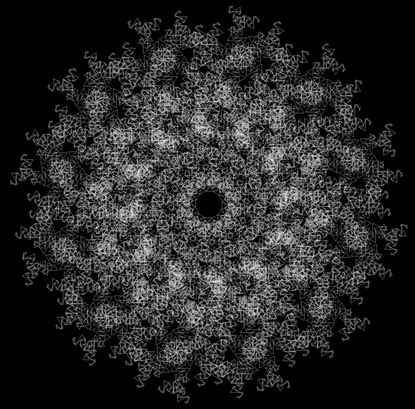
Isaac Sheff

Heliax .dev

TYPHON

Naqib Zarin



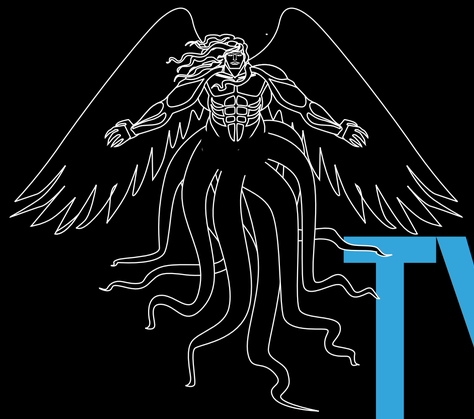
TG x Thoth

anoma

Aleksandr Karbyshev

Heliax.dev

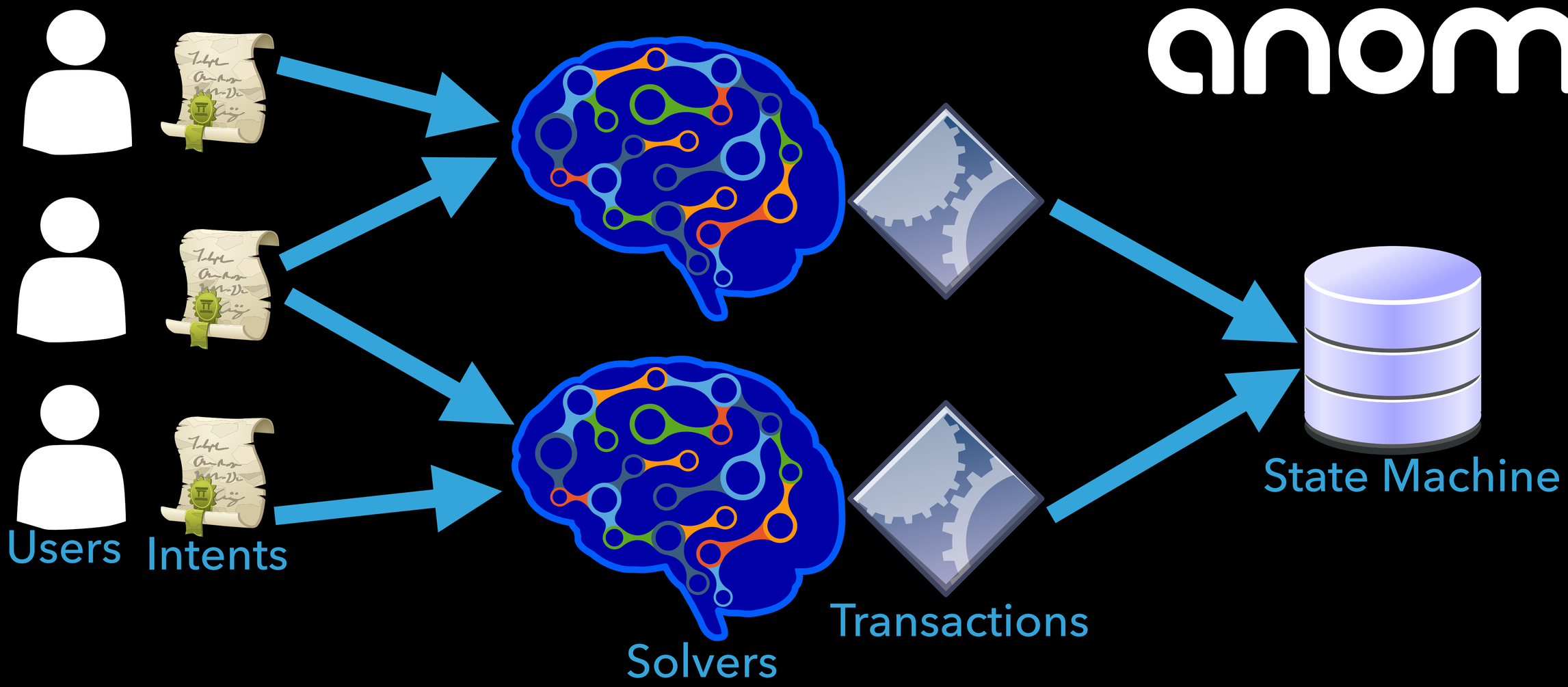
Tobias Heindel



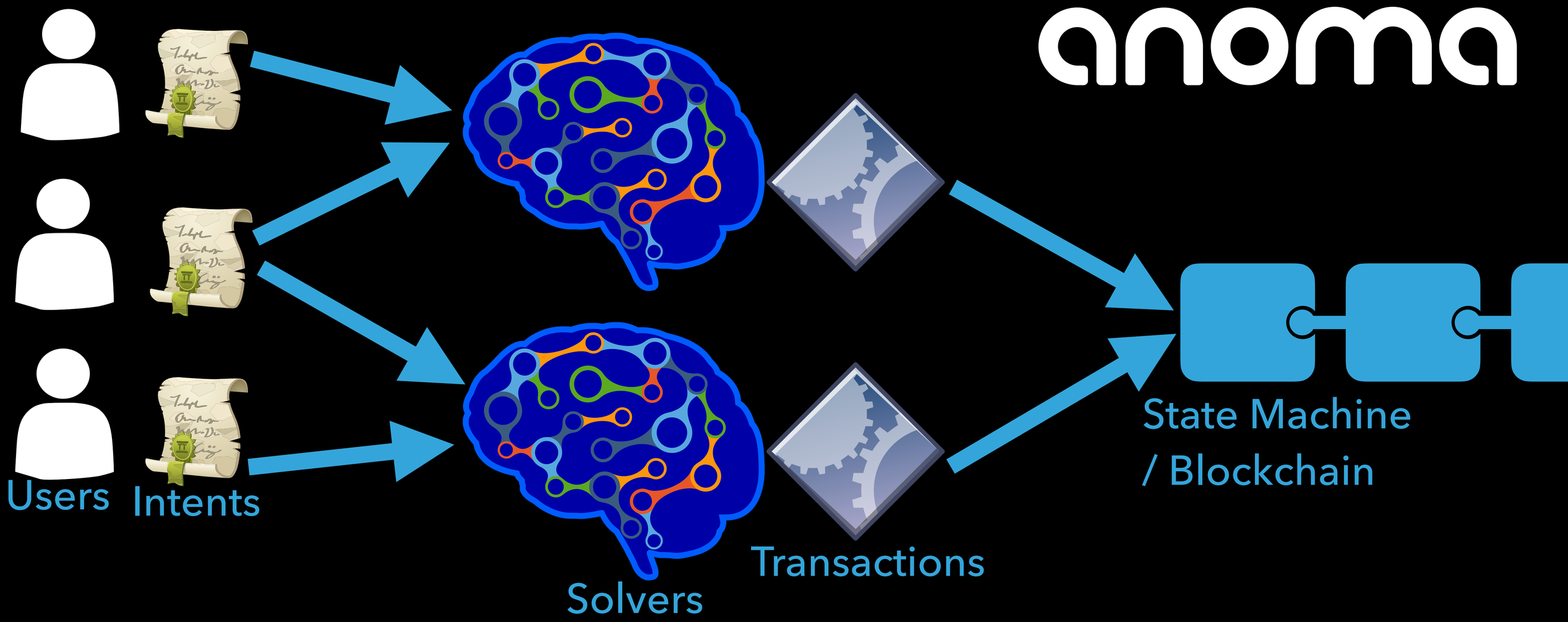
TYPHON

Isaac Sheff

anoma



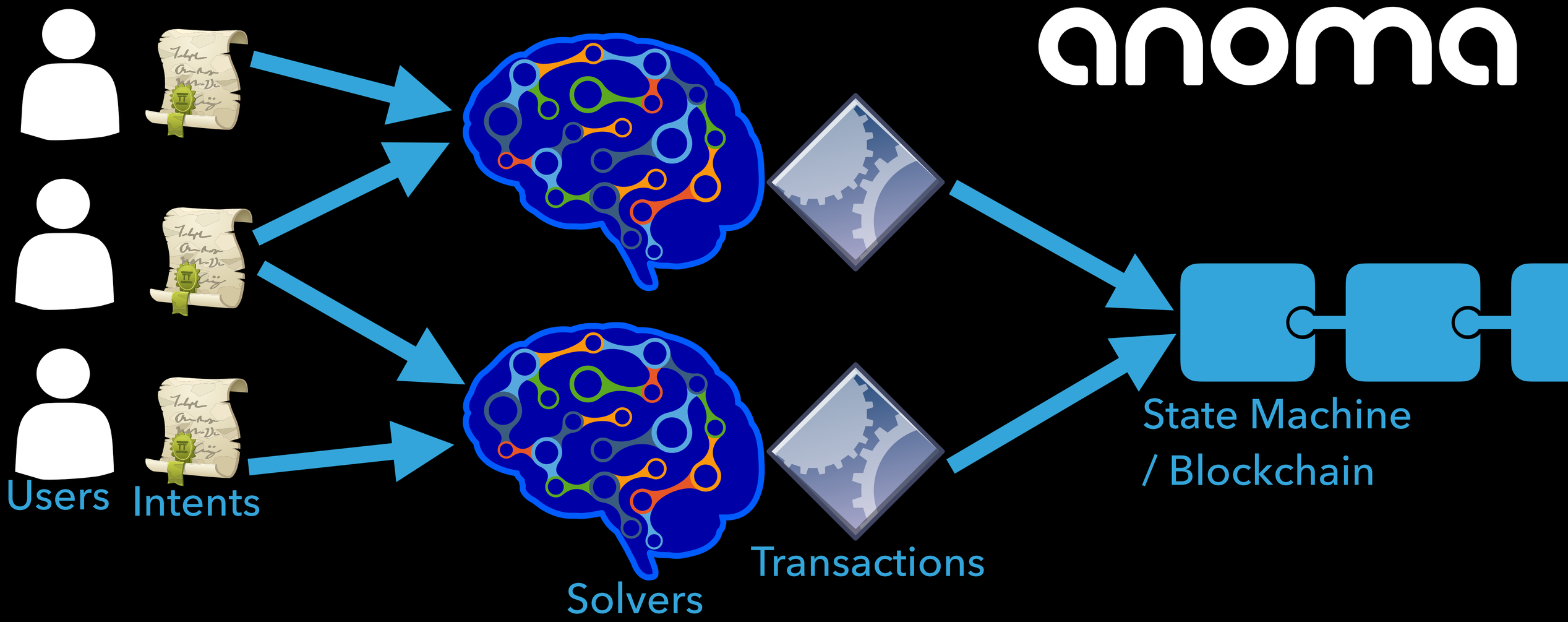
anoma


Users
Intents
Solvers
Transactions
State Machine
/ Blockchain

3 POINTS

- Shared P2P Layer

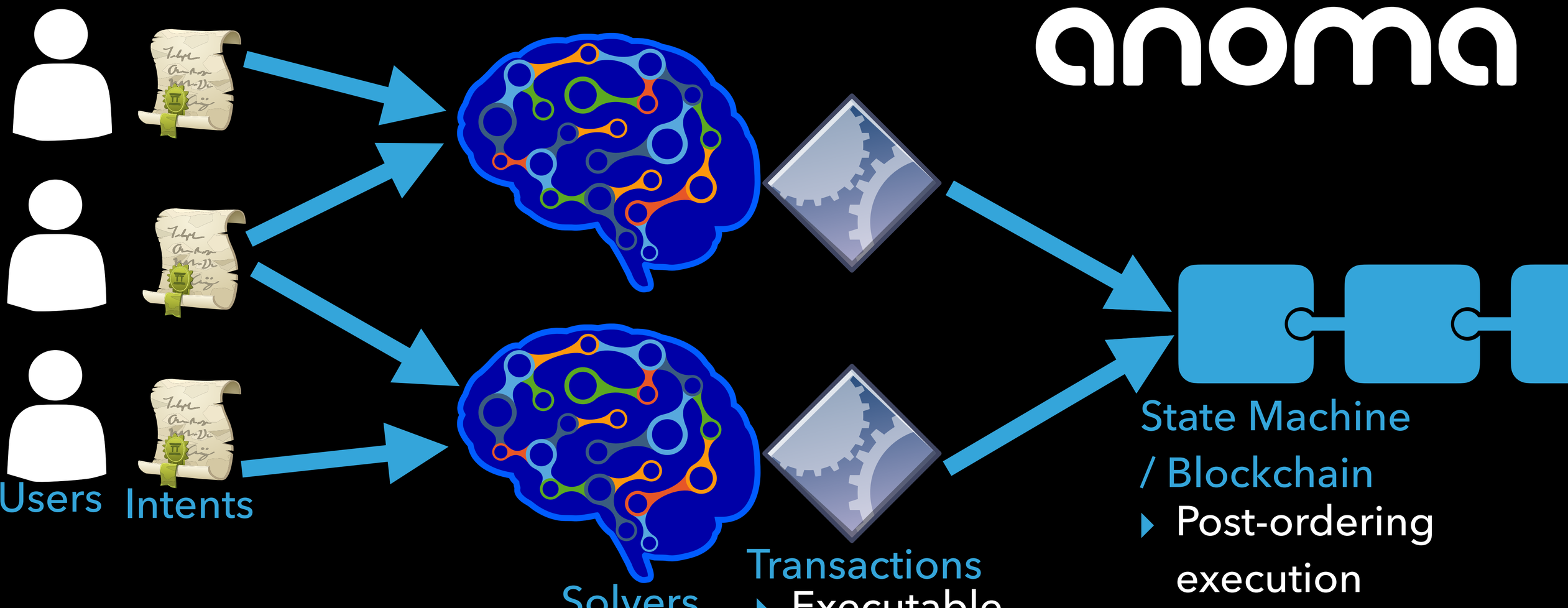
anoma



3 POINTS

- Shared P2P Layer
- Post-ordering execution

