Discussion: Preventing Transaction Reordering Manipulations in Decentralized Finance

Haoqian Zhang

Decentralized and Distributed Systems Laboratory (DEDIS)

École Polytechnique Fédérale de Lausanne (EPFL)

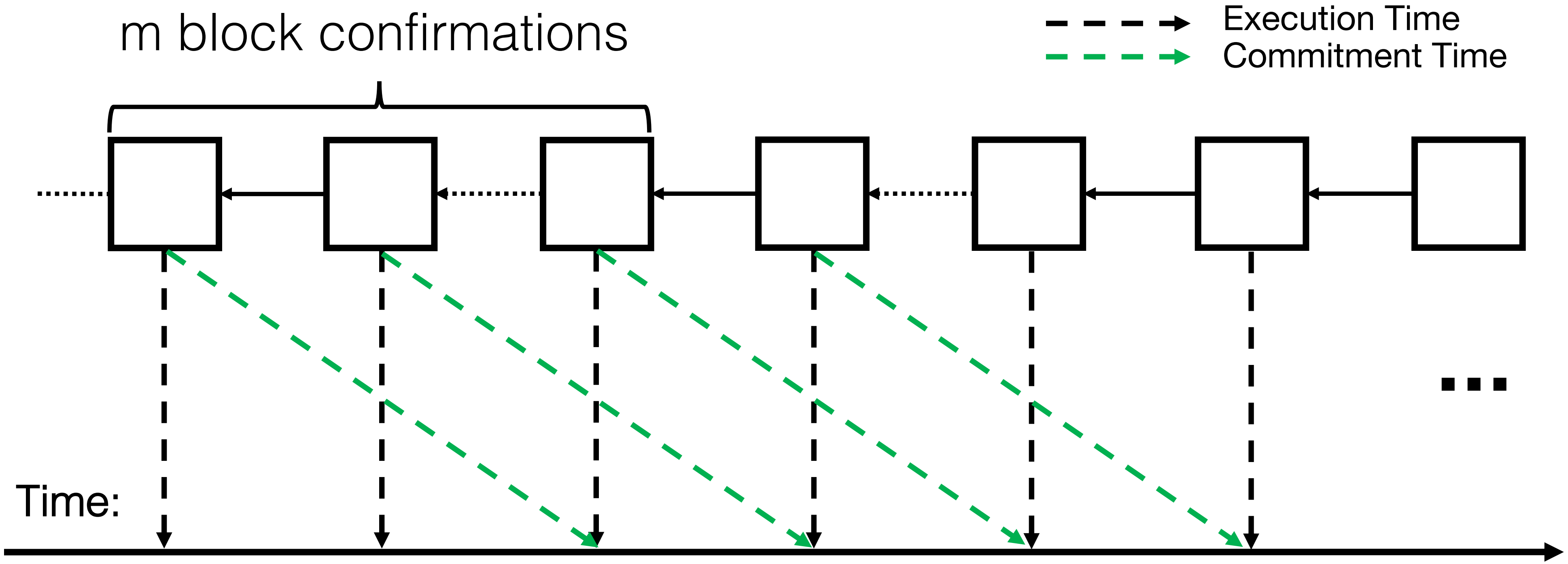
SNB-CIF Conference on Cryptoassets and Financial Innovation 2023

