Seahorse

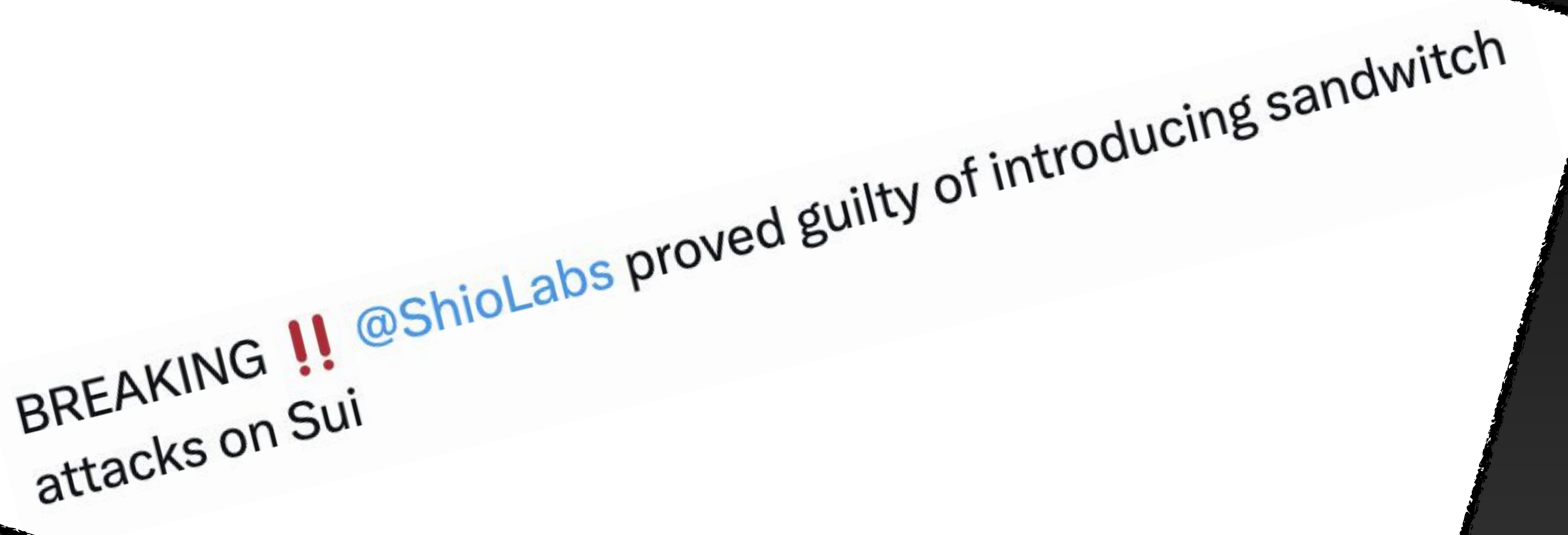
Efficiently Mixing Encrypted and Normal Transactions

