Scaling Blockchains

LIONELLO LUNESU
lio@enuma.io

TAMÁS HERMAN
tamas.herman@enuma.io

Nov 24th 2018, Codeconf

Blockchain Scalability Challenges

- **Every** miner processes **every** transaction
  - ➔ All transactions compete to be included in the next block
- **All** transactions are recorded **indefinitely** by **every** full node
  - ➔ The size of the blockchain data is ever-increasing
- Transactions **must** get mined to be deemed valid
  - ➔ Recipients must wait for N confirmations from miners for transaction finality

Scalability

State Size

- Bitcoin: ~200 GB
- Ethereum: ~1TB

Transaction Speeds

- Bitcoin Core: ~5 tx/sec
- Ethereum: ~20 tx/sec
- Bitcoin Cash: ~100 tx/sec
- Nasdaq: ~10k tx/sec
- Visa: ~25k tx/sec

Scalability Solutions

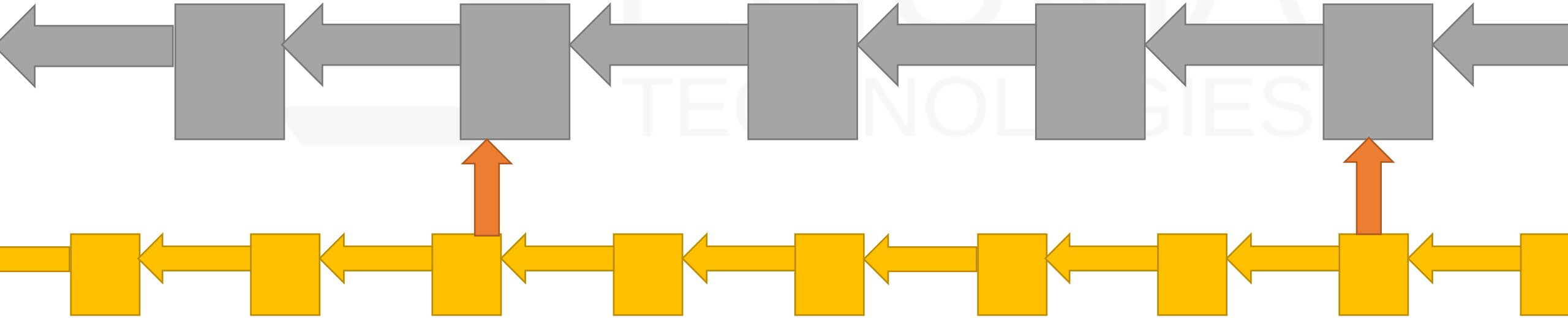
- Layer 1
  - Increase artificial limits (block size, gas limit)
  - New instruction sets
  - New consensus algorithm
  - Sharding
  - Etc.
- Layer 2 Technologies
  - Hierarchy of chains – e.g. Plasma, Cosmos, Polkadot
  - State Channels – e.g. Lightning Network, Raiden, Connext, Sprites

”Layer 2” technologies

- “Layer 1” is the “central” blockchain
- “Layer 2” relies on the security of ”Layer 1”
- “Layer 2” can use different consensus, rules, chain, tx speed, …

