Flash Freezing Flash Boys: Countering Blockchain Front-Running

Haoqian Zhang, Louis-Henri Merino,

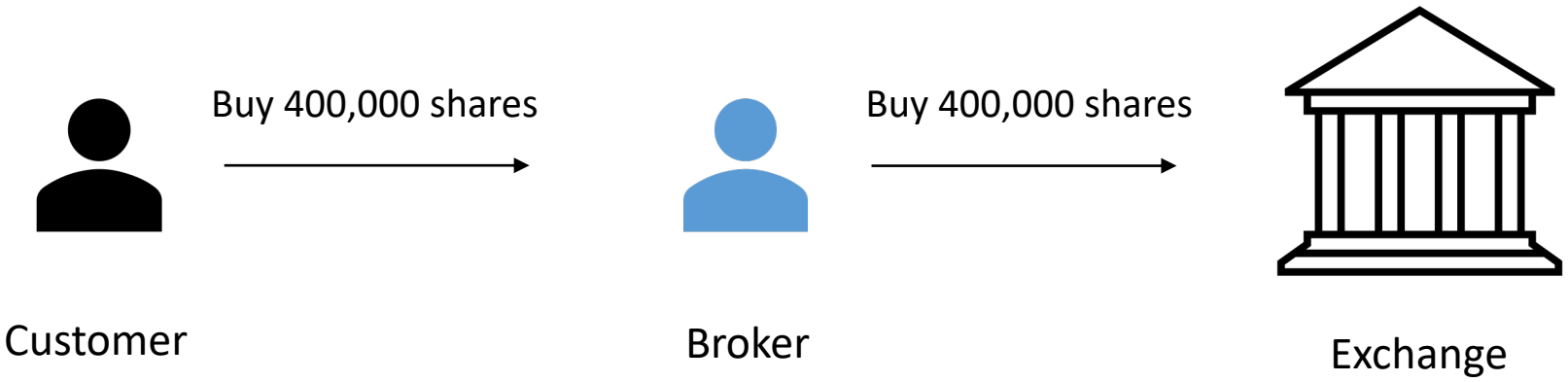
Vero Estrada-Galiñanes and Bryan Ford

École Polytechnique Fédérale de Lausanne (EPFL)