Alberto Sonnino

MEV

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

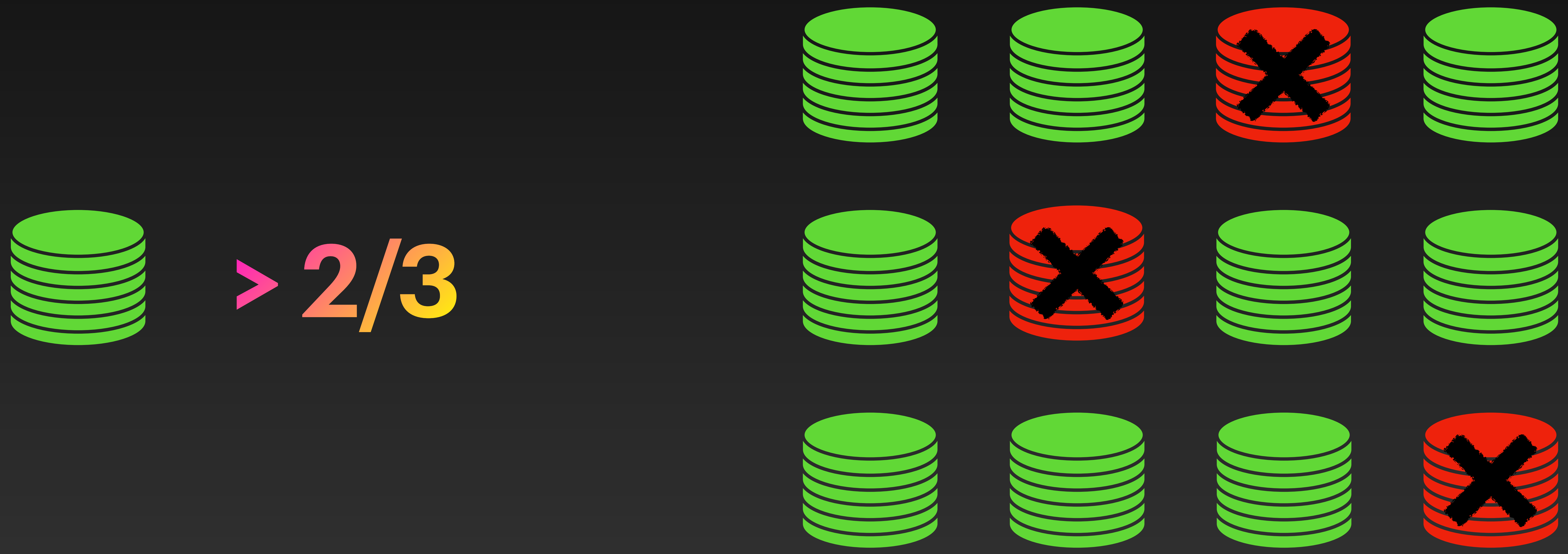
MEV: exciting stuff



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

Byzantine Fault Tolerance

Byzantine Fault Tolerance

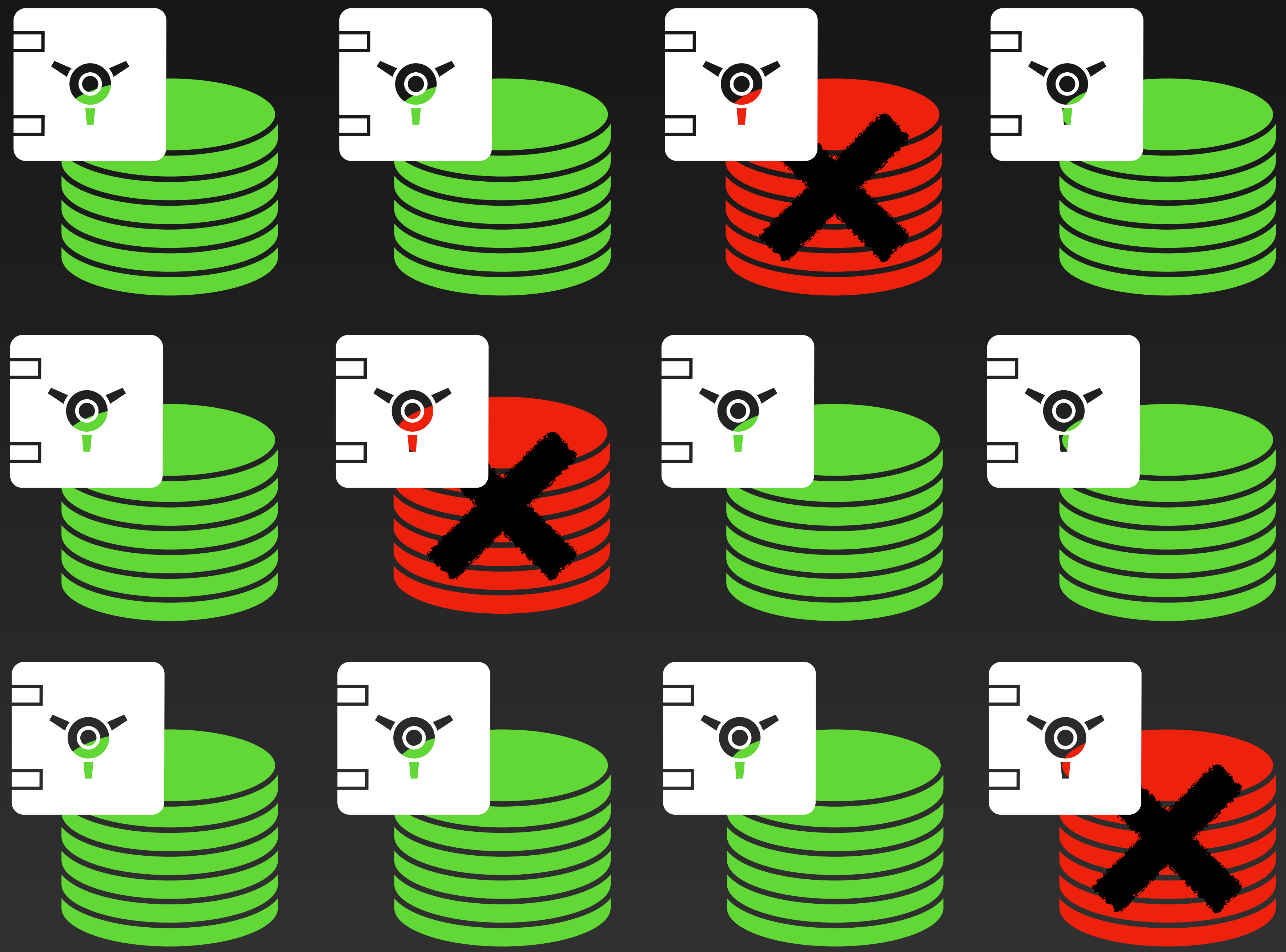


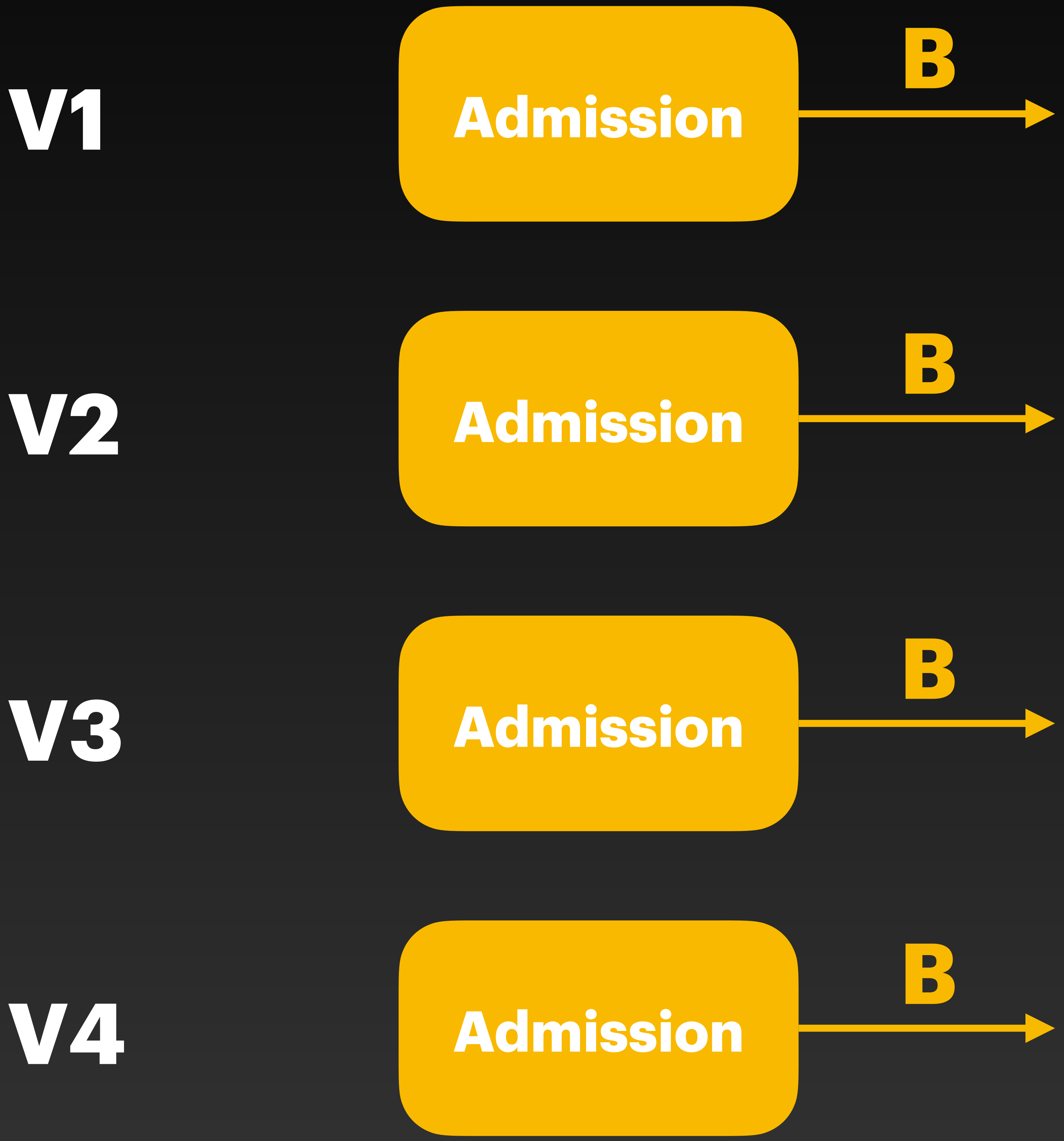
$>2/3$

Delay Duration

Additional latency imposed on normal transactions that follow encrypted ones

Shared Key



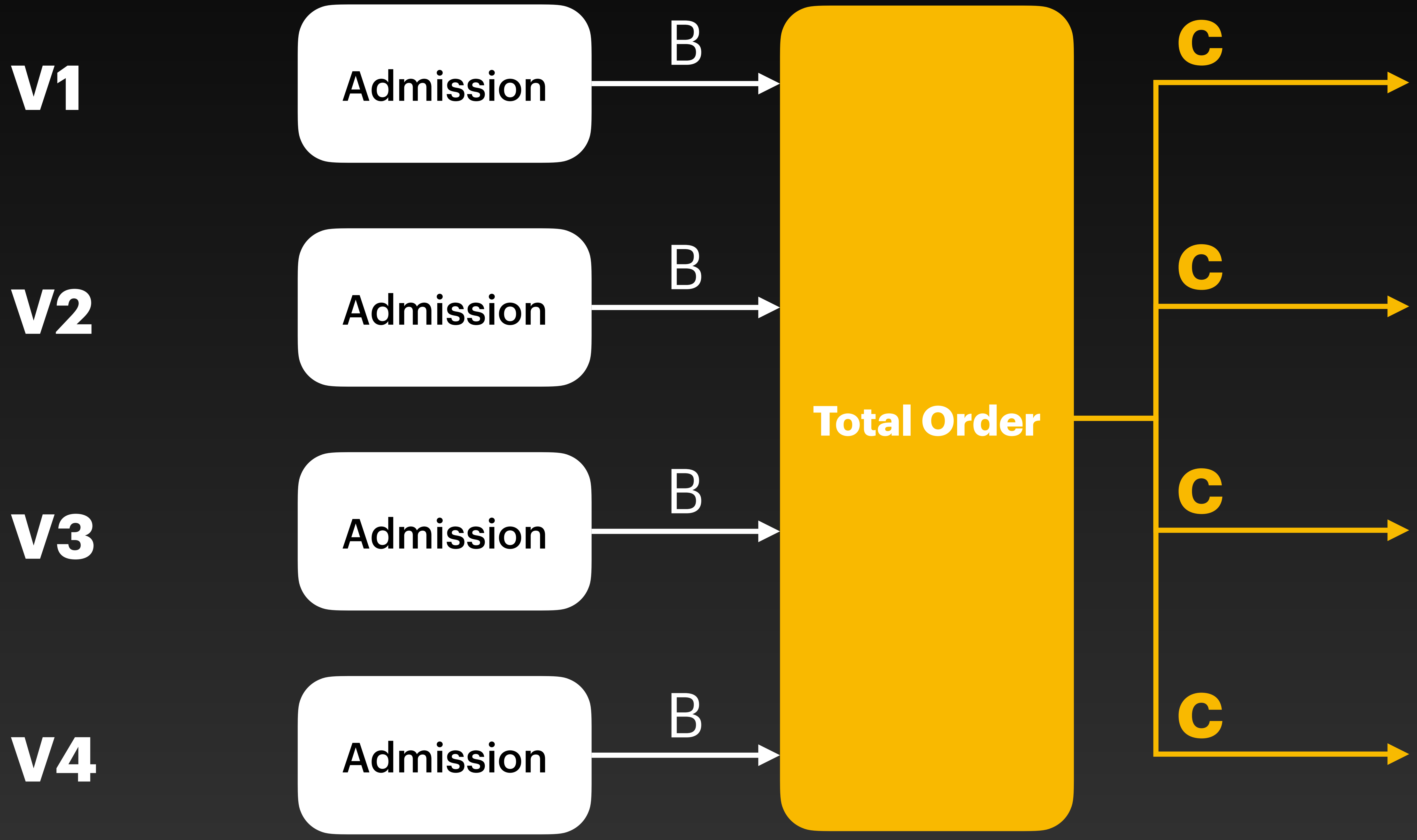


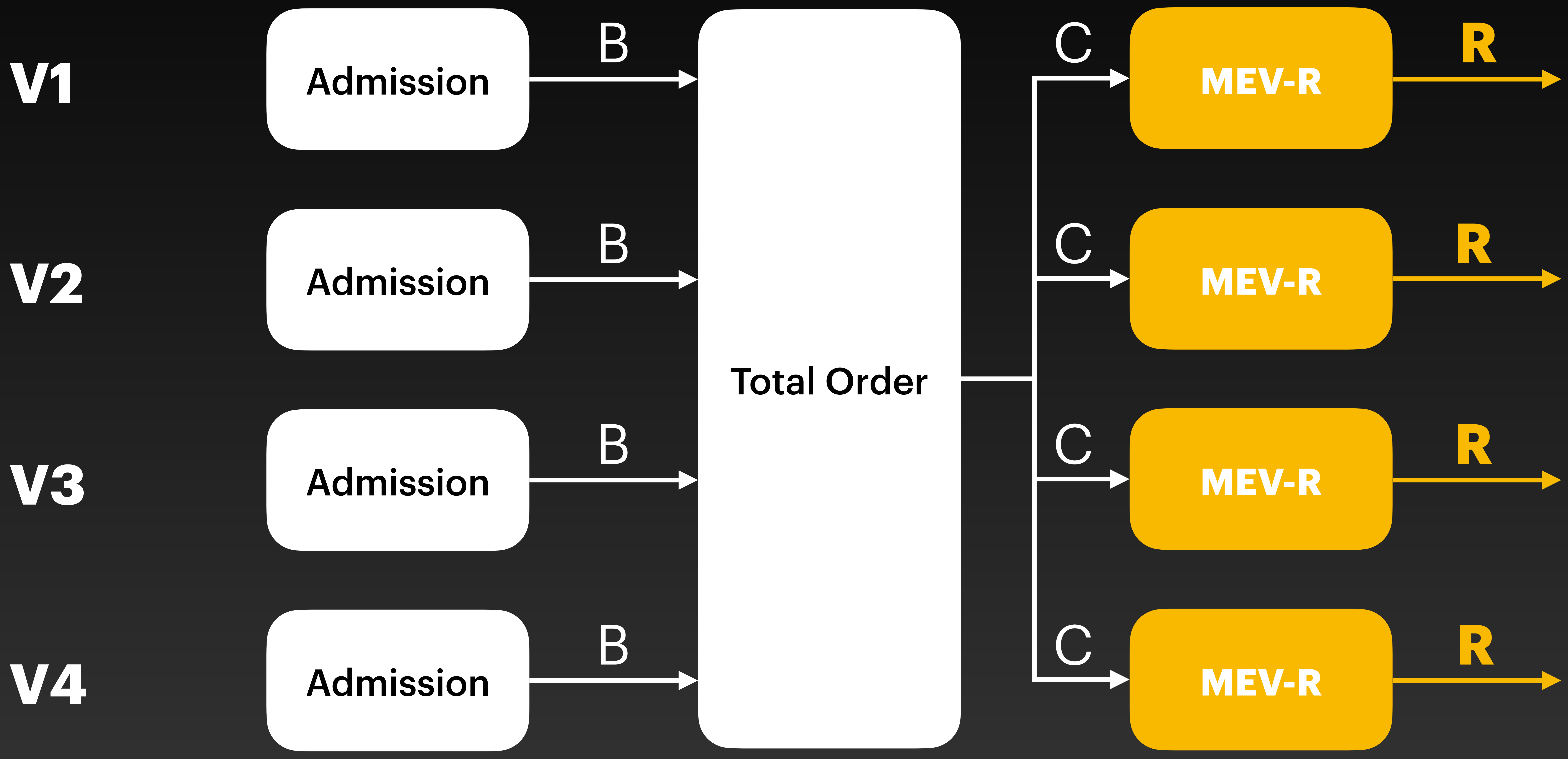
V1 Admission B

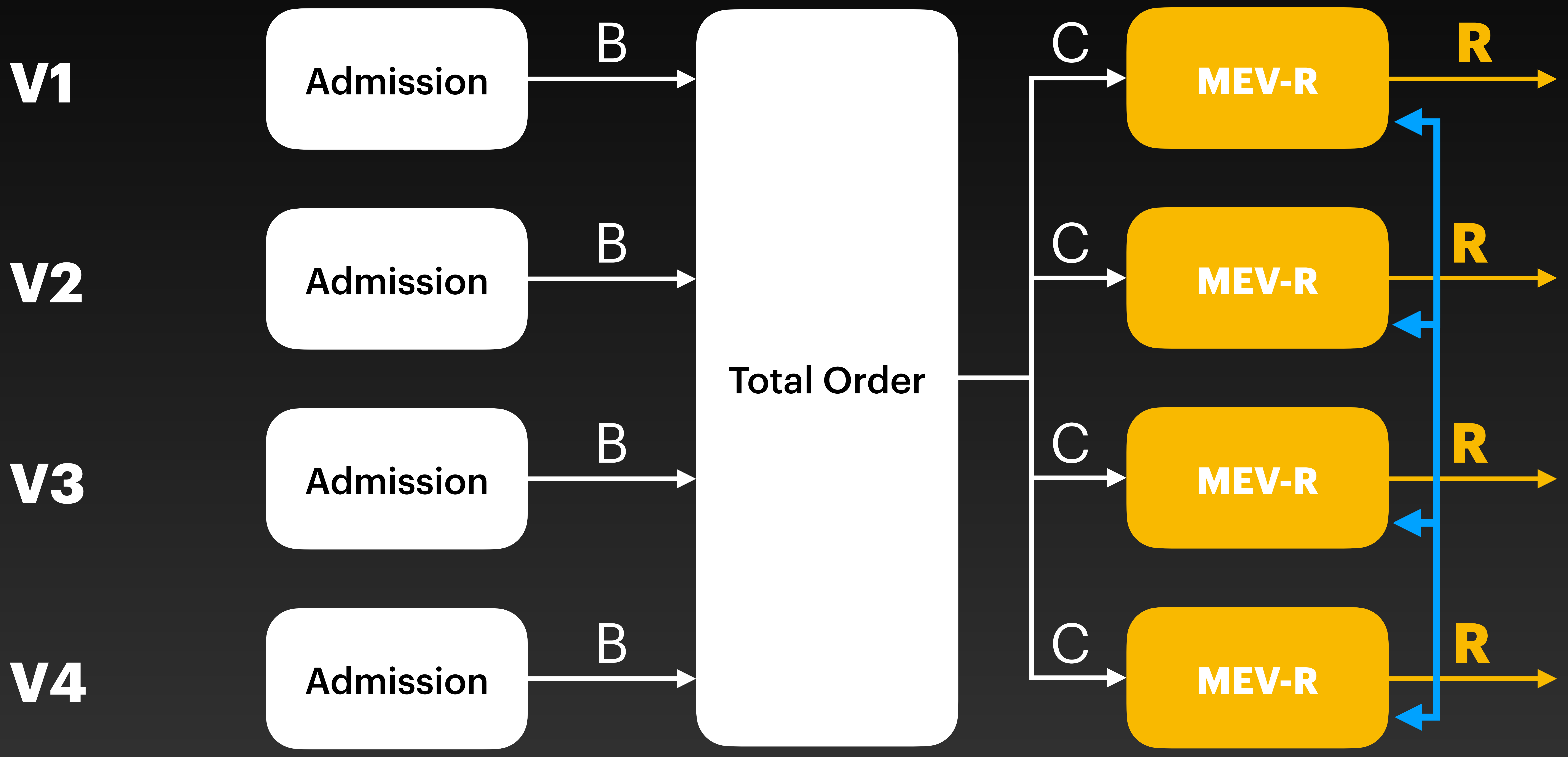