26 May 2023

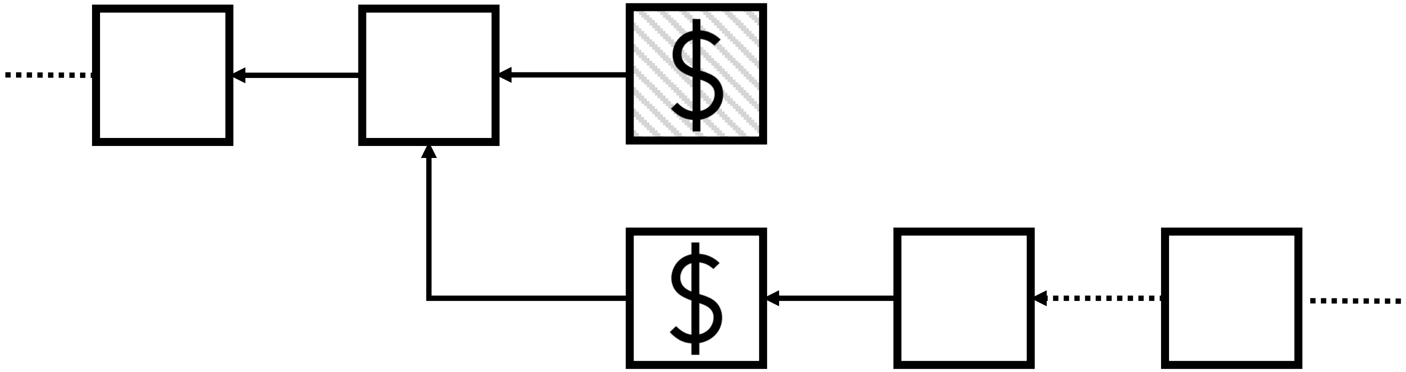
Outline

- Whale Attack with MEV
- Per-Transaction Protection
- Decentralization & Security Assumptions

Transaction Commitment



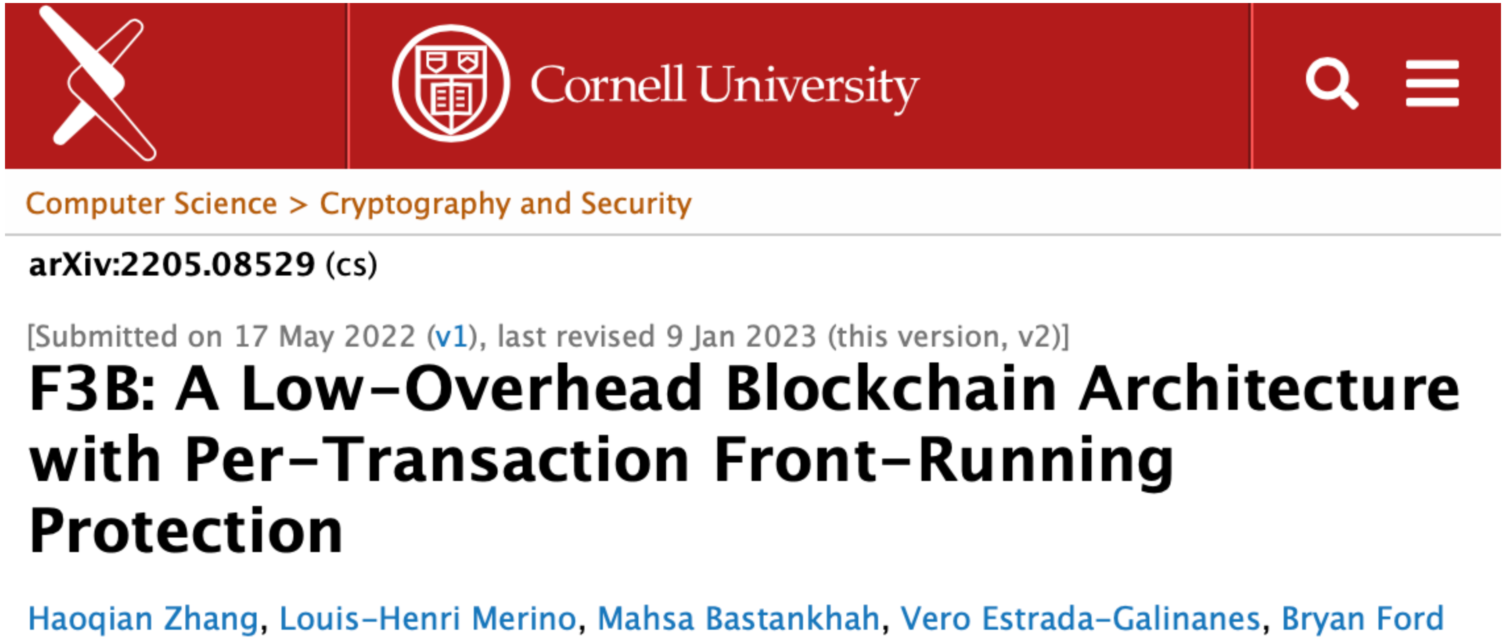
Whale Attack* with MEV



▨ : Targeted block with transaction exploiting a big MEV value

* Liao, Kevin, and Jonathan Katz. "Incentivizing Blockchain Forks via Whale Transactions." FC17

Flash Freezing Flash Boys(F3B)



Computer Science > Cryptography and Security

arXiv:2205.08529 (cs)

