
上海交通大學
Shanghai Jiao Tong University

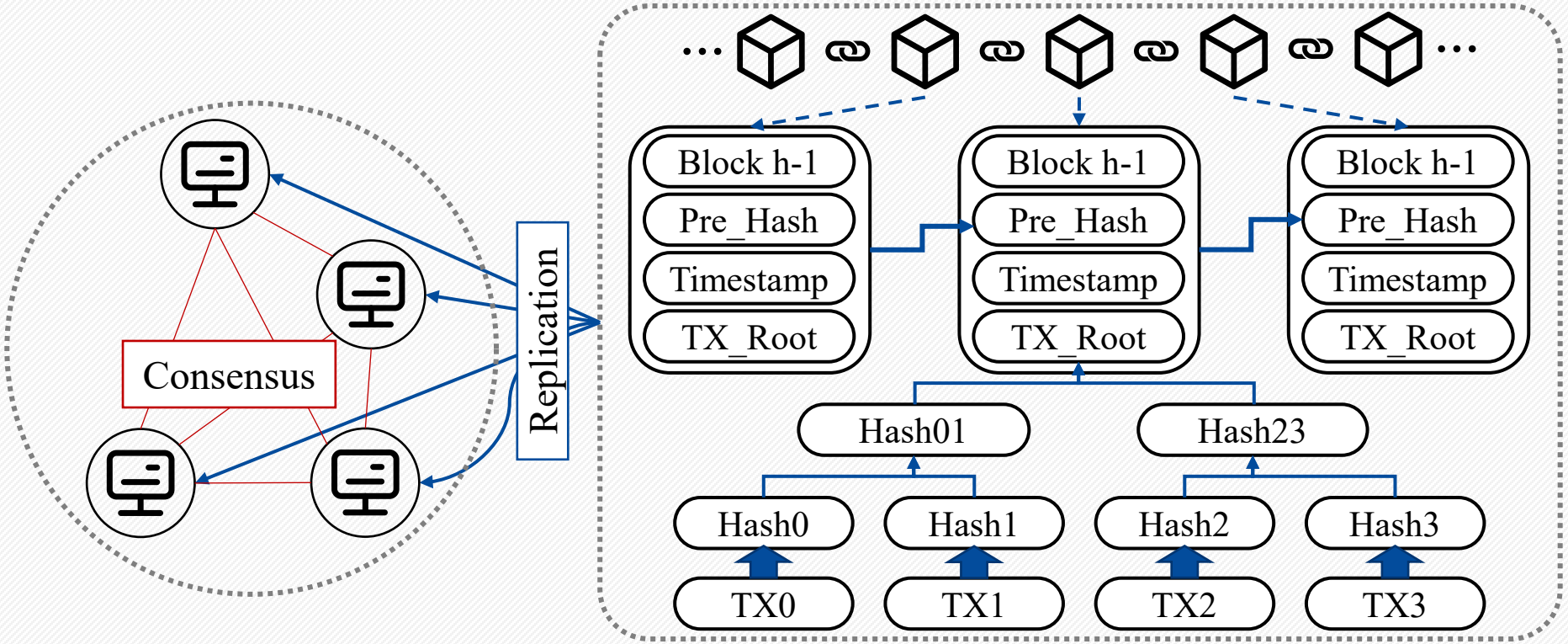
# DCS Chain: A Flexible Private Blockchain System

Jianwu Zheng, Siyuan Zhao, Zheng Wang, Li Pan, Jianhua Li

# OUTLINE

# Introduction Blockchain

- Provide decentralized, immutable, transparent solutions for various fields.
- A pivotal force for social and economic progress.
- Public vs. Private Blockchain


Blockchain system overview

# Introduction

## DCS trilemma

Supposes that it is impossible for a distributed system to simultaneously achieve the three essential properties:

- Decentralization
- Consistency
- Scalability

**Bitcoin**

- ↑ Decentralization
- ↑ Consistency
- ↓ Scalability

**Hyperledger**

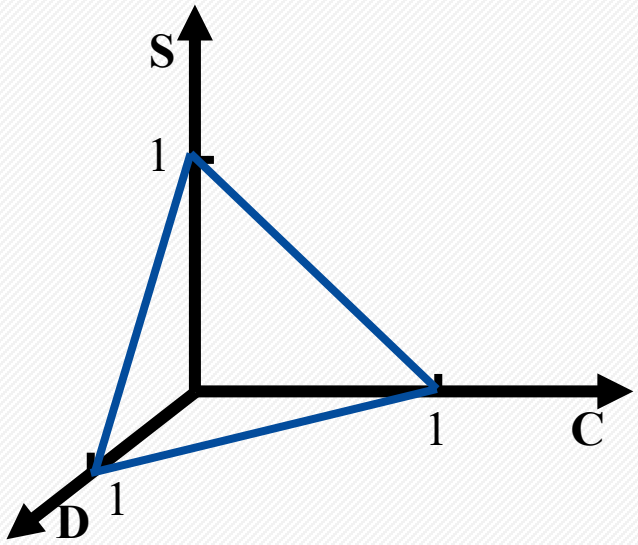
- ↓ Decentralization
- ↑ Consistency
- ↑ Scalability

## Deficiency

- ☒ The applicability is poor and can not be applied to a variety of environments
- ☒ The evaluation indicator can not clearly meet the user's selection requirements

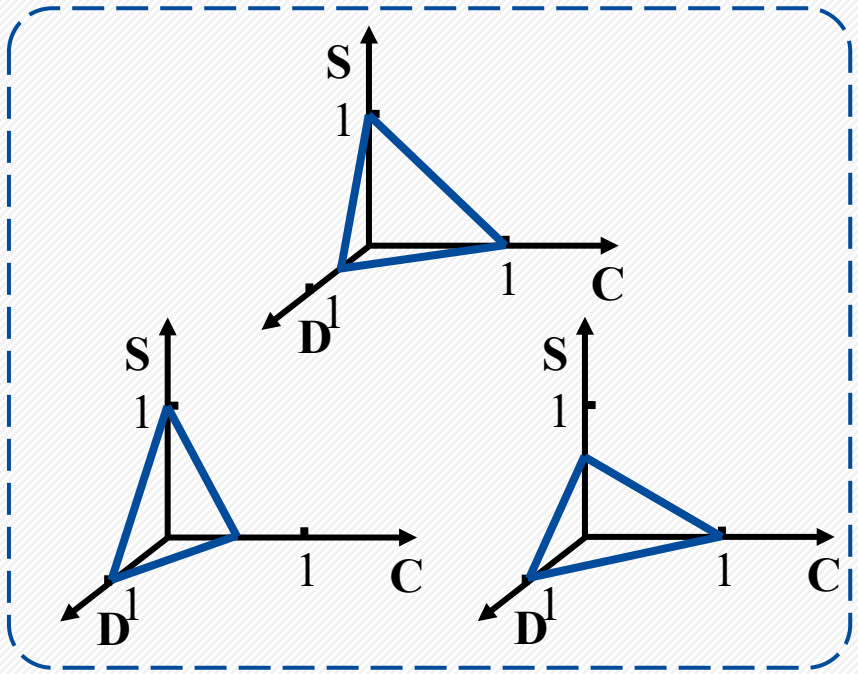
# Introduction Challenge

- How to define and quantify **DCS trilemma properties**?
- How to adjust the system parameters to **adjust the DCS**?
- How to achieve a **complete flexible blockchain system**?




The ideal (but impossible) blockchain system.