Outline

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

Traditional Exchange

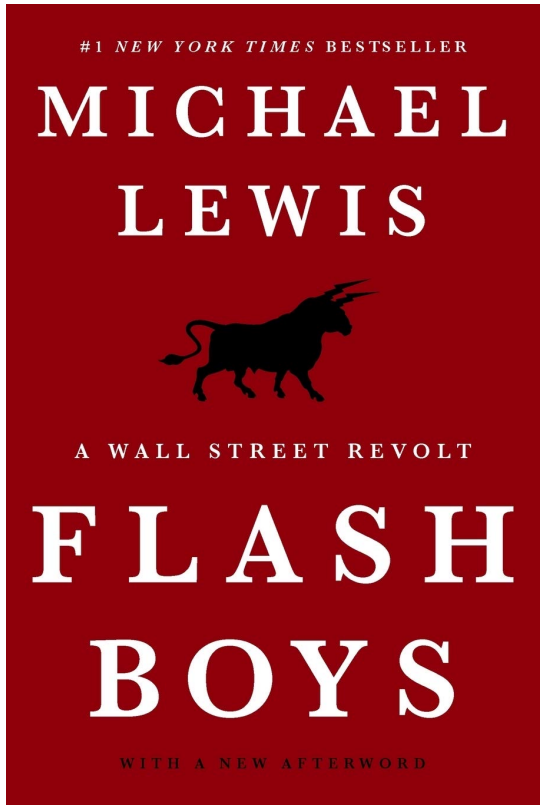


Front-running in Traditional Exchange

Front-running in Traditional Exchange

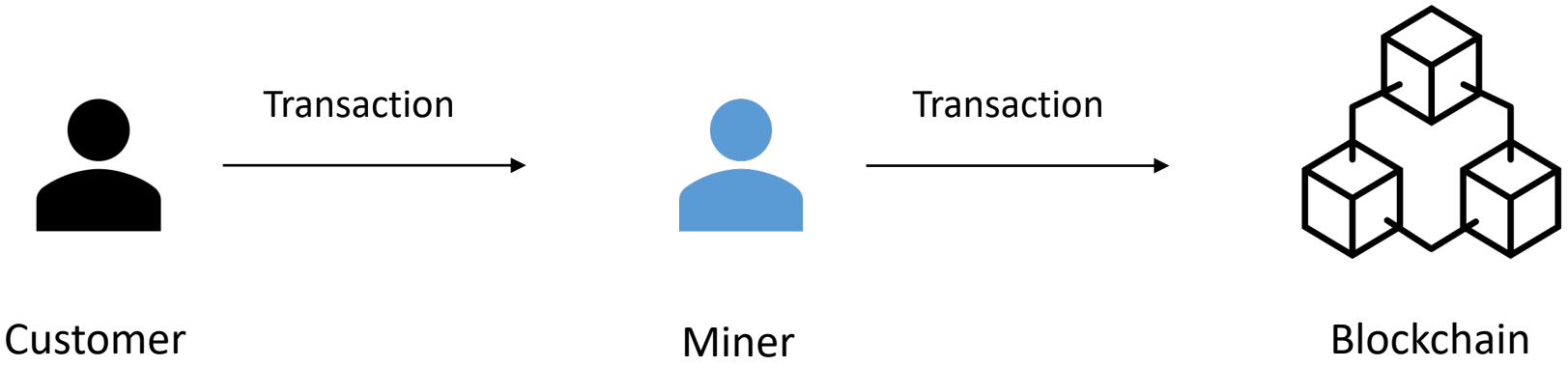
- Front running is the practice of entering into a trade to capitalize on advanced, nonpublic knowledge of a large pending transaction that will influence the price of the underlying security.
- Prohibited practice by regulations.

Flash Boys


#1 NEW YORK TIMES BESTSELLER
MICHAEL LEWIS
A WALL STREET REVOLT
FLASH BOYS
WITH A NEW AFTERWORD


JESSE EISENBERG
ALEXANDER SKARSGÅRD
AND SALMA HAYEK
EVERYTHING IS ON THE LINE.
THE HUMMINGBIRD PROJECT

Blockchain

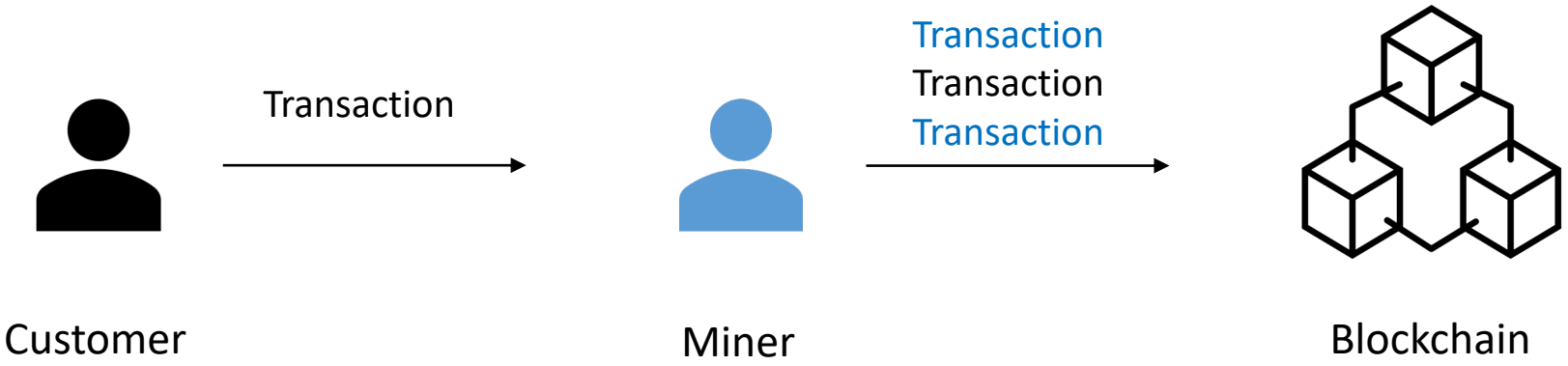


Front-running in Blockchain

Displacement Attack:

