Seahorse

Efficiently Mixing Encrypted and Normal Transactions

Alberto Sonnino

MEV

- On fast blockchains?
- On DAG-Based systems?

MEV: exciting stuff

BREAKING ‼️ @ShioLabs proved guilty of introducing sandwitch attacks on Sui

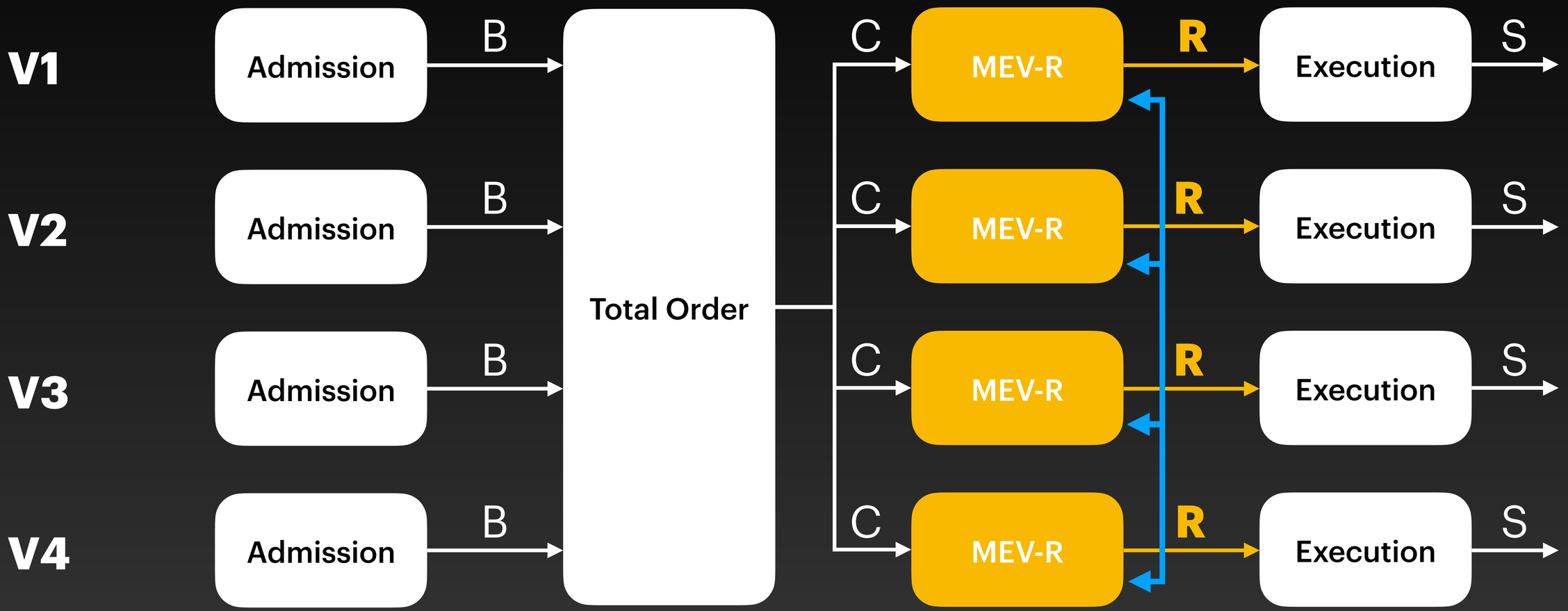
Byzantine Fault Tolerance

Byzantine Fault Tolerance

