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

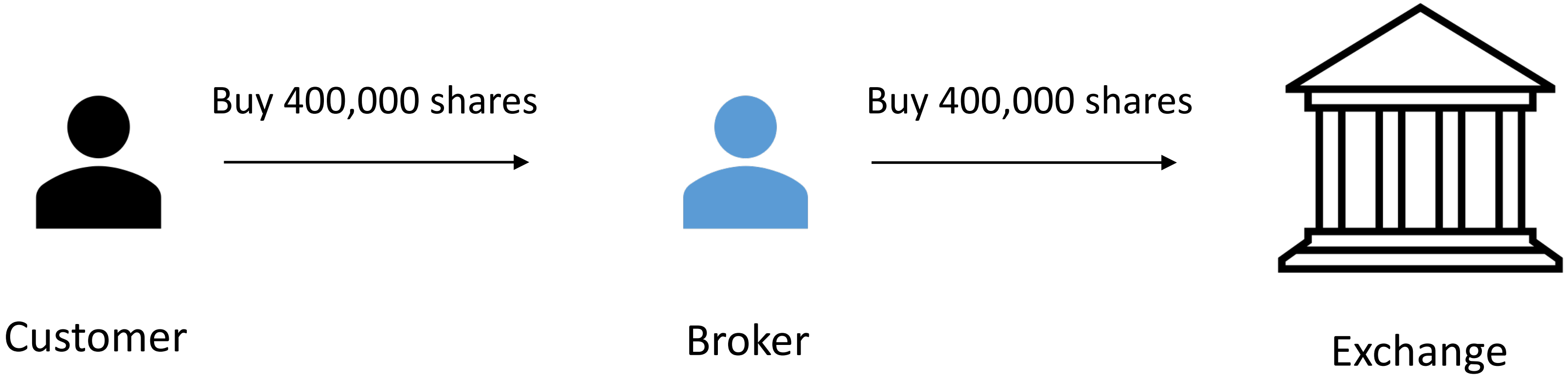
Haoqian Zhang

École Polytechnique Fédérale de Lausanne (EPFL)

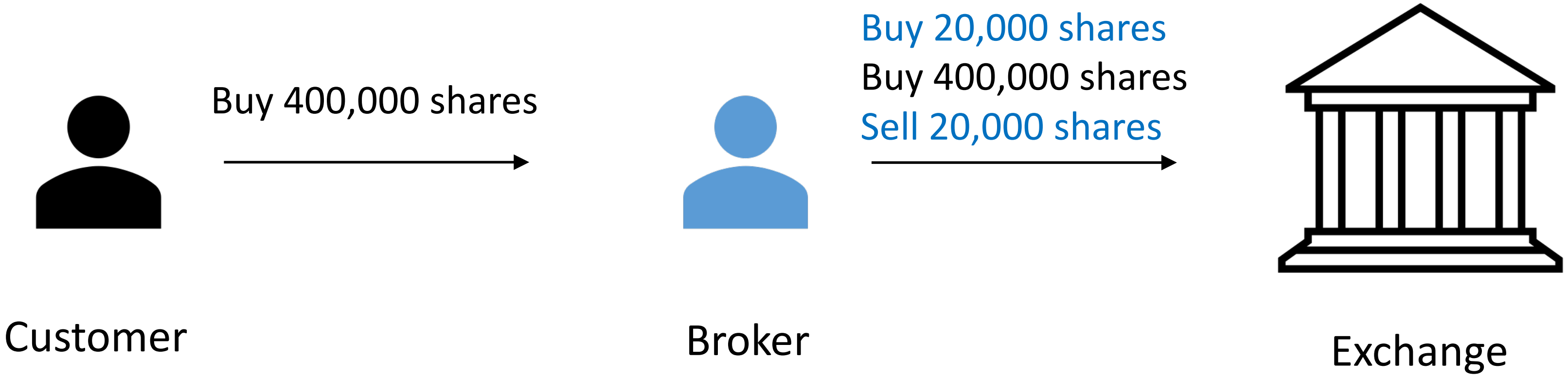
Outline

- Front-running in Traditional Exchange
- Front-running in Blockchain
- Flash Freezing Flash Boys(F3B) Overview