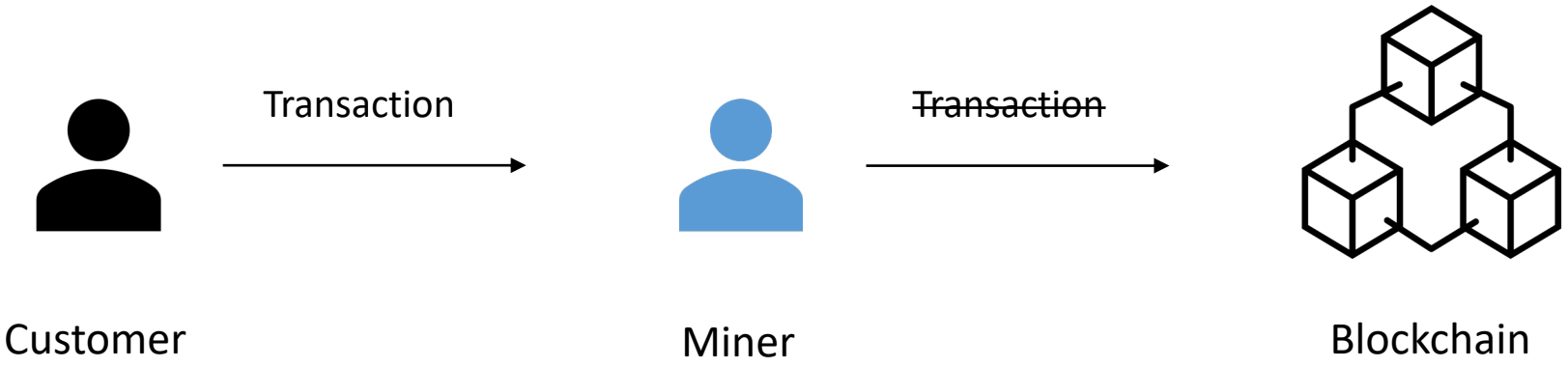
Front-running in Blockchain

Insertion Attack:



Front-running in Blockchain

Suppression Attack:

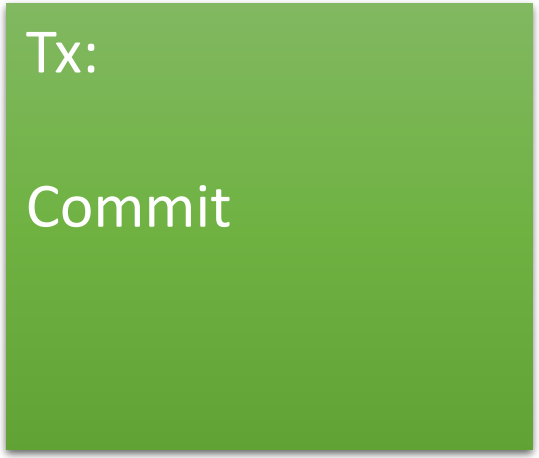


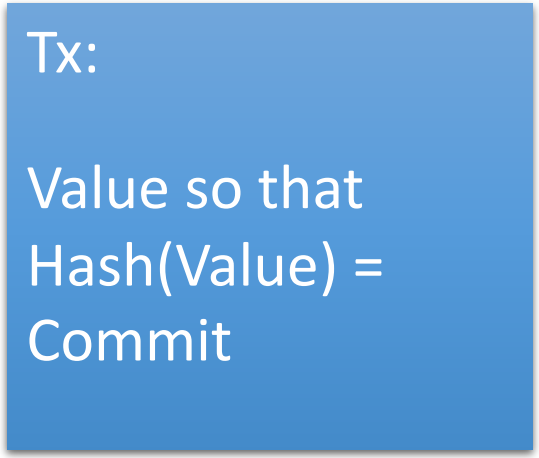
Front-running in Blockchain

- 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



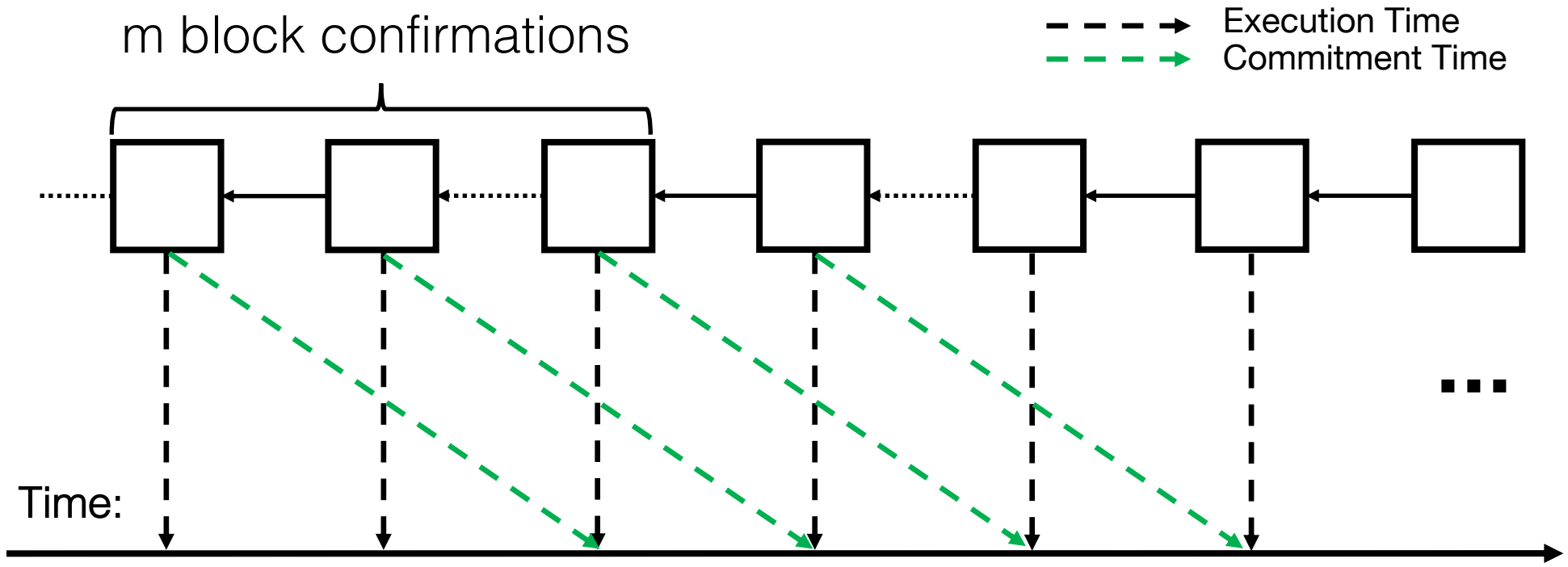


Drawbacks:

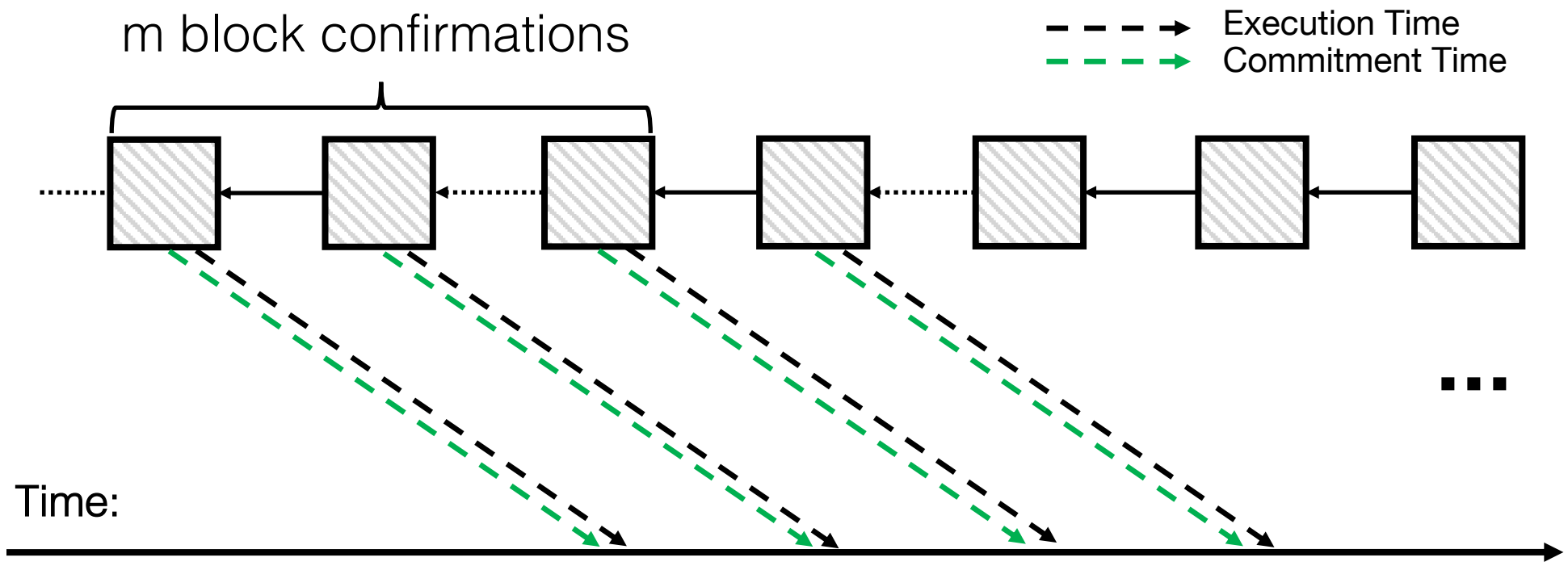
(1) Two transactions

(2) Suppression Attack possible

Transaction Commitment



F3B: Supporting encrypted transactions*

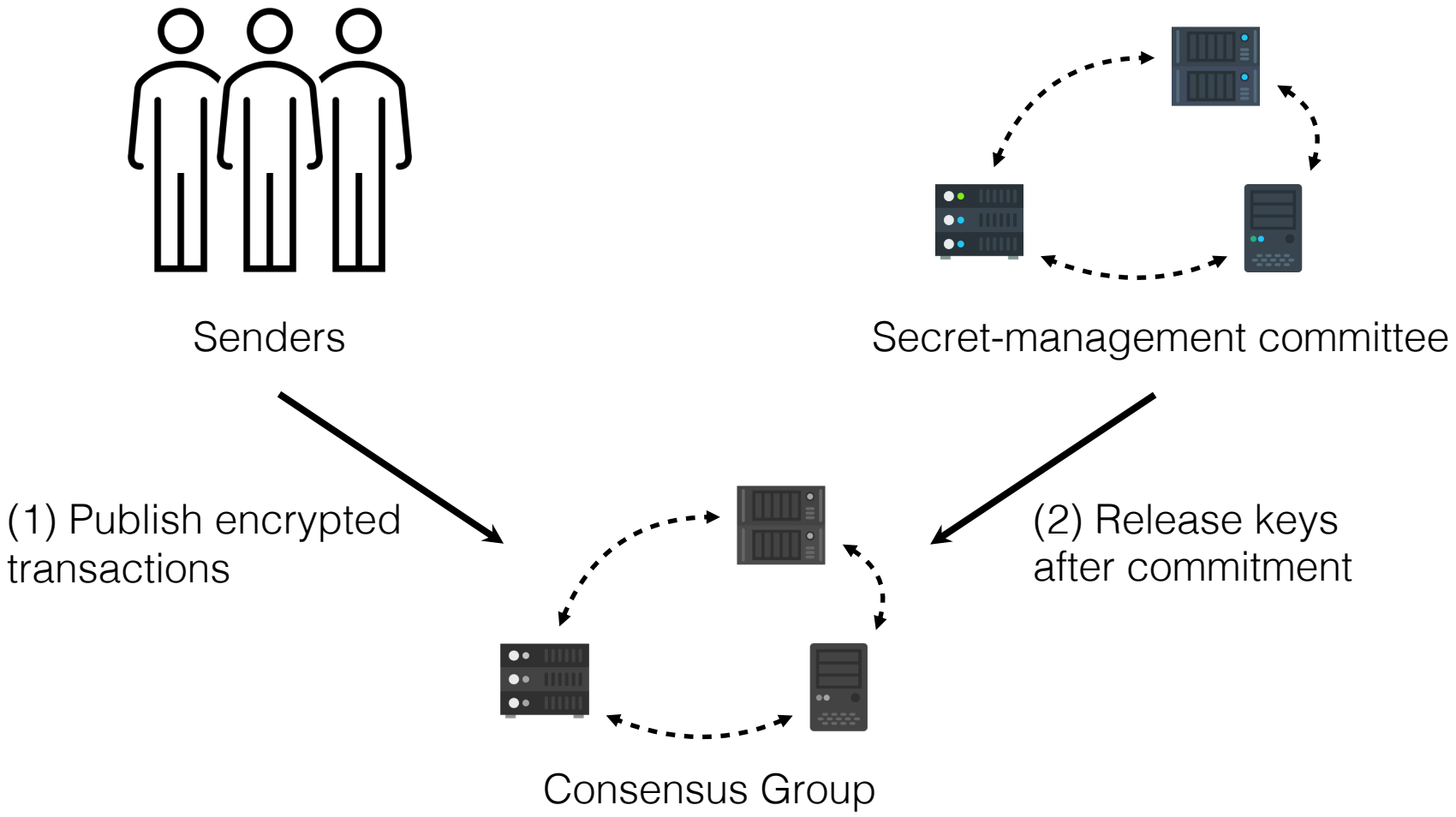