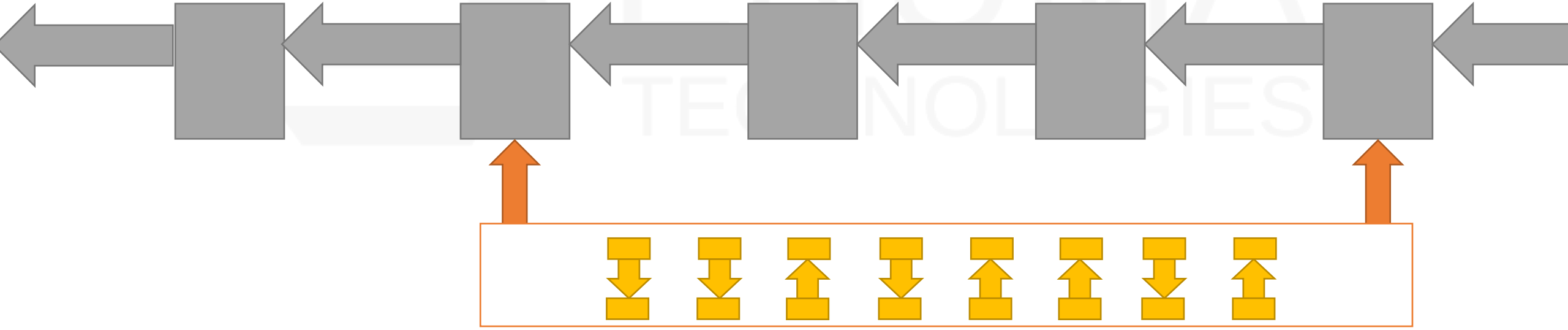
Hierarchy of chains

- Periodically sync the hash to parent to avoid tempering in child
- When the child chain can’t advance, parent allows withdrawal



State Channels

- Opening and closing a channel happens on the main chain
- An open channel allows for secure, off-chain transactions



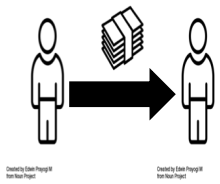
Looks familiar?

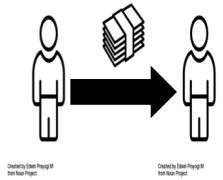
Created by Atif Arshad
from Noun Project

