F3B(Flash Freezing Flash Boys): A Low-Overhead Blockchain Architecture with Per-Transaction Front-Running Protection

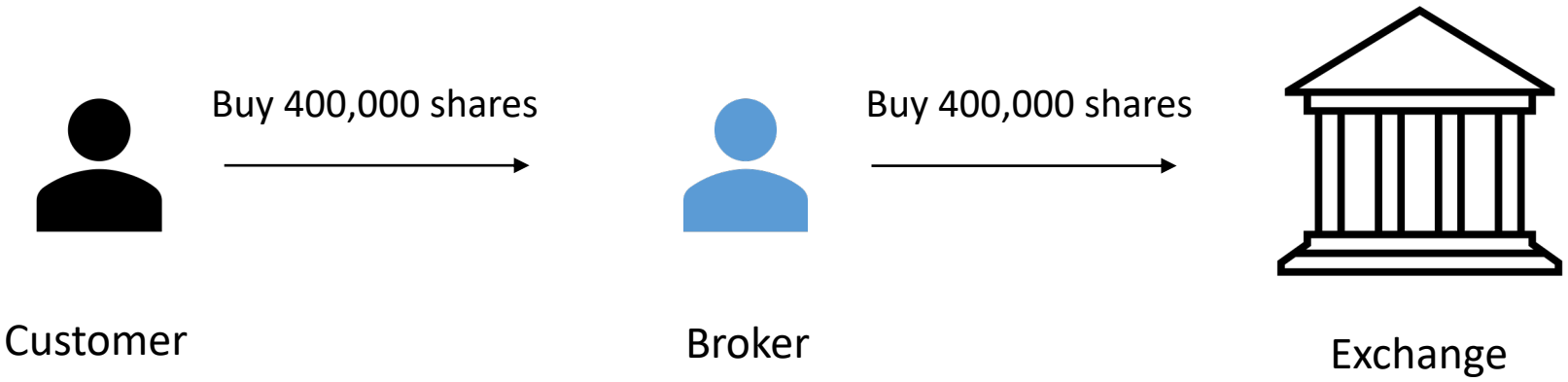
Haoqian Zhang, Louis-Henri Merino, Ziyan Qu, Mahsa Bastankhah,
Vero Estrada-Galinanes, Bryan Ford
Swiss Federal Institute of Technology Lausanne (EPFL)

Advances in Financial Technologies - AFT 2023
October 25, 2023

Outline

- Front-running in Traditional Exchange
- Front-running in Blockchain
- Flash Freezing Flash Boys(F3B) Overview
- Per-transaction protection
- Experimental Results