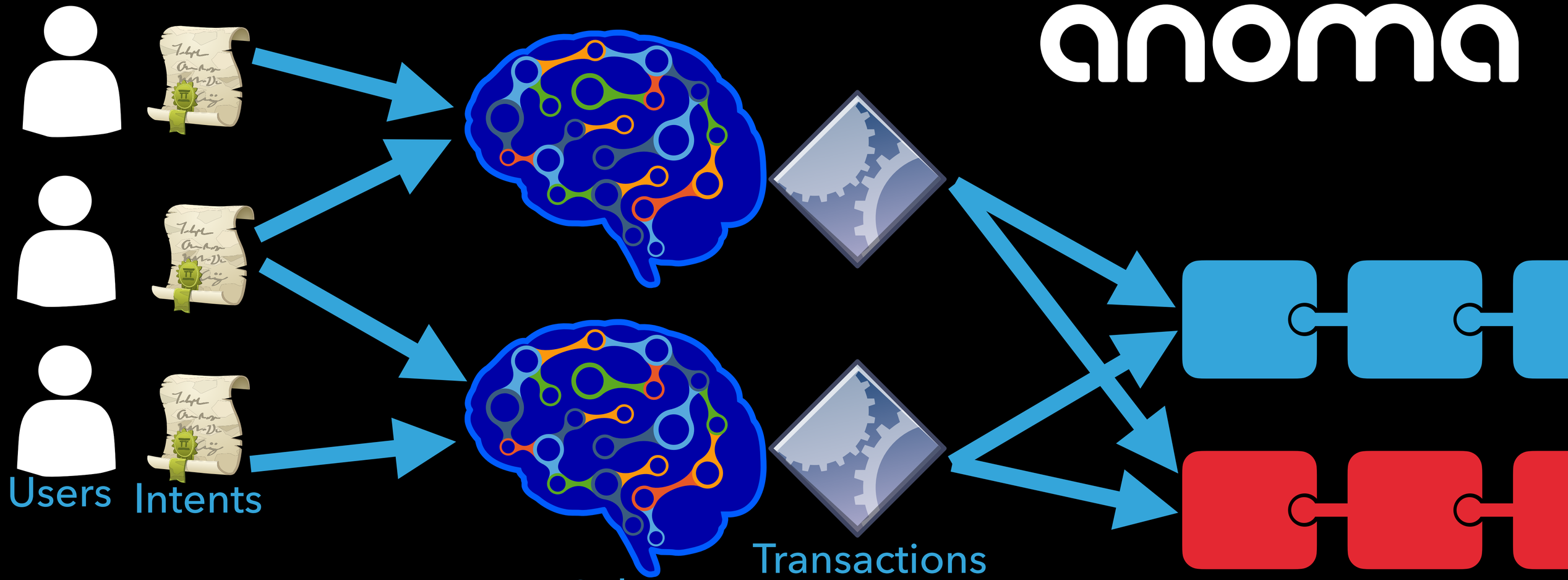
anoma

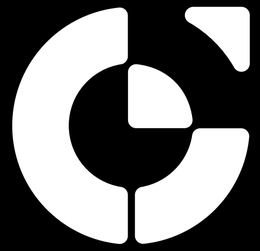


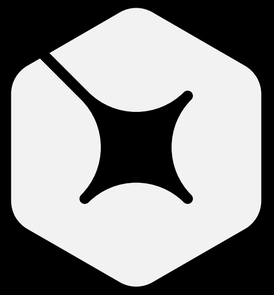
3 POINTS

- Shared P2P Layer
- Post-ordering execution
- Multi-chain transactions

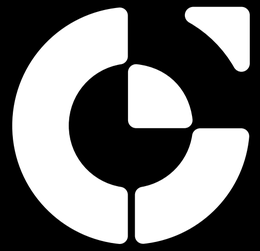
anoma

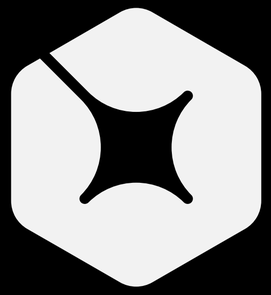






anoma uses CometBFT





anoma uses CometBFT

anoma will use TYPHON, which supports CHIMERA CHAINS

CometBFT

HETEROGENEOUS TRUST

- Many Instances
- Shared Validators
  - Software for multiple instances
  - Add chains on demand
  - Reduce redundancy