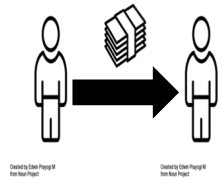
Created by Icon Fair
from Noun Project

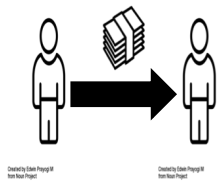
Created by Icon Fair
from Noun Project

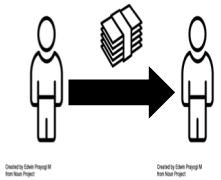
Created by Icon Fair
from Noun Project











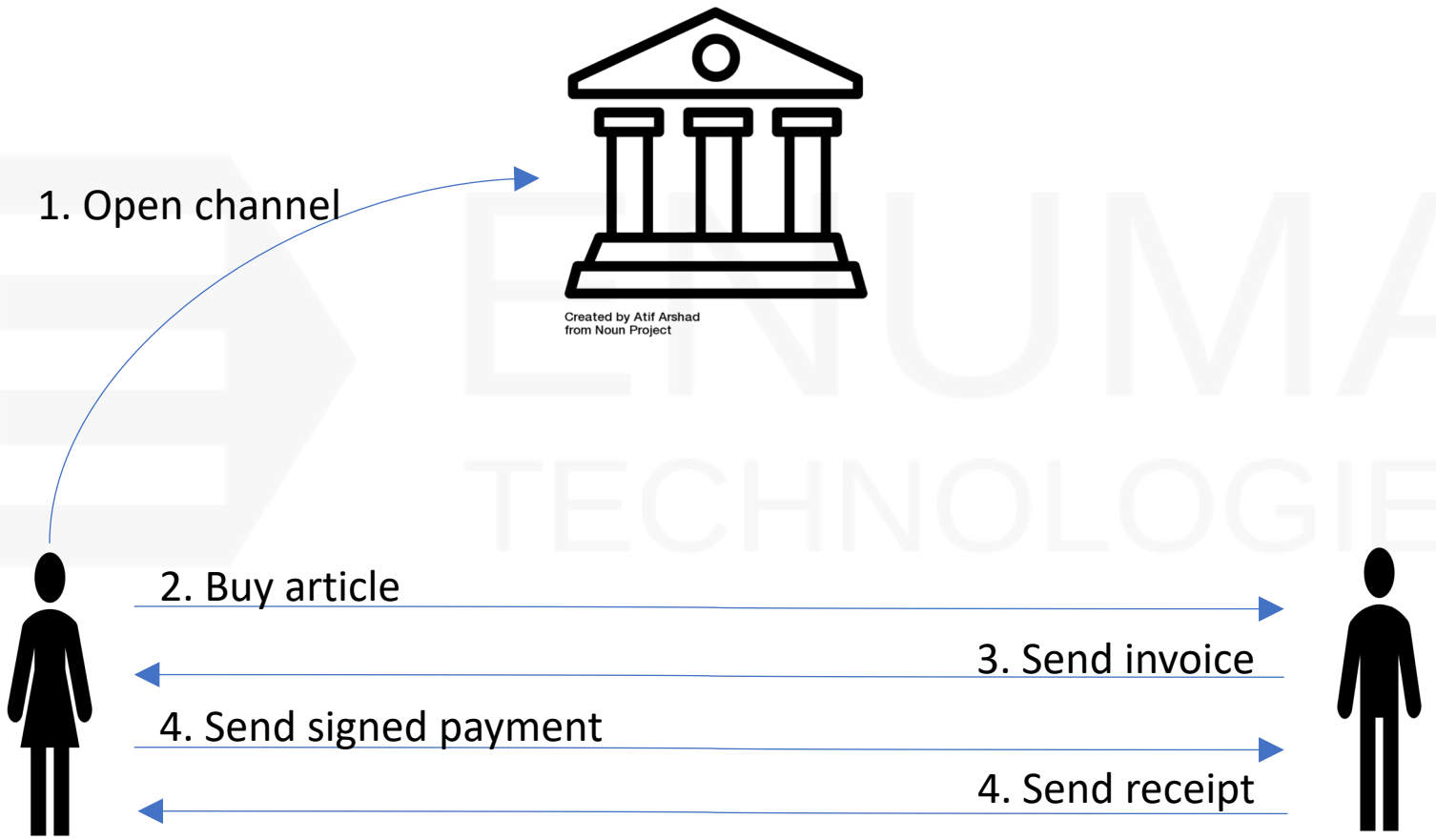
State Channels Scalability

Each state channel

- allows 2 peers to transact
- requires opening (and closing) on-chain
- requires a deposit
- requires client-side bookkeeping