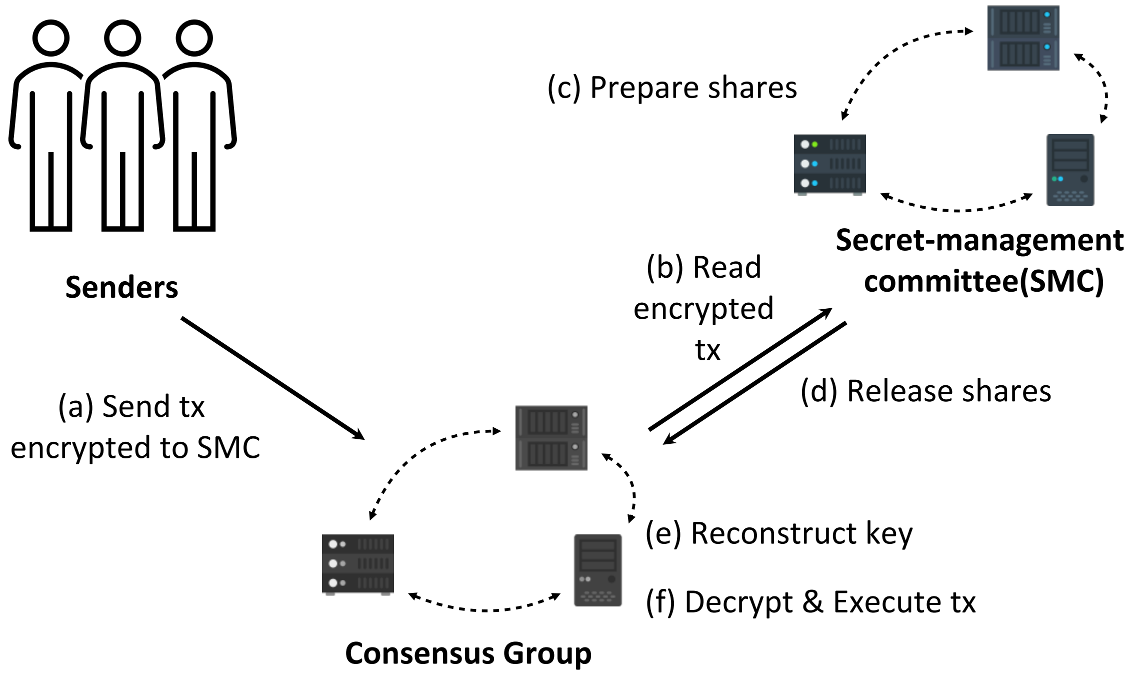
[Submitted on 17 May 2022 (v1), last revised 9 Jan 2023 (this version, v2)]

F3B: A Low-Overhead Blockchain Architecture with Per-Transaction Front-Running Protection