COMPONENTS

Shared P2P Layer

P2P

- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153

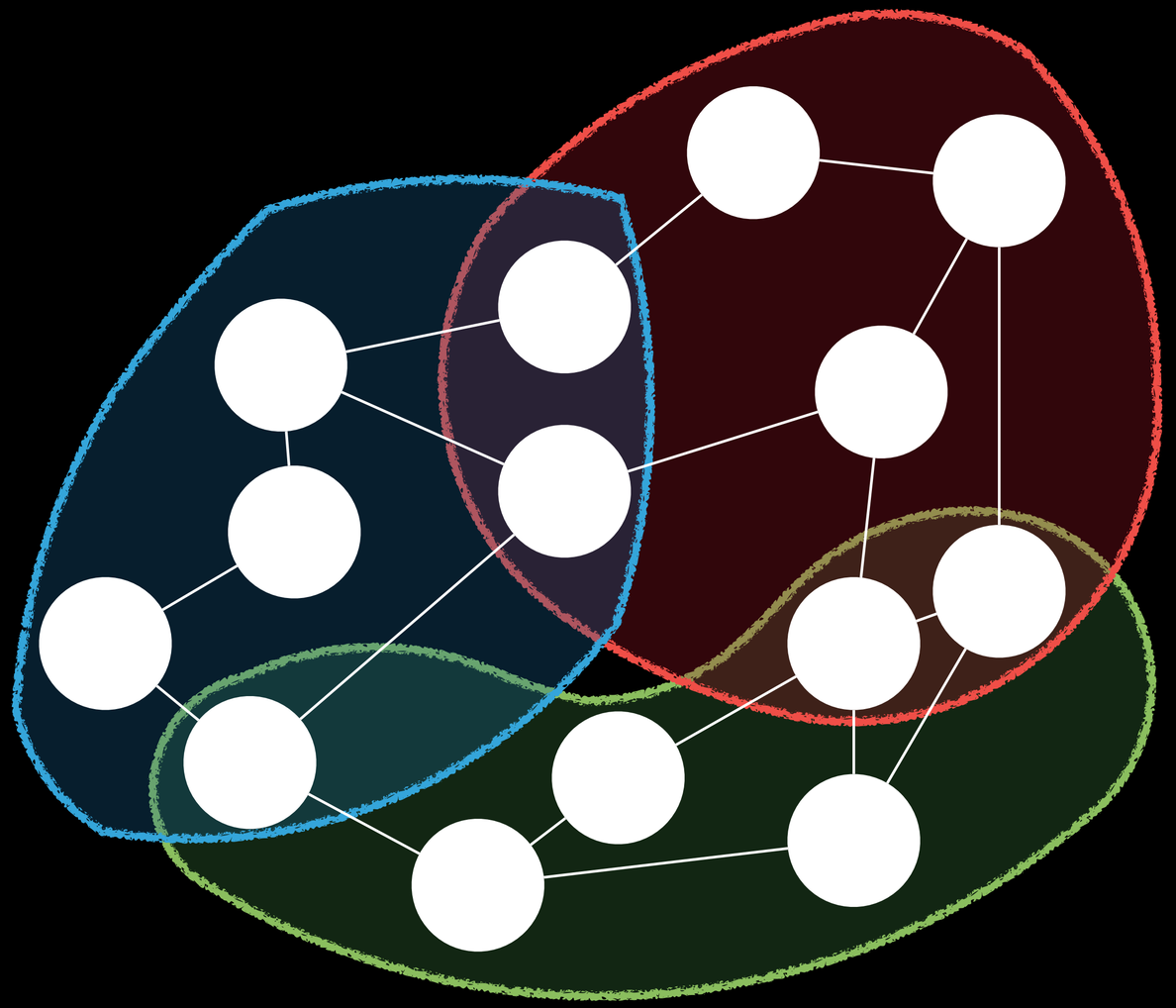
Naqib Zarin

Isaac Sheff

Stefanie Roos
TU Delft