* Requires the modification at the blockchain architecture layer.

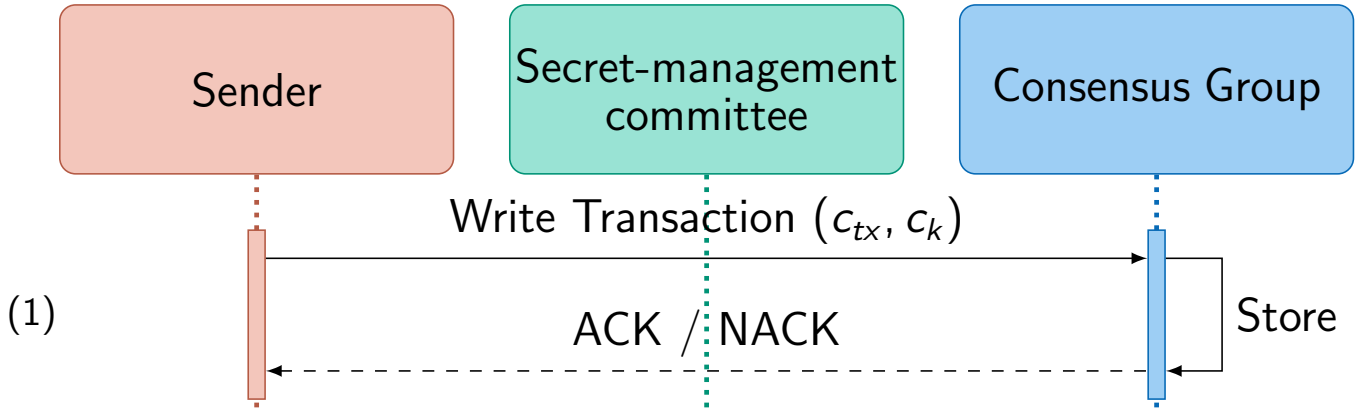
How does F3B mitigate front-running

- 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.

