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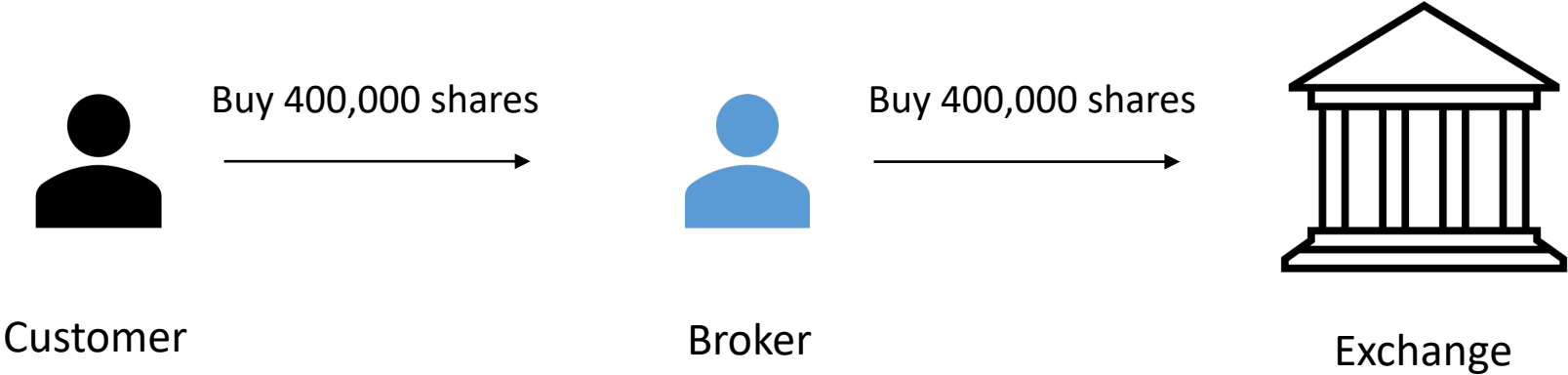
**Haoqian Zhang**

École Polytechnique Fédérale de Lausanne (EPFL)

# Outline

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

# Traditional Exchange



Customer — Buy 400,000 shares → Broker — Buy 400,000 shares → Exchange

# Front-running in Traditional Exchange

Customer

Buy 400,000 shares

Broker

Buy 20,000 shares
Buy 400,000 shares
Sell 20,000 shares

Exchange

# Front-running in Traditional Exchange

- Front running is the practice of entering into a trade to capitalize on advanced, <span style="color:red">nonpublic knowledge</span> of a large <span style="color:red">pending transaction</span> that will influence the price of the underlying security.
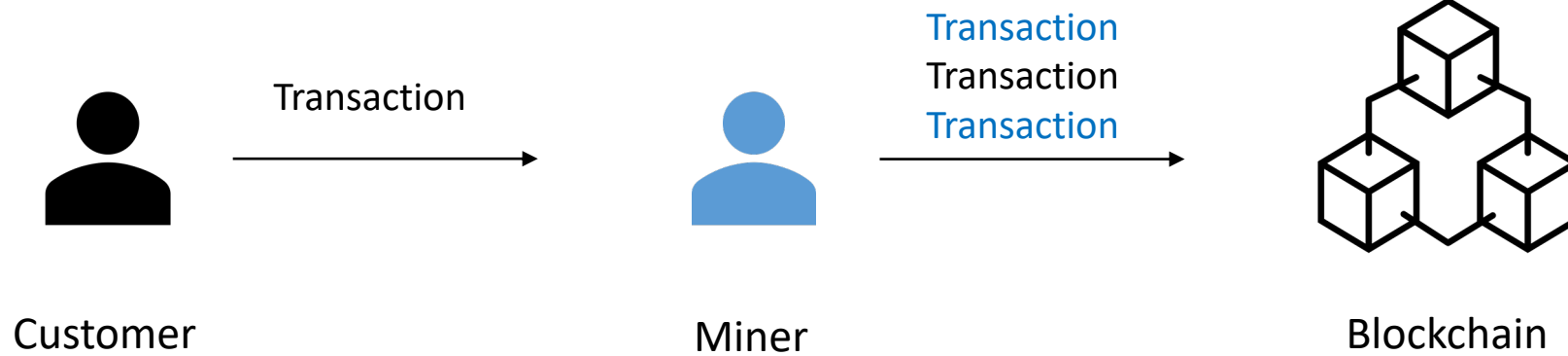
- Prohibited practice by regulations.