V2 Admission B

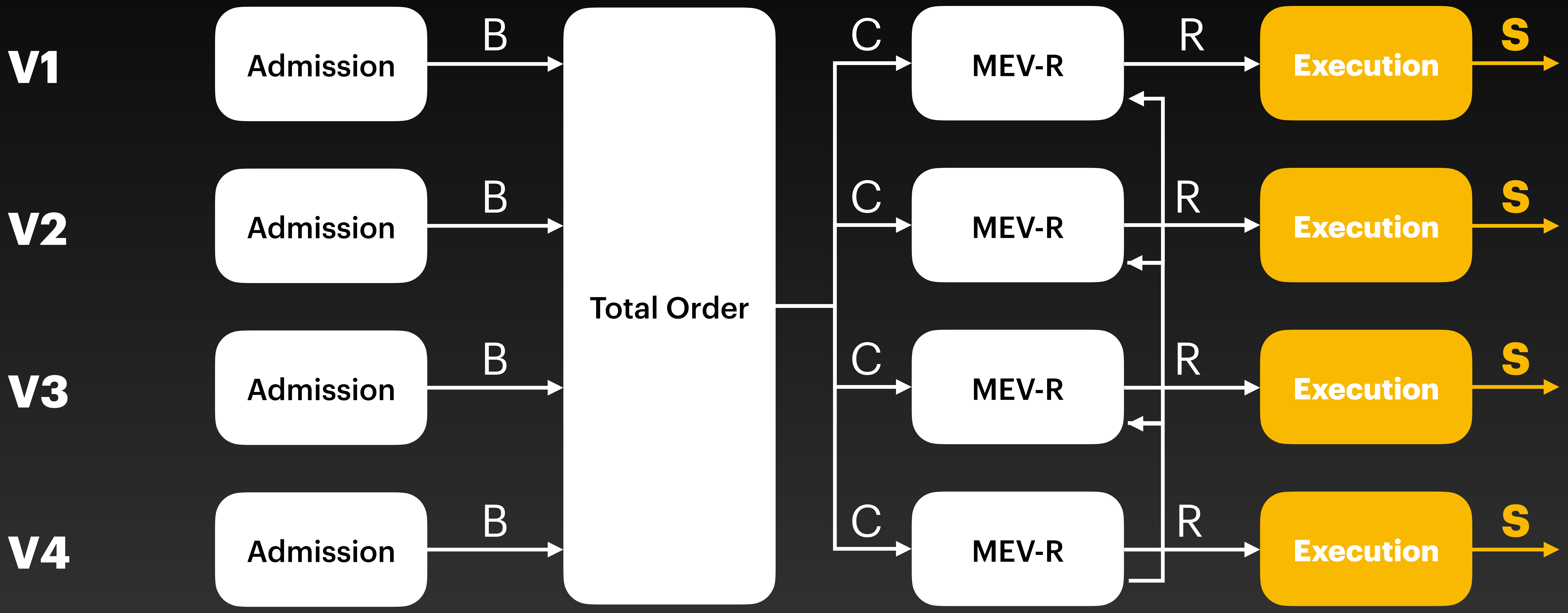
V3 Admission B

V4 Admission B


V1
V2
V3
V4
Admission
Admission
Admission
Admission
B
B
B
B
Total Order
C
C
C
C

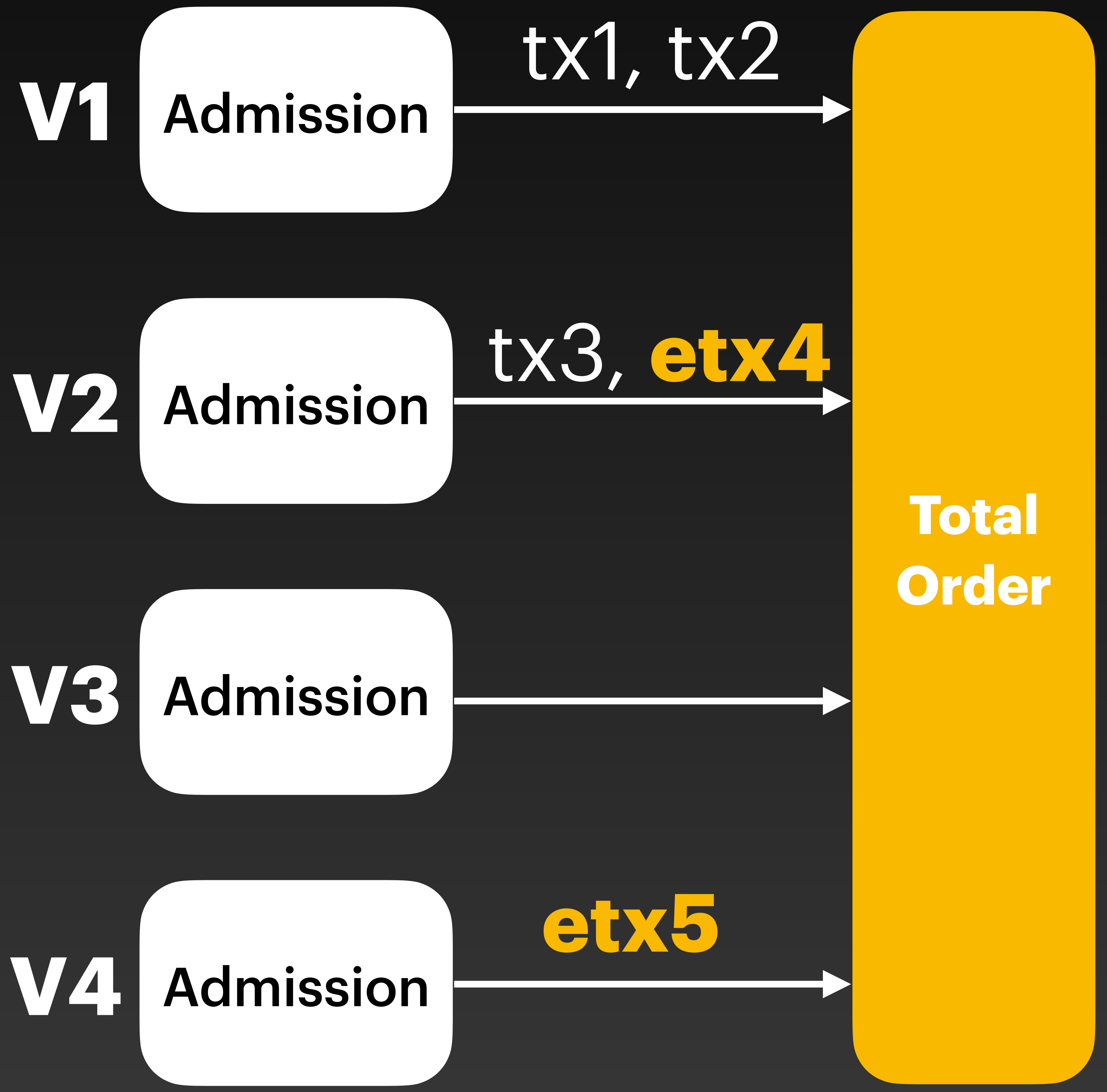

V1
V2
V3
V4
Admission
Admission
Admission
Admission
B
B
B
B
Total Order
C
C
C
C
MEV-R
MEV-R
MEV-R
MEV-R
R
R
R
R


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

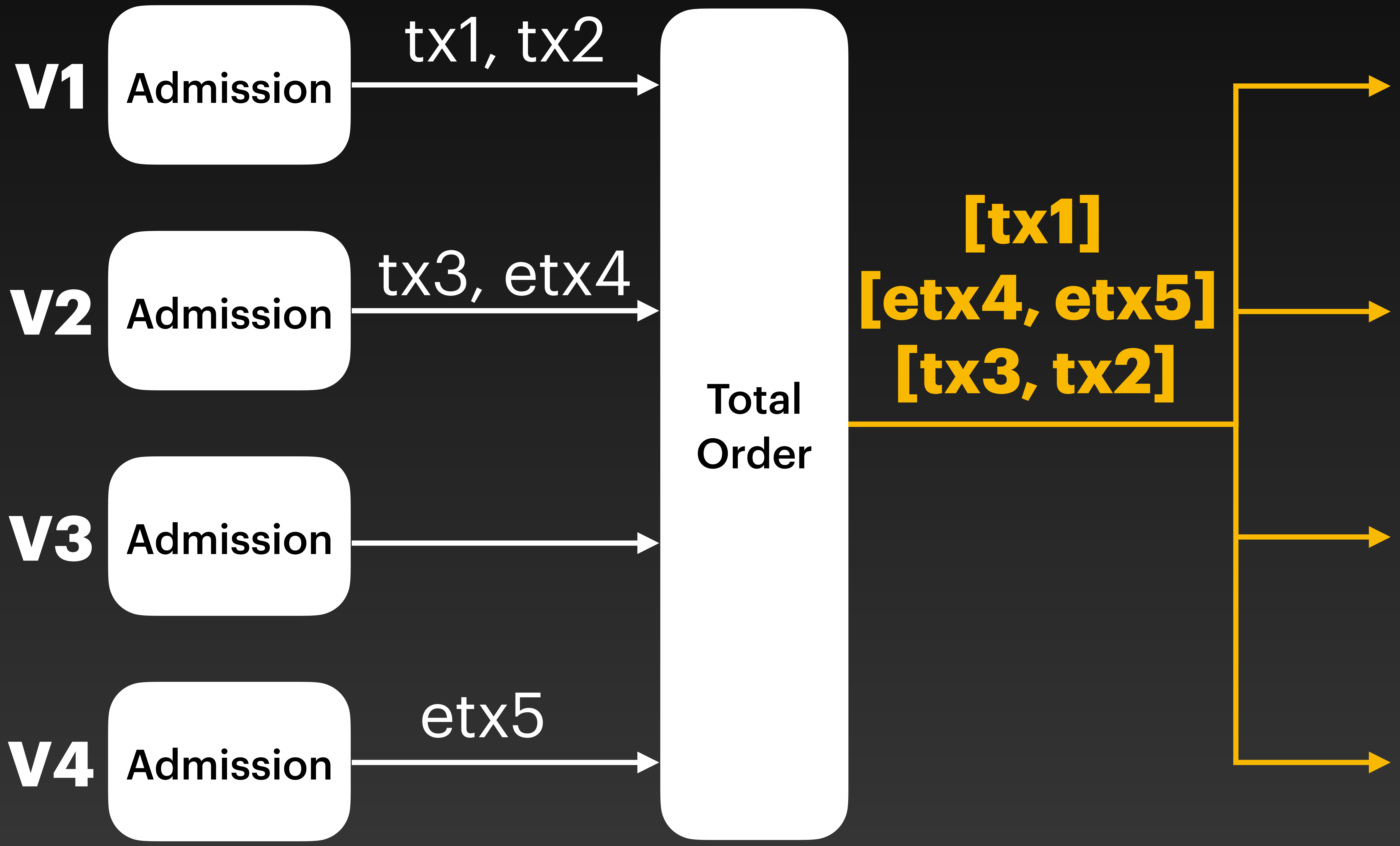

V1
V2
V3
V4
Admission
Admission
Admission
Admission
B
B
B
B
Total Order
C
C
C
C
MEV-R
MEV-R
MEV-R
MEV-R
R
R
R
R
Execution
Execution
Execution
Execution
S
S
S
S