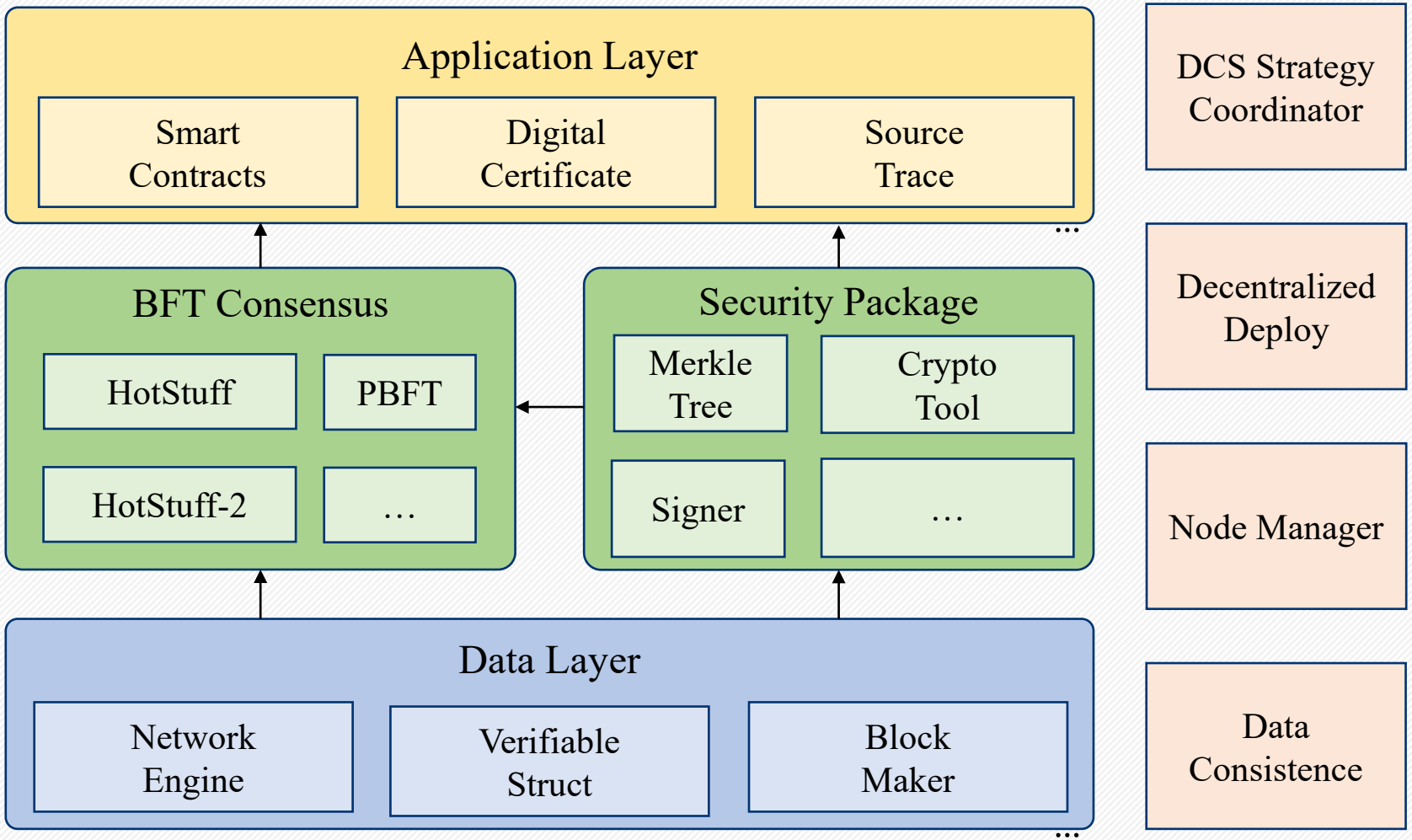
Adjusting
D, C and S.




The resulted optimal blockchain systems.

# OUTLINE

# DCS Chain System Overview




**The architecture of DCS Chain**

# Definition of DCS

- **Decentralization**:
  - Network independence from a trusted third party.
  - Reflects node participation and equity.
- **Consistency**:
  - Immutable and uniform data across nodes.
  - Verifiable state via complete history.
- **Scalability**:
  - The performance of a blockchain system.
  - Performance scales with resource allocation.

# Quantification of DCS

- $D_{rate}$ : **Decentralization** strength correlates with consensus nodes.
- $C_{rate}$ : **Consistency** quantified inversely to consensus delay.
- $S_{rate}$ : **Scalability** gauged by high throughput for data tasks.

$$D_{rate} = 1 - \frac{1}{n}$$

$$C_{rate} = \frac{1}{e^{t}}$$

$$S_{rate} = 1 - \frac{1}{\log_{10}\theta}$$

where $n$ represents the total number of consensus nodes, $t$ denotes the latency, and $\theta$ signifies the throughput.

# DCS Chain Dynamic Adjustment Mechanism

The dynamic adjustment mechanism is the core feature for achieving optimal performance under the guidance of the DCS theory.