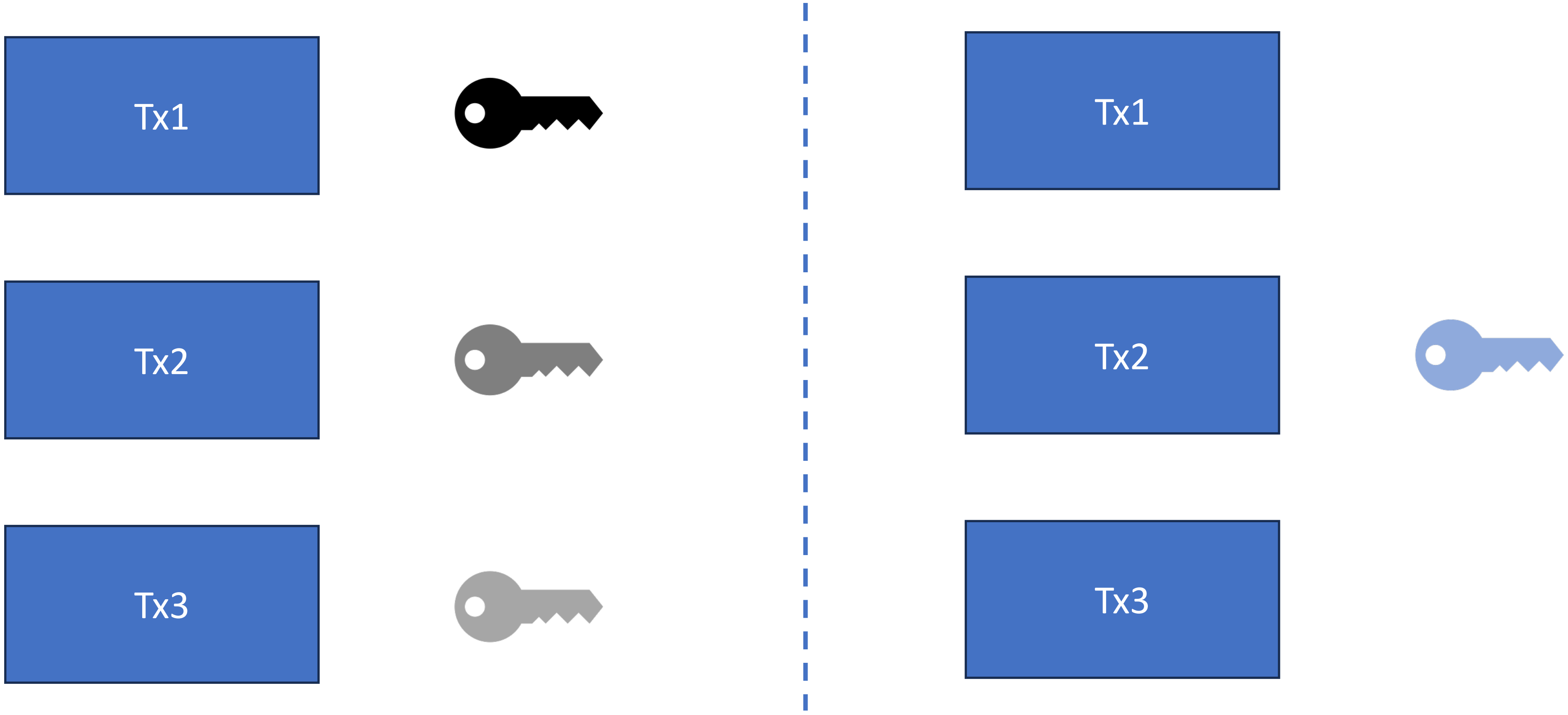
Haoqian Zhang, Louis-Henri Merino, Mahsa Bastankhah, Vero Estrada-Galinanes, Bryan Ford

Flash Freezing Flash Boys(F3B)

- Off-chain commit & reveal solution
- Per-transaction protection



Per-Transaction vs Per-Block



Tx1

Tx2

Tx3

Tx1

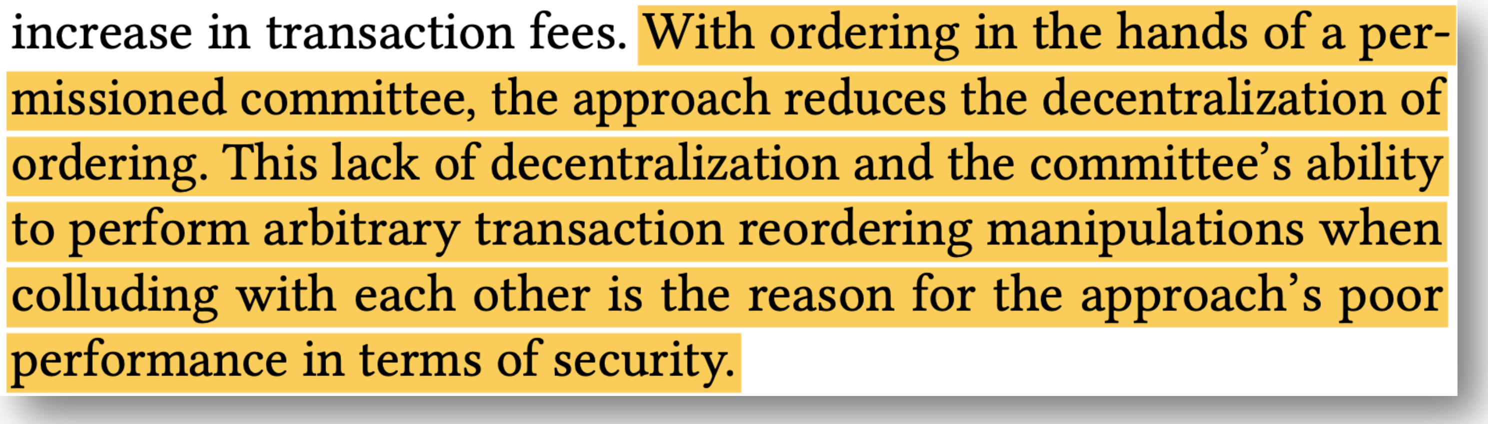
Tx2

Tx3

Per-Transaction

- Per-Transaction protection is necessary
- Transaction can be revealed with block key
  - When it fails to be included in the specified block
  - Congestion
  - DoS attacks