# Blockchain

Customer → Transaction → Miner → Transaction → Blockchain
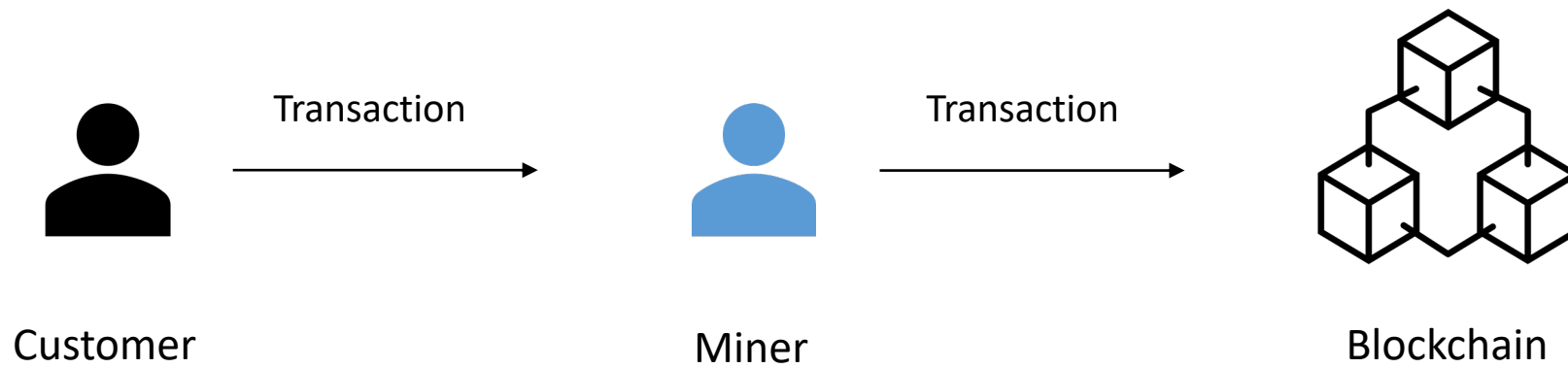
# Front-running in Blockchain

Displacement Attack:

Customer → Transaction → Miner → Transaction → Blockchain

# Front-running in Blockchain

Insertion Attack:



Customer → Transaction → Miner → Transaction / Transaction / Transaction → Blockchain

# Front-running in Blockchain

Suppression Attack:

Customer    → Transaction →    Miner    → ~~Transaction~~ →    Blockchain
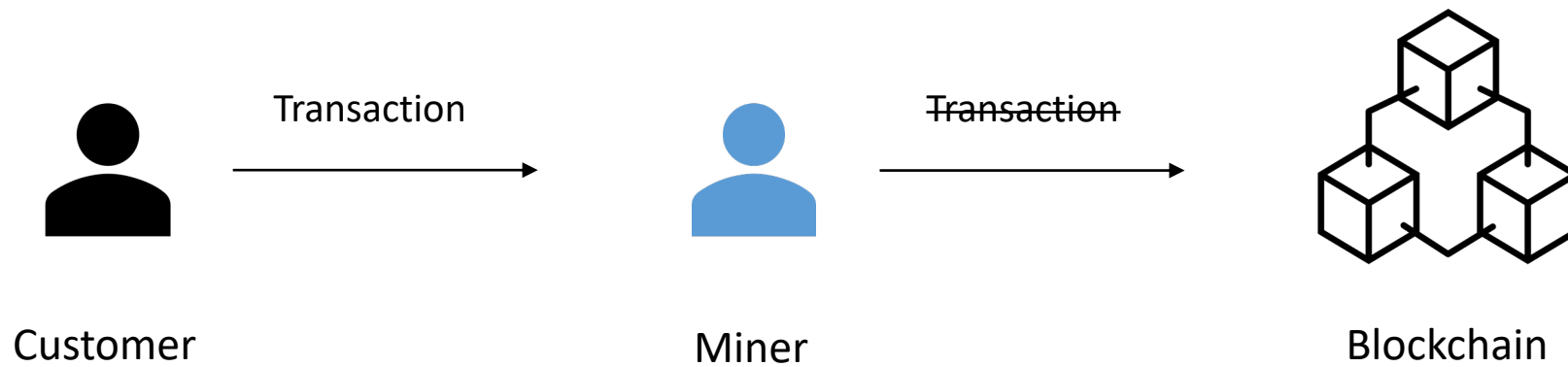
# Front-running in Blockchain