Sprites – unconditional payments

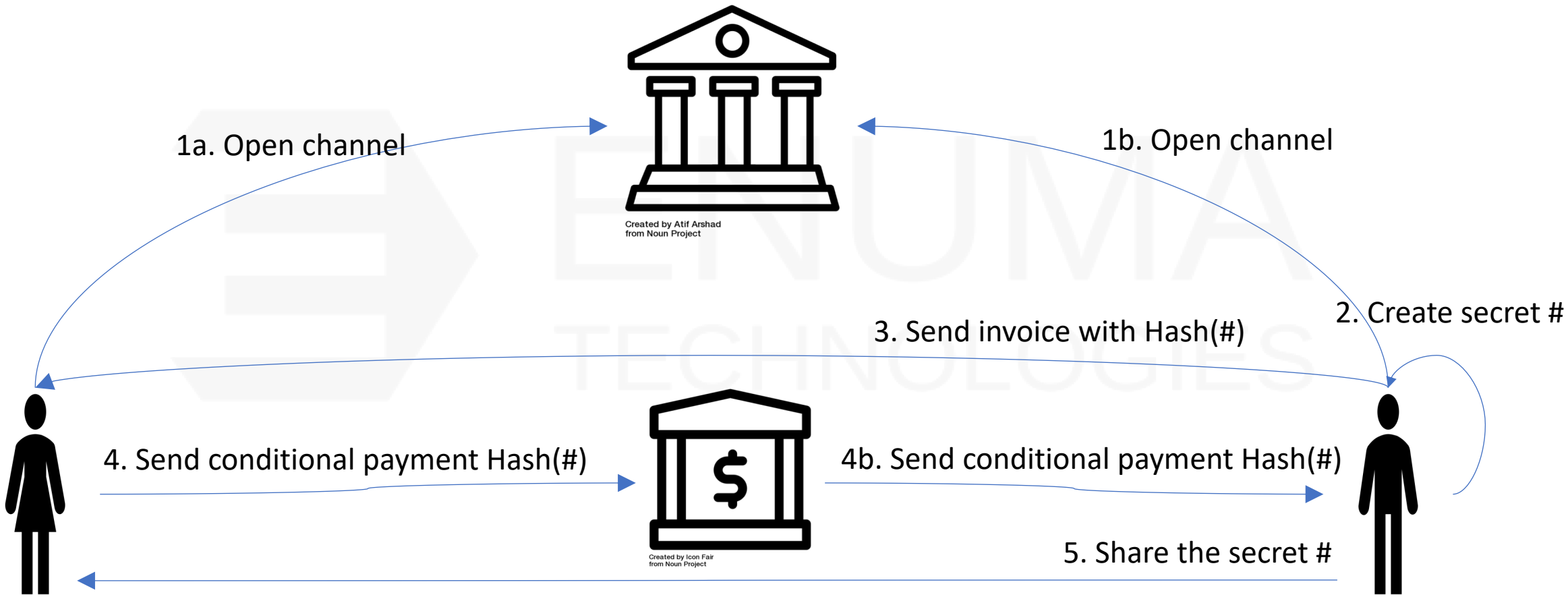
ethereum foundation grants



ENUMA TECHNOLOGIES

Sprites – conditional payments

ethereum foundation grants



ENUMA TECHNOLOGIES

Demo