Decentralization & Security Assumptions



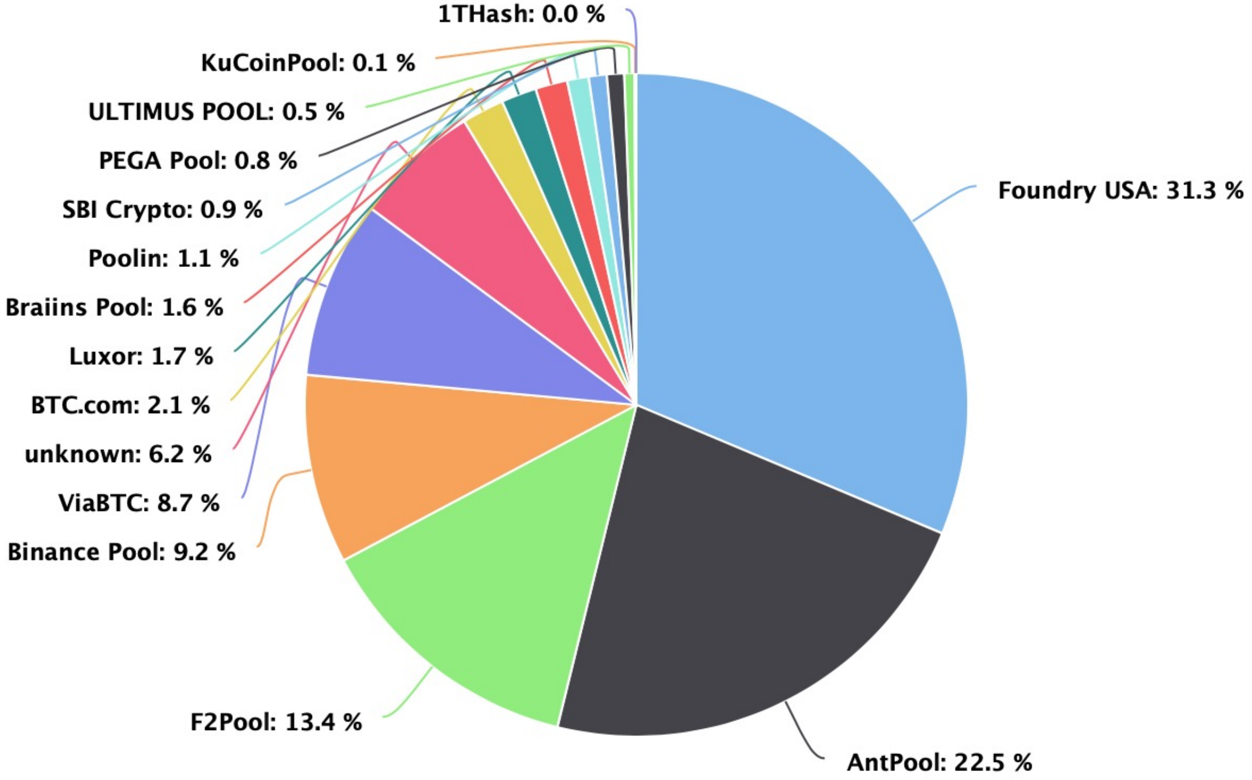
increase in transaction fees. With ordering in the hands of a permissioned committee, the approach reduces the decentralization of ordering. This lack of decentralization and the committee's ability to perform arbitrary transaction reordering manipulations when colluding with each other is the reason for the approach's poor performance in terms of security.

- Assumptions:
  1. Permissionless blockchain is more decentralized
  2. Permissionless blockchain is more secure
- But are those valid assumptions?

* Heimbach, Lioba, and Roger Wattenhofer. "SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance." *AFT22*.