Solution 1: Per-Tx Decryption

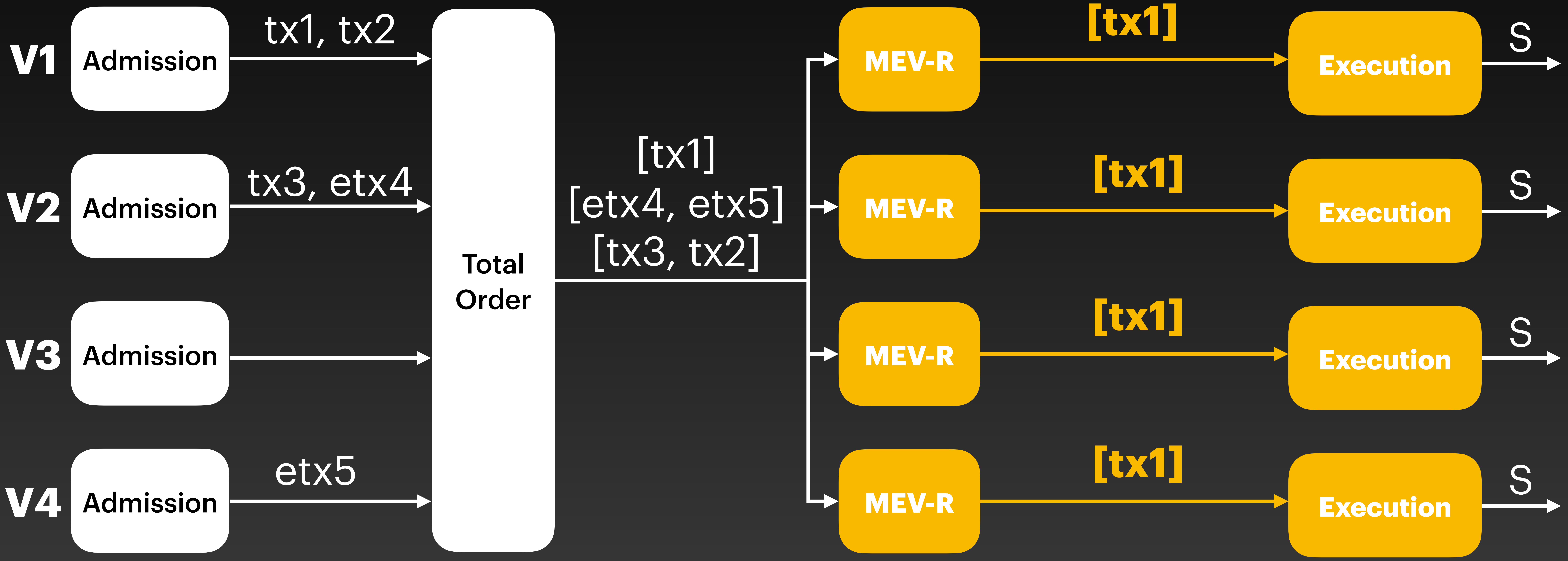
Solution 1: Per-Tx Decryption



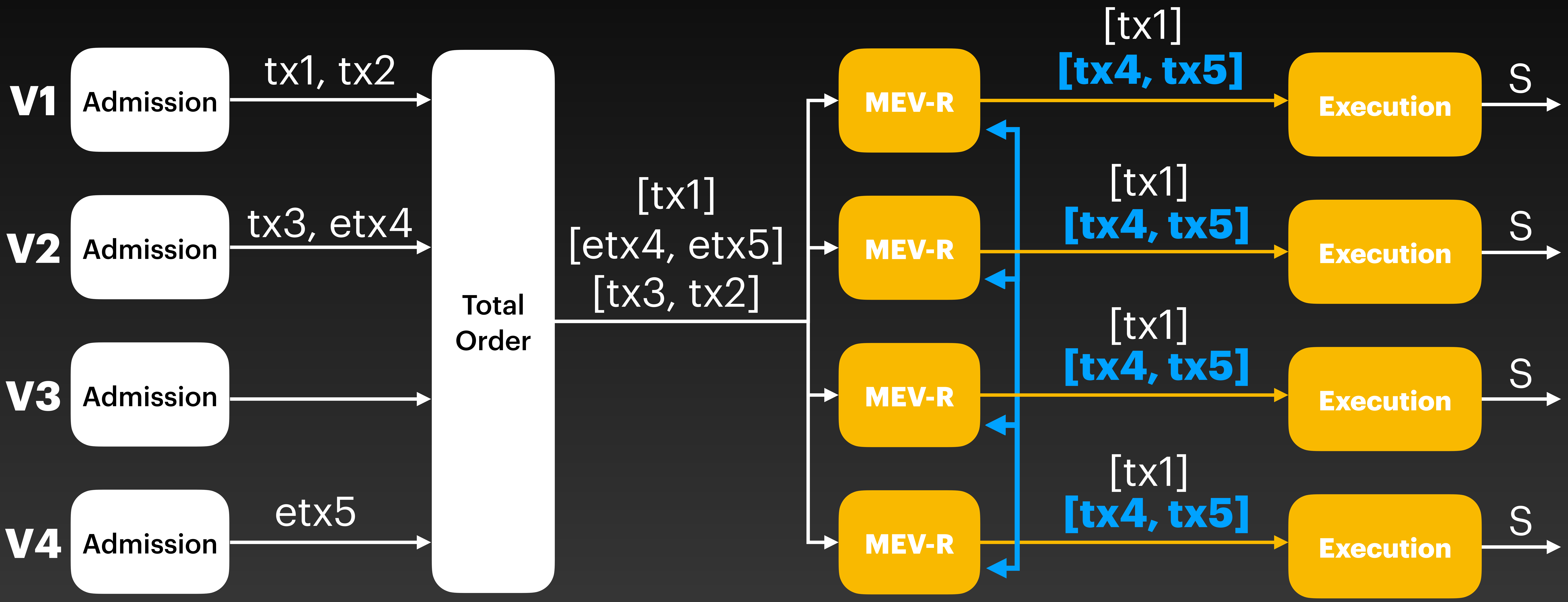
Solution 1: Per-Tx Decryption



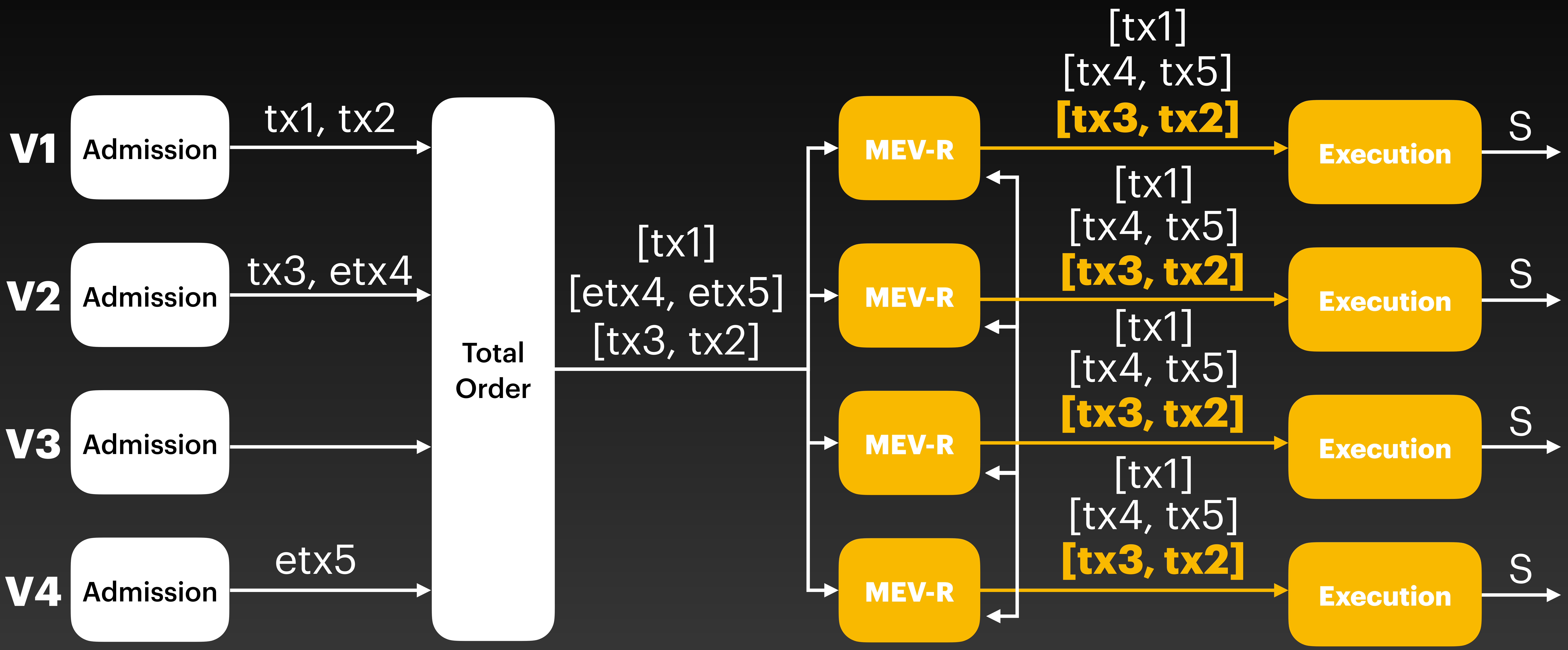
Solution 1: Per-Tx Decryption



Solution 1: Per-Tx Decryption

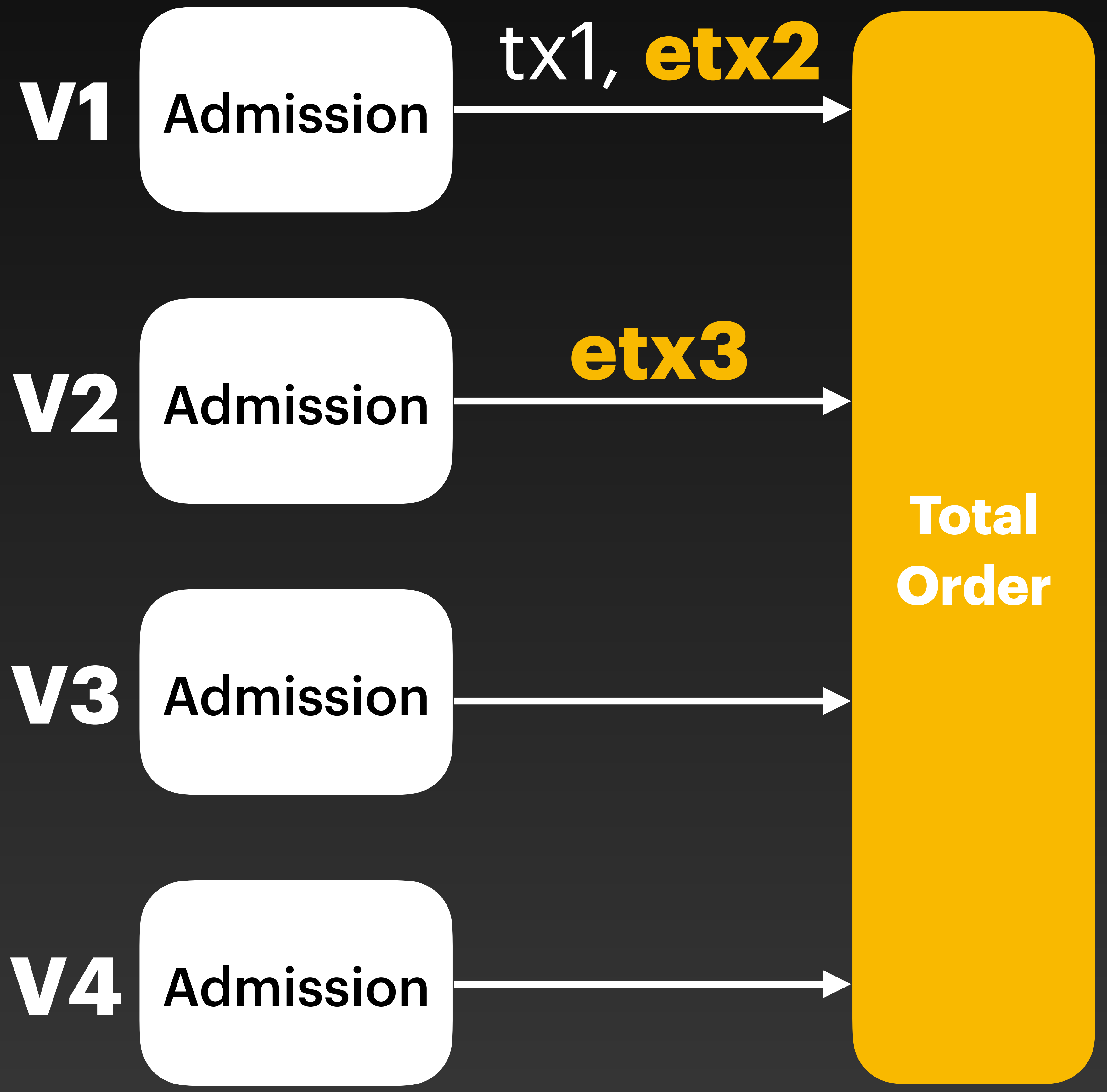


Solution 1: Per-Tx Decryption

