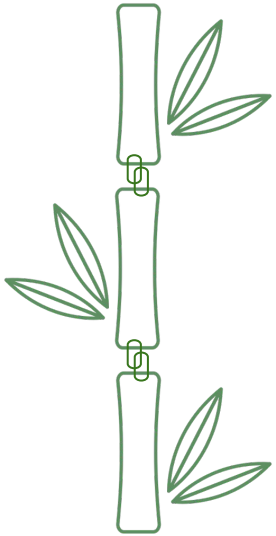
- Abstract the key differences
- Implement common components
- Modeling using the queuing theory

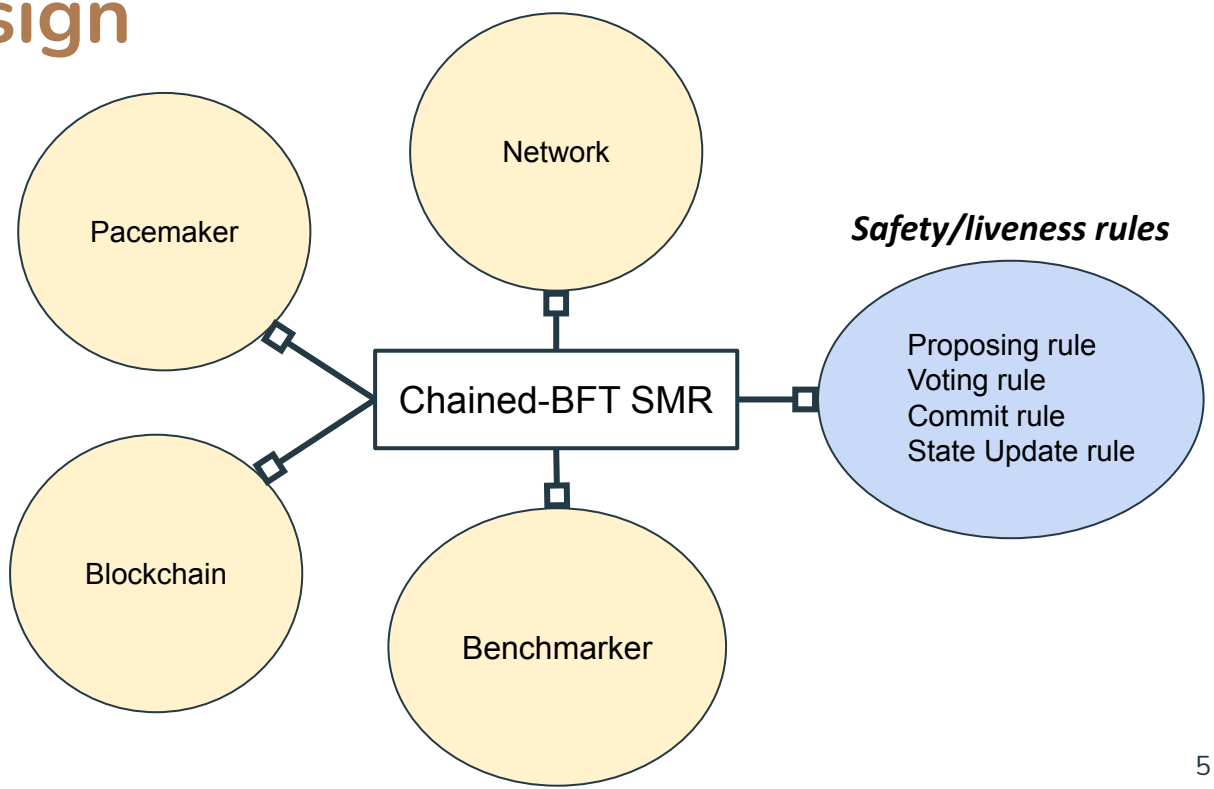


Bamboo is a prototype and benchmark framework

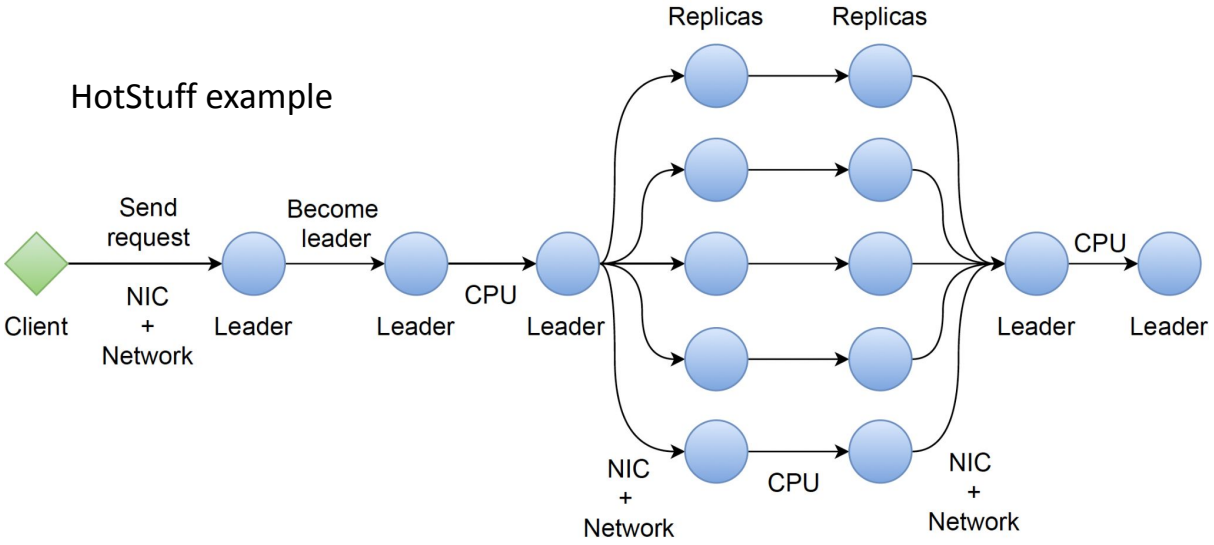
https://github.com/gitferry/bamboo

Bamboo Design





Modeling CBFT using queuing theory



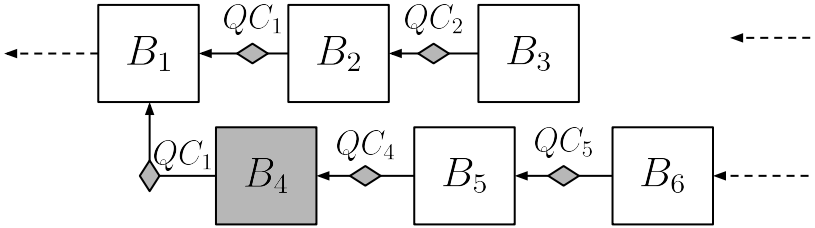
- t_L: round-trip time
- t_S: service time
- t_{Commit}: commit time
- w_Q: waiting time

$$Latency = t_L + t_s + t_{Commit} + w_Q$$

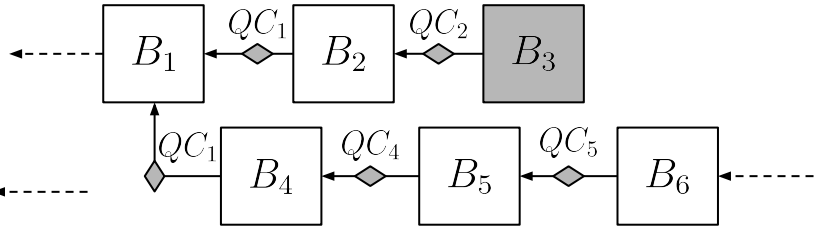
$$Throughput_{peak} = 1/t_s$$

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



Forking attack on chained-HotStuff



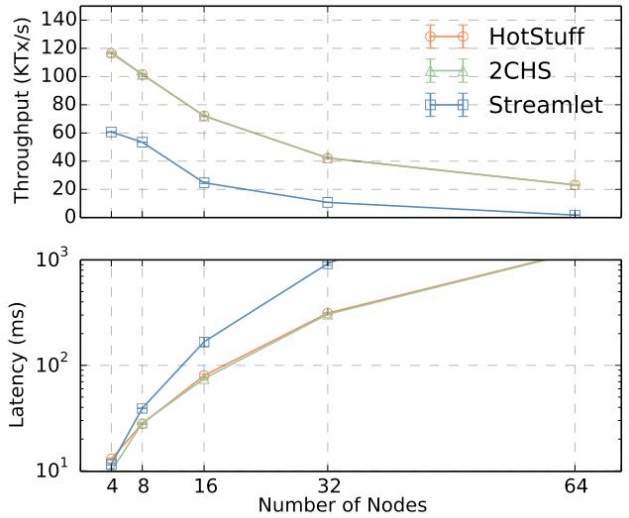
Silence attack on chained-HotStuff

*Jiangyu Niu, Fangyu Gai et al. ***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

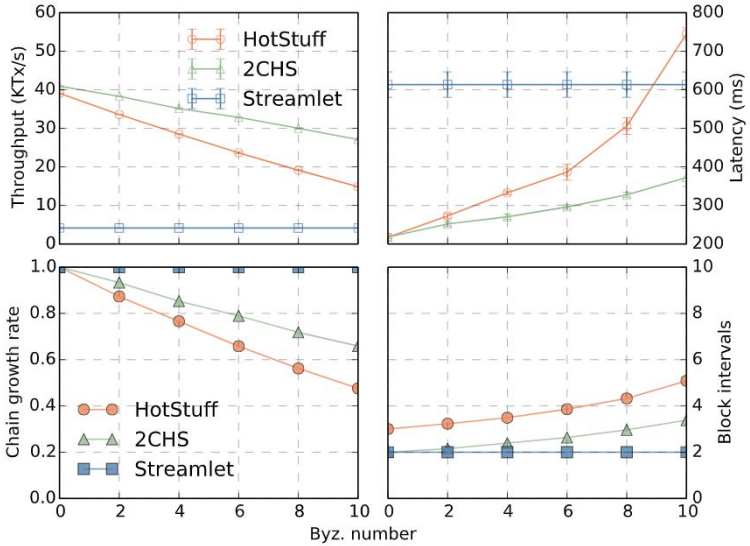


Scalability test

We implemented HotStuff, Two-chain HotStuff, and Streamlet using Bamboo, which provides fair comparisons.

- Performance drops as more nodes join the network
- HotStuff and 2CHS have very close performance in LAN
- Streamlet performs the worst

Evaluation Results



Protocols under forking attack with 32 fixed nodes

- Streamlet has the best resilience to forking
- 2CHS has better resilience to forking than HotStuff
- Rapid growth in HotStuff's latency

For more juicy results please see the paper.

Limits && Future Work

- Queuing model and evaluation in WAN
- More design choices, e.g., picking the highest QC other than the latest one
- More protocol implementations and comparisons, e.g., leaderless protocols

Summary

Contact me at: fangyu.gai@ubc.ca !

- Bamboo prototype and benchmarking framework at 4,600 LoC using Golang
  - **https://github.com/gitferry/bamboo**
  - *Dissecting the Performance of Chained-BFT, ICDCS'21*
- Three prototype implementations and evaluations
- Performance modeling, validation, and dissection