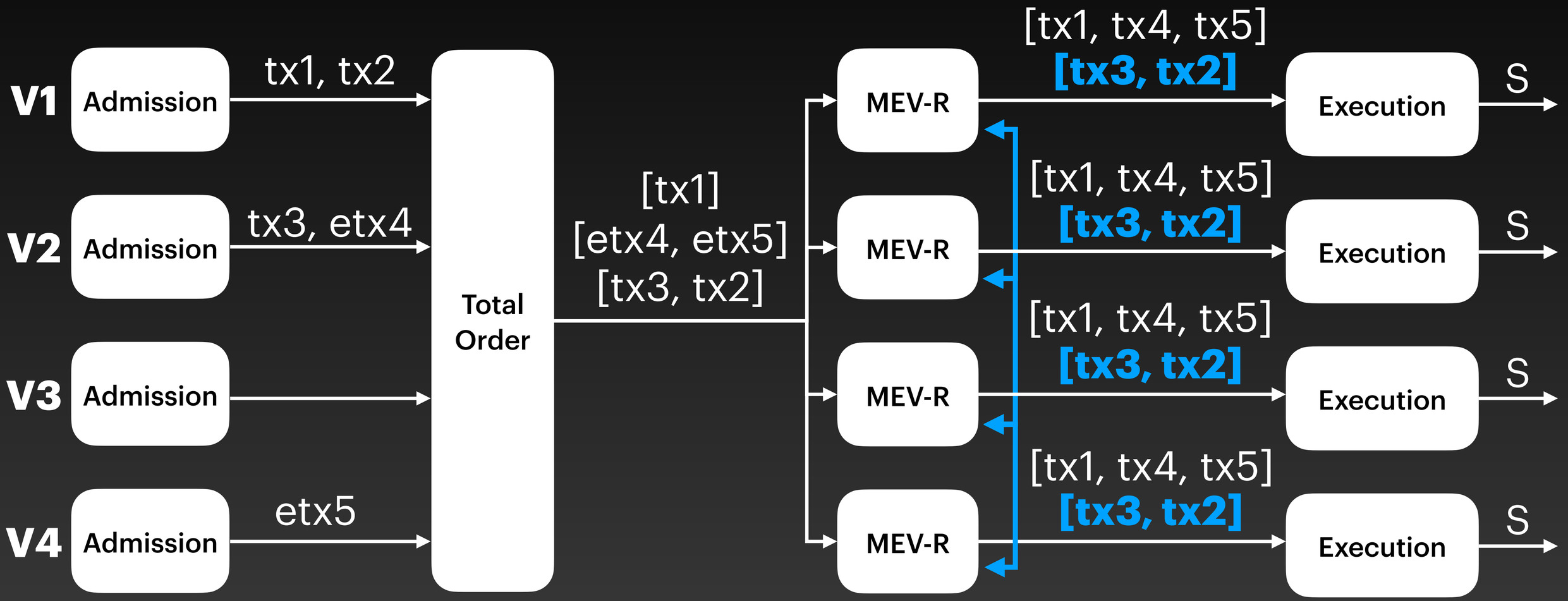
Delay Duration

Additional latency imposed on normal transactions that follow encrypted ones

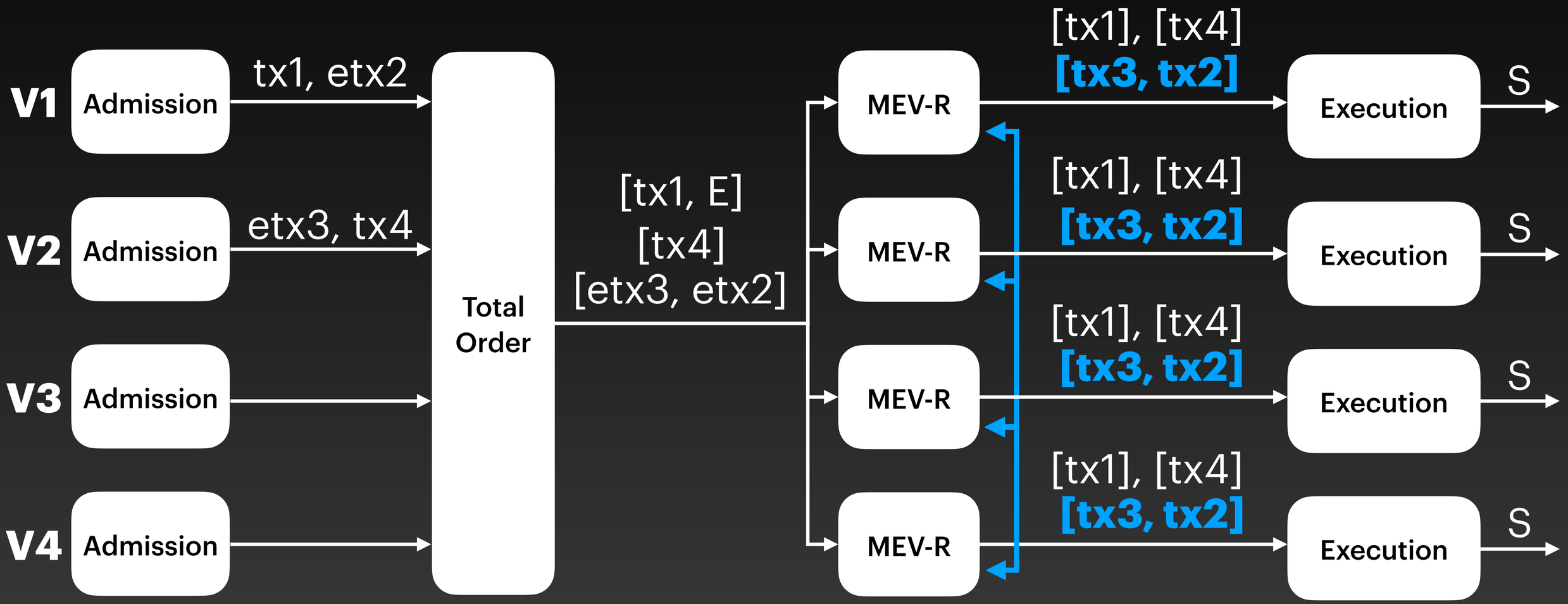
Shared Key


V1
V2
V3
V4
Admission
Admission
Admission
Admission
B
B
B
B
Total Order
C
C
C
C
MEV-R
MEV-R
MEV-R
MEV-R
R
R
R
R
Execution
Execution
Execution
Execution
S
S
S
S