Traditional Exchange

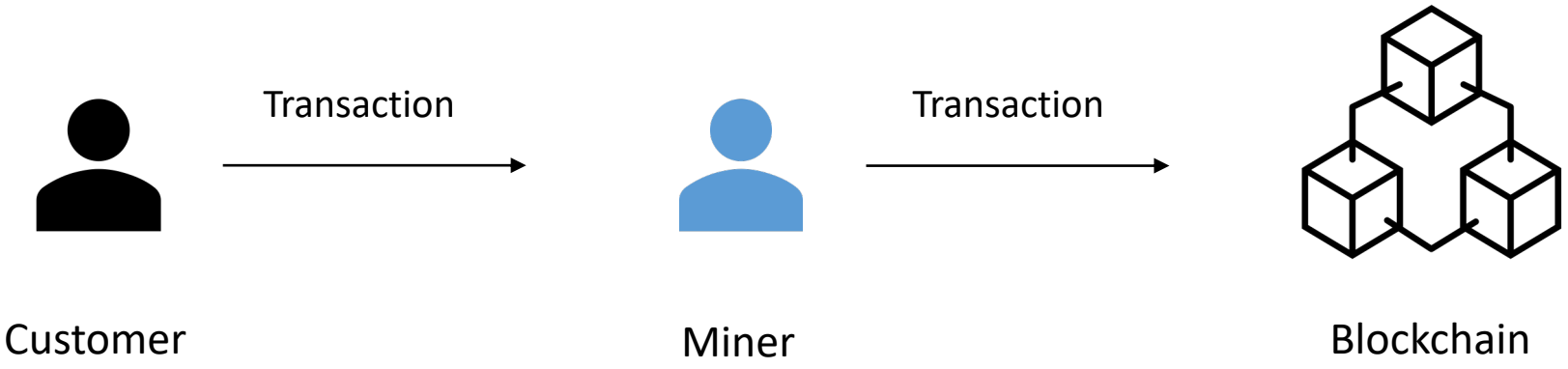


Front-running in Traditional Exchange

Front-running in Traditional Exchange

- Front running is the practice of entering into a trade to capitalize on advanced, nonpublic knowledge of a large pending transaction that will influence the price of the underlying security.
- Prohibited practice by regulations.

Blockchain

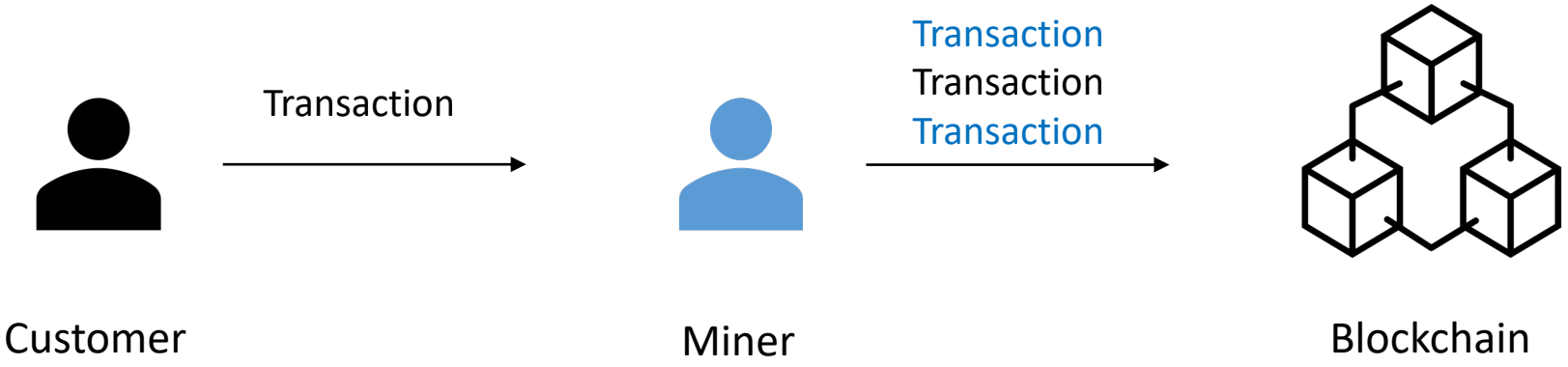


Front-running in Blockchain

Displacement Attack:

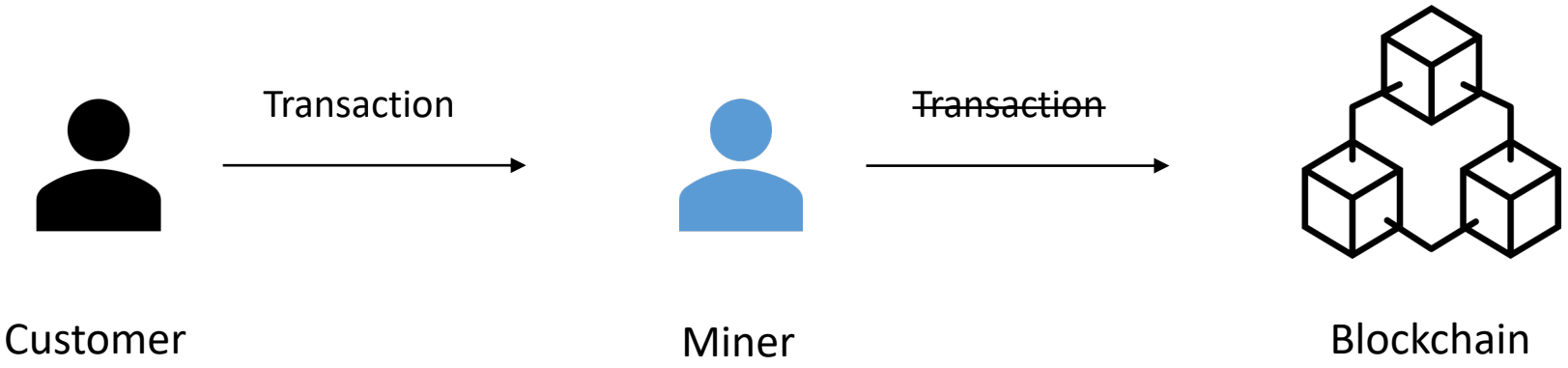
Front-running in Blockchain

Insertion Attack:



Front-running in Blockchain

Suppression Attack:

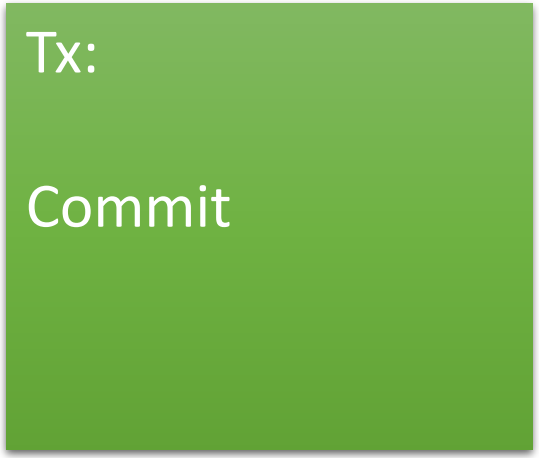


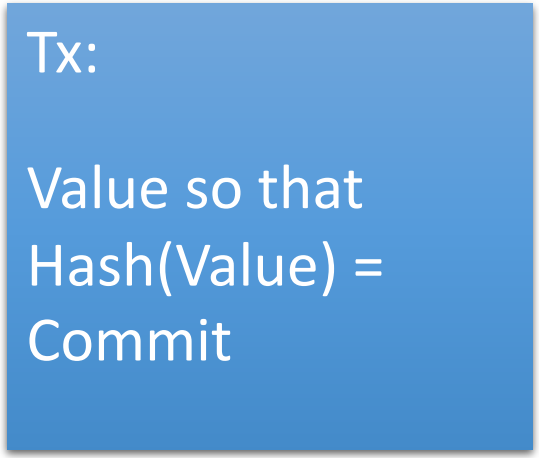
Front-running in Blockchain

- A front-running attack is a practice where an entity benefits from early access to some pending transactions.
- No regulation.
- Front-running attacks cause a loss of $280M each month worldwide*.

* https://cybernews.com/crypto/flash-boys-2-0-front-runners-draining-280-million-per-month-from-crypto-transactions/