Traditional Exchange



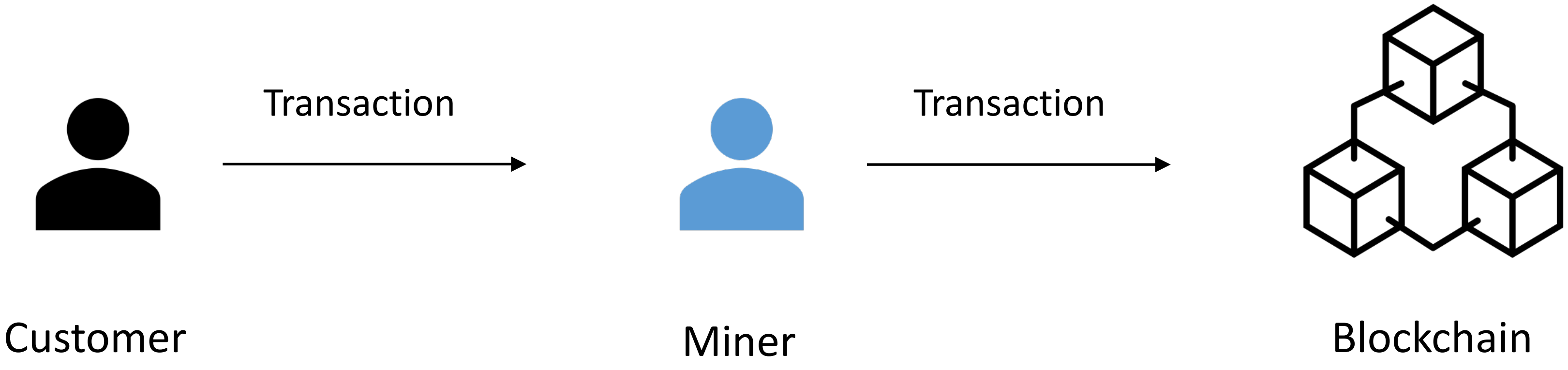
Front-running in Traditional Exchange



Front-running in Traditional Exchange

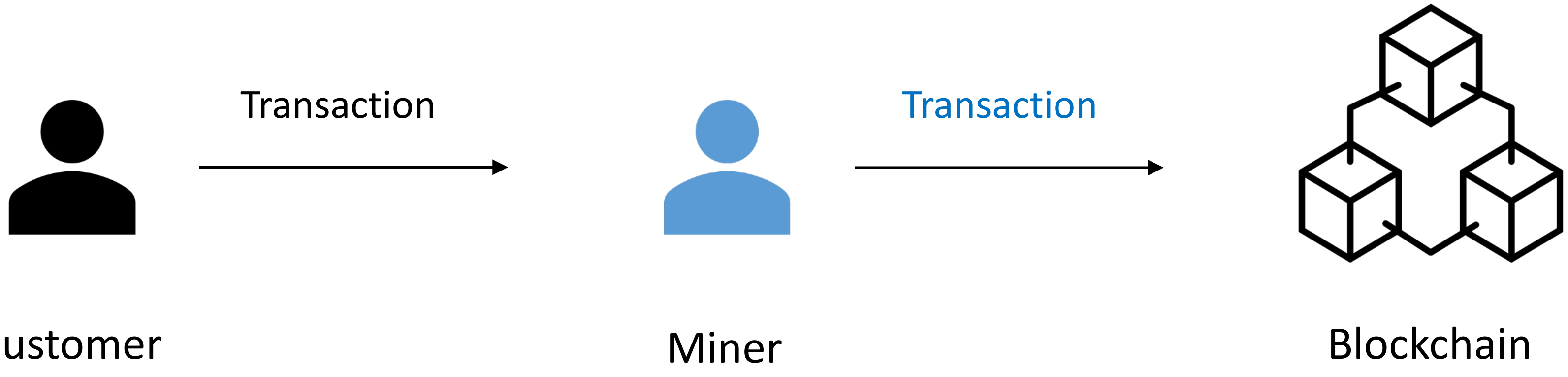
- Front running is the practice of entering into a trade to capitalize on advanced, nonpublic knowledge of a large pending transaction that will influence the price of the underlying security.
- Prohibited practice by regulations.