Decentralization & Security Assumptions

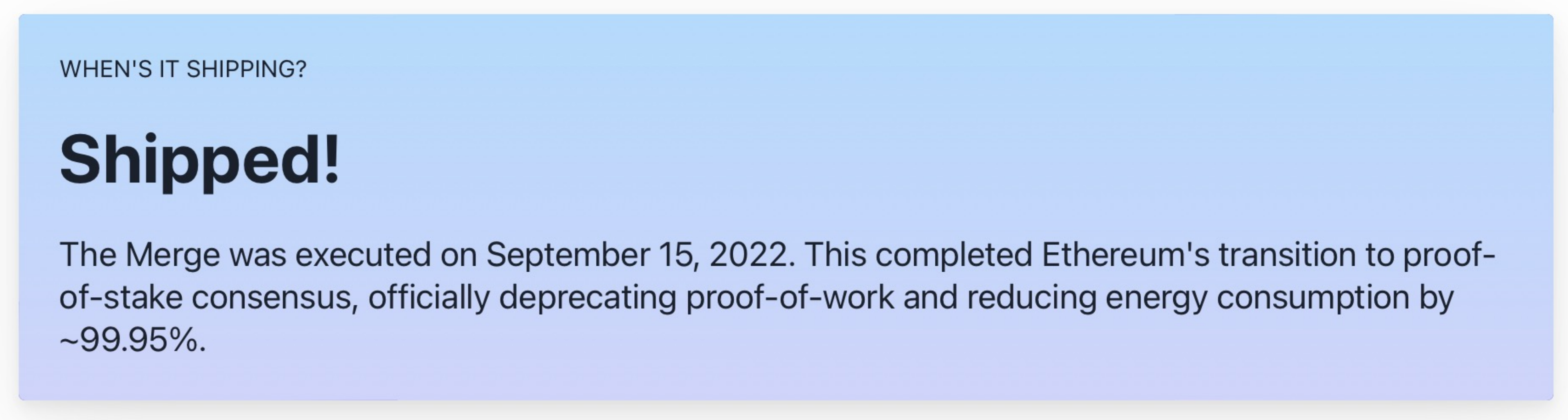
- Permissionless blockchain with less decentralization & security