- https://github.com/enumatech/sprites

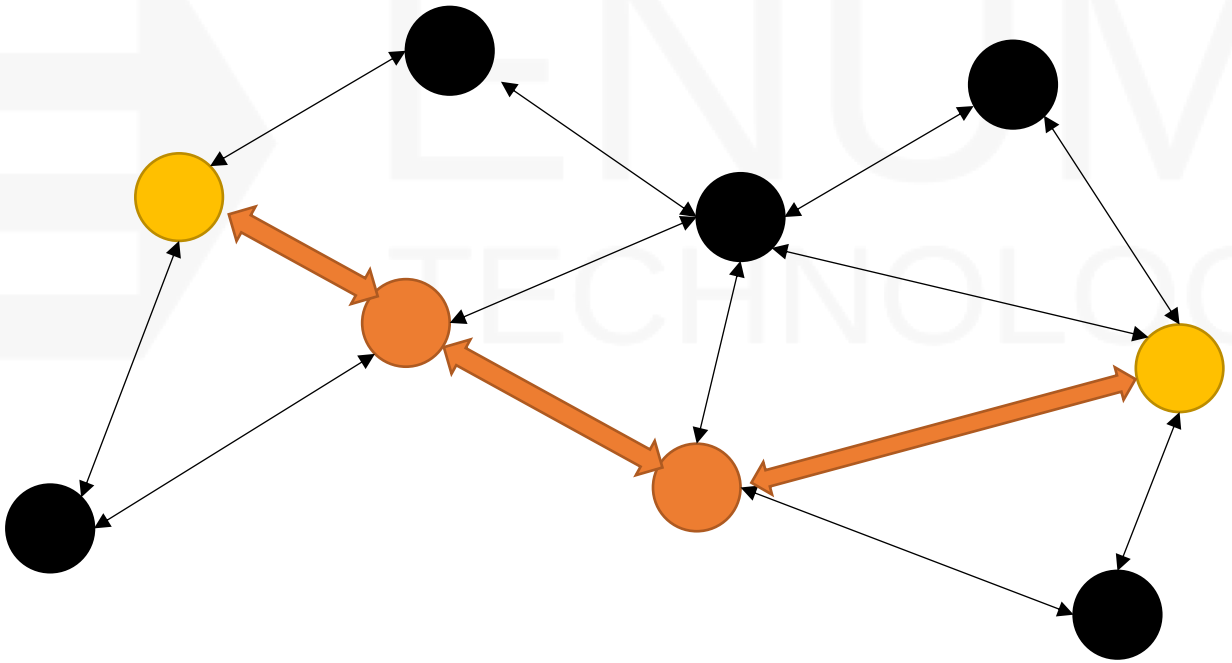
- Using

  nix, direnv, overmind, pnpm, node, solc, geth, rambda

ENUMA
TECHNOLOGIES

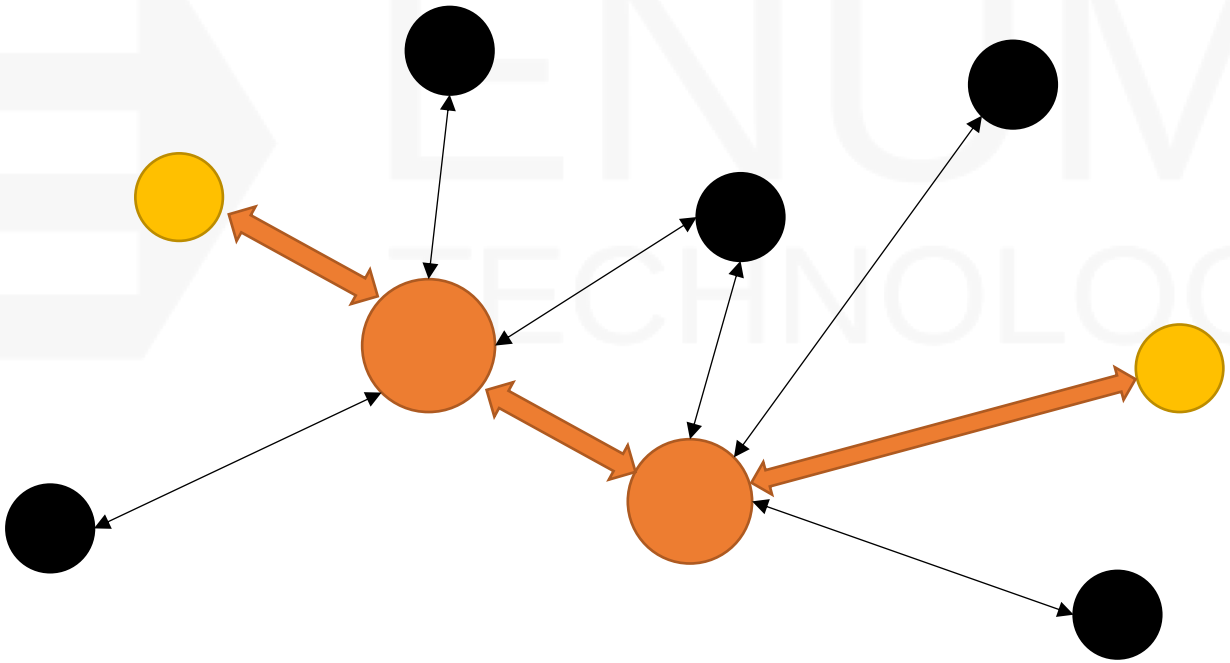