- **Number of Consensus Nodes**
  - It directly affects decentralization.
  - Increased nodes lead to lower throughput and higher latency.
- **Consensus Protocol**
  - Consensus protocols influence blockchain performance.
  - Protocols' complexities impact throughput and latency.
- **Batch Size**
  - Batch size affects block packaging efficiency and overhead.
  - Larger batches can boost throughput but increase latency.

# System Fundamentals



## Consensus Protocols

- **PBFT**

  Polynomial time, Practical, 2 phases

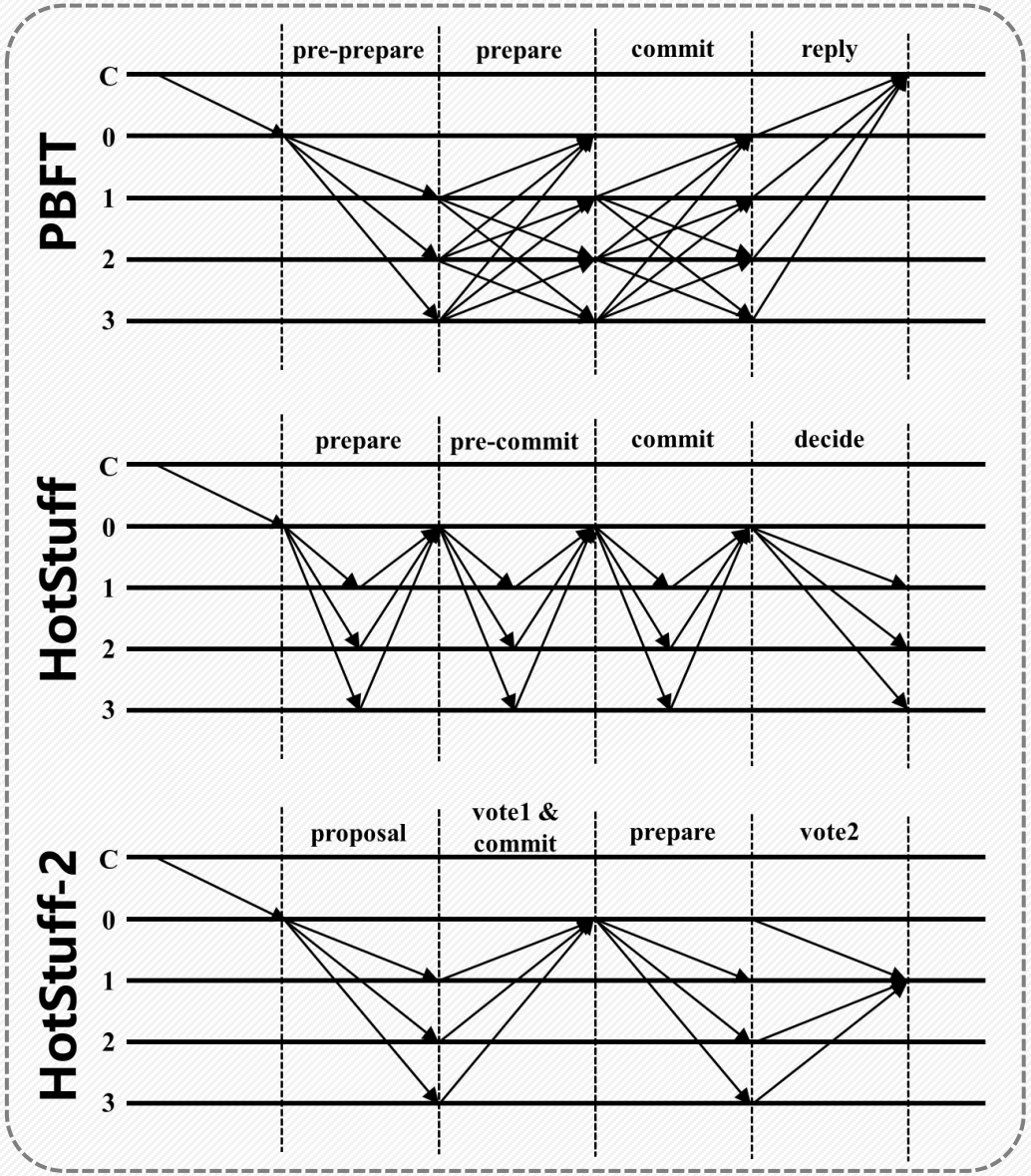
- **HotStuff**

  Linear view-change, Optimistic responsiveness, 3 phases

- **HotStuff-2**

  Two view-change path, 2 phases

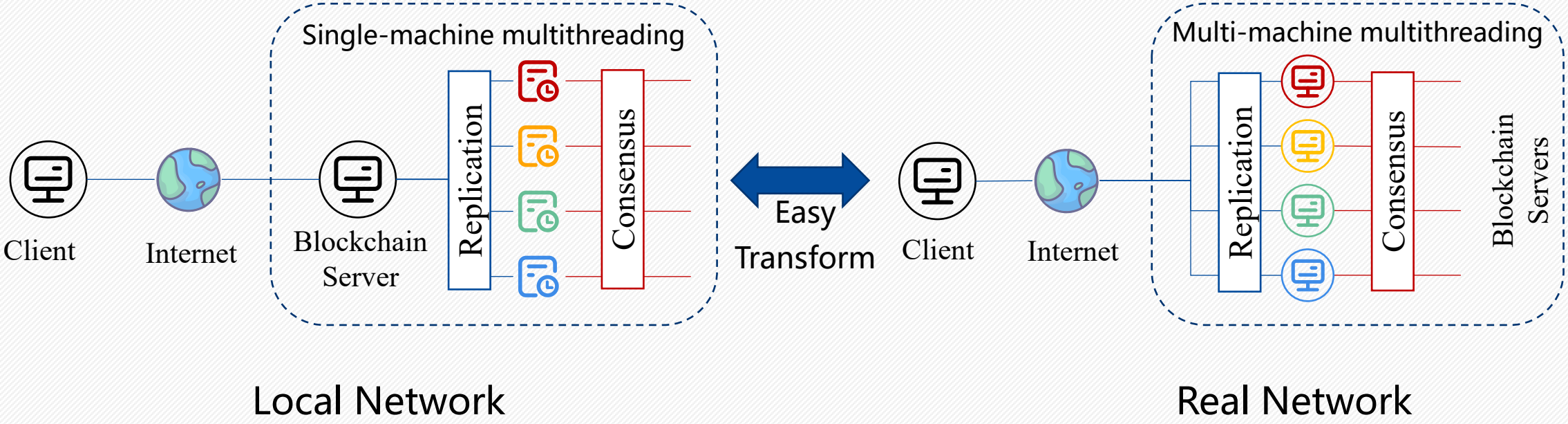
| Protocol | Comp. | Worst | View-Change | Phases |
|---|---|---|---|---|
| **PBFT** | $O(n^2)$ | $O(n^3)$ | $O(n^2)$ | 2 |
| **HotStuff** | $O(n)$ | $O(n^2)$ | $O(n)$ | 3 |
| **HotStuff-2** | $O(n)$ | $O(n^2)$ | $O(n)$ | 2 |



## Local Network Simulation

Construct a quickly deployable local cluster architecture through local network.

- **Modular Design for Scalability and Flexibility**
- **Control Over Network Conditions**
- **Cost-Effective testing and deployment**



# OUTLINE

# Evaluation

## Experiment Setup

The system was deployed on a local machine (Core(TM) i5-1240P 1.70GHz with 16.0GB of memory) by measuring end-to-end experimental data on the client side.

## Task

DCS performance on the following three elements:

- Number of nodes: {4, 10, 16, 22}
- BatchSize: {512, 1024, 2048, 4096, 9182, 16384}
- Protocol type: {PBFT, HotStuff, HotStuff-2}

