Espresso Systems

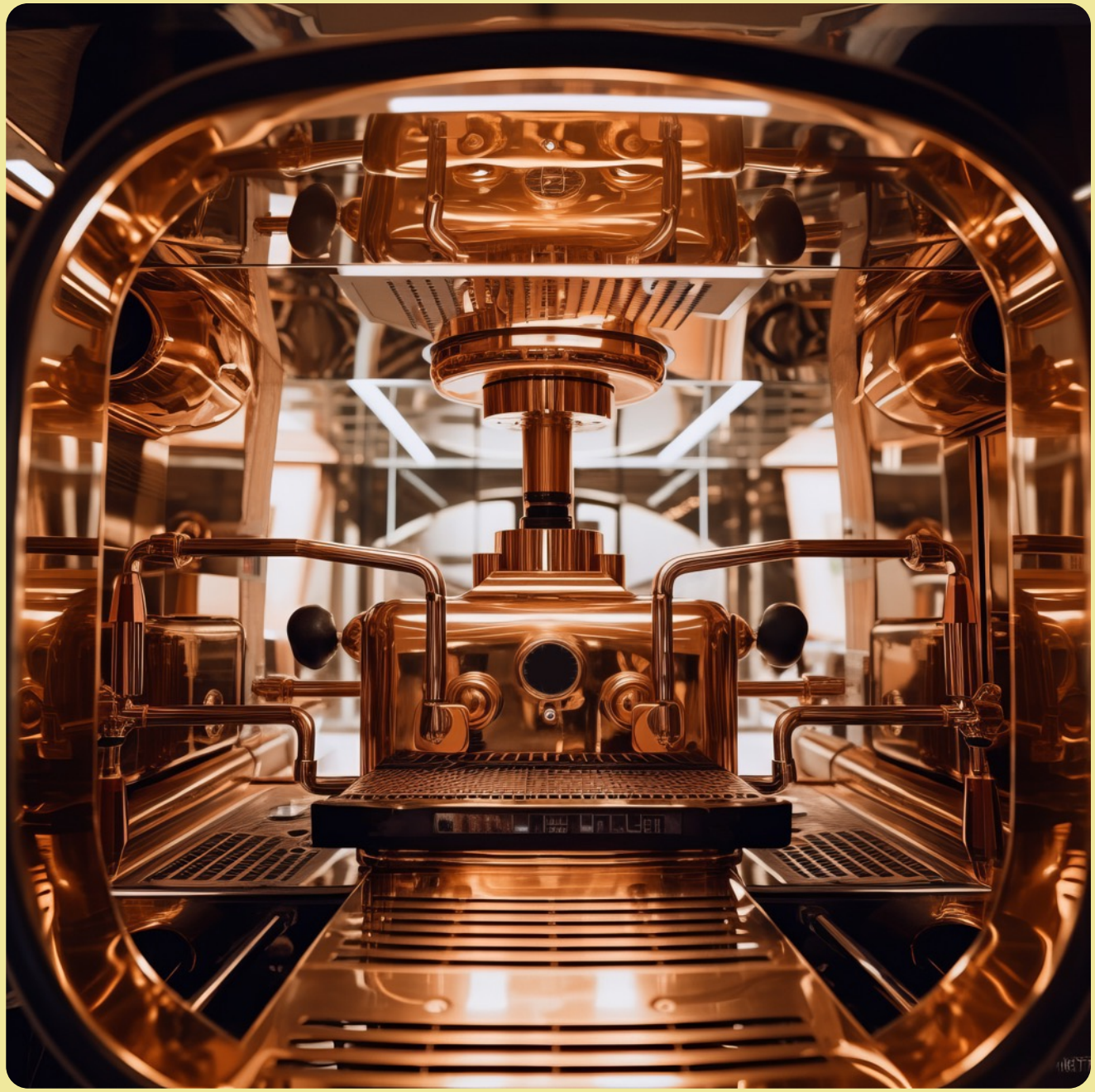
Shared sequencing for rollups

Solidity Singapore Meetup

Sept 2023

Alex Xiong

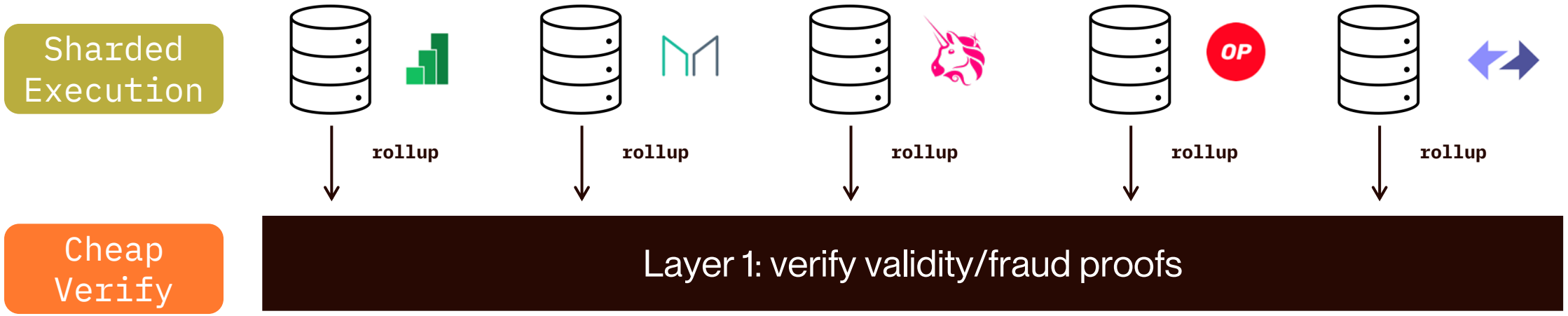
Senior Cryptography Engineer



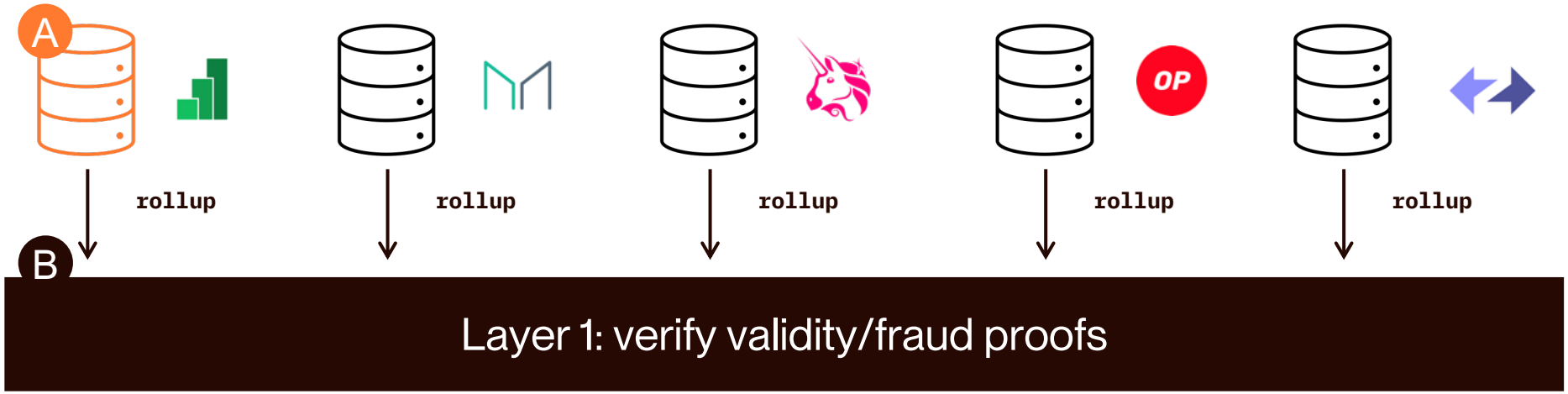