- 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*.
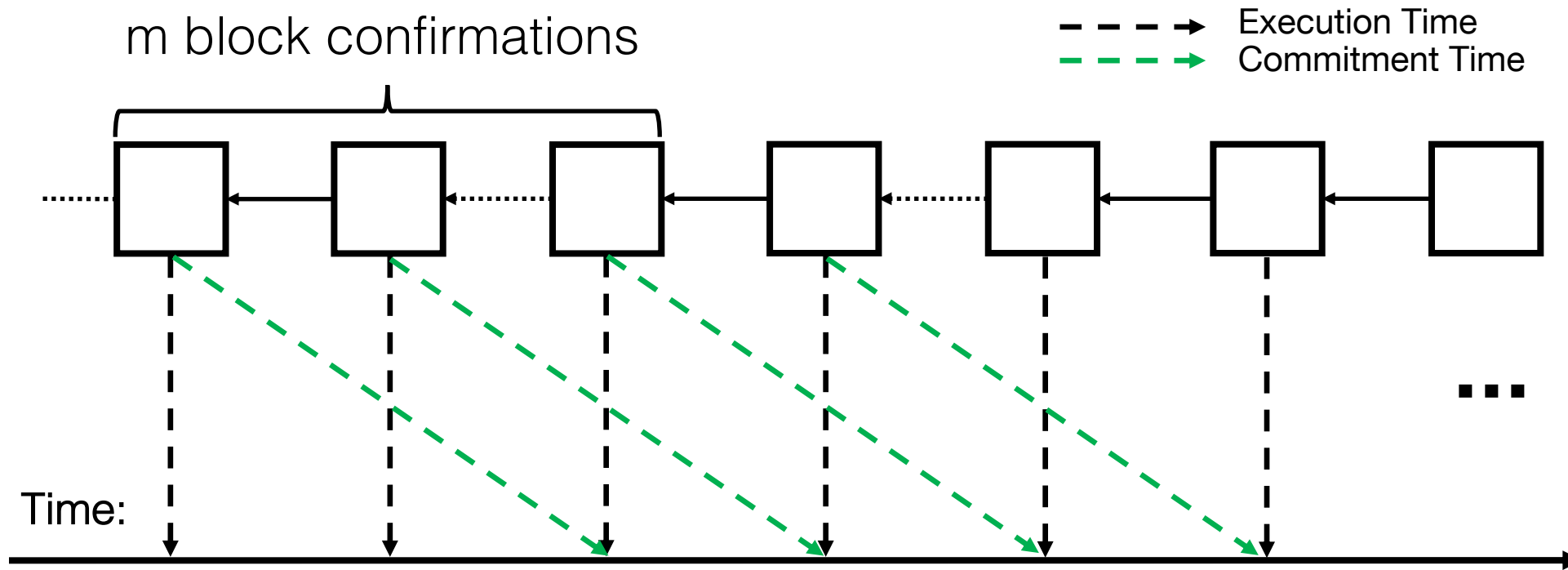