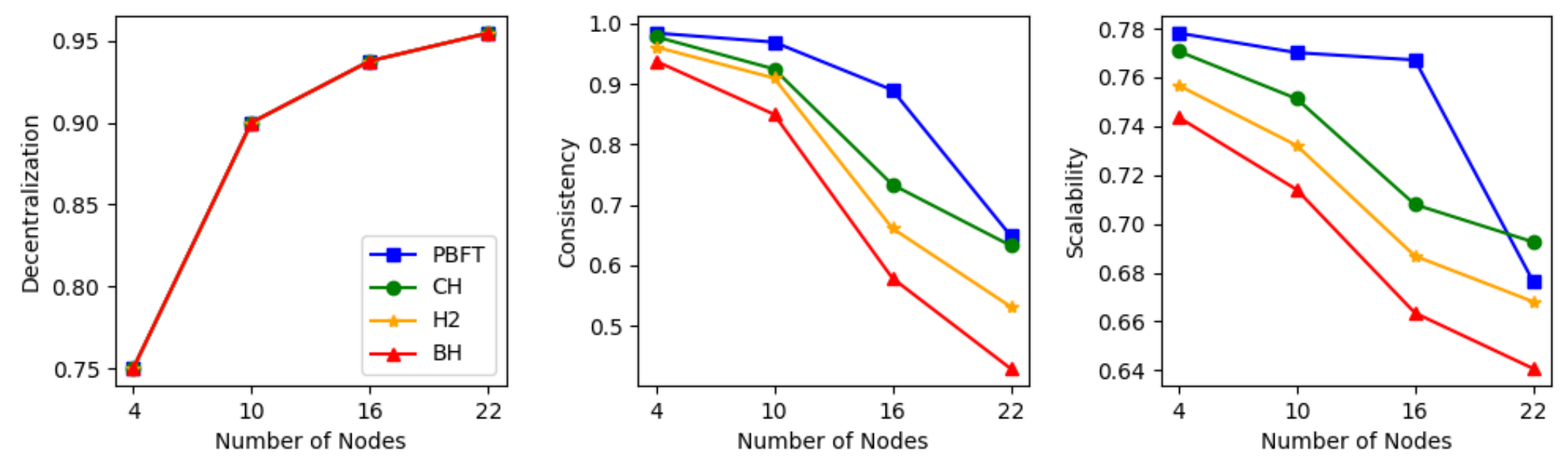
| Protocol | Comm. | Worst | View-Change | Phases |
|---|---|---|---|---|
| PBFT | $O(n^2)$ | $O(n^3)$ | $O(n^2)$ | 2 |
| HotStuff | $O(n)$ | $O(n^2)$ | $O(n)$ | 3 |
| HotStuff-2 | $O(n)$ | $O(n^2)$ | $O(n)$ | 2 |

https://github.com/zhengwang100/DCSChain.

# Evaluation DCS Performance

## Impact of Number of Nodes on DCS Performance Metrics

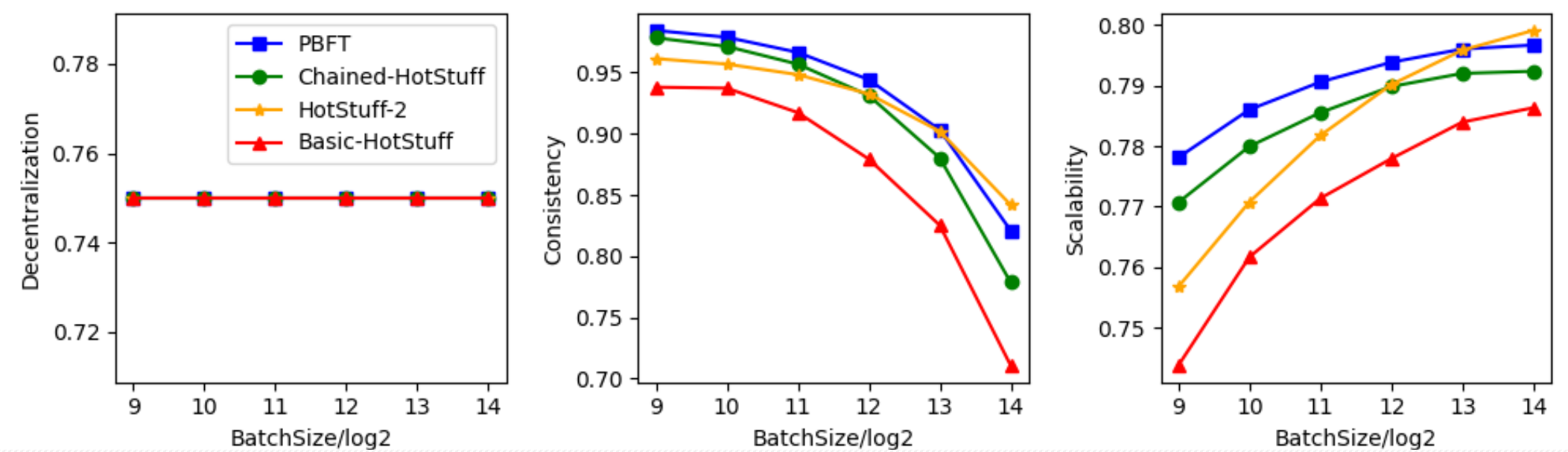
- Decentralization: Shows a **positive correlation** ↗ with the number of nodes.
- Consistency: Shows a **negative correlation** ↘ with the number of nodes.
- Scalability: Shows a **negative correlation** ↘ with the number of nodes.