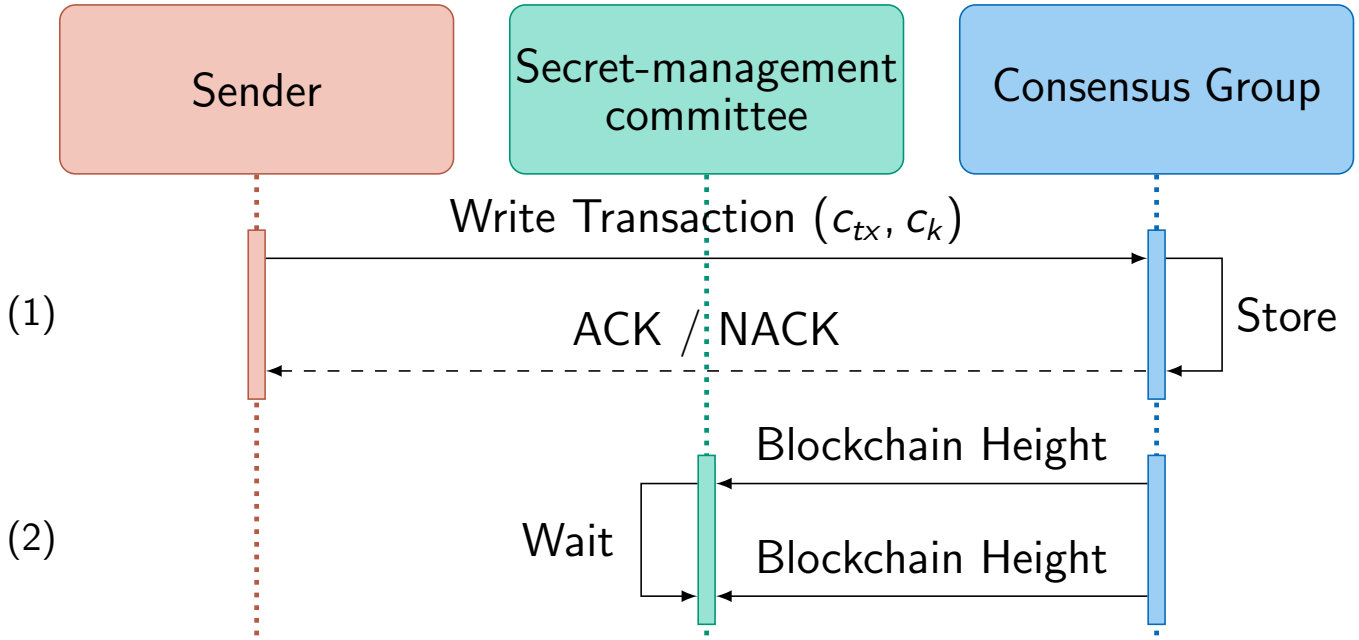
Architecture Overview



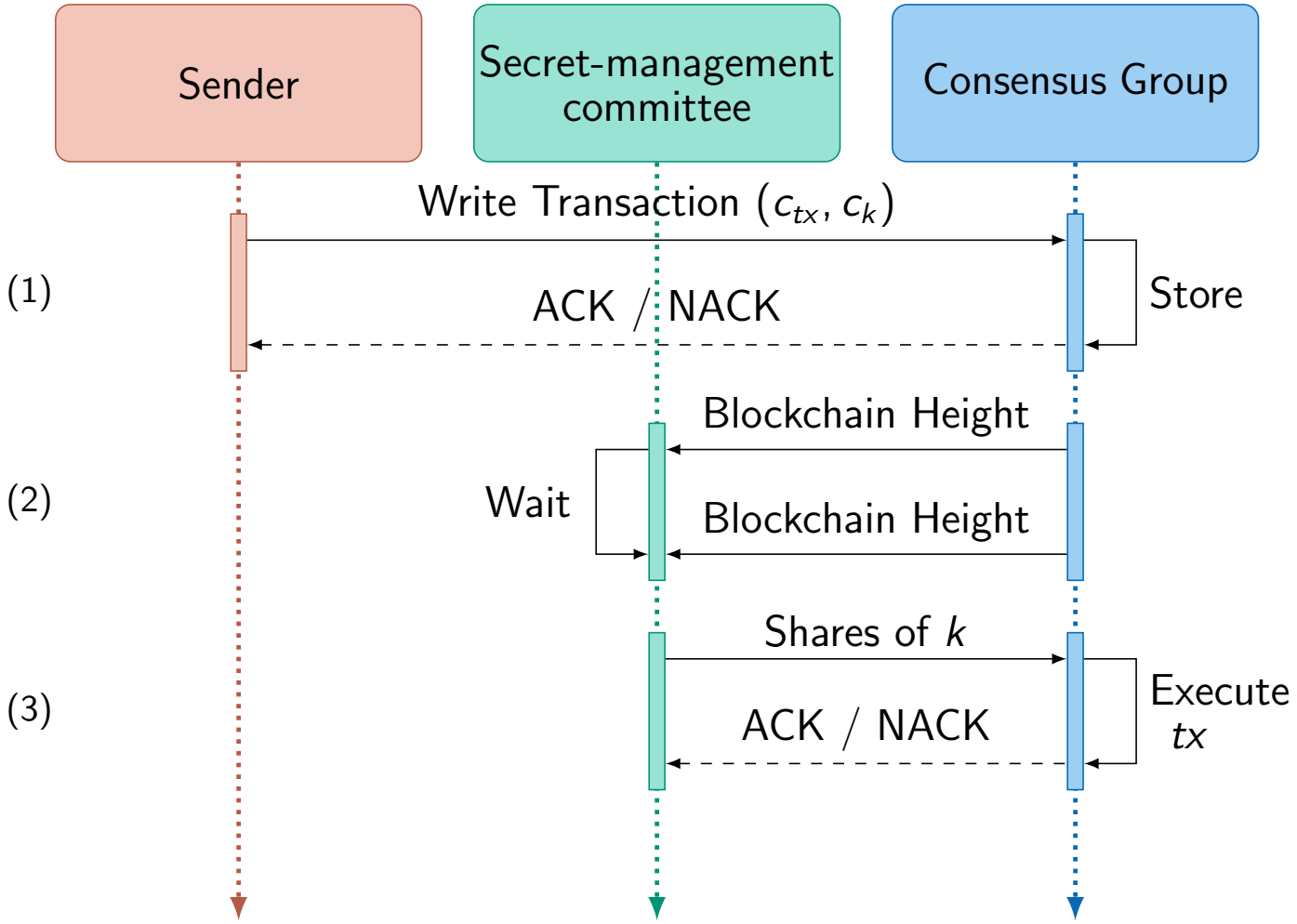
Protocol


Sender
Secret-management committee
Consensus Group
Write Transaction (c_{tx}, c_k)
(1)
ACK / NACK
Store