Agenda

1. Why decentralized?
2. Why shared?
3. Roughly how?
4. Demo!

Rollups: horizontal scaling



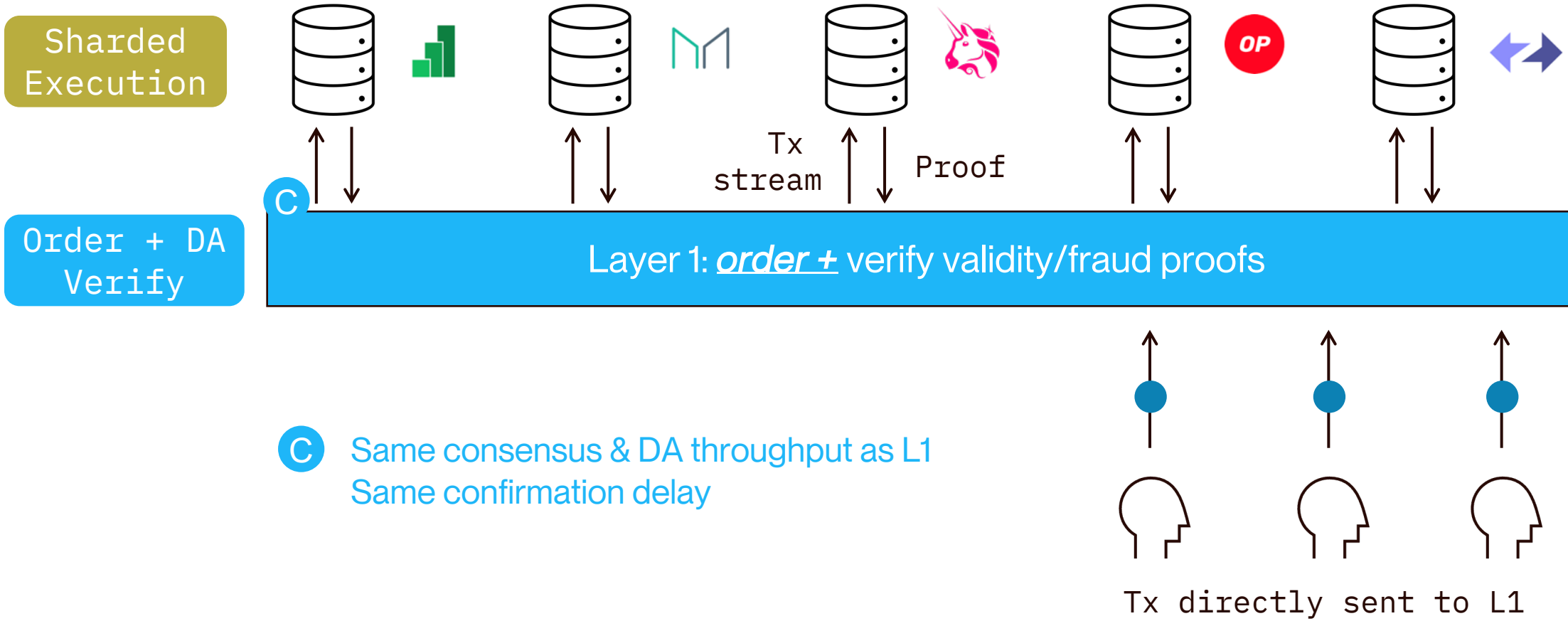
Today: Rollup servers control a lot



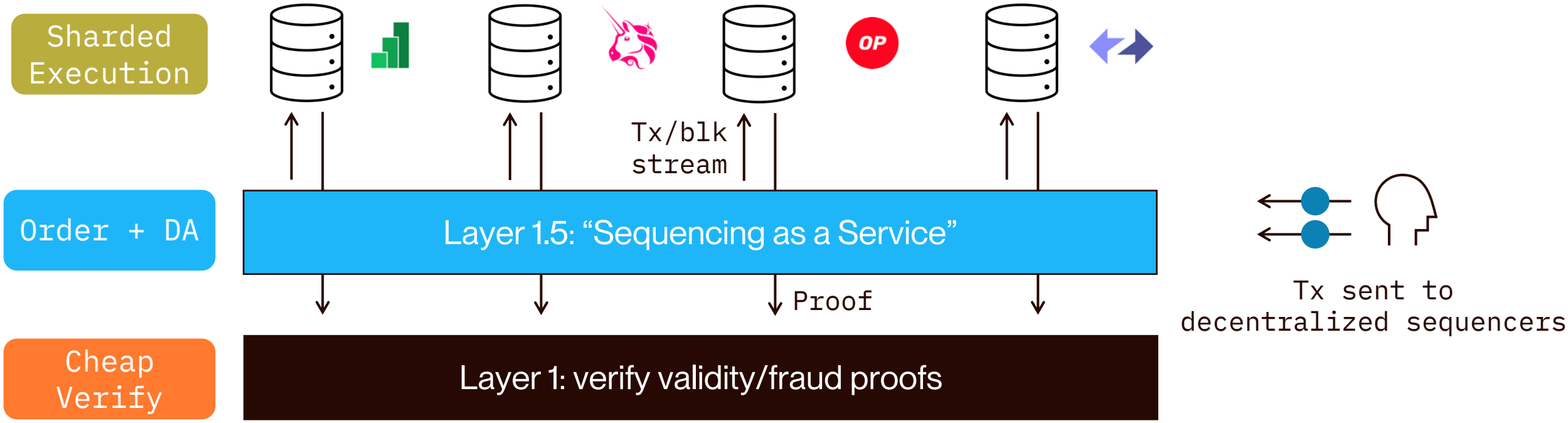
A Centralizes entire decision on
- which txs to include → `Censorship`
- in what order → `Monopolizing MEV`

B Escape Hatch can't handle
- mass exit (esp. can't slash liveness failure)
- price gouging → `Monopolistic Pricing`