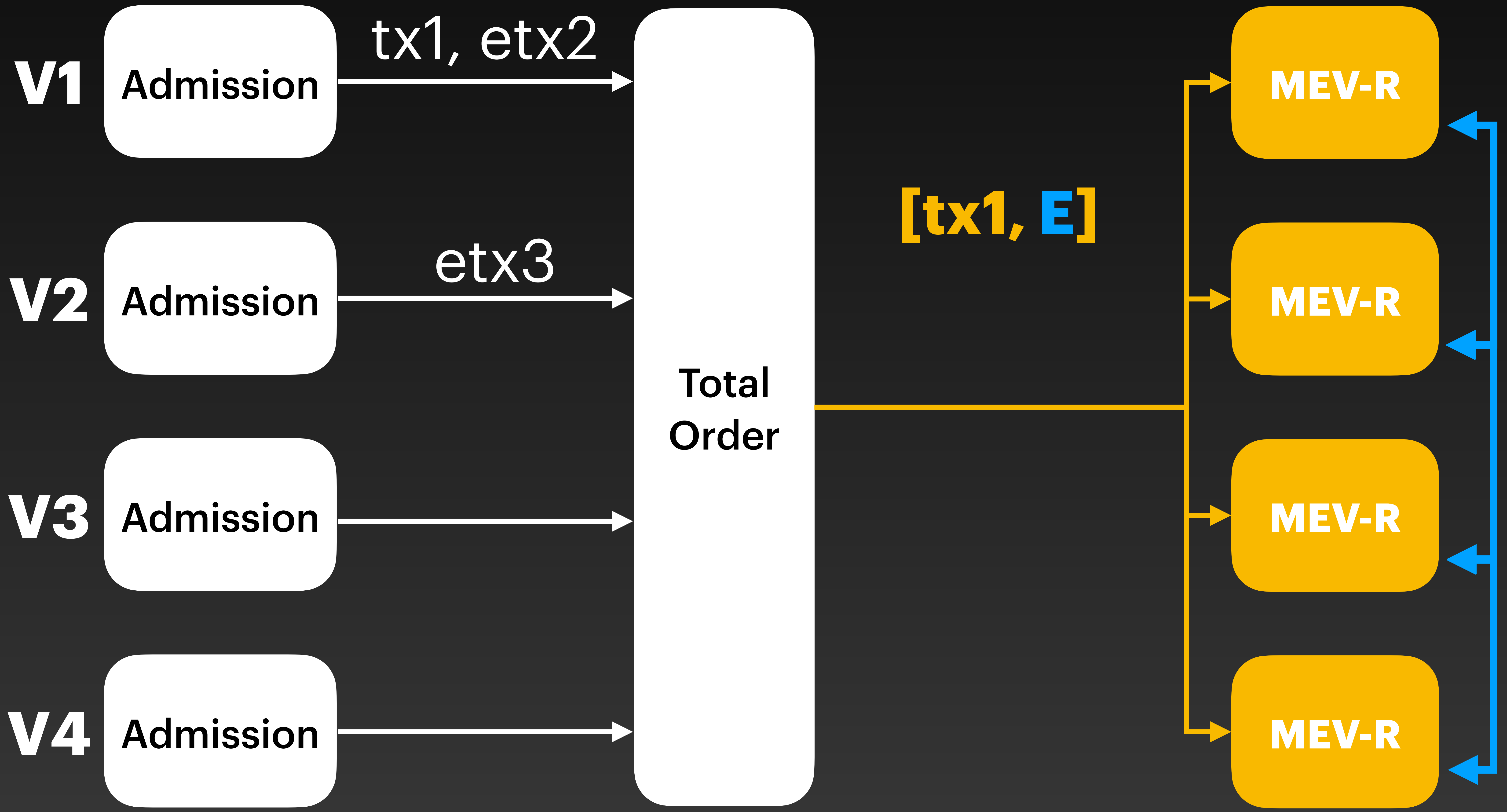


Solution 2: Per-Event Decryption

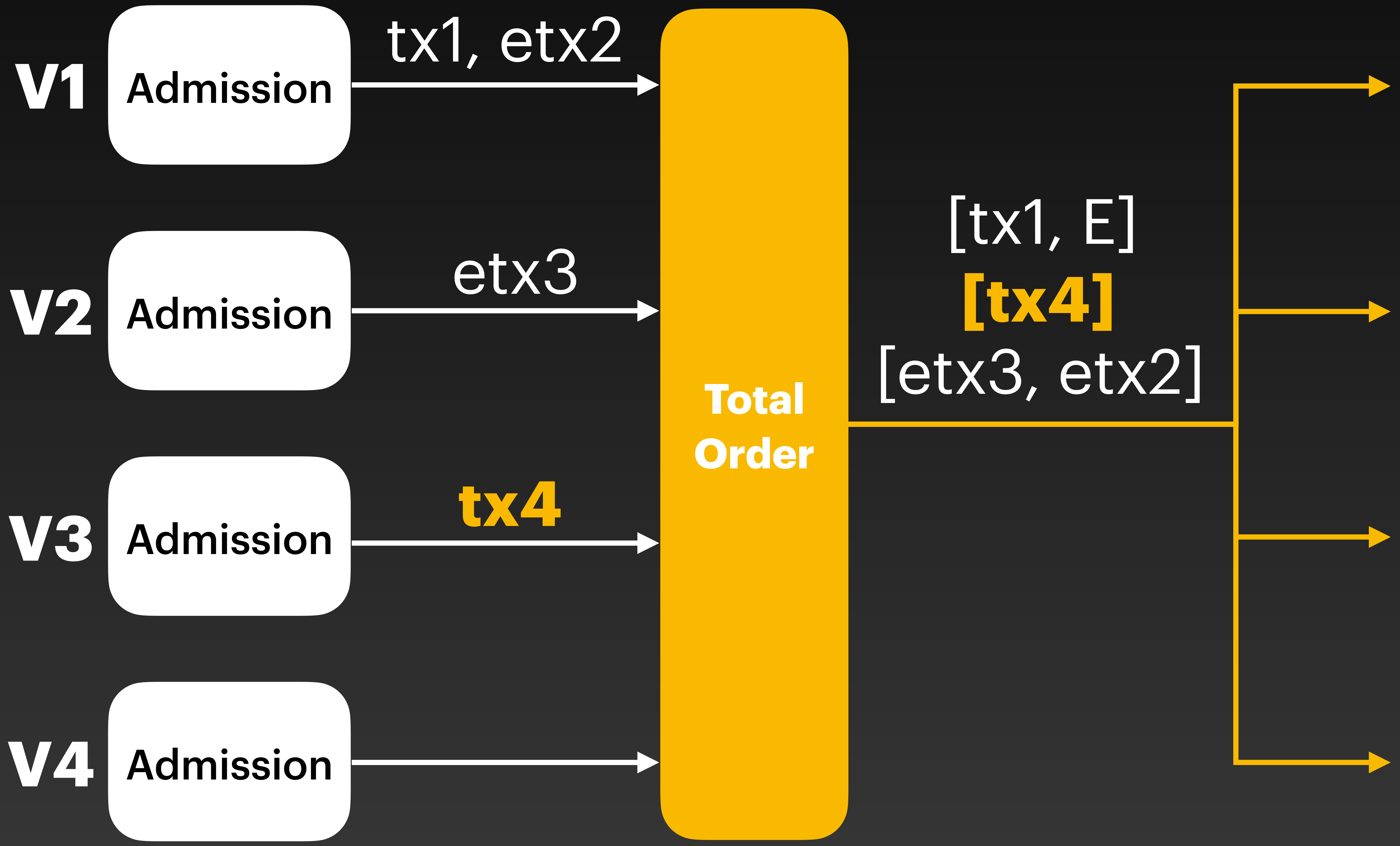
Solution 2: Per-Event Decryption



Solution 2: Per-Event Decryption



Solution 2: Per-Event Decryption



V1 Admission

tx1, etx2

V2 Admission

etx3

V3 Admission

tx4

V4 Admission

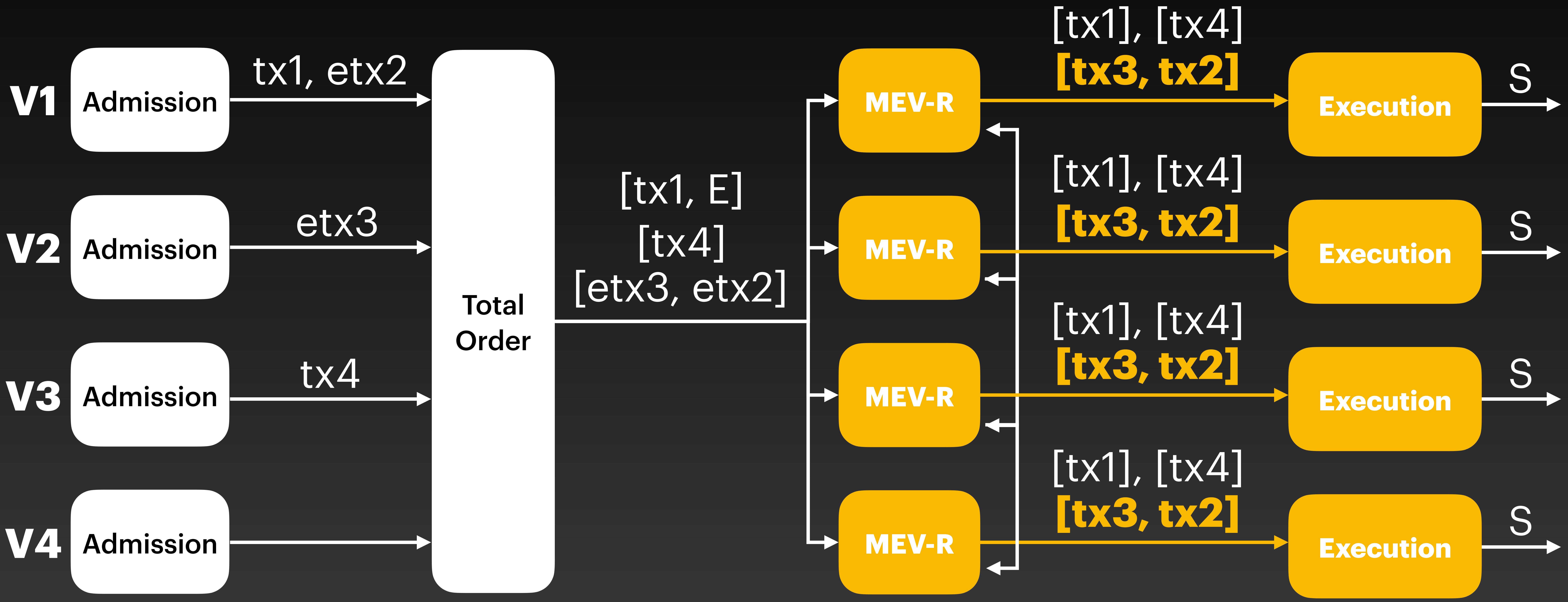
Total Order

[tx1, E]

[tx4]

[etx3, etx2]