# Evaluation DCS Performance

## Impact of BatchSize on DCS Performance Metrics

- Decentralization: Shows **no correlation** with the BatchSize.
- Consistency: Shows a **negative correlation** ↘ with the BatchSize.
- Scalability: Shows a **positive correlation** ↗ with the BatchSize.



# Evaluation

## Comparison of signature

Comparison of the efficiency of the sm2 signature in PBFT and the threshold signature in HotStuff

Sm2: github.com/xlcetc/cryptogm/sm/sm2

TSS: go.dedis.ch/kyber/v3

**When the number of nodes reaches 40, the cost of threshold signature is smaller than that of sm signature.**

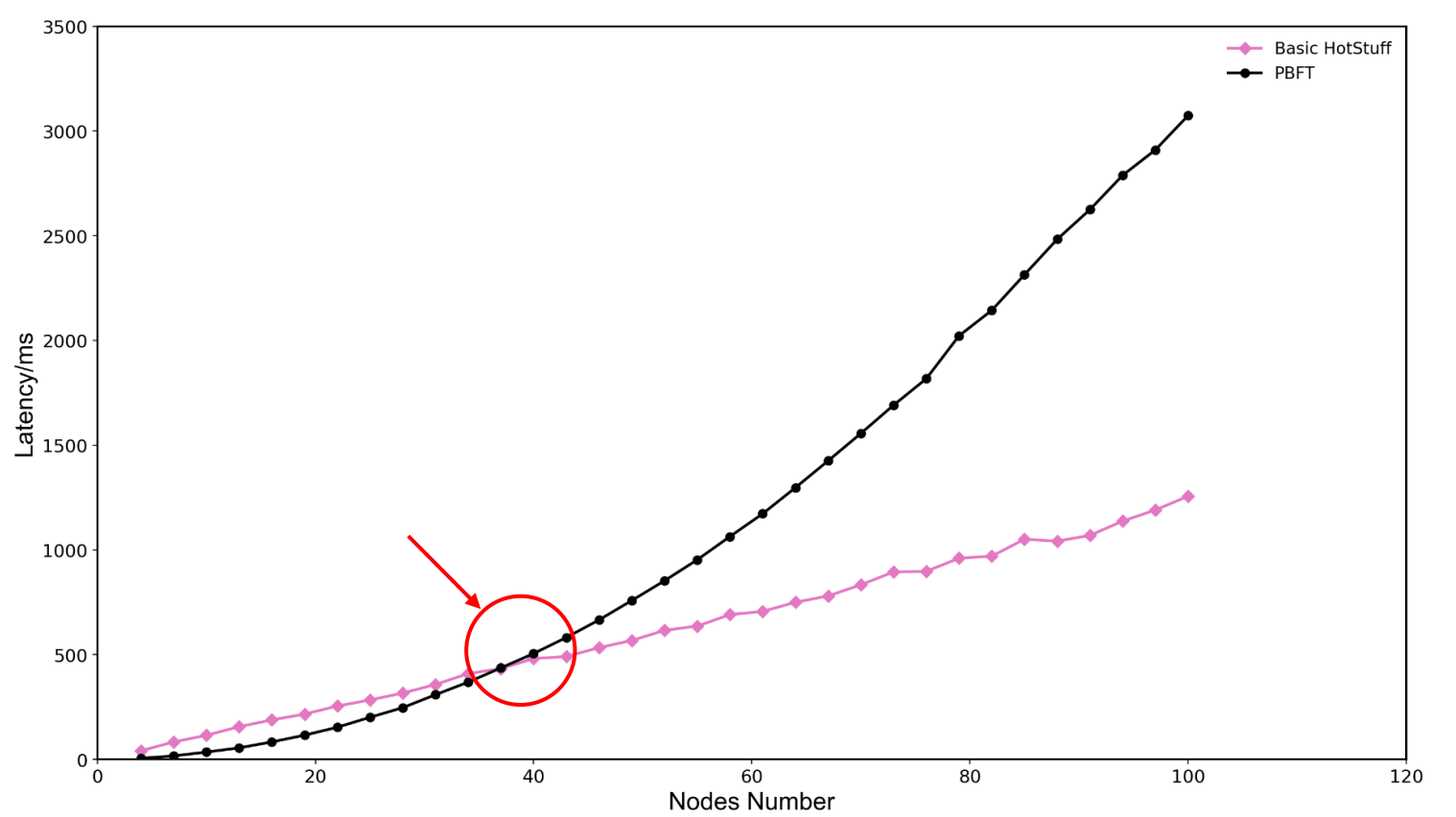
| | Basic-HotStuff | | | | | | | PBFT | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| node | tss_sign | tss_comb | tss_verify | sign_num | comb_num | verify_num | one round | sm2_sign | sm2_verify | sign_num | verify_num | one round |
| 4 | 0.137 | 5.583 | 1.817 | 12 | 3 | 16 | 41.145 | 0.020 | 0.073 | 9 | 36 | 5.022 |
| 13 | 0.143 | 16.435 | 1.752 | 39 | 3 | 52 | 155.948 | 0.021 | 0.080 | 27 | 351 | 54.873 |
| 22 | 0.151 | 29.792 | 1.732 | 66 | 3 | 88 | 254.577 | 0.020 | 0.072 | 45 | 990 | 153.298 |
| 31 | 0.169 | 41.321 | 1.870 | 93 | 3 | 124 | 357.435 | 0.031 | 0.074 | 63 | 1953 | 308.673 |
| 40 | 0.184 | 55.164 | 1.866 | 120 | 3 | 160 | 481.300 | 0.026 | 0.078 | 81 | 3240 | 505.518 |
| 49 | 0.143 | 66.793 | 1.737 | 147 | 3 | 196 | 567.818 | 0.025 | 0.075 | 99 | 4851 | 758.537 |
| 58 | 0.147 | 82.659 | 1.876 | 174 | 3 | 232 | 691.204 | 0.021 | 0.083 | 117 | 6786 | 1064.016 |