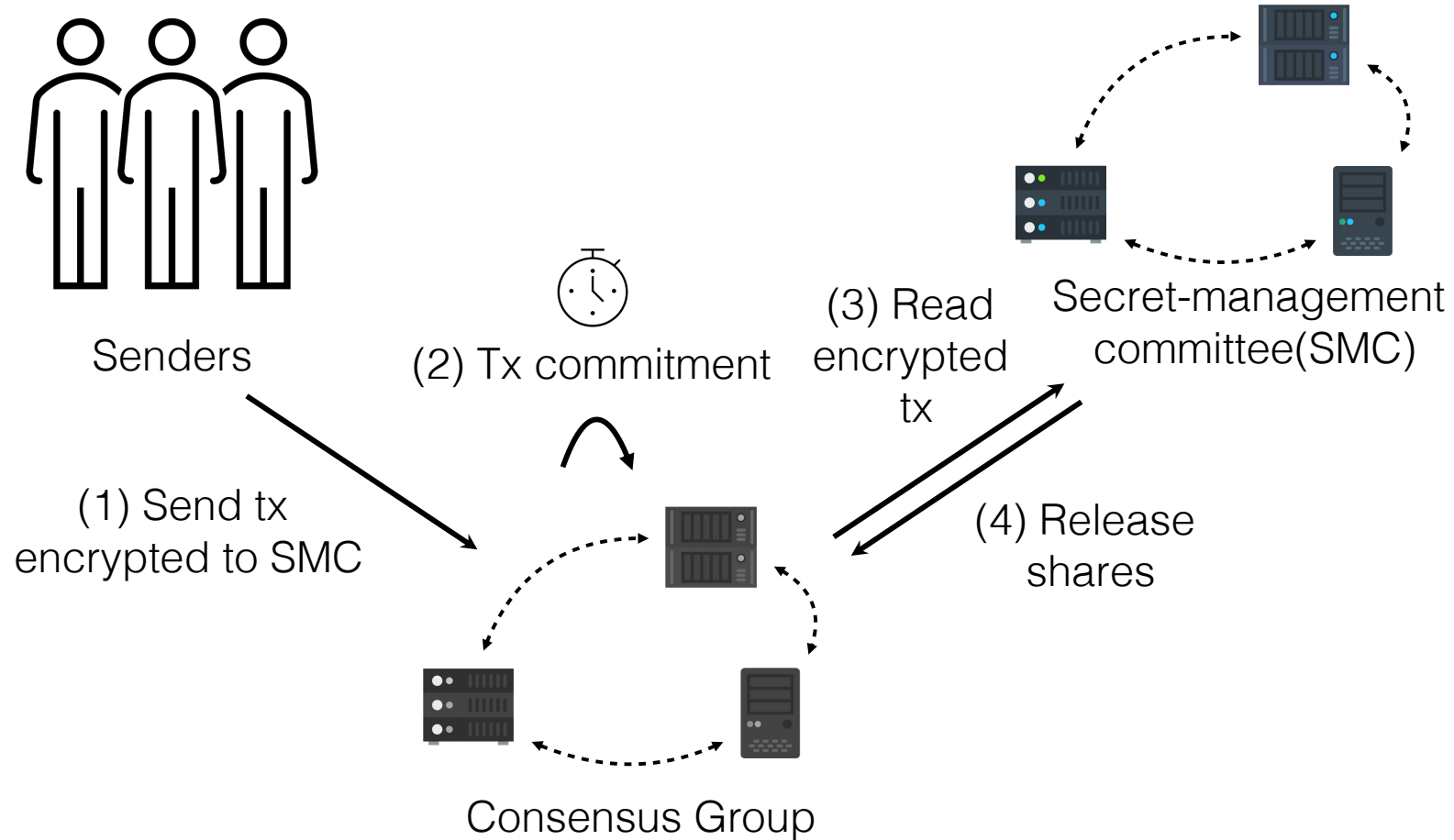# Strawman: Commit-and-Reveal by User