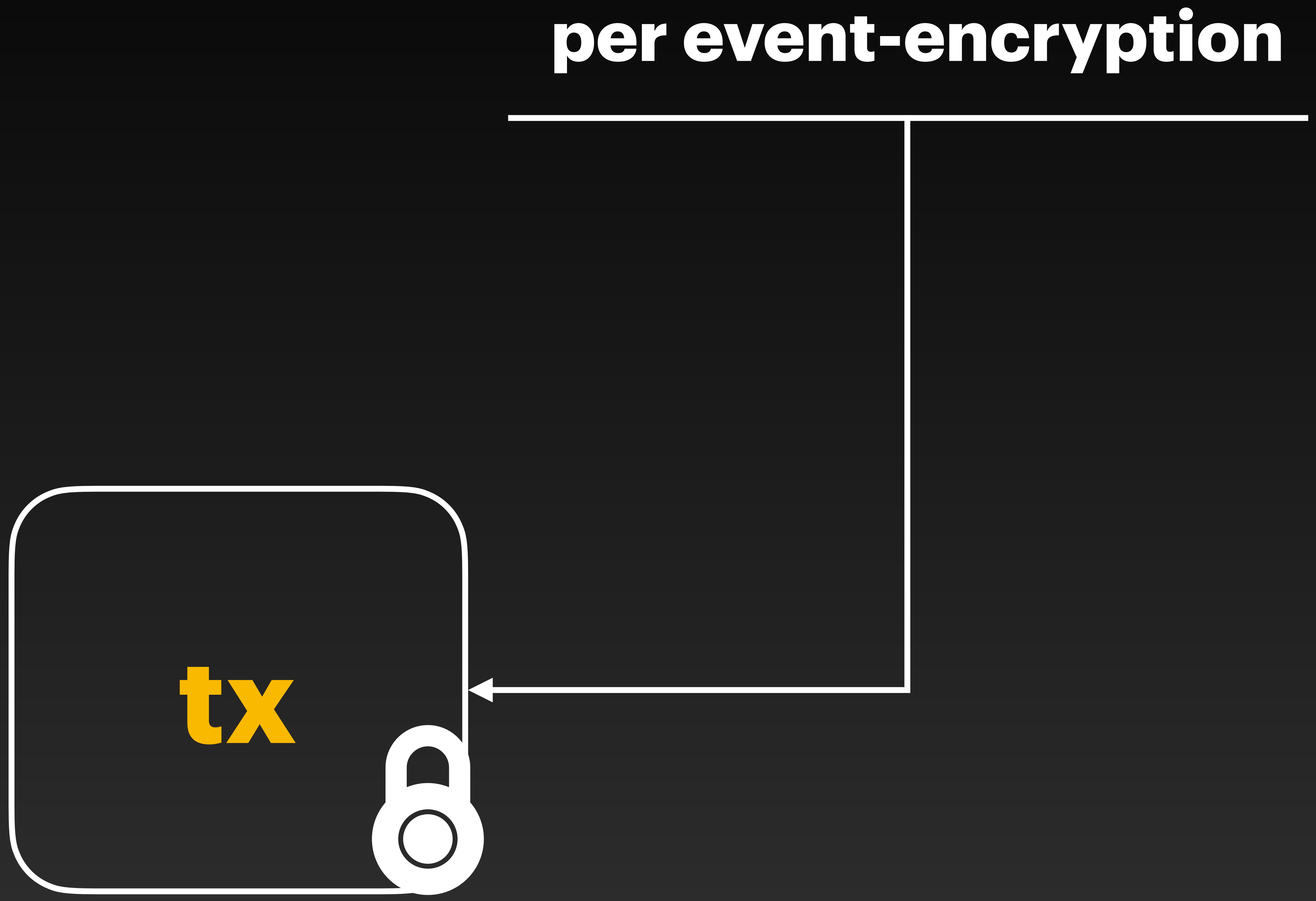
Solution 2: Per-Event Decryption



Seahorse

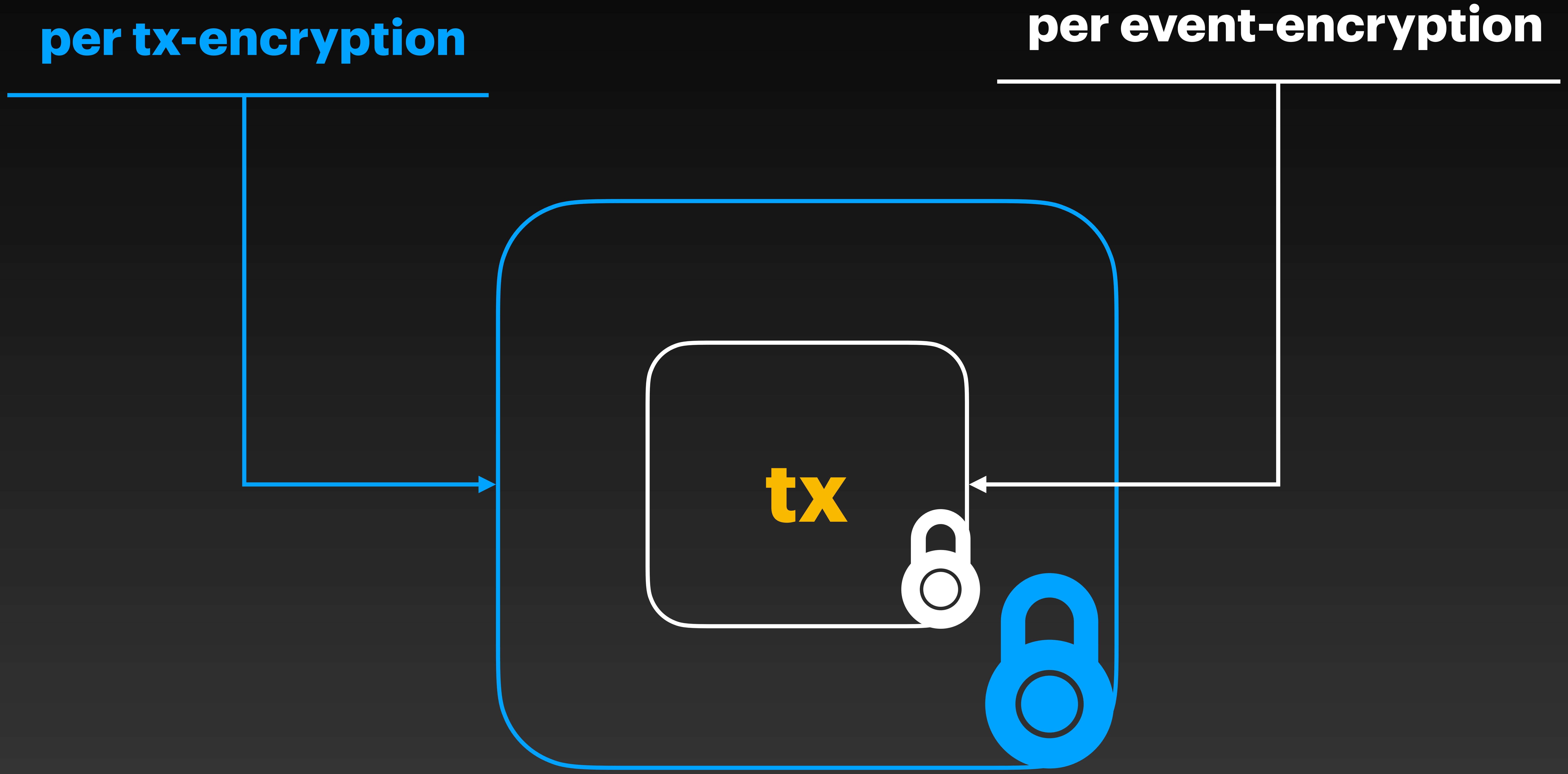
Mix per-transaction and per-event decryption

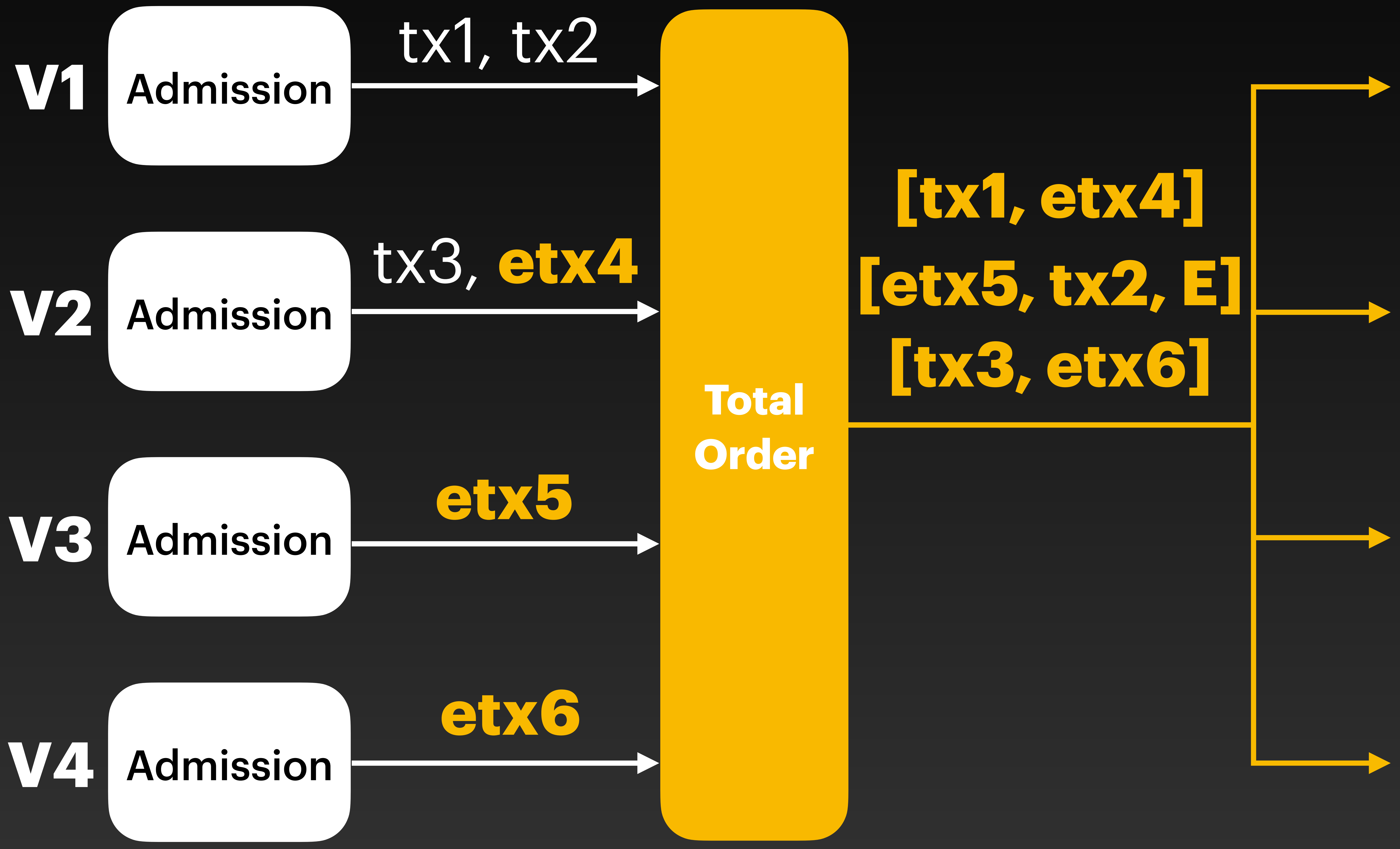
tx

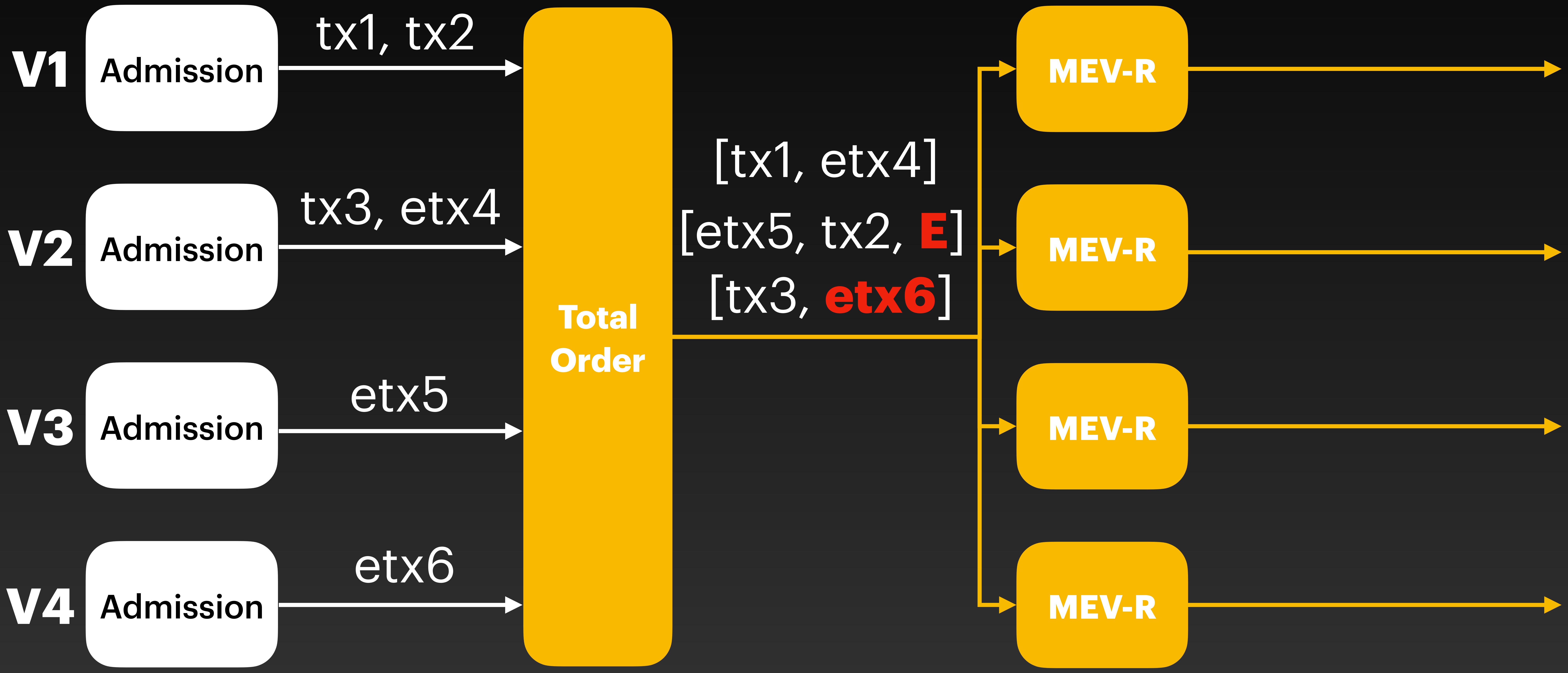


per event-encryption

tx


per tx-encryption
per event-encryption
tx


V1
Admission
tx1, tx2
V2
Admission
tx3, etx4
V3
Admission
etx5
V4
Admission
etx6
Total Order
[tx1, etx4]
[etx5, tx2, E]
[tx3, etx6]



V1 Admission

tx1, tx2

V2 Admission

tx3, etx4

V3 Admission

etx5

V4 Admission

etx6

Total Order

[tx1, etx4]