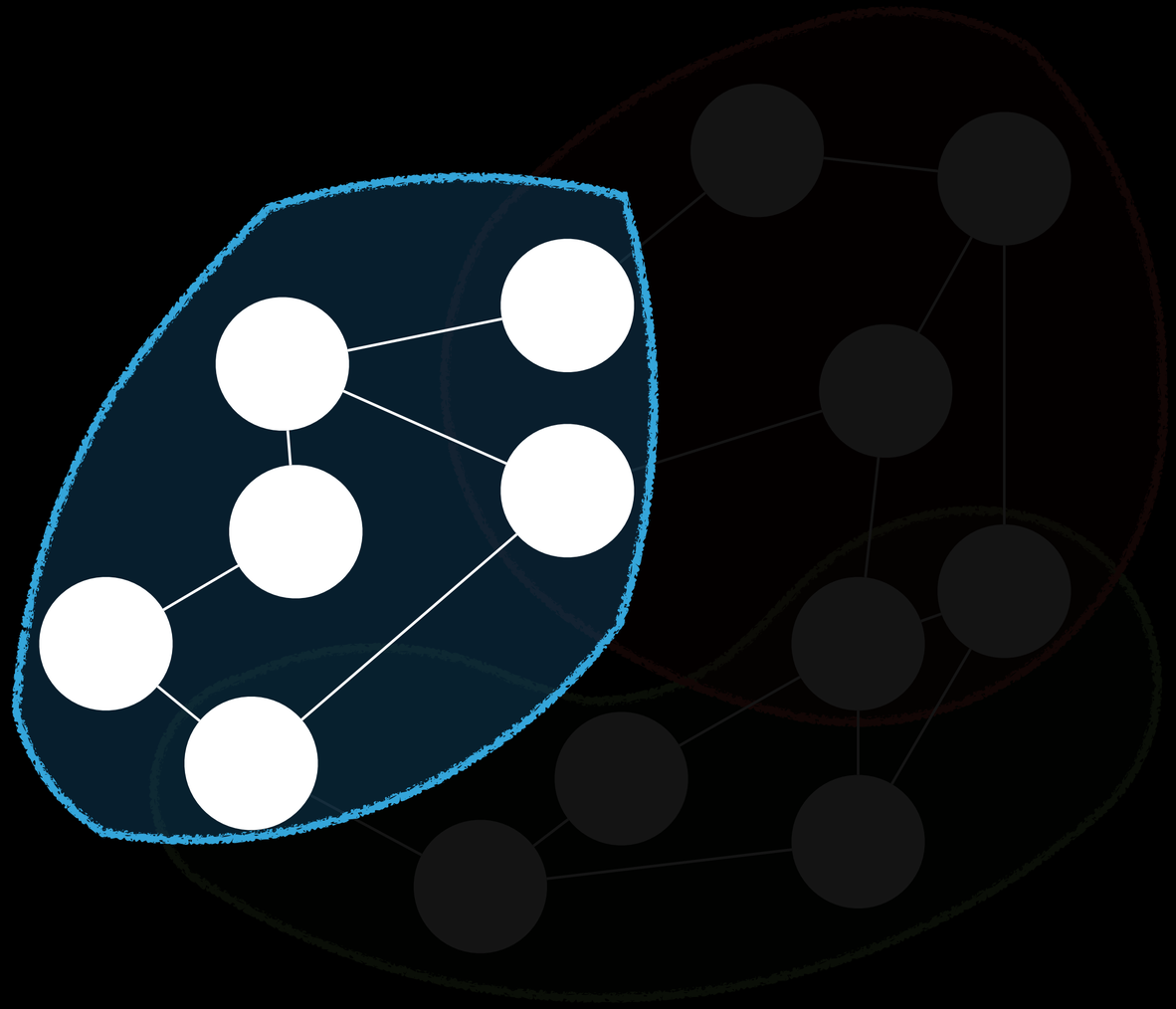
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)



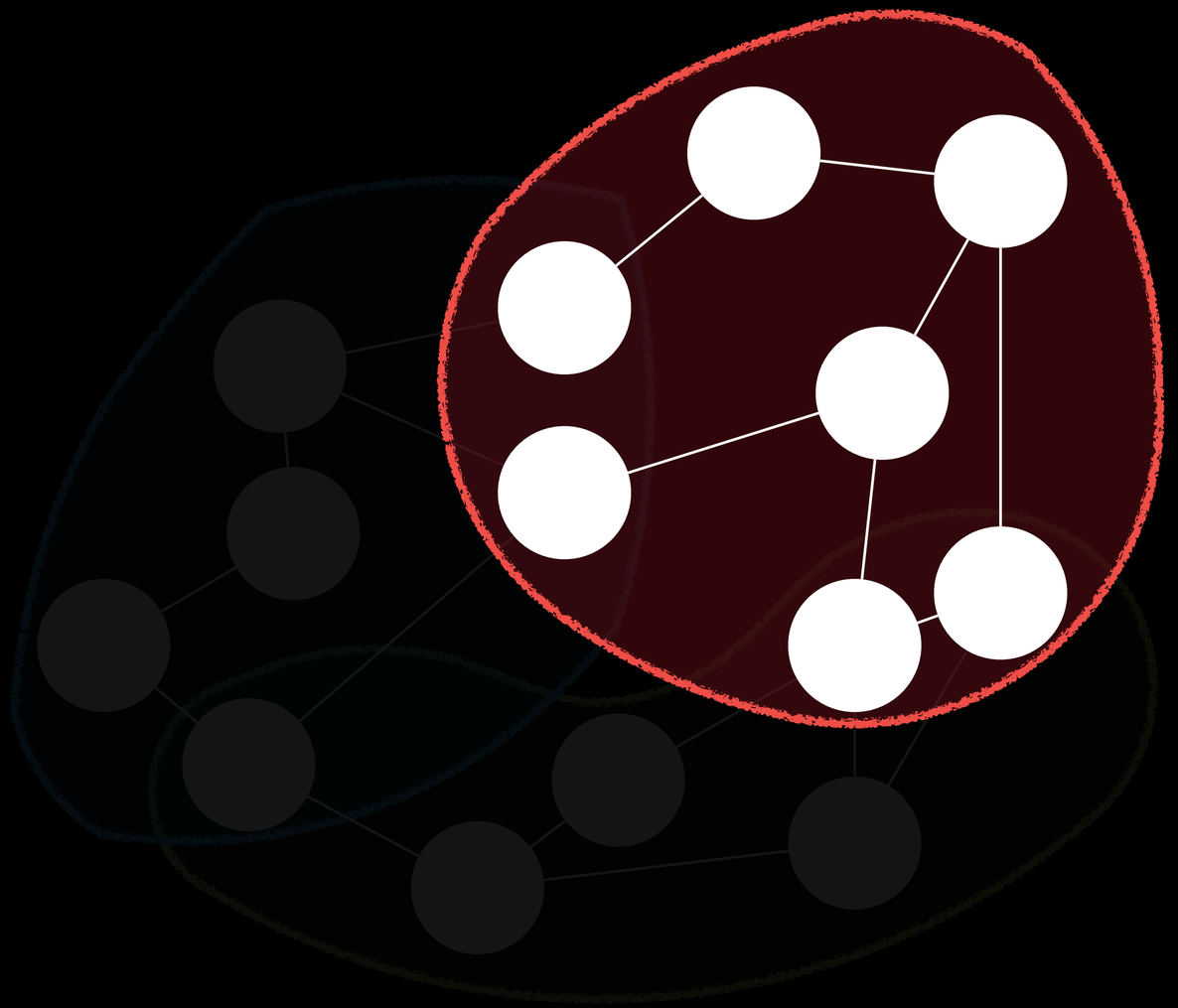
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)