“Based Rollup”: Separate ordering from execution



Specialized sequencing layer



Optionally: (duplicated) DA on L1

Reasons for a separate sequencing layer

1

Protocol **modularity**

2

Different design tradeoffs from L1 consensus*

`Fast finality v.s. Dynamically available`

3

Fast Pre-confirmations

`Choose your “settlement layer”`

`*: 12s is block time, finality gadget takes ~15 min`

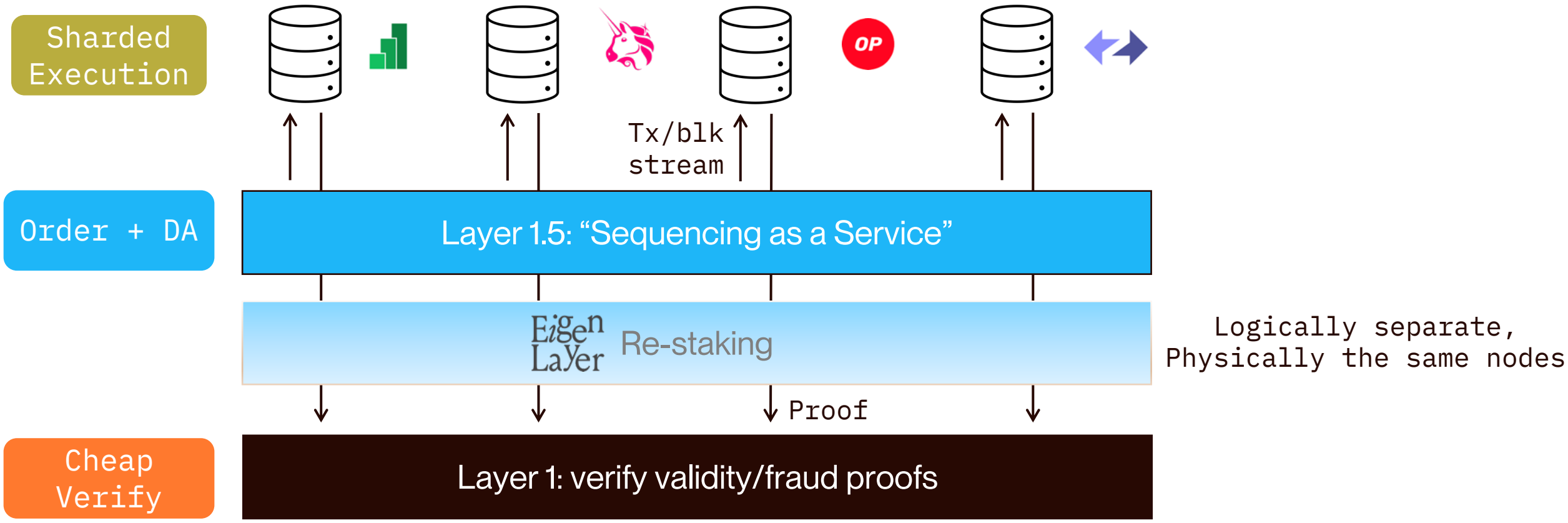
Economic incentive alignment w/ L1

Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

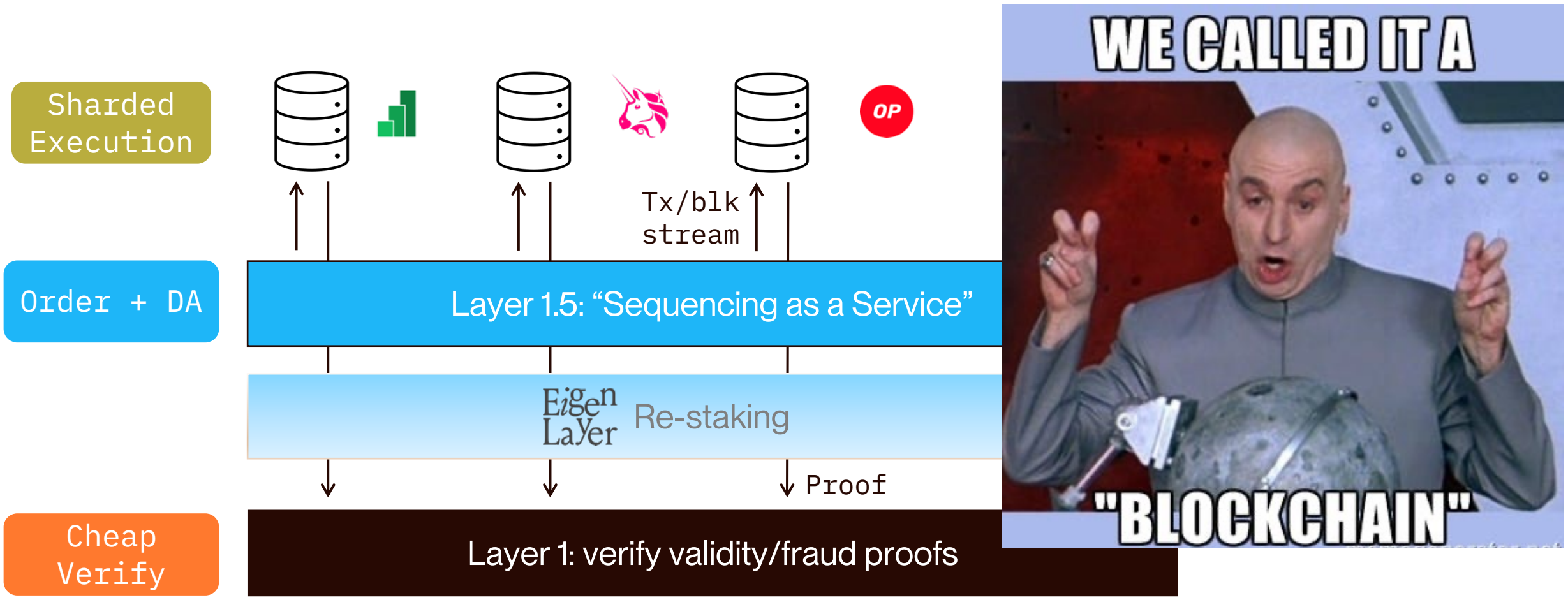
Philip Daian, *Cornell Tech*, phil@cs.cornell.edu
Steven Goldfeder, *Cornell Tech*, goldfeder@cornell.edu
Tyler Kell, *Cornell Tech*, sk3259@cornell.edu
Yunqi Li, *UIUC*, yunqil3@illinois.edu
Xueyuan Zhao, *CMU*, xyzhao@cmu.edu
Iddo Bentov, *Cornell Tech*, ib327@cornell.edu
Lorenz Breidenbach, *ETH Zürich*, lorenz.breidenbach@inf.ethz.ch
Ari Juels, *Cornell Tech*, juels@cornell.edu