State Channels Solutions: Routing

- Route transactions through other channels

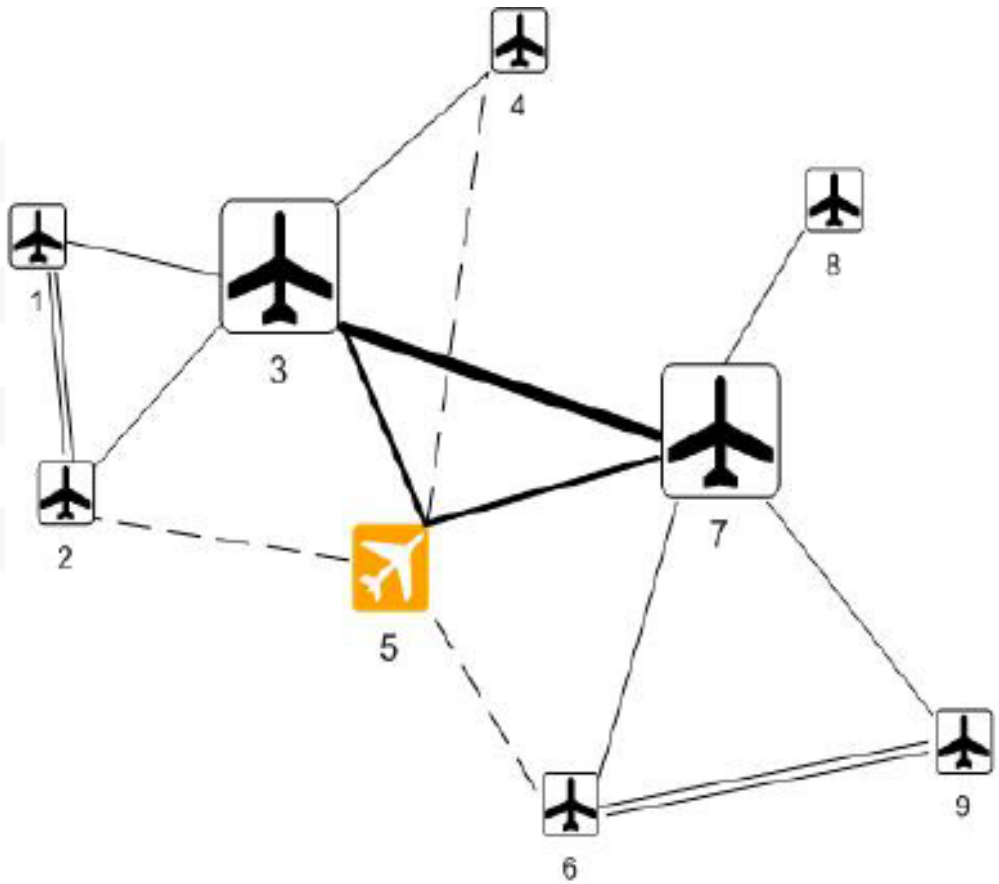


State Channels Solutions: Hub-Spoke

- Route transactions through **hubs**



Looks familiar?