Tx:

Commit

Tx:

Value so that
Hash(Value) =
Commit

Drawbacks:

(1) Two transactions

(2) Suppression Attack possible

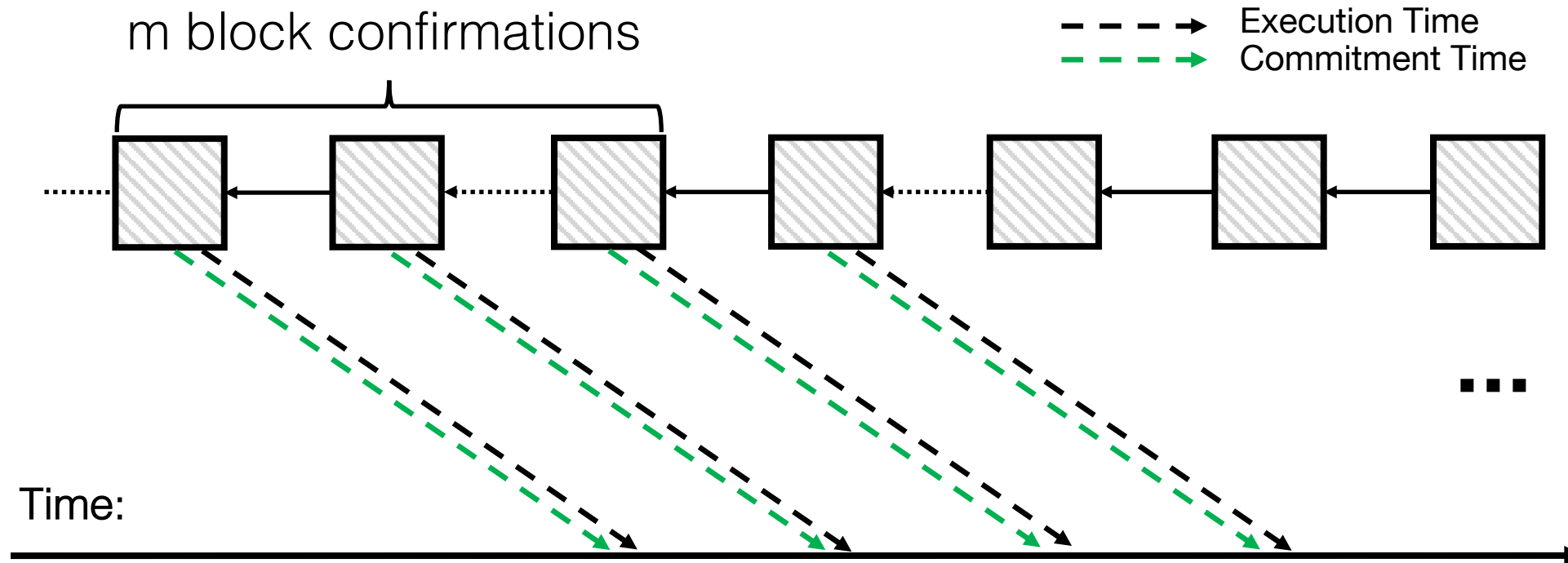# Transcription Commitment

# Architecture Overview



Senders

(2) Tx commitment

(3) Read encrypted tx

Secret-management committee(SMC)

(1) Send tx encrypted to SMC

(4) Release shares

Consensus Group

# F3B



Legend:
- Execution Time (black dashed arrow)
- Commitment Time (green dashed arrow)