Solution 1: Per-Tx Decryption

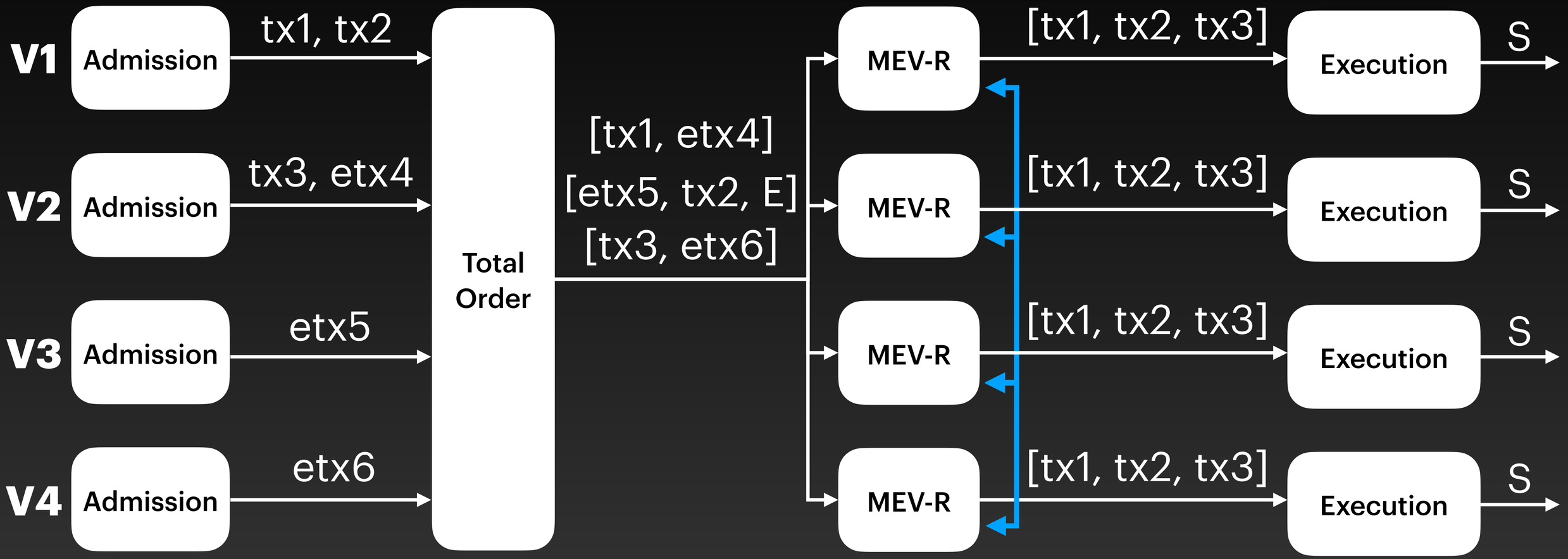


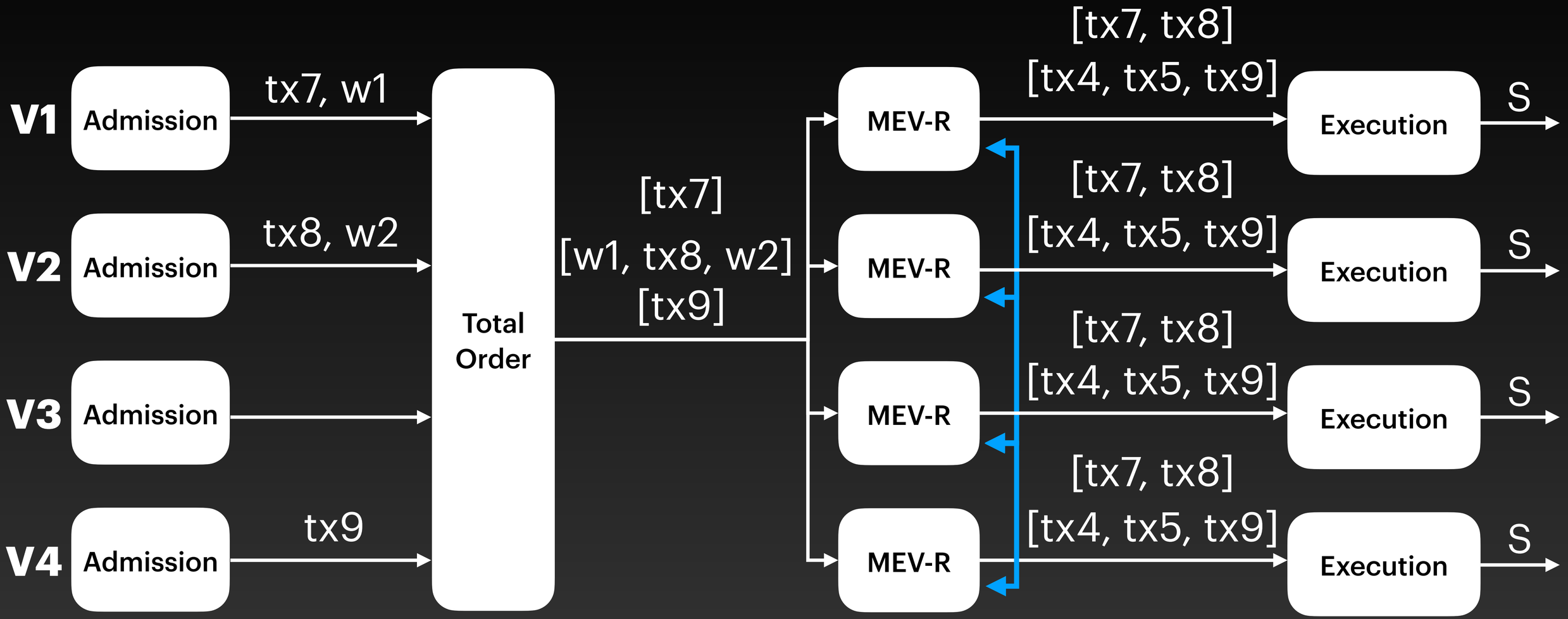
Solution 2: Per-Event Decryption



Seahorse

Mix per-transaction and per-event decryption


V1
Admission
tx1, tx2
V2
Admission
tx3, etx4
V3
Admission
etx5
V4
Admission
etx6
Total Order
[tx1, etx4]
[etx5, tx2, E]
[tx3, etx6]
MEV-R
MEV-R
MEV-R
MEV-R
[tx1, tx2, tx3]
[tx1, tx2, tx3]
[tx1, tx2, tx3]
[tx1, tx2, tx3]
Execution
Execution
Execution
Execution
S
S
S
S


V1
Admission
tx7, w1
V2
Admission
tx8, w2
V3
Admission
V4
Admission
tx9
Total Order
[tx7]
[w1, tx8, w2]
[tx9]
MEV-R
MEV-R
MEV-R
MEV-R
[tx7, tx8]
[tx4, tx5, tx9]
[tx7, tx8]
[tx4, tx5, tx9]
[tx7, tx8]
[tx4, tx5, tx9]
[tx7, tx8]
[tx4, tx5, tx9]
Execution
Execution
Execution
Execution
S
S
S
S

Latency?

Goes up for encrypted txs

Research Gifts

(please keep it short)