We additionally show that high fees paid for priority transaction ordering poses a systemic risk to *consensus-layer* security. We explain that such fees are just one form of a general phenomenon in DEXes and beyond—what we call *miner extractable value* (MEV)—that poses concrete, measurable, consensus-layer security risks. We show empirically that MEV poses a realistic threat to Ethereum today.

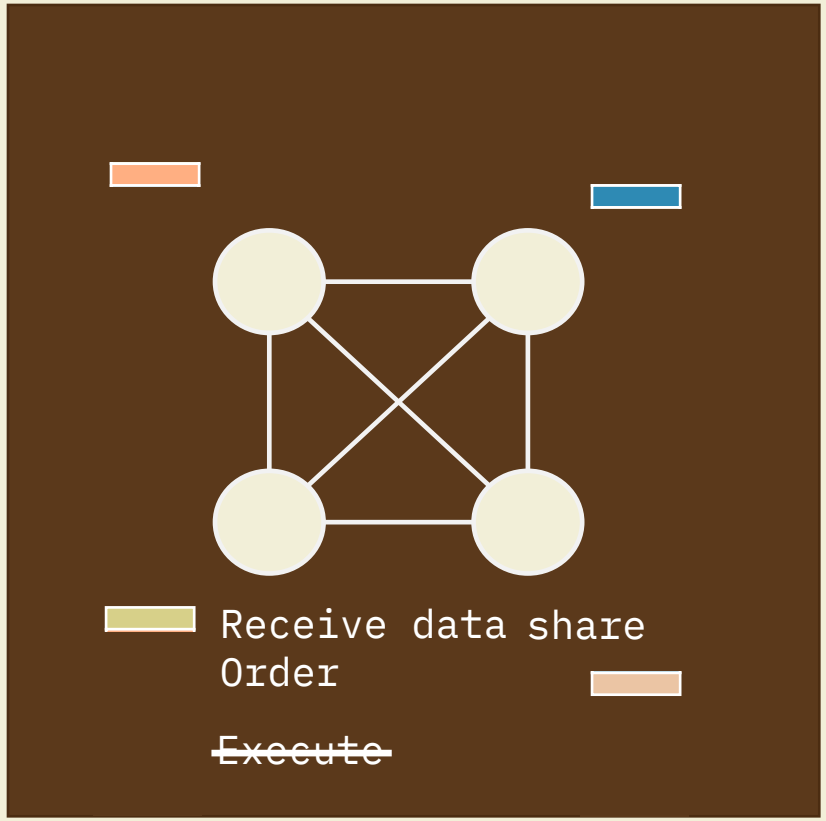
Economic incentive alignment w/ L1



Just another blockchain? Sequencing ≤ SMR!



Key Requirements for ~~SMR~~ Sequencer



~~(Data broadcast)~~ ~~Ensuring transaction data is broadcast to every non-faulty node~~