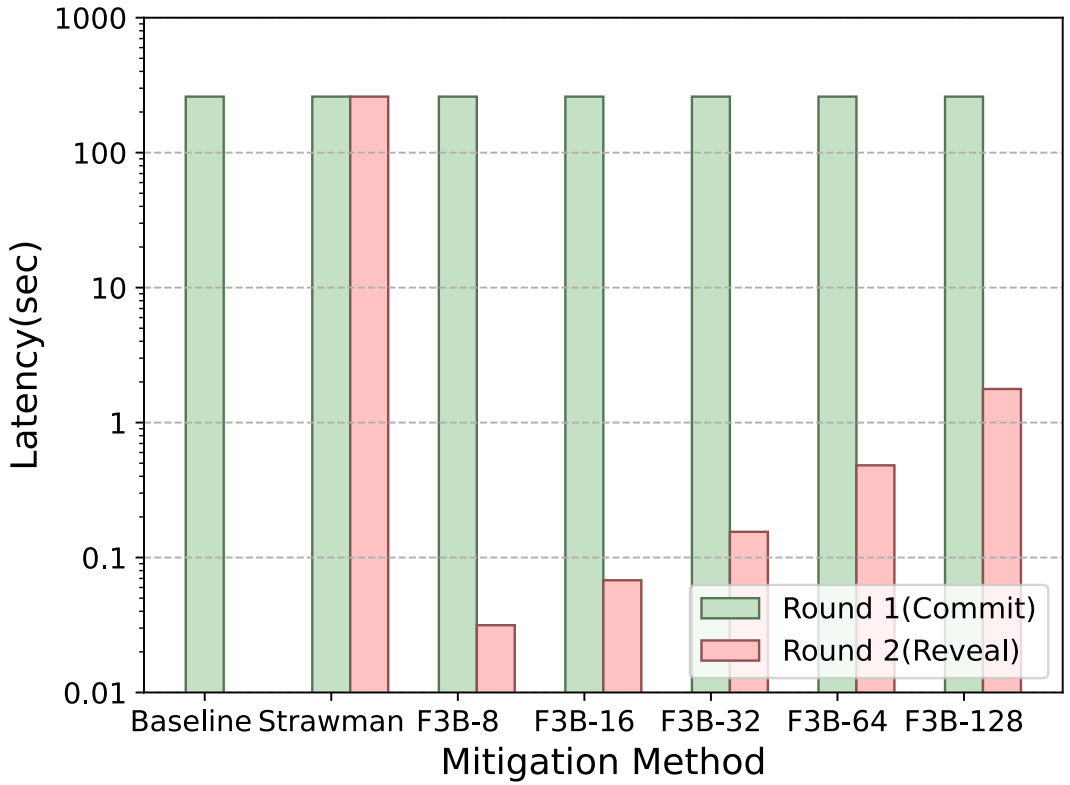
Protocol


Sender
Secret-management committee
Consensus Group
Write Transaction (c_{tx}, c_k)
(1)
ACK / NACK
Store
Blockchain Height
(2)
Wait
Blockchain Height

Protocol


Sender
Secret-management committee
Consensus Group
Write Transaction (c_{tx}, c_k)
(1)
ACK / NACK
Store
Blockchain Height
(2)
Wait
Blockchain Height
Shares of k
(3)
ACK / NACK
Execute tx

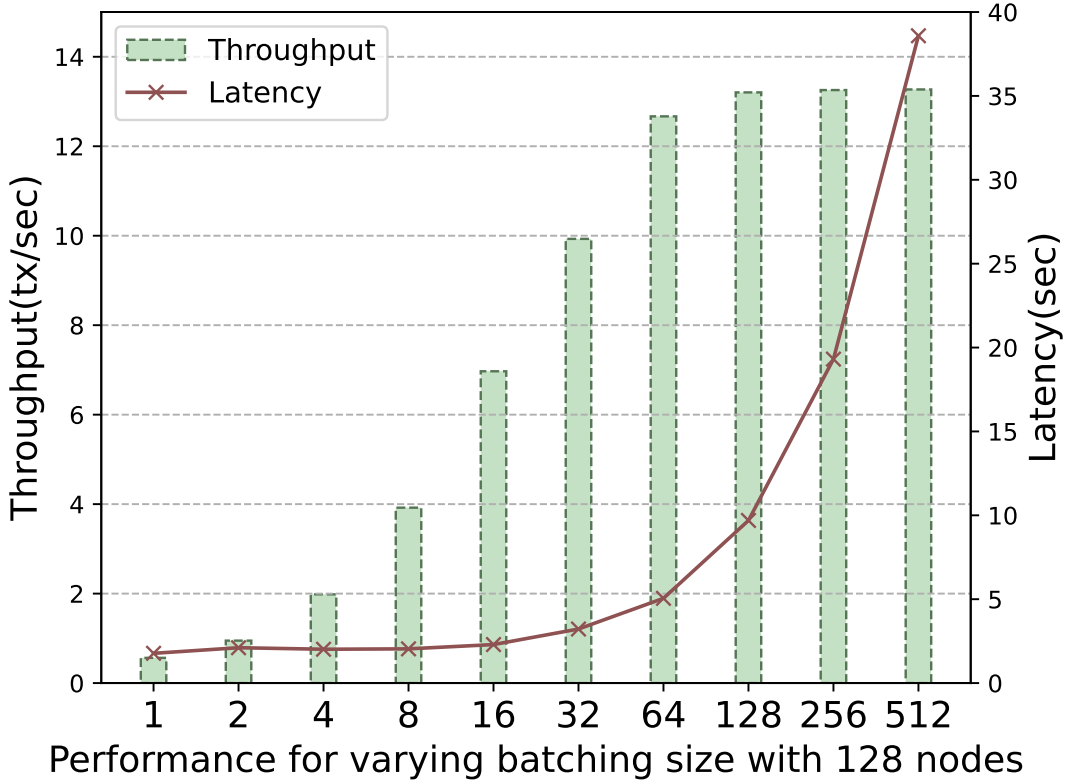
Latency*



- Ethereum
  - Block Time = 13s
  - Block confirmations = 20
  - => Latency = 260s
- F3B with 128 nodes
  - Latency 1.77s
  - 0.68% latency overhead in Ethereum

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

Throughput*



- Ethereum
  - Around 15tps
- F3B with 128 nodes
  - 13.2tps
  - Latency 9.7 seconds
  - 3.7% 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
- Requires modification of blockchain architecture
- Presents low latency overhead

Latency Result