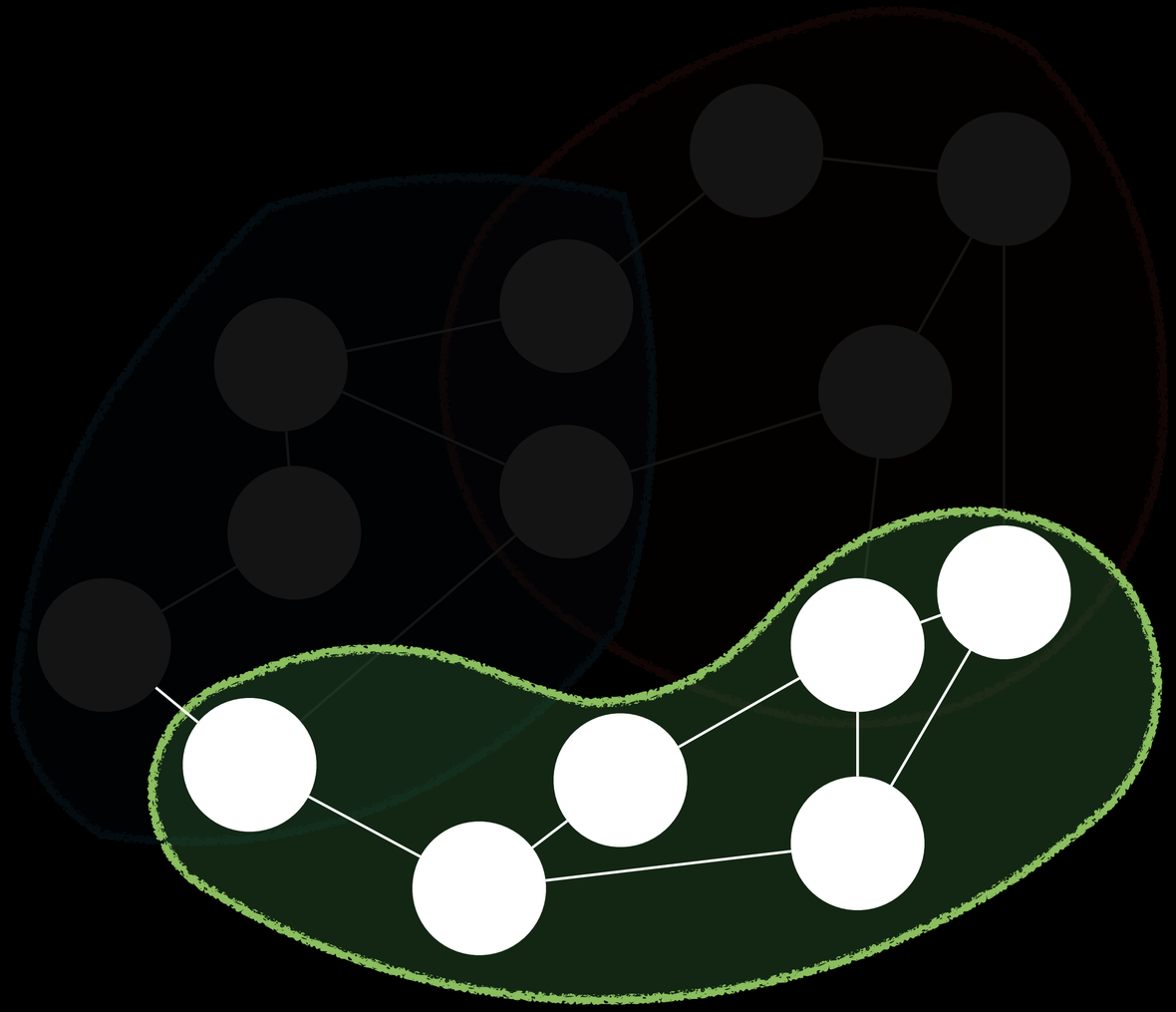
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)



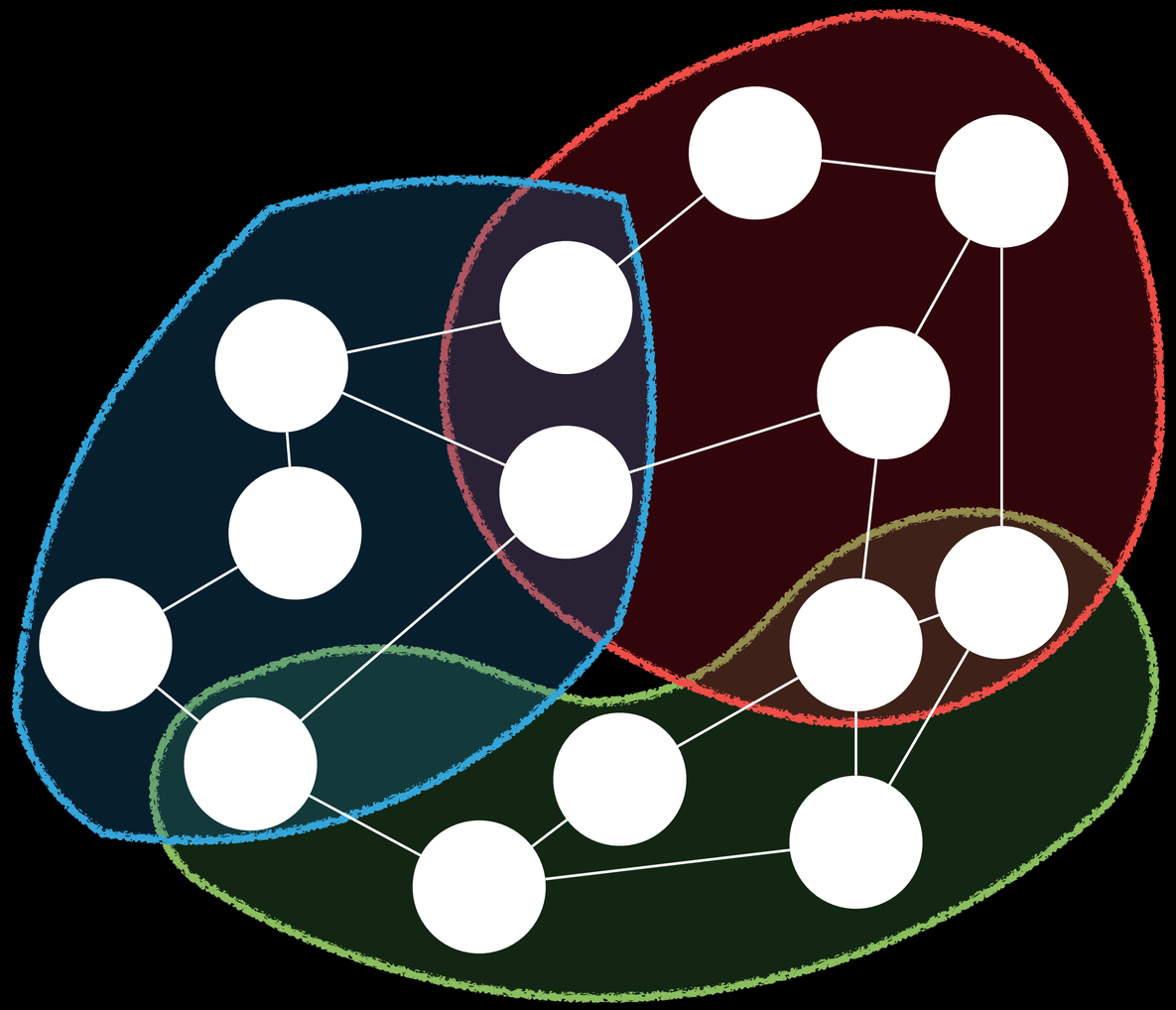
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)