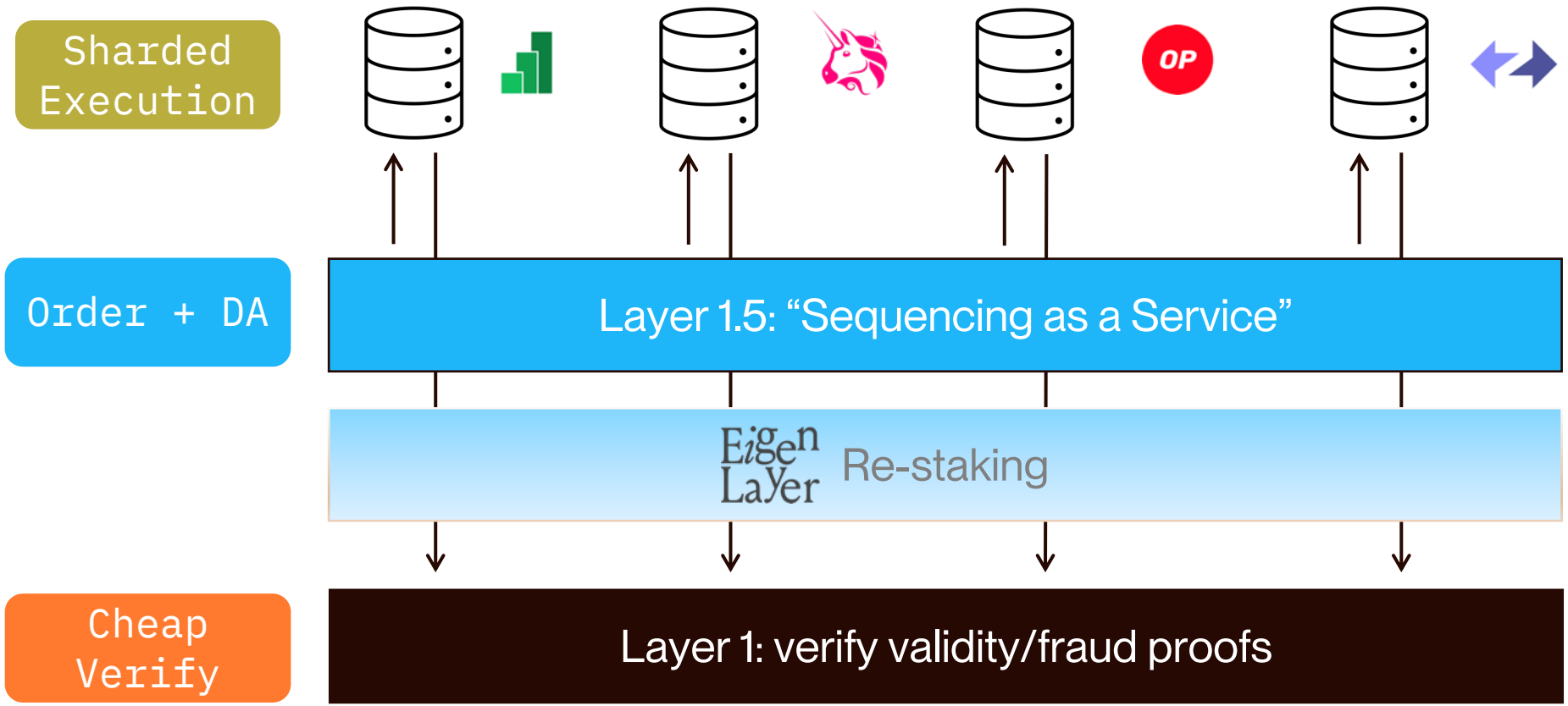
(Data availability) Ensuring availability of data to those who need it

(Consensus) Agree on the order of transactions

~~(Execution)~~ ~~Execute transactions and update state machine~~ No execution

Credit: Kartik Nayak SBC'23 Consensus Talk

Shared sequencing: no fragmentation



Three Advantages of Shared Sequencers

1

Easier bridging

2

Mitigate systemic **security risks** of bridges

3

Support **x-rollup building** with economic bonding

We only provides “**atomic inclusion**”, NOT “atomic execution”.
But this is as good as it gets w/ heterogenous exec env.

Easier bridging

Scenario 1: Siloed Sequencers

- Rollup B verifies
  inclusion of lock on rollup A &
  the validity of A's consensus
- Async, one-way

Scenario 2: Shared Sequencers

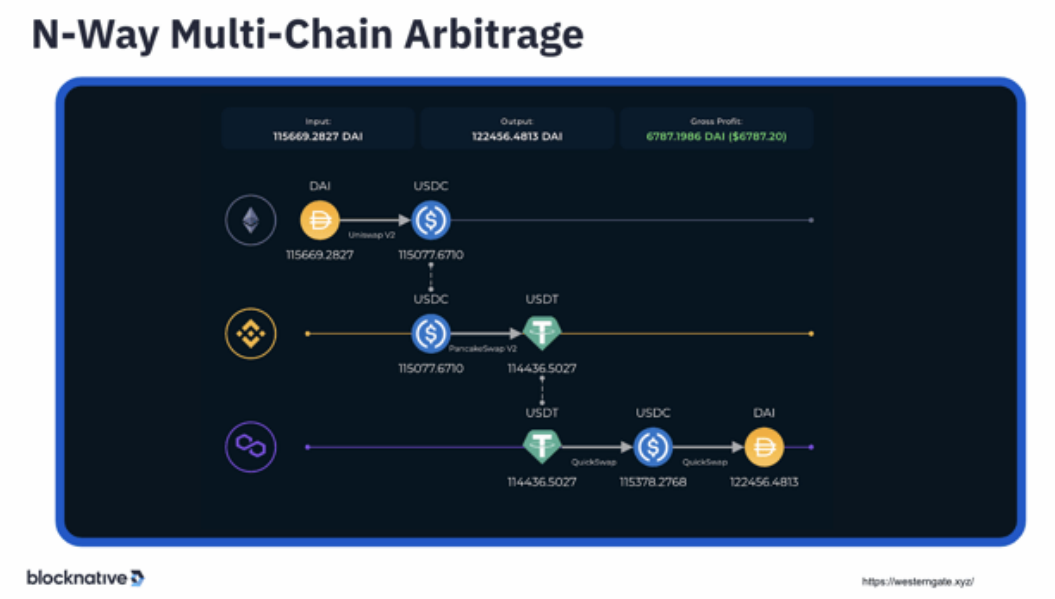
- Rollup B verifies
  inclusion of mint & lock in the same tx
  bundle
- ~Sync, two-way