[etx5, tx2, **E**]

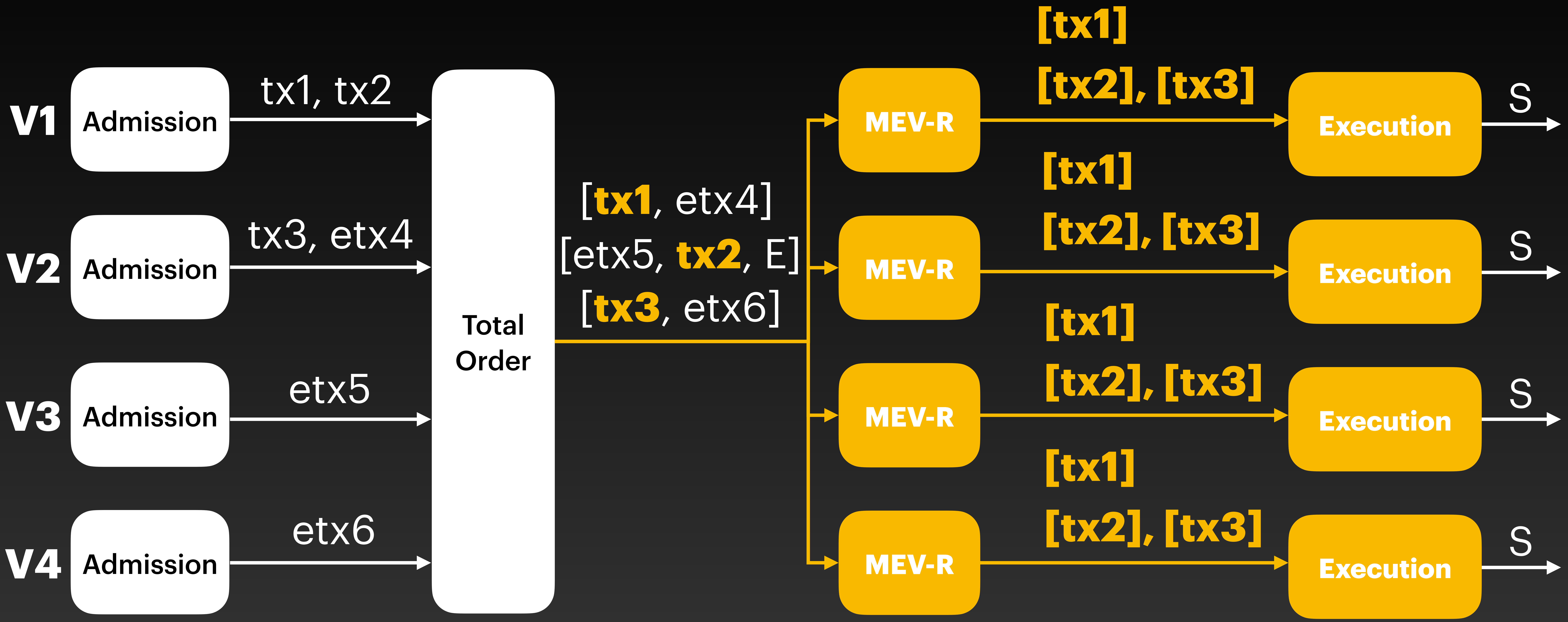
[tx3, **etx6**]