m block confirmations

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.
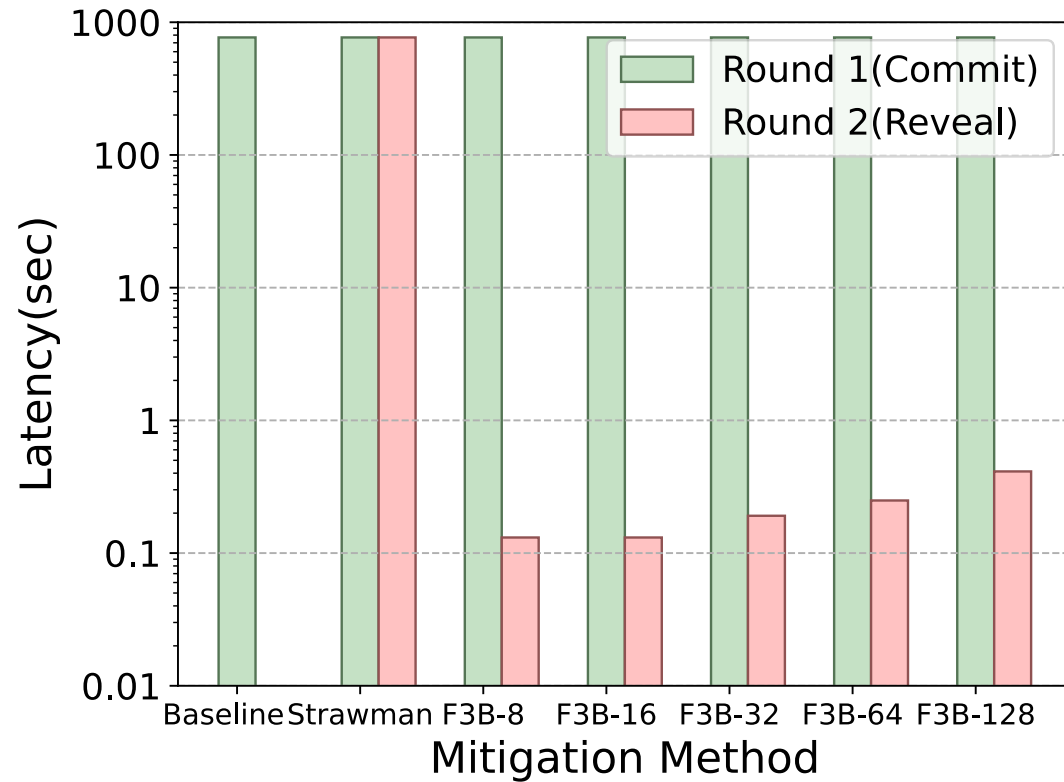
# Per-Transaction Front-Running Protection

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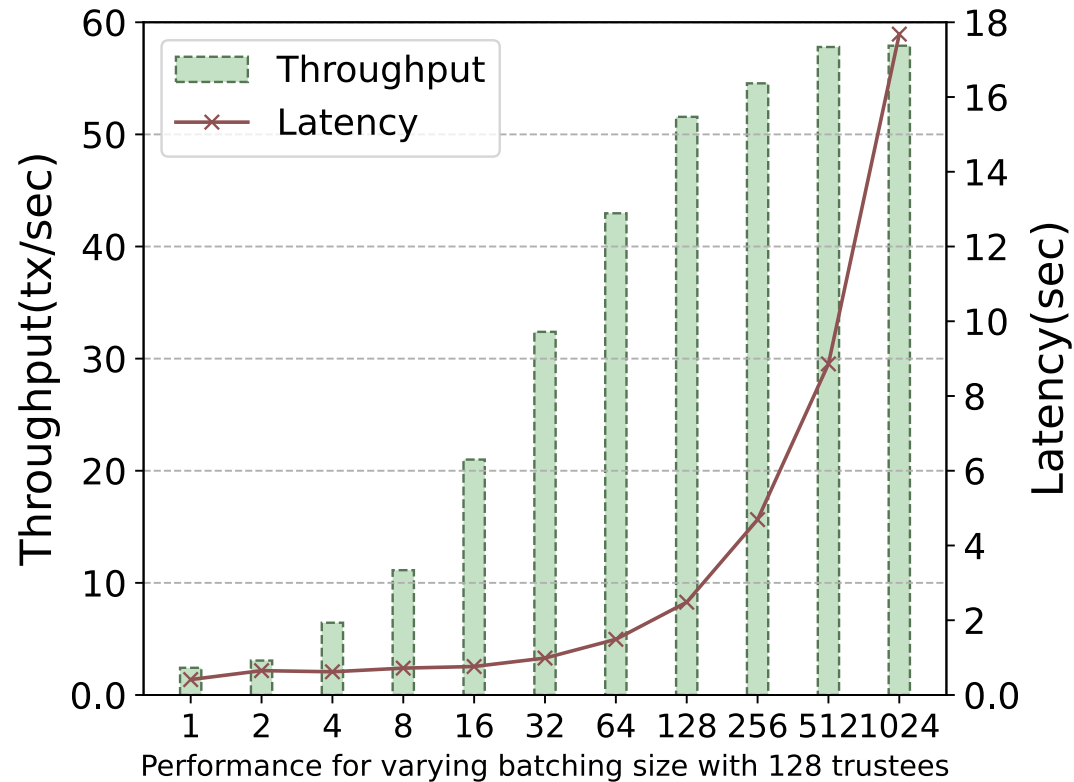  - DoS attacks