Image credit: https://chaindebrief.com/blockchain-bridges-how-they-work/

Lower security risk of bridging

- **Consensus reorg** leads to double holding of locked funds
- Shared finality layer ensures **atomicity**
  - Finality is hard to violate
  - Even w/ reorg, both lock & mint are reverted

Easier X-rollup building



Scenario 1: Siloed Sequencers

- Win PBS auctions on both chains, simultaneously!
- Just be proposer simultaneously ! → higher stake required, centralization risk

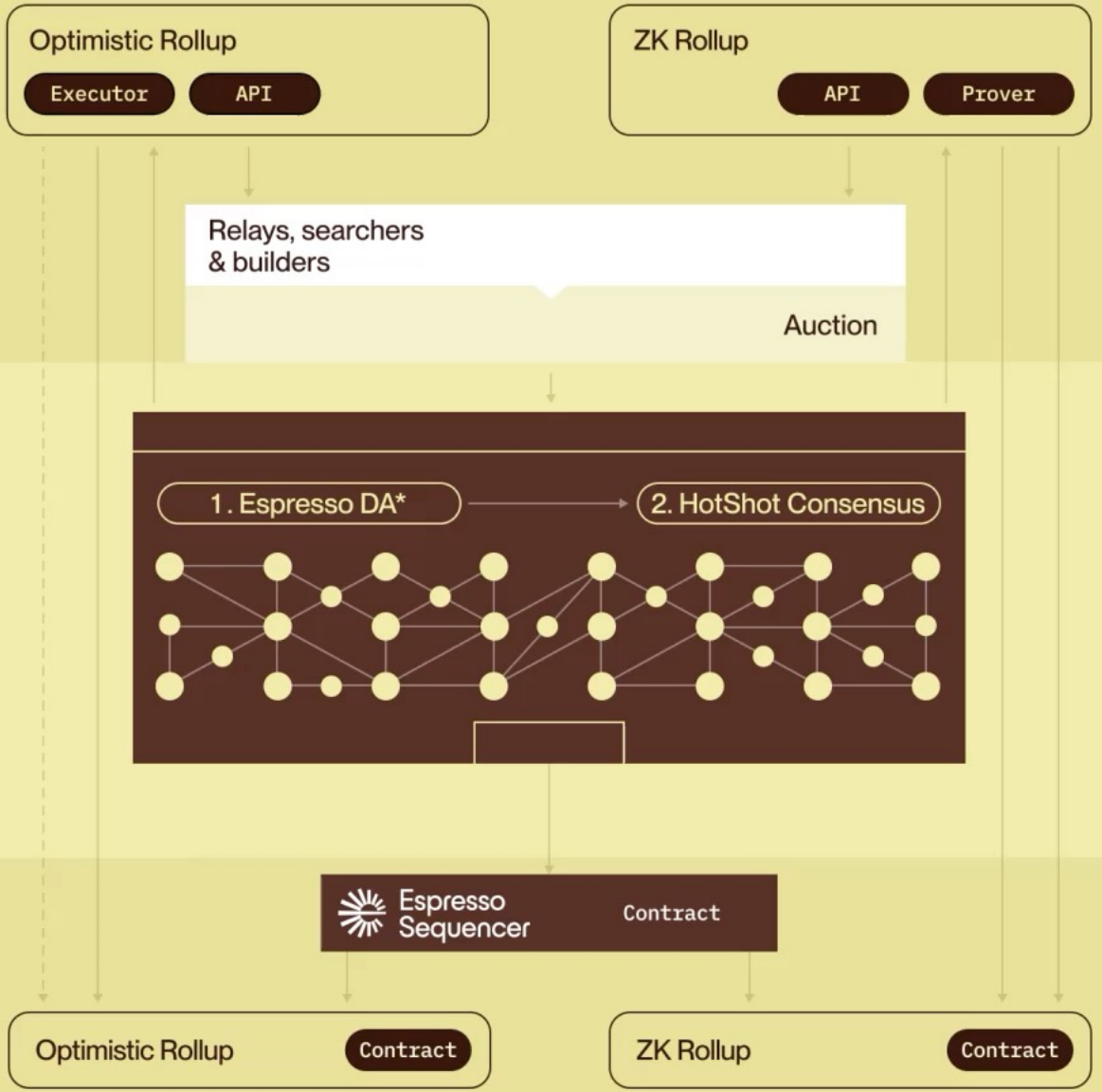
Scenario 2: Shared Sequencers

- Win PBS auction once
- Builder gives economically-bonding promise of atomic inclusion