Strawman: Commit-and-Reveal by User



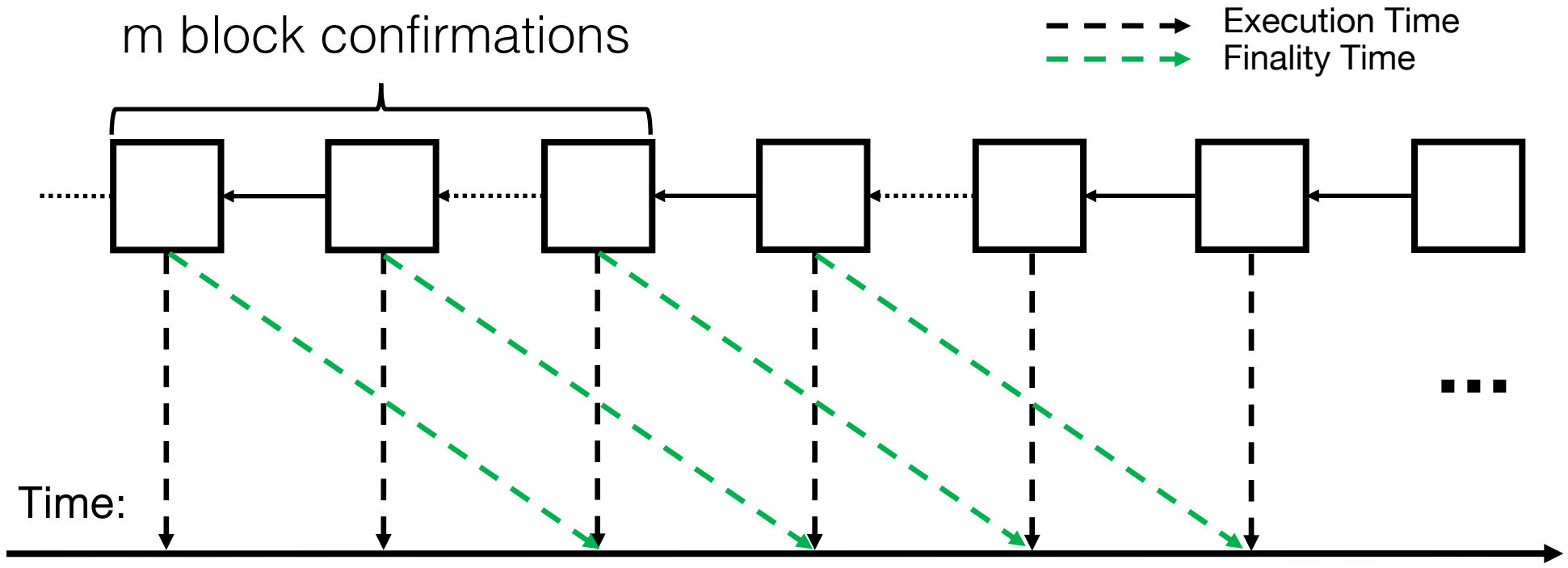


Drawbacks:

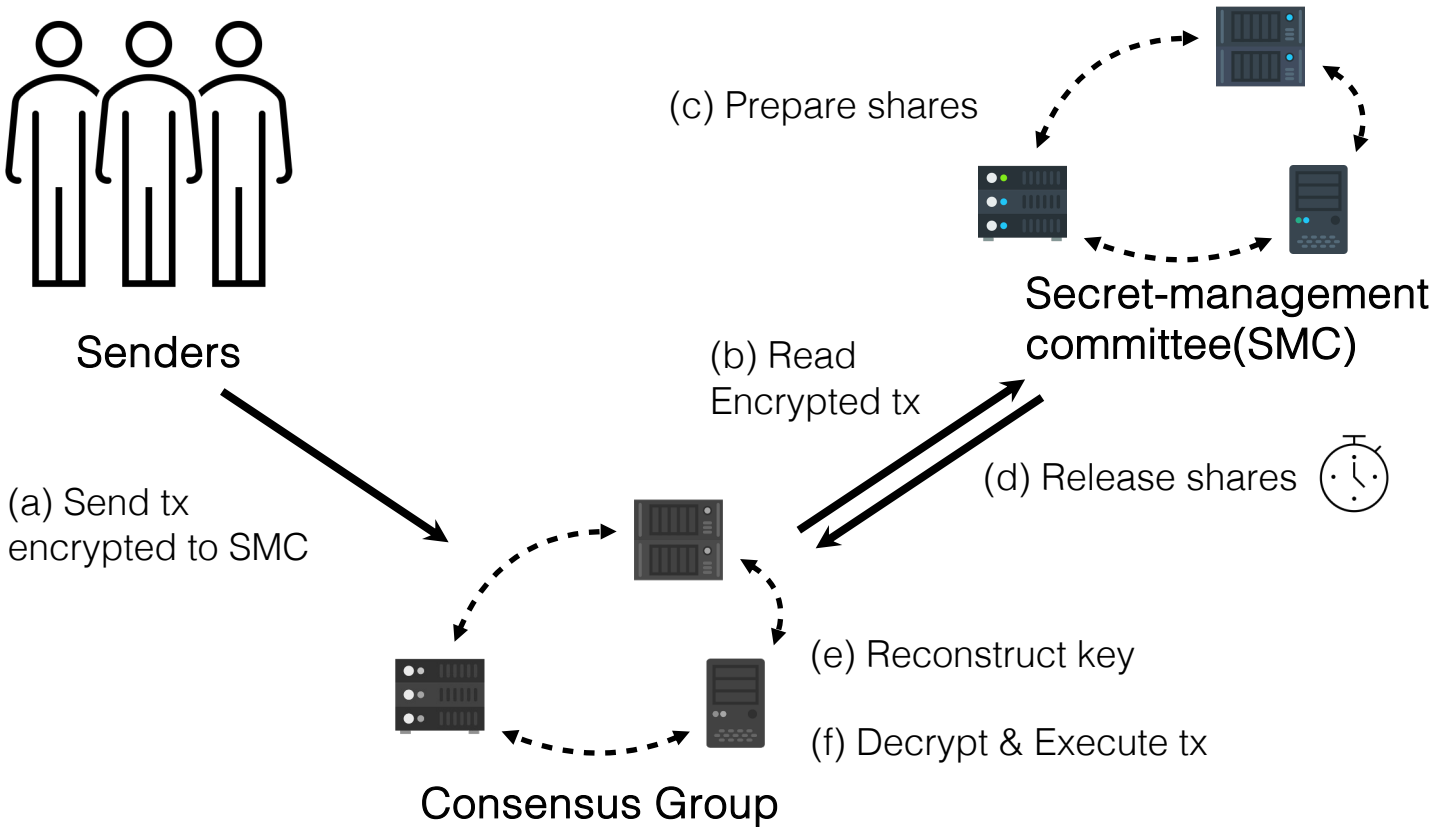
(1) Two transactions

(2) Suppression Attack possible

Transaction Finality

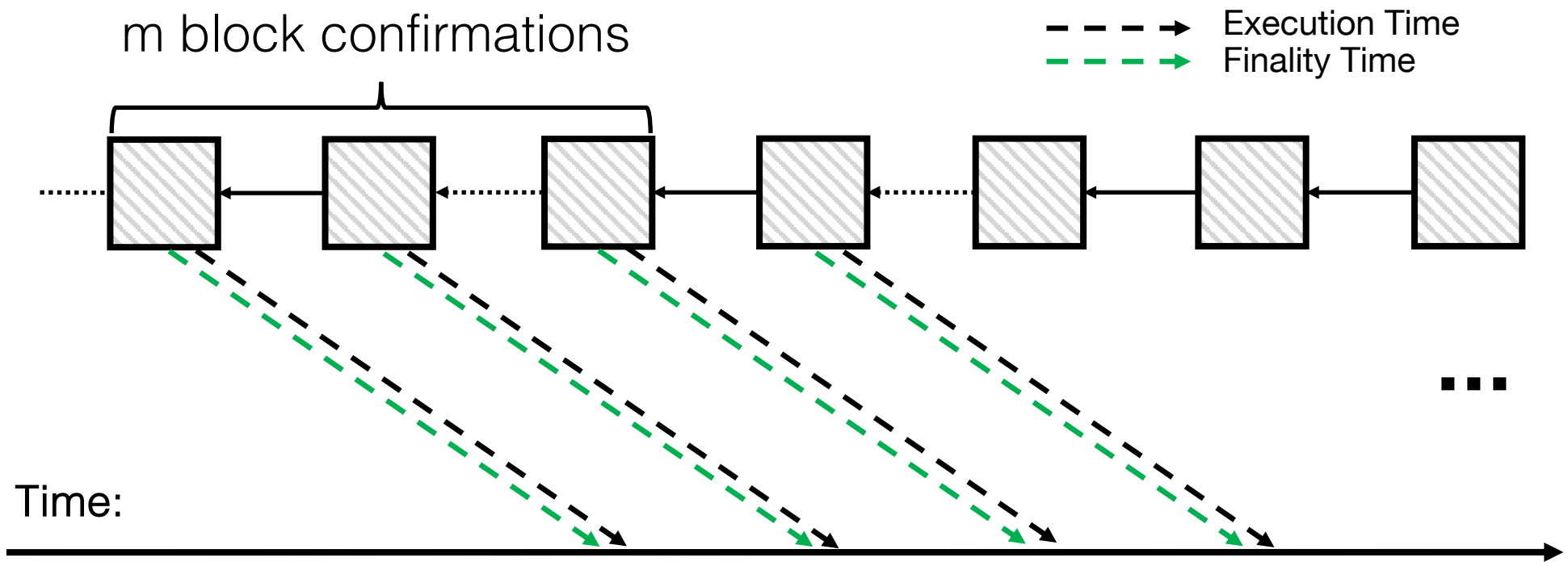


Architecture Overview

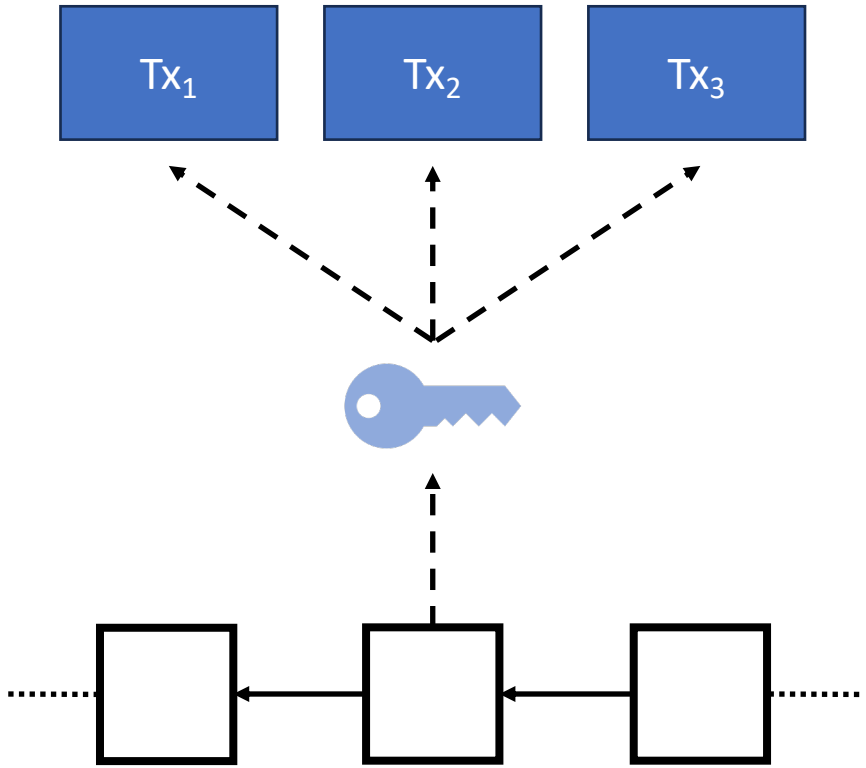


*The secret-management committee and the consensus group can consist of the same set of servers. For clarity in this presentation, we logically separate them into two different entities.