# F3B with Ethereum
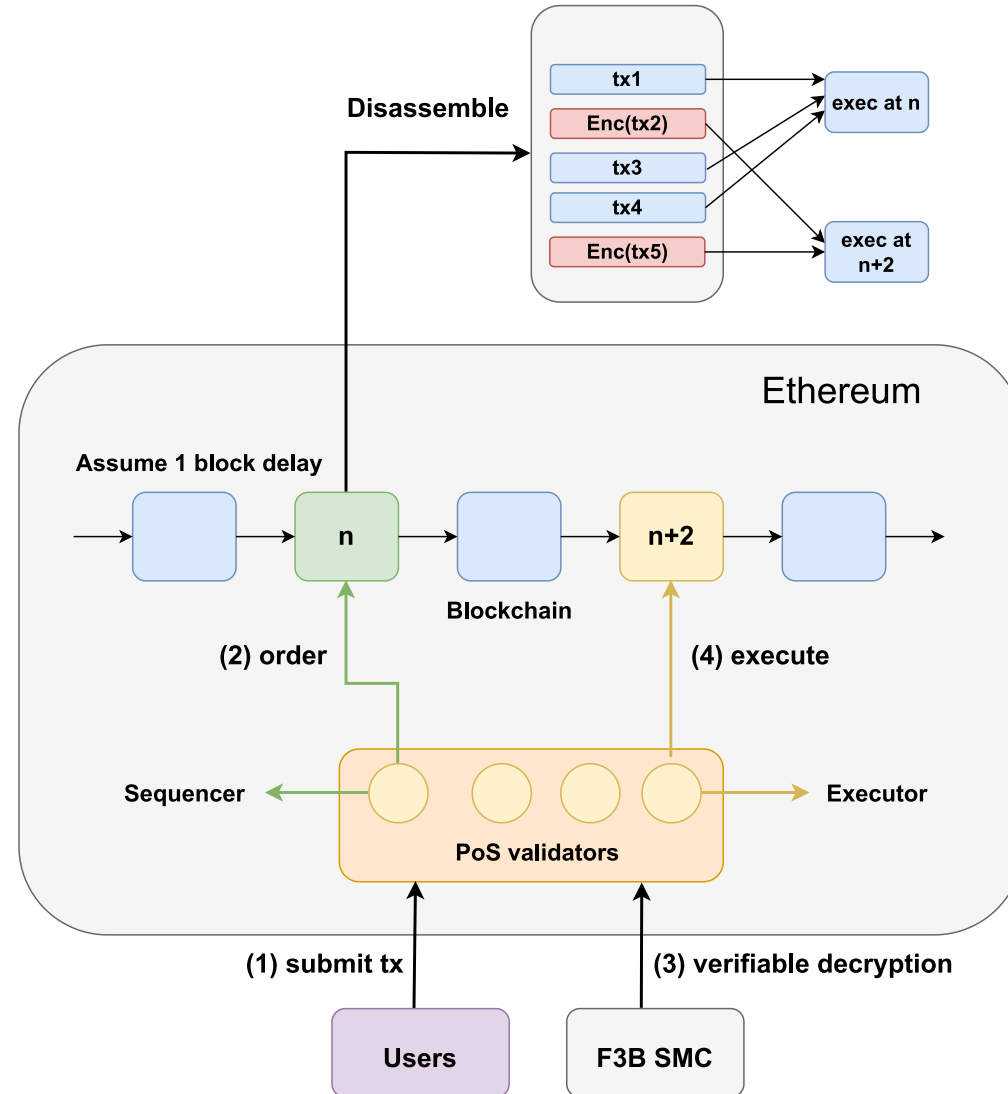
# Latency



- 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.

# Conclusion

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



Preprint