* Pool Distribution by BTC.com

Decentralization & Security Assumptions

- Ethereum is a moving baseline
- Changed to proof-of-stake

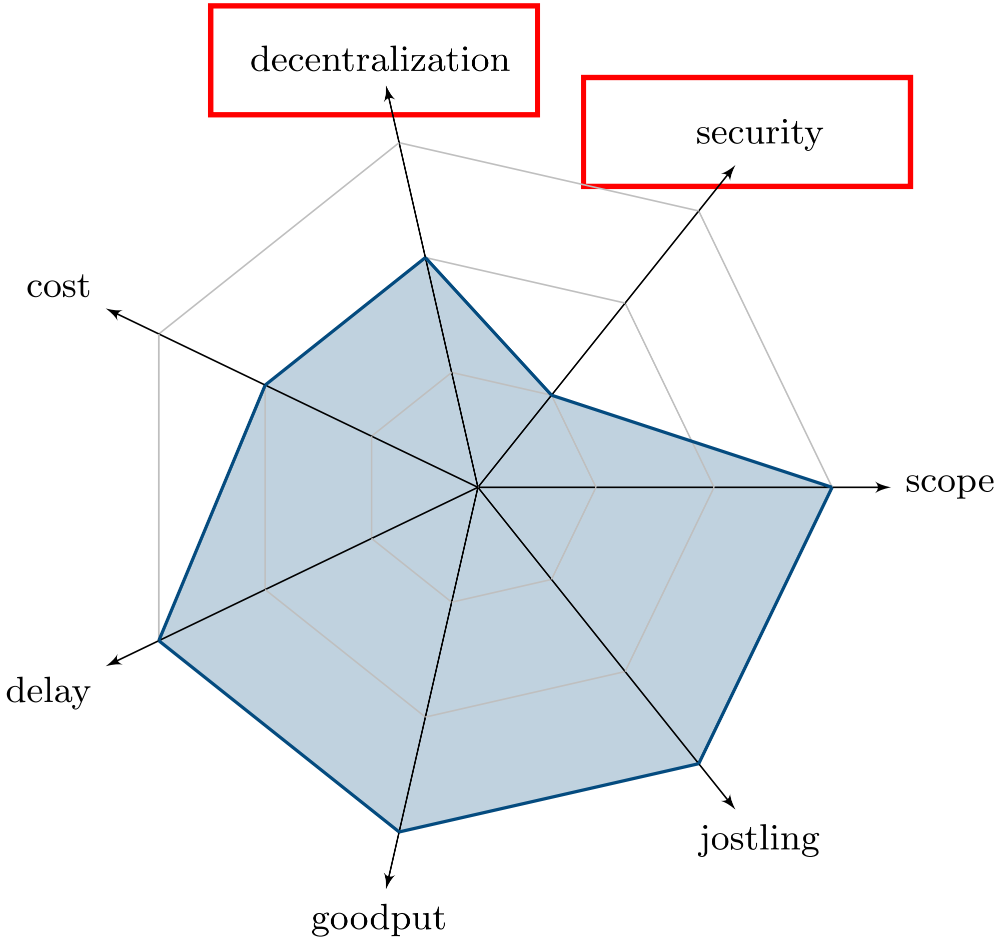


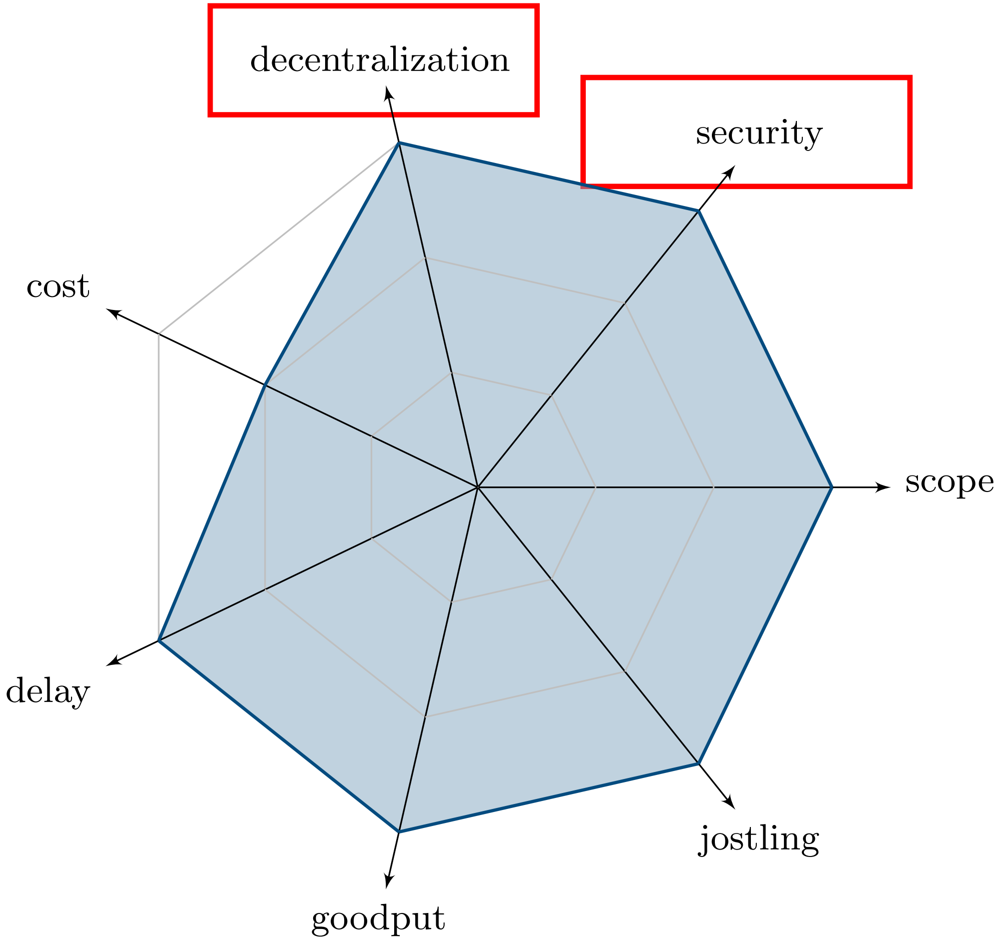
WHEN'S IT SHIPPING?

Shipped!

The Merge was executed on September 15, 2022. This completed Ethereum's transition to proof-of-stake consensus, officially deprecating proof-of-work and reducing energy consumption by ~99.95%.

Decentralization & Security Assumptions





Conclusion

- Off-chain commit and reveal approach can achieve good performance in all measures except cost
- But we need to do it right
  - Transaction Commitment
  - Per-transaction Protection