Image credit: https://www.blocknative.com/blog/fundamentals-of-cross-chain-mev

End user clients

L2



Espresso Sequencer

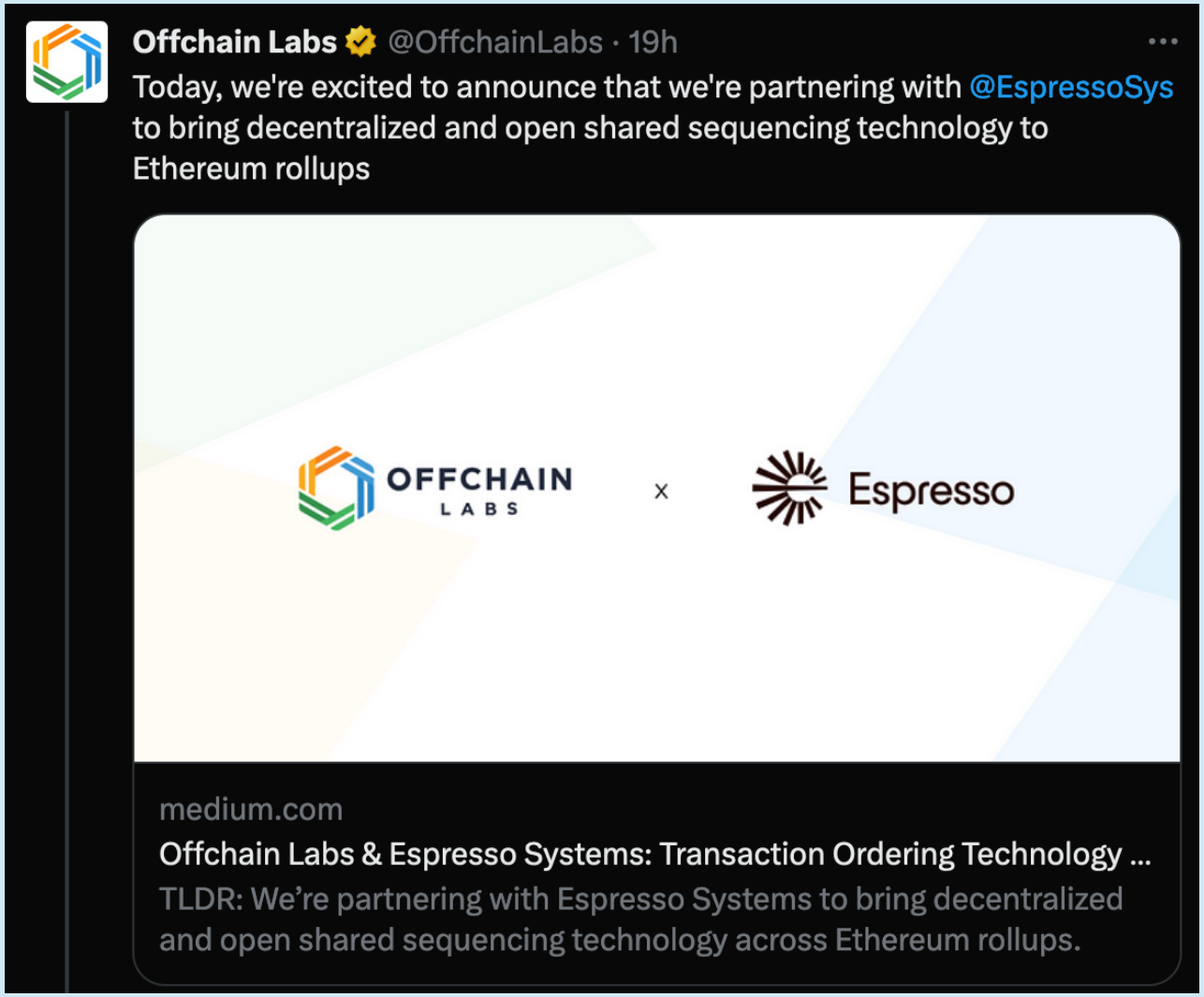
*Rollups may aditionally use Ethereum for data availability.

L1

Demo: Optimism + Cortado testnet!

Github: https://github.com/EspressoSystems/op-espresso-integration

Partnership: Offchain Labs & Espresso



Espresso Systems

espressosys.com

Reach out to us!

Ben Fisch
CEO

Charles Lu
COO

Benedikt Bünz
Chief Scientist

Jill Gunter
Chief Strategy Officer

Binyi Chen
Chief Cryptographer

Fernando Krell
VP Engineering