F3B

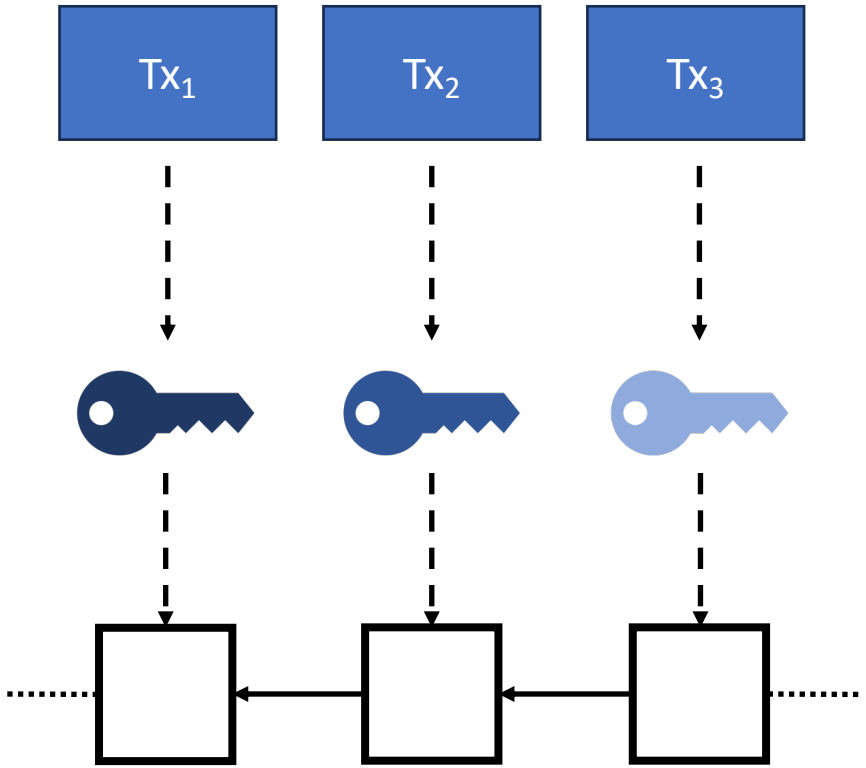


Per-Block vs Per-Transaction Encryption



Per-block Protection

Fairblock, Shutter



Per-transaction Protection

F3B

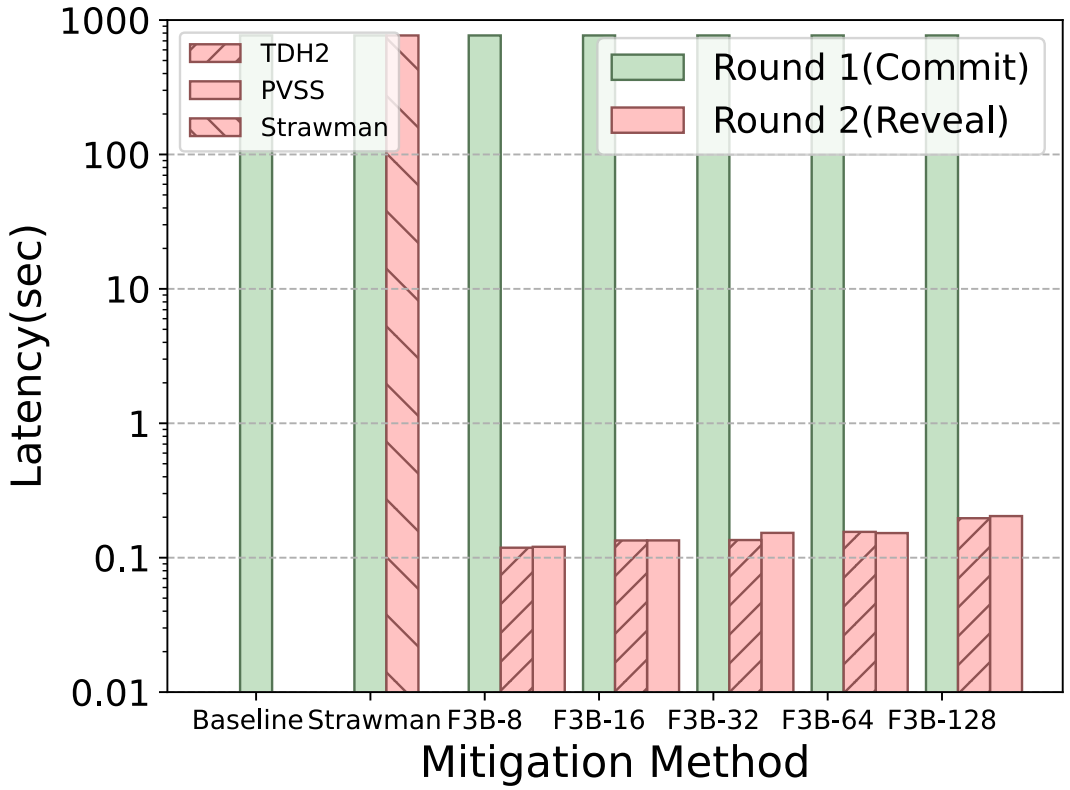
How does F3B mitigate front-running

- A front-running attack is a practice where an entity benefits from early access to some pending transactions.
- Reasoning from definition: transactions are encrypted before their finality -> attackers can not benefit from pending transactions.