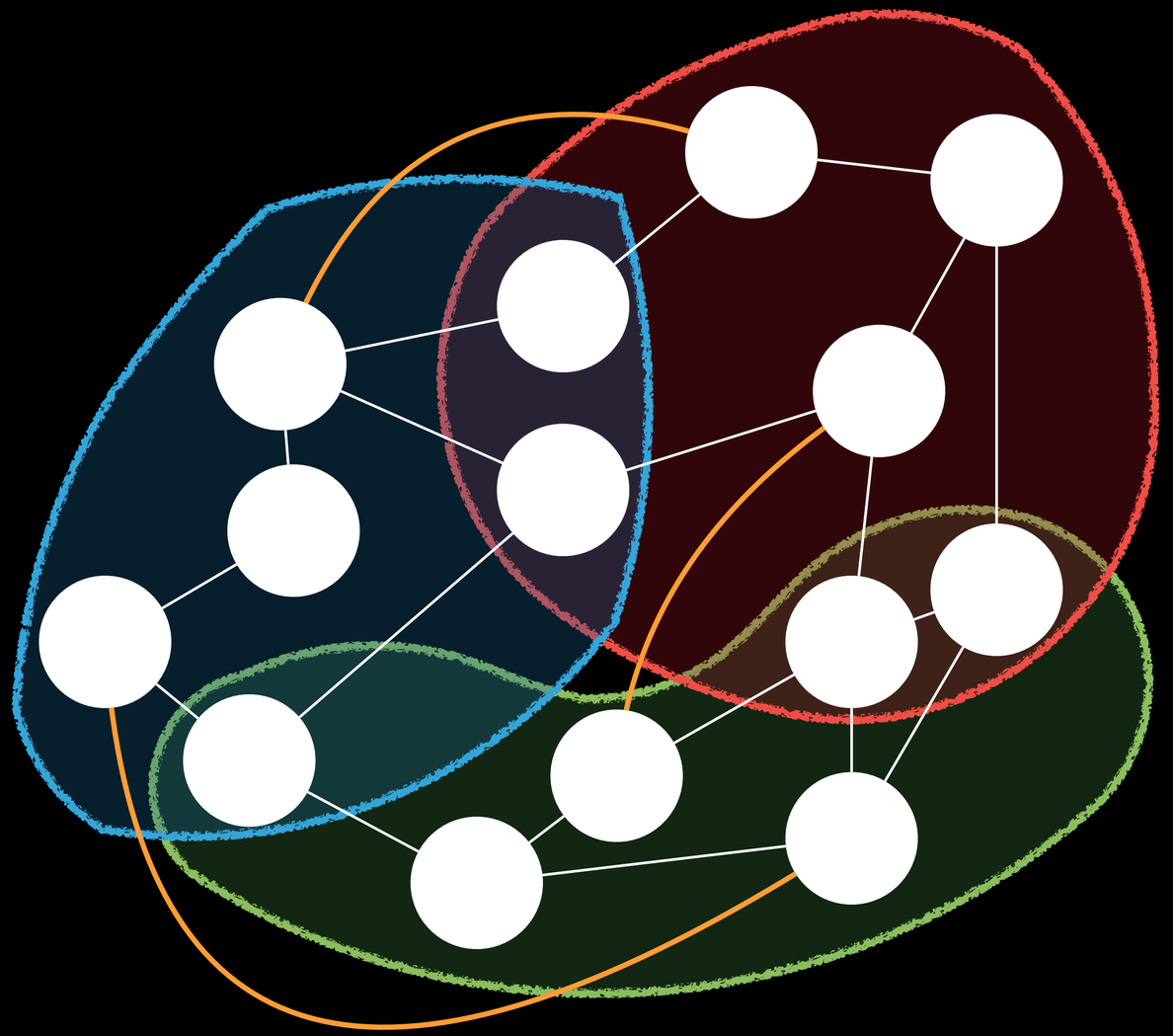
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)
  - Performance of a small overlay



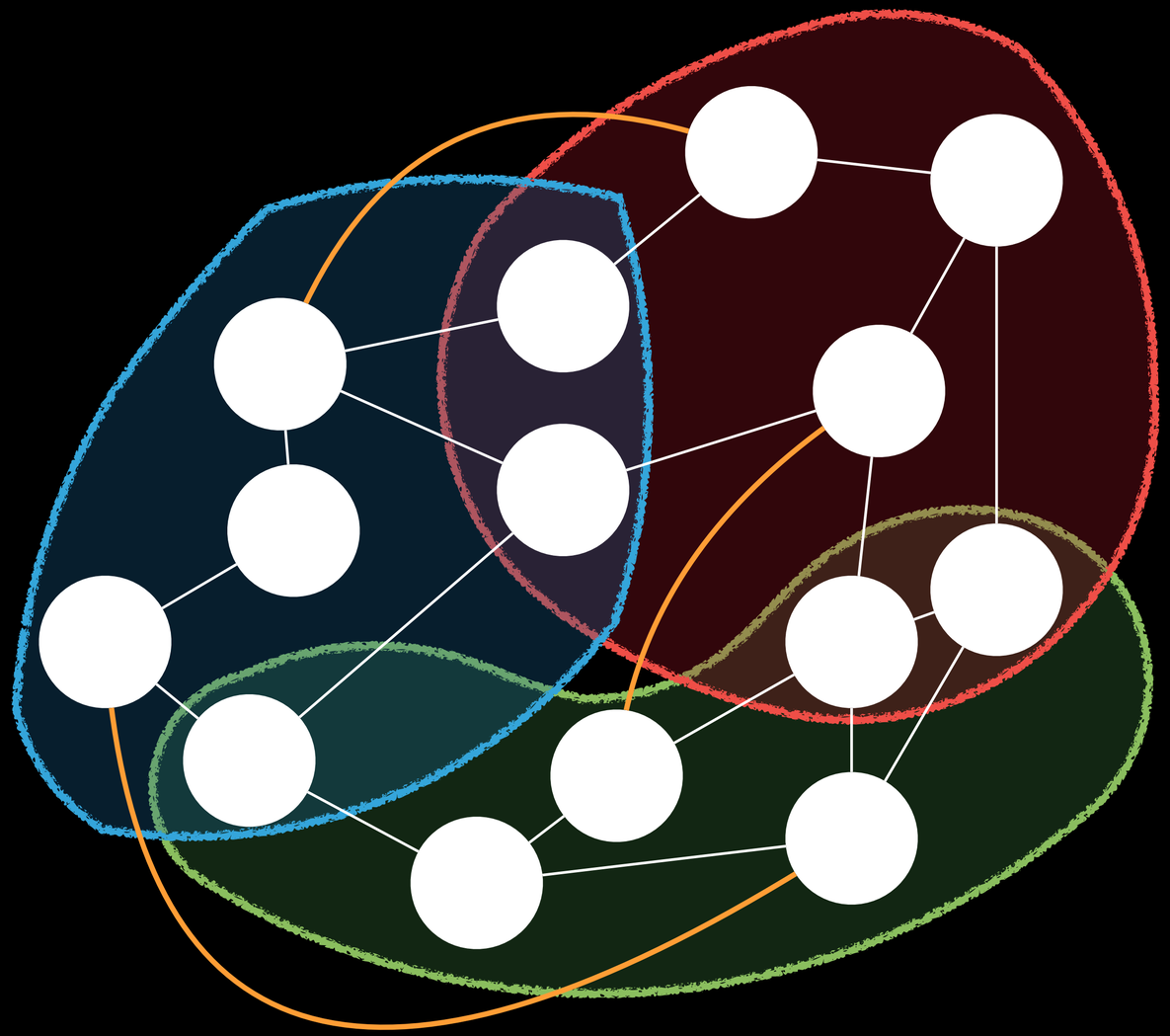
P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)
  - Performance of a small overlay
- Inter-Domain Routing