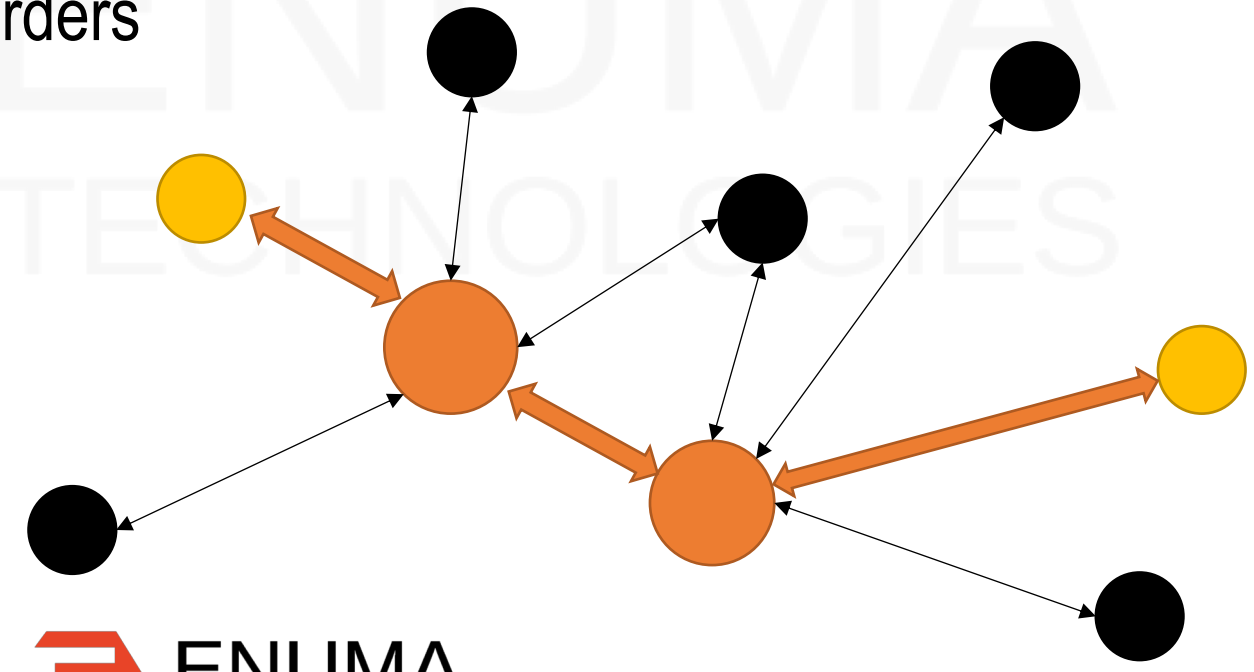


ENUMA
TECHNOLOGIES

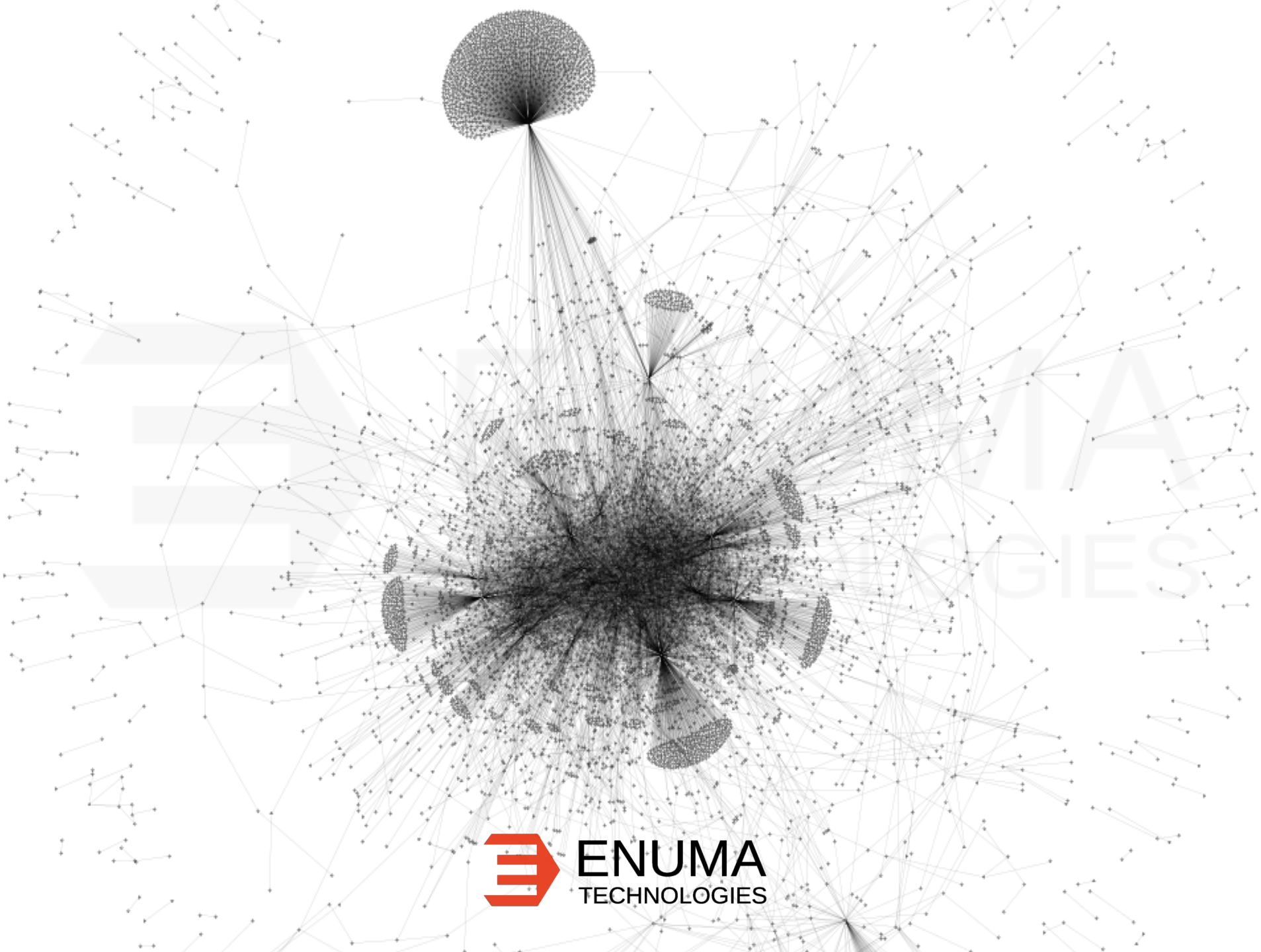
Decentralized Exchange

OAX DEX

- Open channel with an exchange
- Atomic swap
- Exchanges aggregate their orders



Q?



ENUMA
TECHNOLOGIES

Thank You
多謝

LIONELLO LUNESU
lio@enuma.io

TAMÁS HERMAN
tamas.herman@enuma.io

blog.enuma.io
github.com/enumatech

ENUMA
TECHNOLOGIES