TDH2 and PVSS

	TDH2	PVSS
Preprocessing	DKG per epoch	Prepare shares per transaction
Membership	Fixed per epoch	Changeable per transaction
Cyphertext	Constant length	Length grows linearly

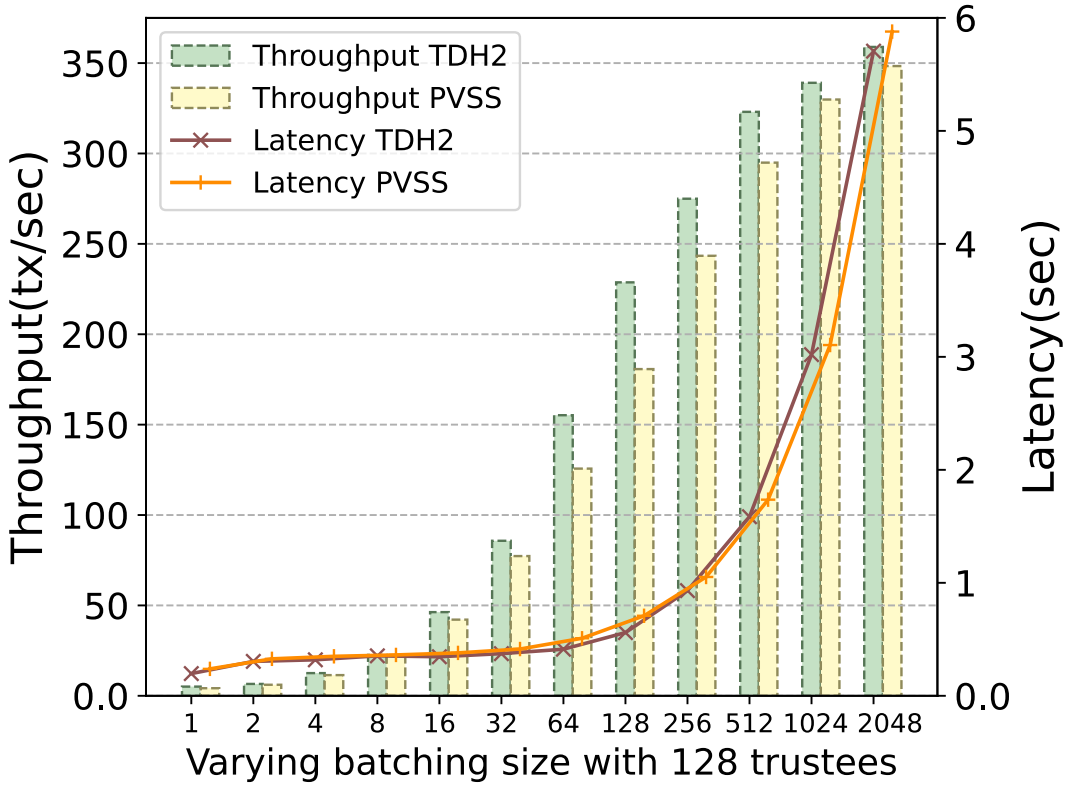
Latency (TDH2 & PVSS)



- Ethereum
  - Block Time = 12s
  - Block confirmations = 64
  - => Latency = 768s
- F3B with 128 nodes
  - Latency 197/205ms
  - 0.0026/0.0027% latency overhead in Ethereum

* We ran our experiment on a server with 32GB of memory and 40 CPU cores running at 2.1GHz.

Throughput (TDH2 & PVSS)



- Ethereum
  - Around 15 tps
- F3B with 128 nodes
  - 359/348tps
  - Latency 5.71/5.88 seconds
  - 0.74/0.77% latency overhead in Ethereum

* We ran our experiment on a server with 32GB of memory and 40 CPU cores running at 2.1GHz.

Conclusion

- Front-running is a significant problem in DeFi
- F3B: Flash Freezing Flash Boys
  - (+) Per-transaction protection
  - (+) Achieves low-latency overhead
  - (–) Requires modification of execution layer

Full Paper