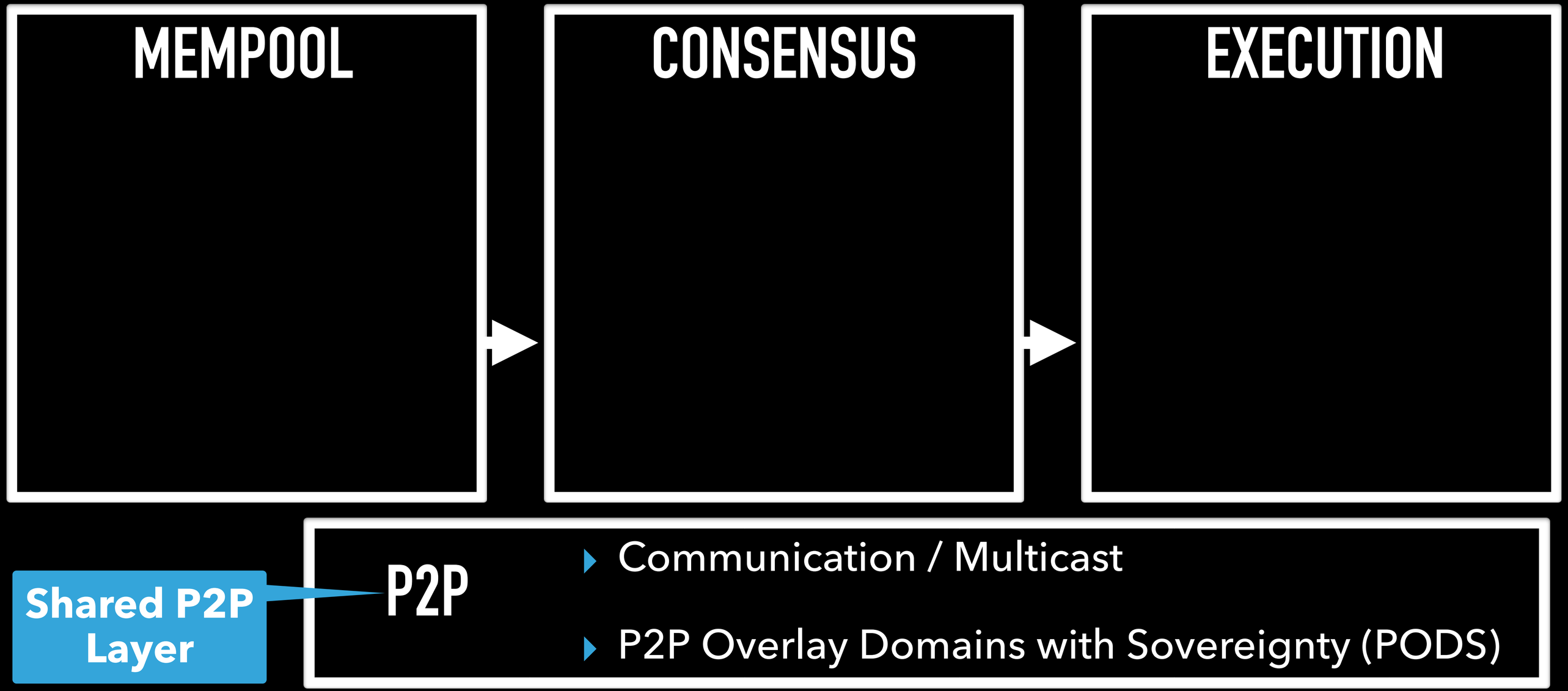


P2P OVERLAY DOMAINS WITH SOVEREIGNTY (PODS)

- https://arxiv.org/abs/2306.16153
- Multiple Independent Overlay Networks (Domains)
  - Performance of a small overlay
- Inter-Domain Routing
- Cross-domain attack response
  - Security of a large overlay



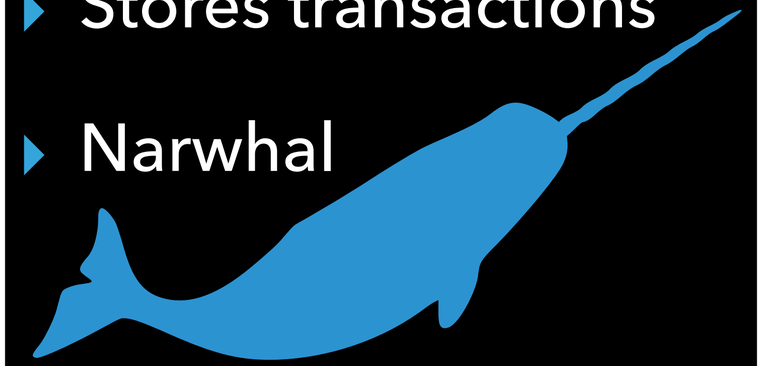
COMPONENTS


MEMPOOL
CONSENSUS
EXECUTION
Shared P2P Layer
P2P
Communication / Multicast
P2P Overlay Domains with Sovereignty (PODS)

COMPONENTS

MEMPOOL

- Receives from clients / solvers
- Stores transactions
- Narwhal



CONSENSUS

EXECUTION

Shared P2P Layer

P2P

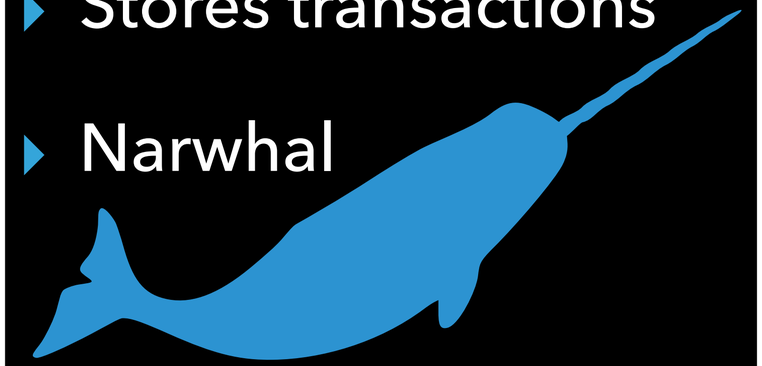
- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