| 67 | 0.143 | 95.363 | 1.788 | 201 | 3 | 268 | 780.069 | 0.029 | 0.080 | 135 | 9045 | 1425.550 |
| 76 | 0.131 | 110.441 | 1.689 | 228 | 3 | 304 | 897.952 | 0.022 | 0.082 | 153 | 11628 | 1817.495 |
| 85 | 0.131 | 128.841 | 1.955 | 255 | 3 | 340 | 1050.857 | 0.032 | 0.094 | 171 | 14535 | 2313.922 |
| 94 | 0.131 | 141.685 | 1.782 | 282 | 3 | 376 | 1137.699 | 0.031 | 0.088 | 189 | 17766 | 2788.523 |
| 100 | 0.133 | 151.305 | 1.775 | 300 | 3 | 400 | 1256.474 | 0.020 | 0.093 | 201 | 20100 | 3073.888 |
| Note | - | - | - | 3n | 3 | 4n | - | - | - | 2n+1 | n(2n+1) | - |

# Evaluation

## Comparison of signature

This explains why PBFT performed better than HotStuff in the previous experiment.

Common sm2 signatures have been optimized enough. However, the threshold signature needs to be optimized.




The cost of signature and verification in a consensus protocol round

# OUTLINE

# Conclusion

This paper presents a flexible private blockchain system based on the DCS trilemma—**DCS Chain**.

- The **definition and quantification of the DCS indicators**, allowing for a multidimensional description of system performance.
- A **dynamic adjustment mechanism**, achieving theoretically optimal blockchain performance.
- A **complete and flexible set of core private blockchain components**, making it suitable for common application scenarios.


上海交通大學

Shanghai Jiao Tong University

# Thank you!

Paper: https://arxiv.org/abs/2406.12376

Code: https://github.com/zhengwang100/DCSChain