Blockchain



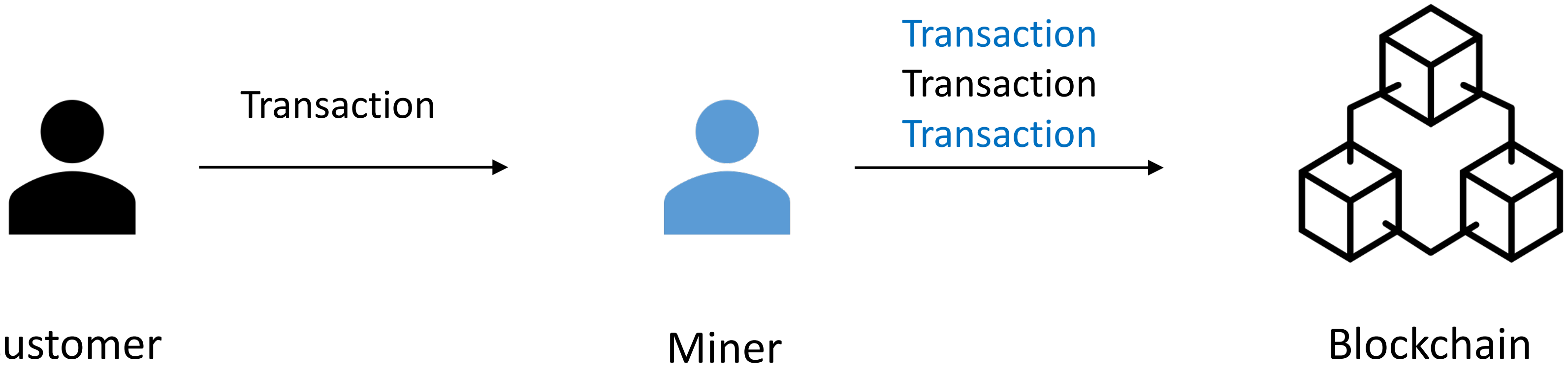
Front-running in Blockchain

Displacement Attack:



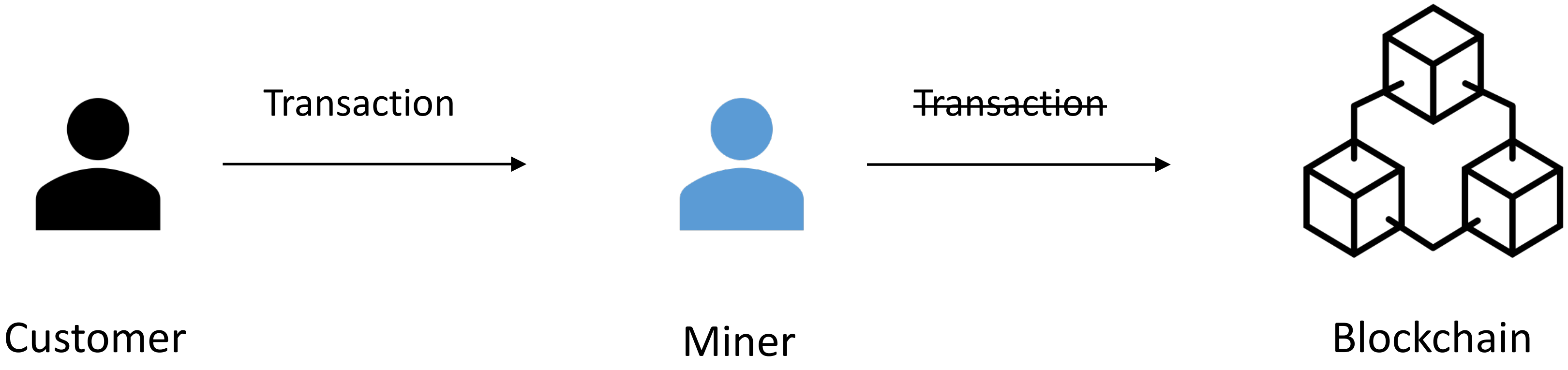
Front-running in Blockchain

Insertion Attack:



Front-running in Blockchain

Suppression Attack:



Transaction

~~Transaction~~

Customer

Miner

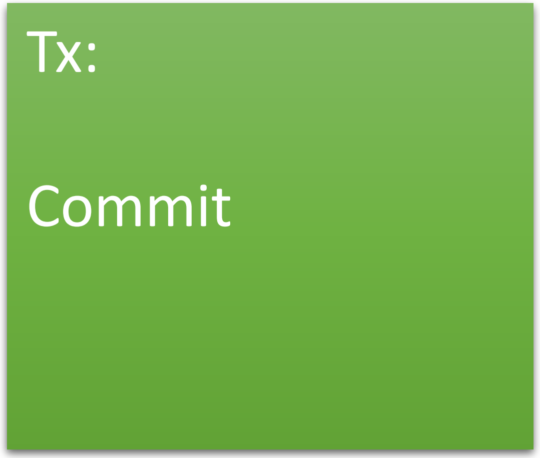
Blockchain

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*.

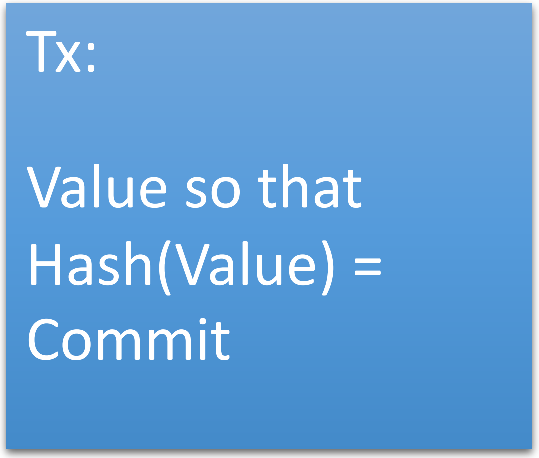
* https://cybernews.com/crypto/flash-boys-2-0-front-runners-draining-280-million-per-month-from-crypto-transactions/

Strawman: Commit-and-Reveal by User



Tx:

Commit



Tx:

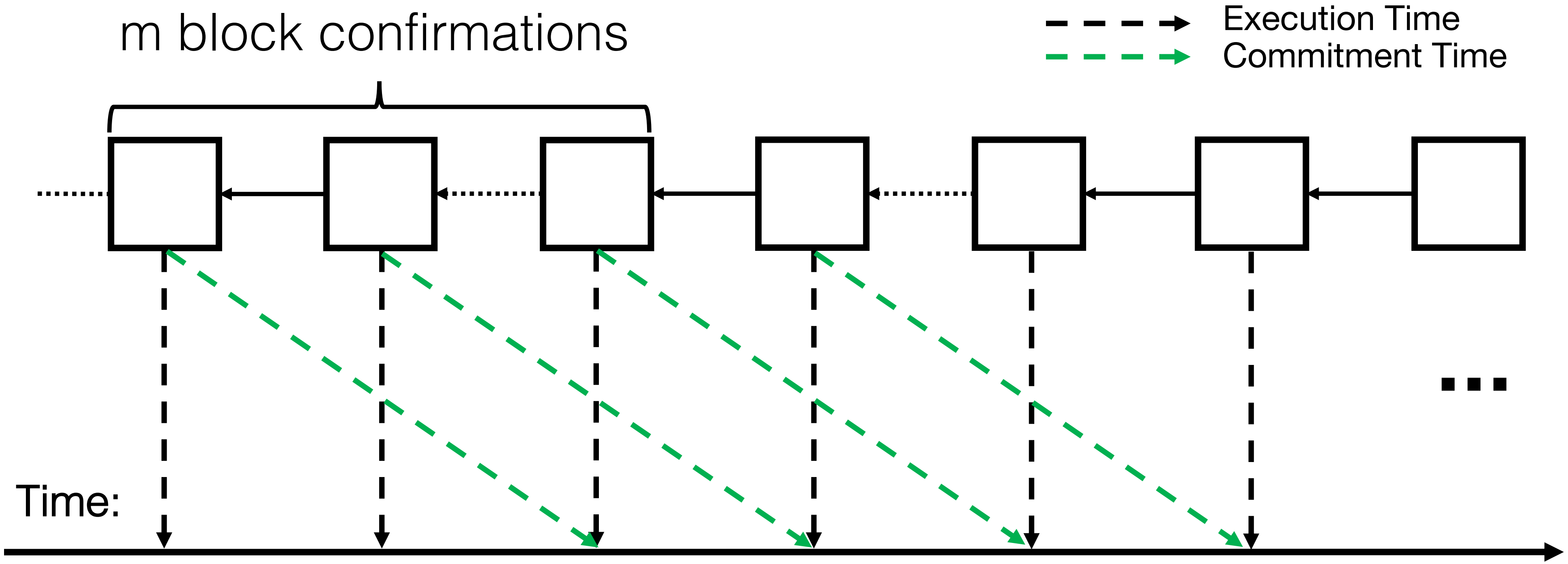
Value so that Hash(Value) = Commit

Drawbacks:

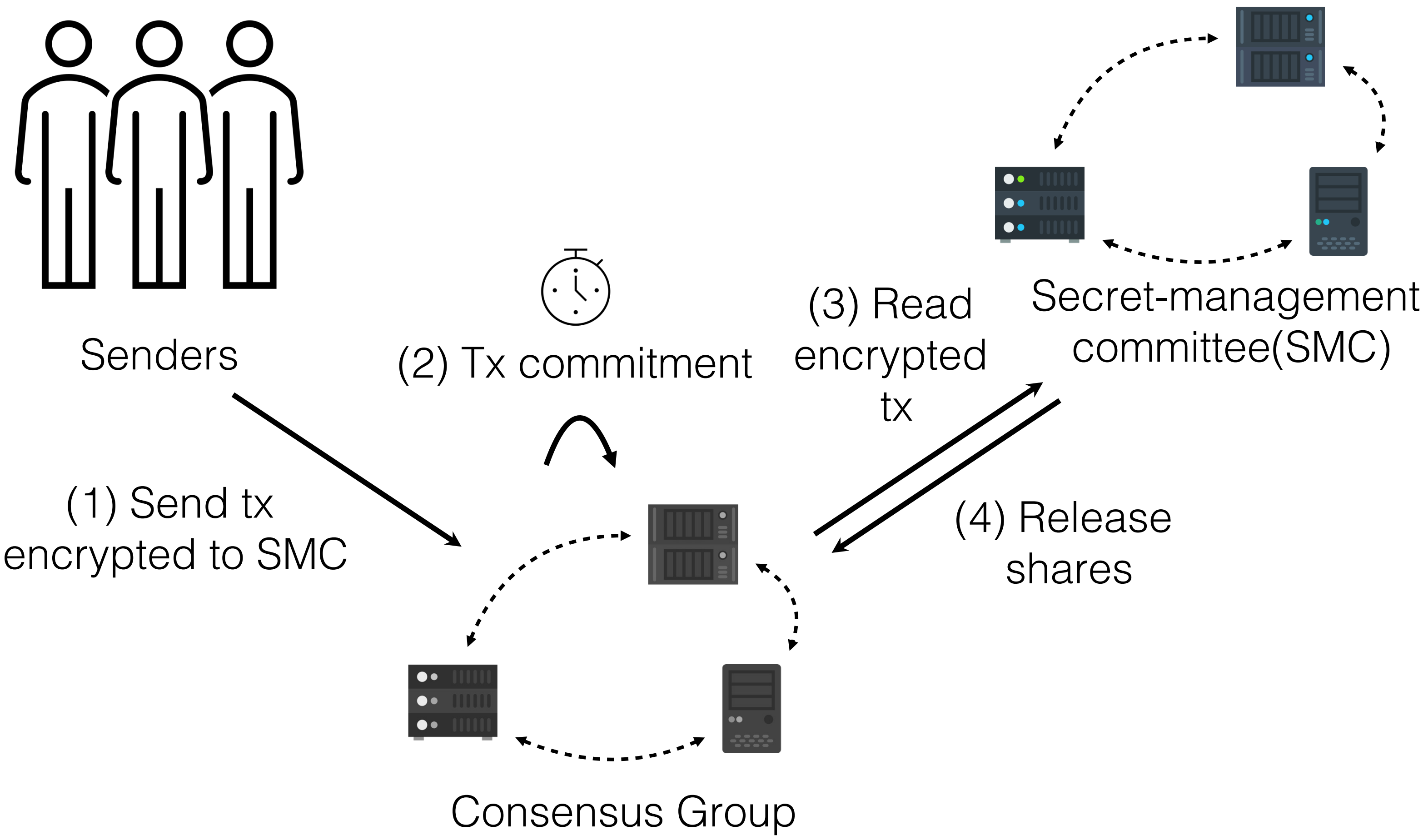
(1) Two transactions

(2) Suppression Attack possible

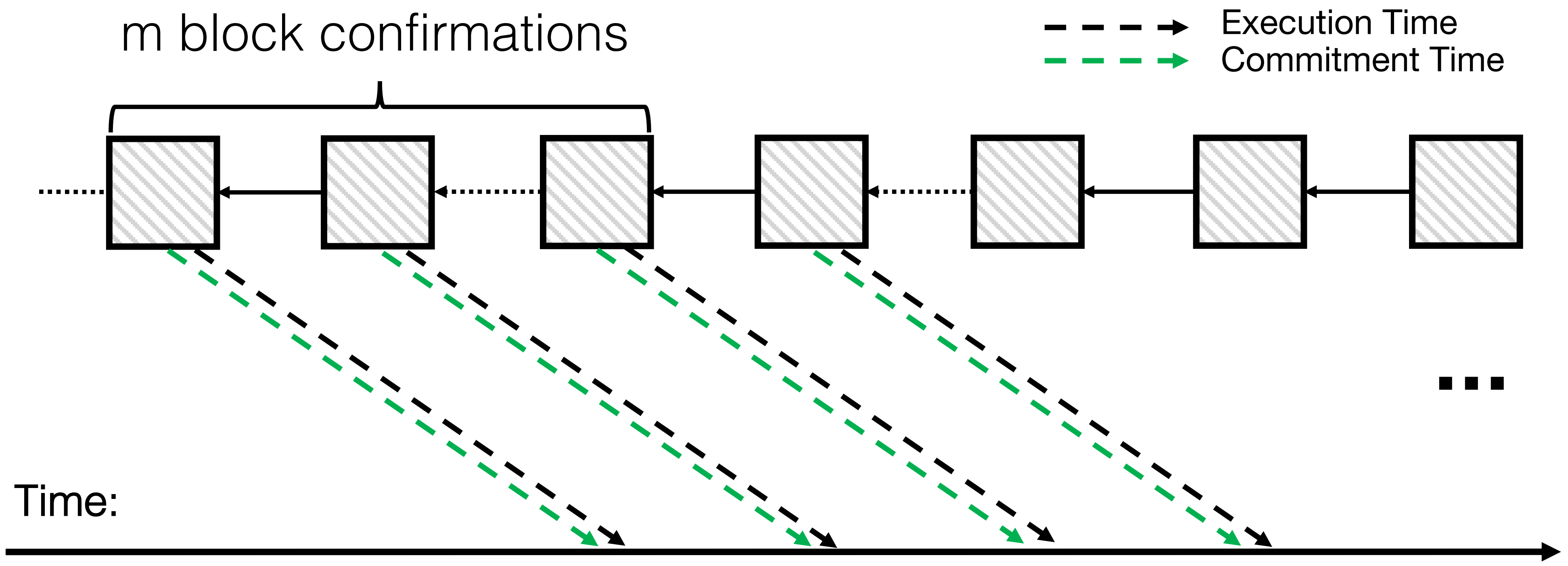
Transaction Commitment



Architecture Overview



F3B


m block confirmations
Execution Time
Commitment Time
...
Time:

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 commitment -> attackers can not benefit from pending transactions.

Per-Transaction Front-Running Protection

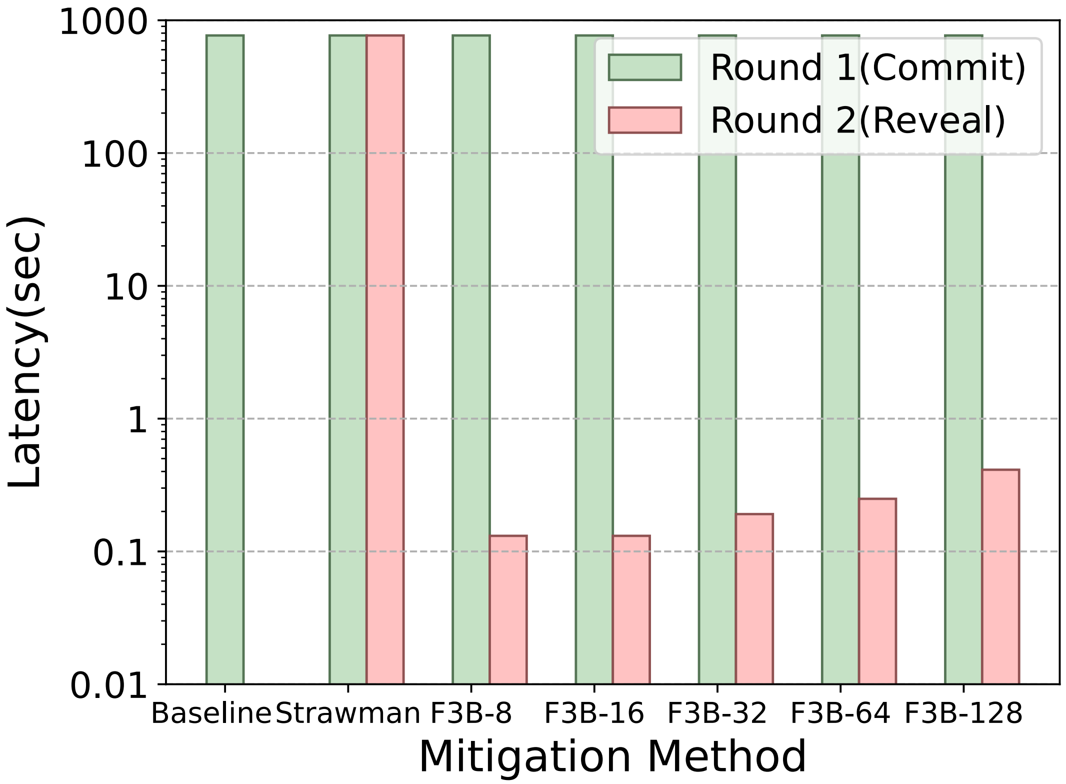
- Rather than threshold encryption with block key
  - Fairblock
  - Shutter
- Transaction can be revealed
  - When it fails to be included in the specified block
  - Congestion
  - DoS attacks