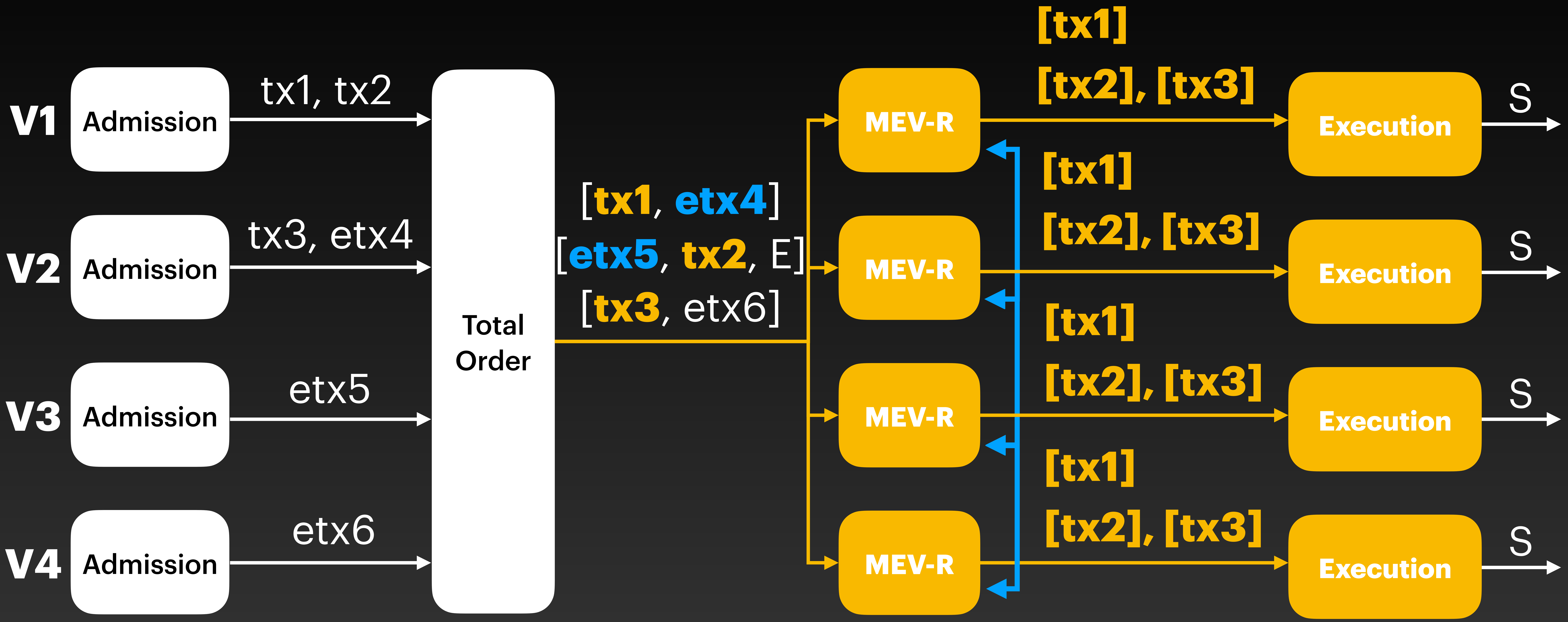
MEV-R

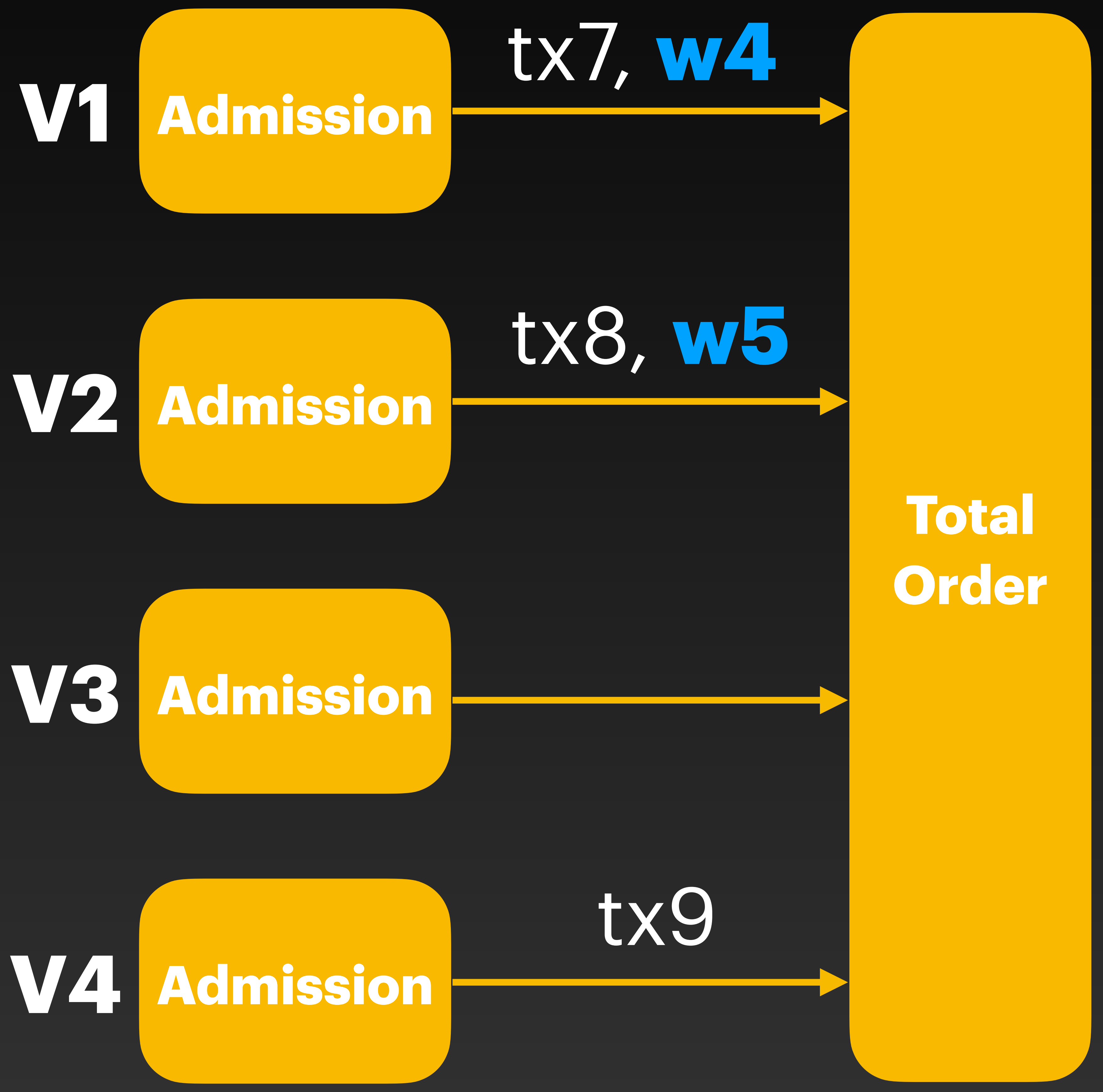
MEV-R

MEV-R

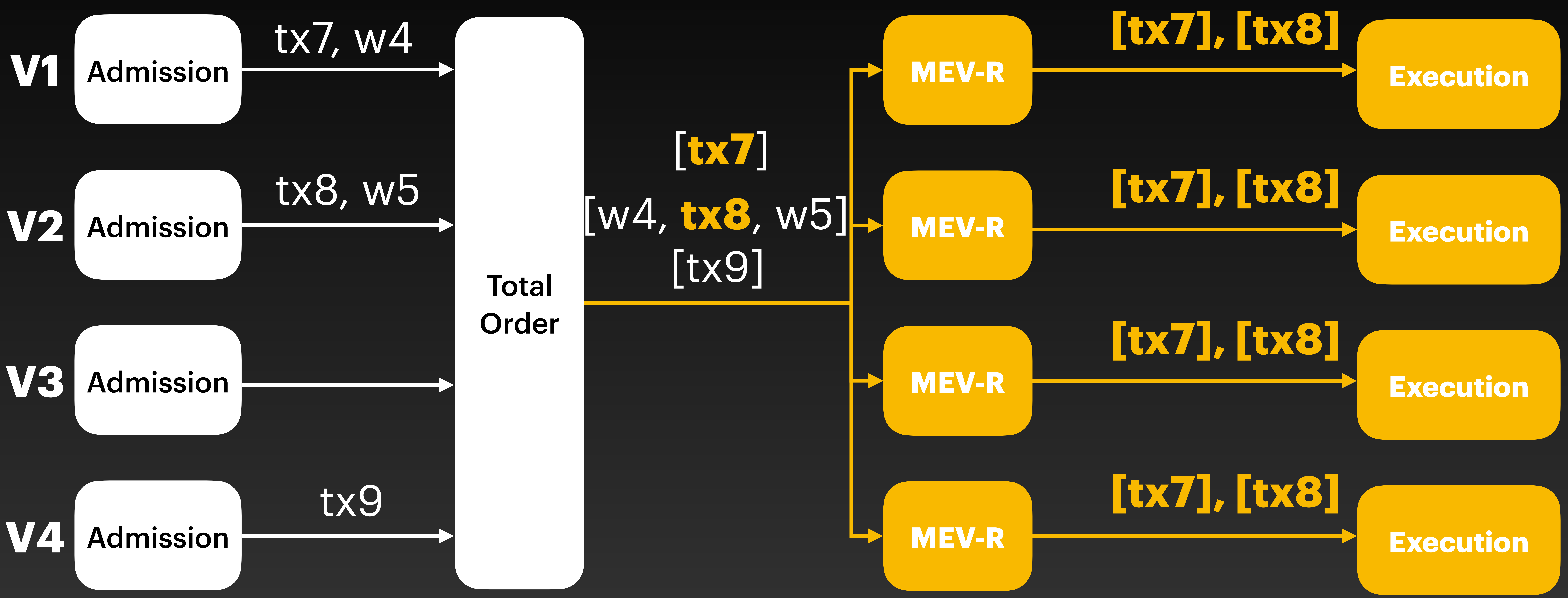
MEV-R

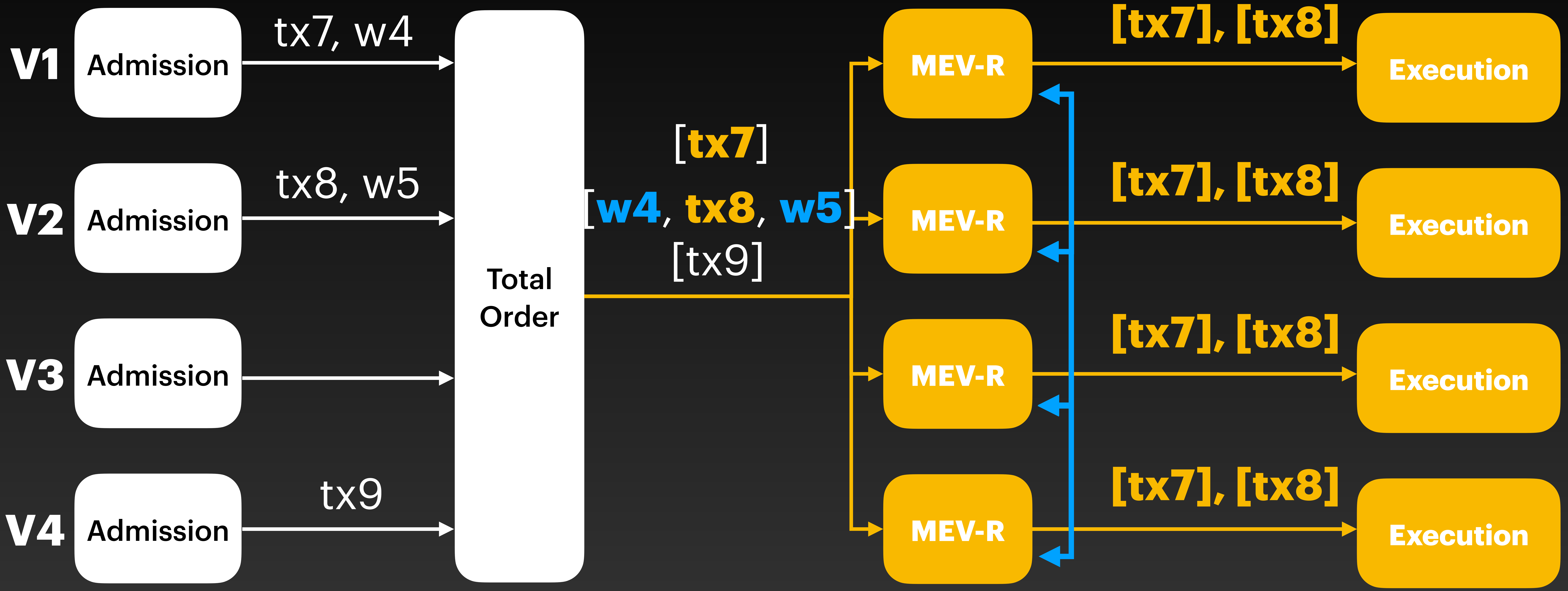

V1
Admission
tx1, tx2
V2
Admission
tx3, etx4
V3
Admission
etx5
V4
Admission
etx6
Total Order
[tx1, etx4]
[etx5, tx2, E]
[tx3, etx6]
MEV-R
[tx1]
[tx2], [tx3]
Execution
S
MEV-R
[tx1]
[tx2], [tx3]
Execution
S
MEV-R
[tx1]
[tx2], [tx3]
Execution
S
MEV-R
[tx1]
[tx2], [tx3]
Execution
S

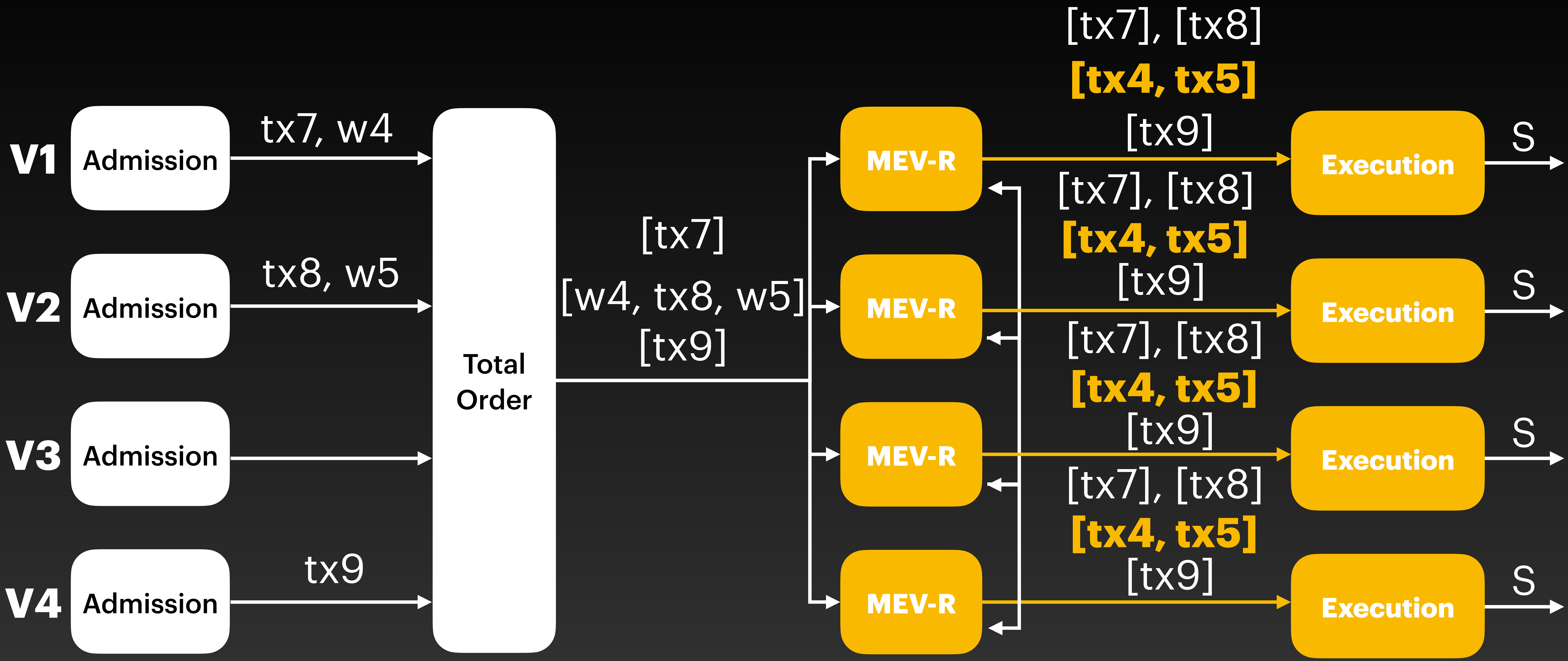

V1
Admission
tx1, tx2
V2
Admission
tx3, etx4
V3
Admission
etx5
V4
Admission
etx6
Total Order
[tx1, etx4]
[etx5, tx2, E]
[tx3, etx6]
MEV-R
MEV-R
MEV-R
MEV-R
[tx1]
[tx2], [tx3]
[tx1]
[tx2], [tx3]
[tx1]
[tx2], [tx3]
[tx1]
[tx2], [tx3]
Execution
Execution
Execution
Execution
S
S
S
S

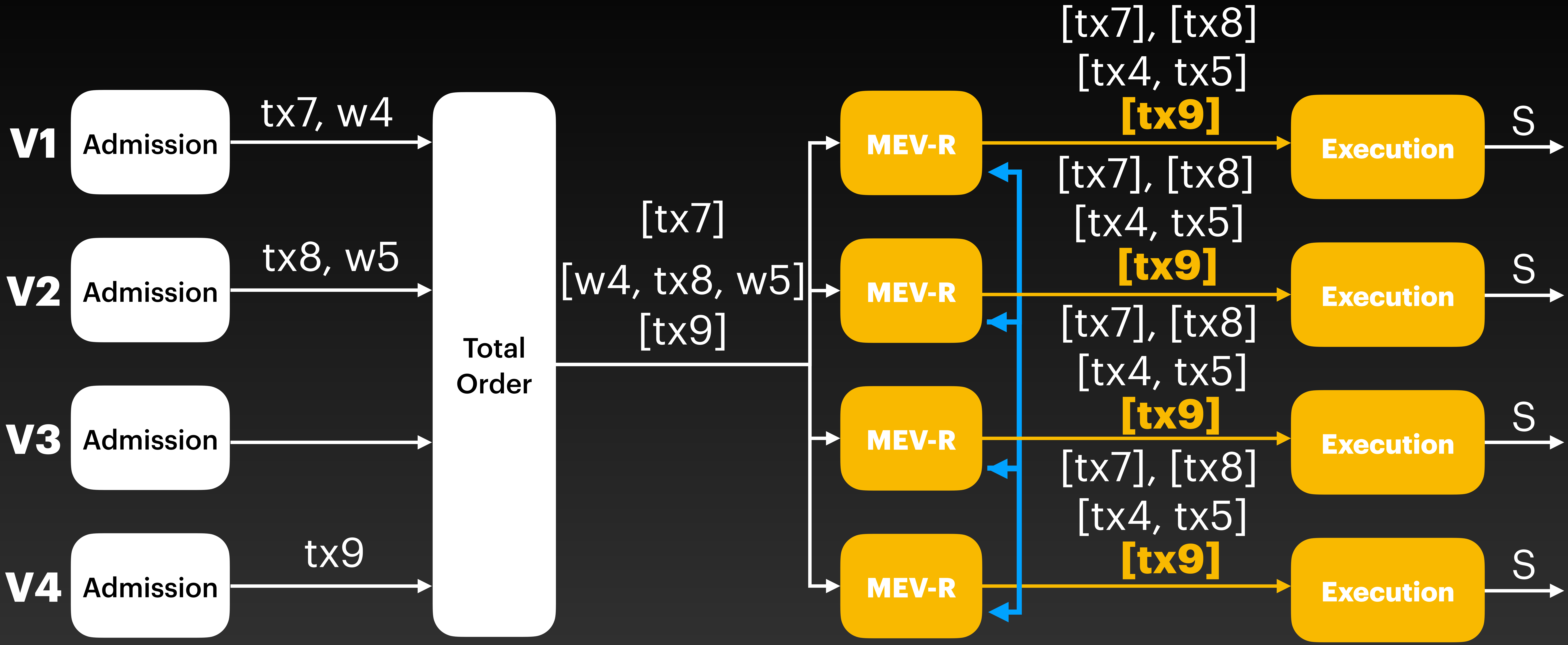


V1
Admission
tx7, w4
V2
Admission
tx8, w5
V3
Admission
V4
Admission
tx9
Total Order


V1
Admission
tx7, w4
V2
Admission
tx8, w5
V3
Admission
V4
Admission
tx9
Total Order
[tx7]
[w4, tx8, w5]
[tx9]
MEV-R
[tx7], [tx8]
Execution
MEV-R
[tx7], [tx8]
Execution
MEV-R
[tx7], [tx8]
Execution
MEV-R
[tx7], [tx8]
Execution


V1
Admission
tx7, w4
V2
Admission
tx8, w5
V3
Admission
V4
Admission
tx9
Total Order
[tx7]
[w4, tx8, w5]
[tx9]
MEV-R
MEV-R
MEV-R
MEV-R
[tx7], [tx8]
[tx7], [tx8]
[tx7], [tx8]
[tx7], [tx8]
Execution
Execution
Execution
Execution


V1
Admission
tx7, w4
V2
Admission
tx8, w5
V3
Admission
V4
Admission
tx9
Total Order
[tx7]
[w4, tx8, w5]
[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


V1
Admission
tx7, w4
V2
Admission
tx8, w5
V3
Admission
V4
Admission
tx9
Total Order
[tx7]
[w4, tx8, w5]
[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?

Increases for encrypted transactions

Research Gifts

(please keep it short)