Algorand: Scaling Byzantine Agreements for Cryptocurrencies

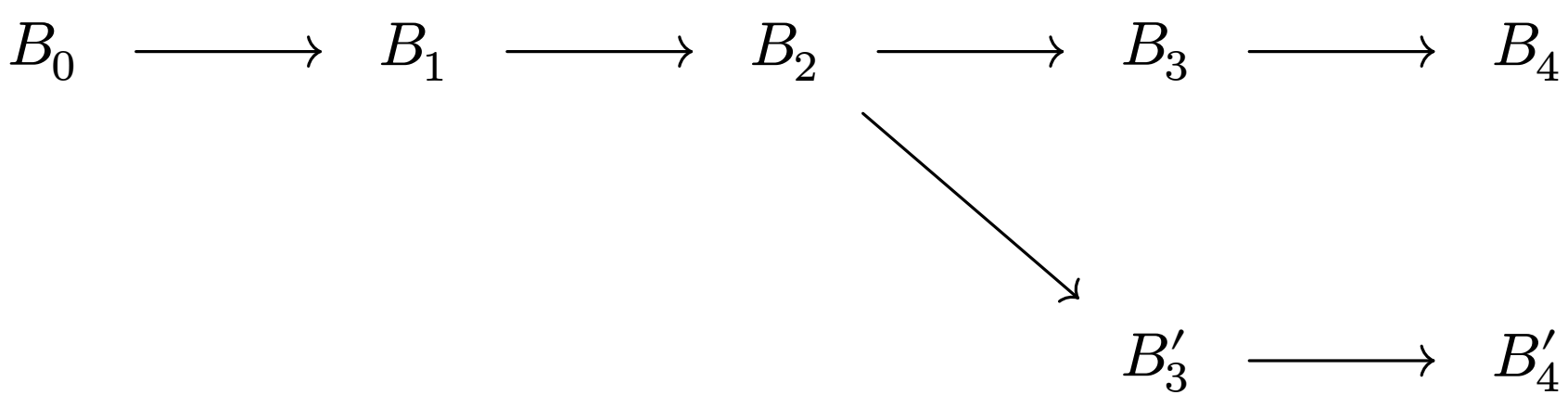
Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich MIT CSAIL

SOSP'17

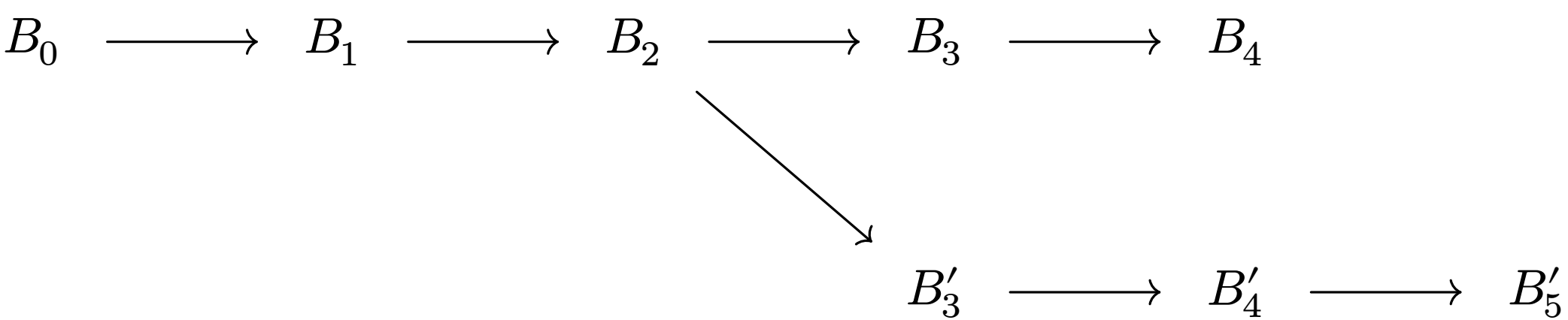
Context Introduction

- Cryptographic currencies
- Avoiding centralized authorities
- Trade-off between latency and confidence

Nakamoto consensus & Proof of Work



Nakamoto consensus & Proof of Work



Nakamoto consensus & Proof of Work

- No confident commit
- Possible forks
- Latency problem
- Scalabillity

BFT Consensus

- Predefined set of servers
- Denial of service attack
- All to All communication
- Scalabillity

Algorand

- New cryptocurrency
- Confiramttion in order of minute
- Scallable (No all to all communication)

Algorand: Network structure

- Dynamic size
- Confiramttion in order of minute
- Scallable (No all to all communication)

Algorand: Key components

Algorand: Sortition

Algorand: BA*

Algorand: Evaluation