Conclusion

- Front-running is a big issue in blockchain/DeFi
- Mitigates front-running attacks
- Presents low latency overhead
- Requires modification of execution layer

Preprint

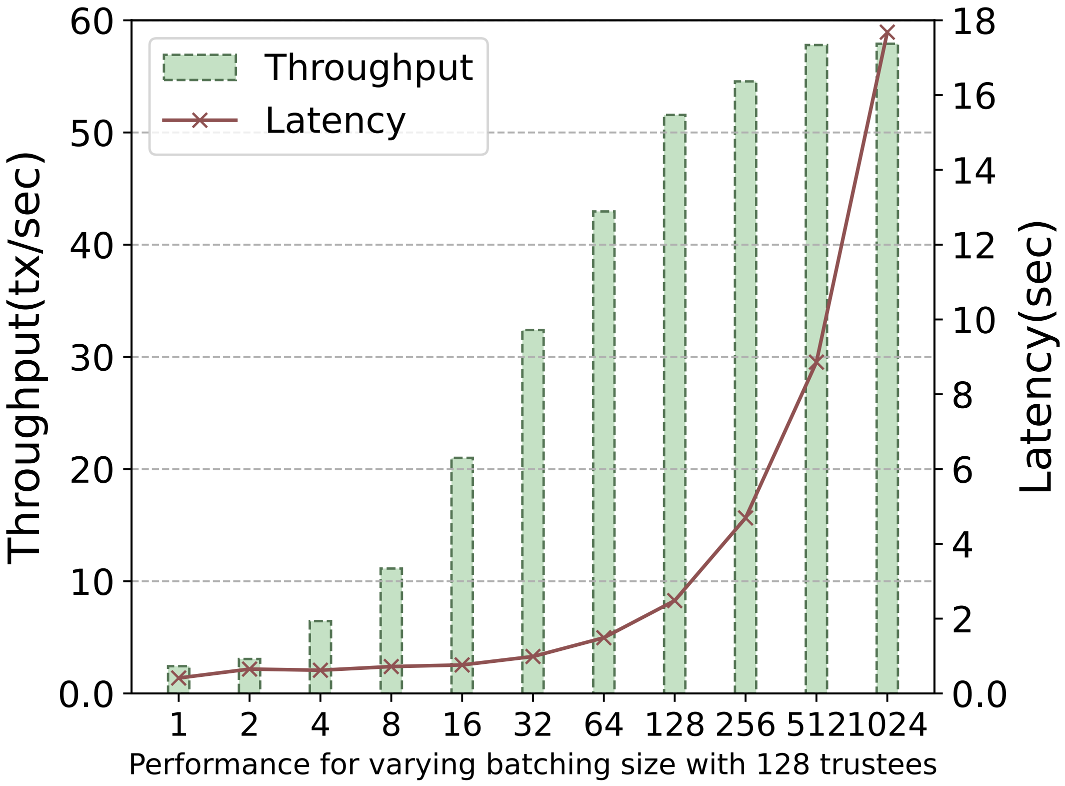
Latency*



- Ethereum
  - Block Time = 12s
  - Block confirmations = 64
  - => Latency = 768s
- F3B with 128 nodes
  - Latency 413ms
  - 0.05% latency overhead in Ethereum

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

Throughput*



Performance for varying batching size with 128 trustees

- Ethereum
  - Around 15 tps
- F3B with 128 nodes
  - 58 tps
  - Latency 8.85 seconds
  - 1.15% latency overhead in Ethereum

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