Cross-chain transactions

COMPONENTS

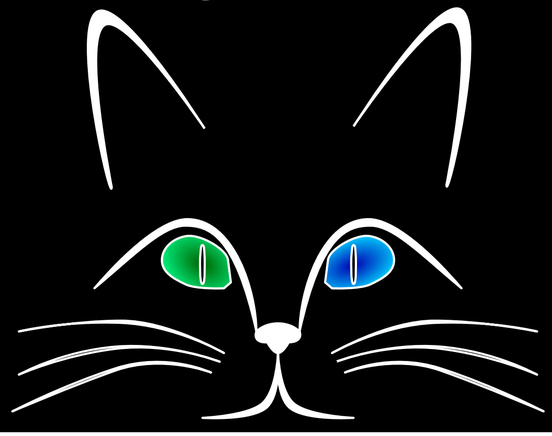
MEMPOOL

- Receives from clients / solvers
- Stores transactions
- Narwhal



CONSENSUS

- Orders transactions
- Heterogeneous Paxos



EXECUTION

Shared P2P Layer

P2P

- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

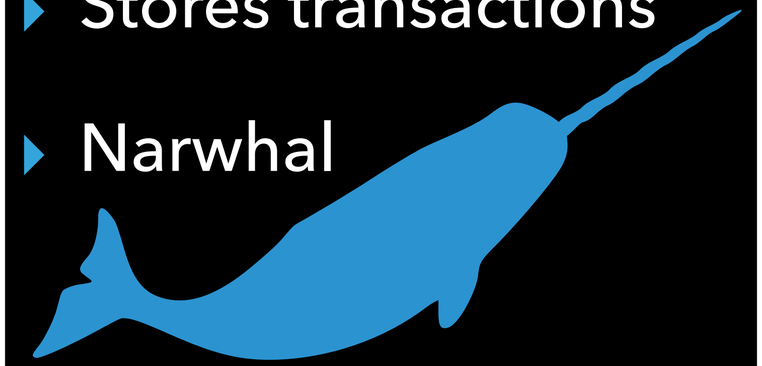
COMPONENTS

Cross-chain transactions

Post-ordering execution

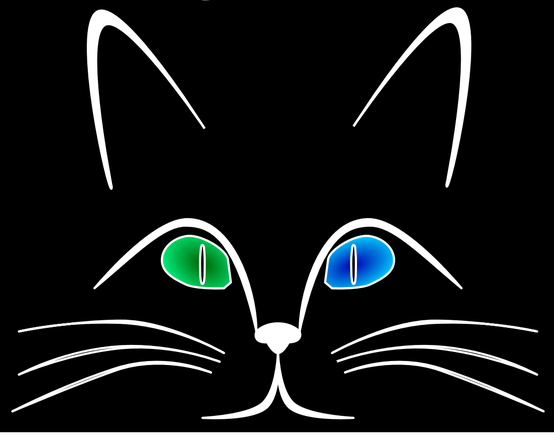
MEMPOOL

- Receives from clients / solvers
- Stores transactions
- Narwhal



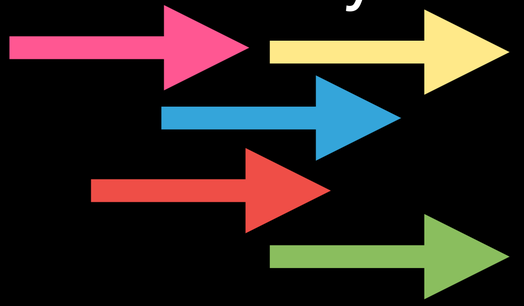
CONSENSUS

- Orders transactions
- Heterogeneous Paxos



EXECUTION

- State machine
- Client reads
- Concurrency



Shared P2P Layer

P2P

- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

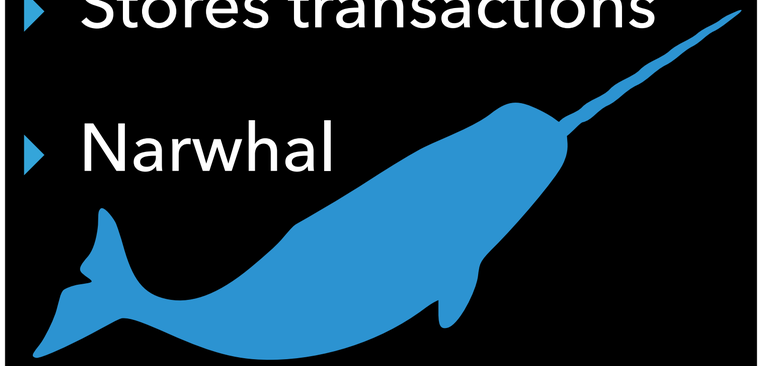
COMPONENTS

Cross-chain transactions

Post-ordering execution

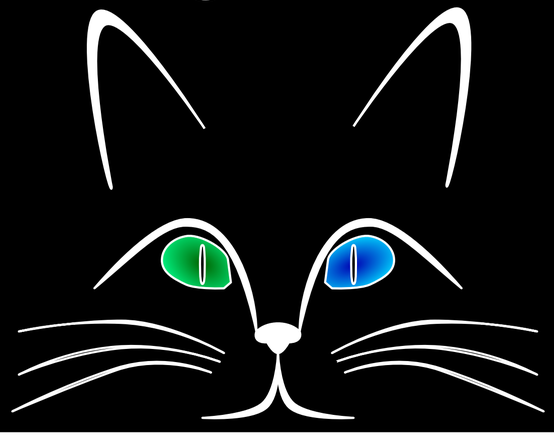
MEMPOOL

- Receives from clients / solvers
- Stores transactions
- Narwhal



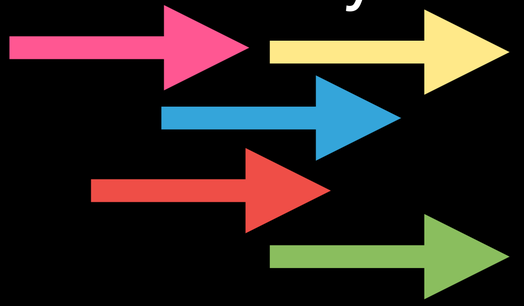
CONSENSUS

- Orders transactions
- Heterogeneous Paxos



EXECUTION

- State machine
- Client reads
- Concurrency



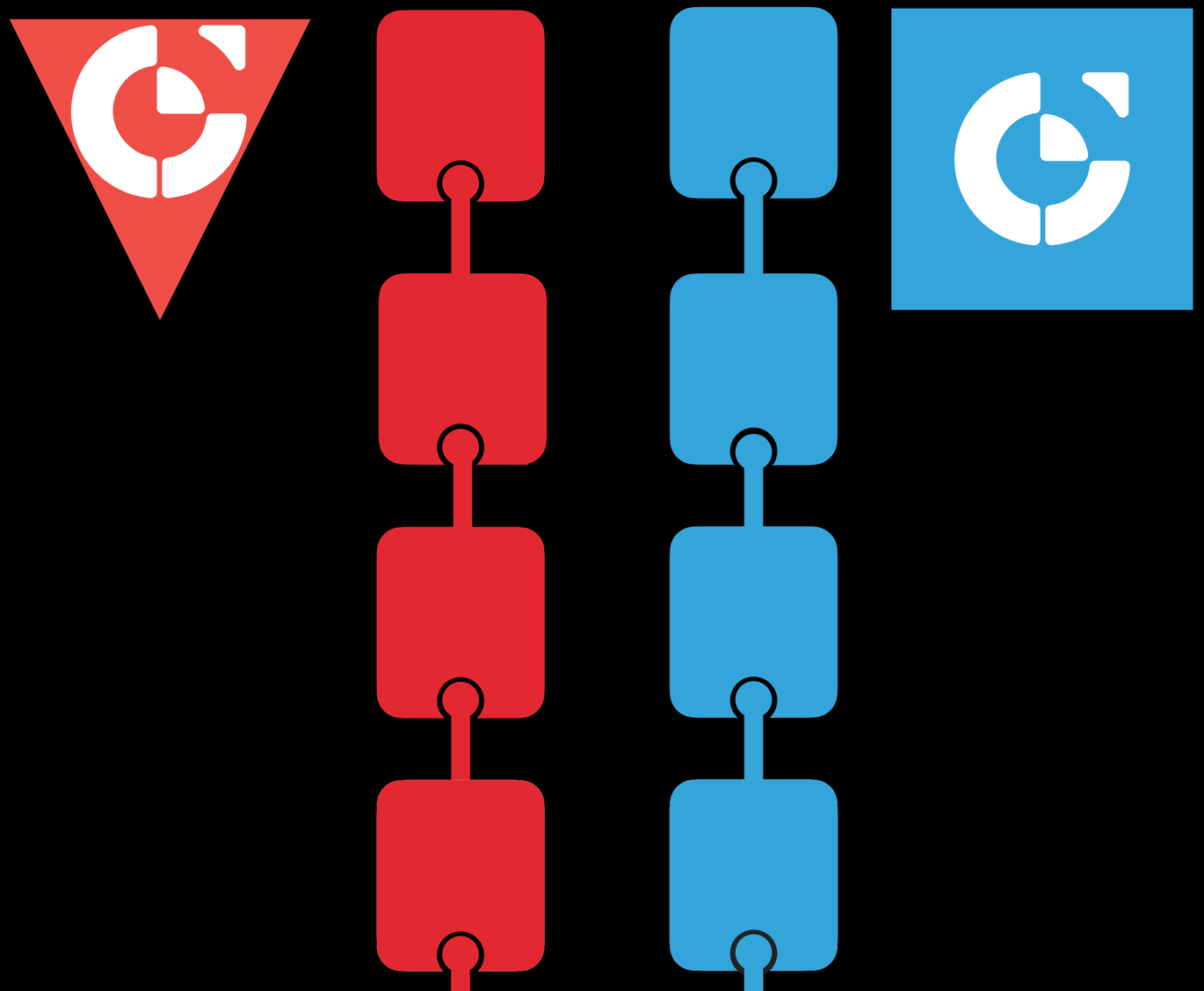
Shared P2P Layer

P2P

- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

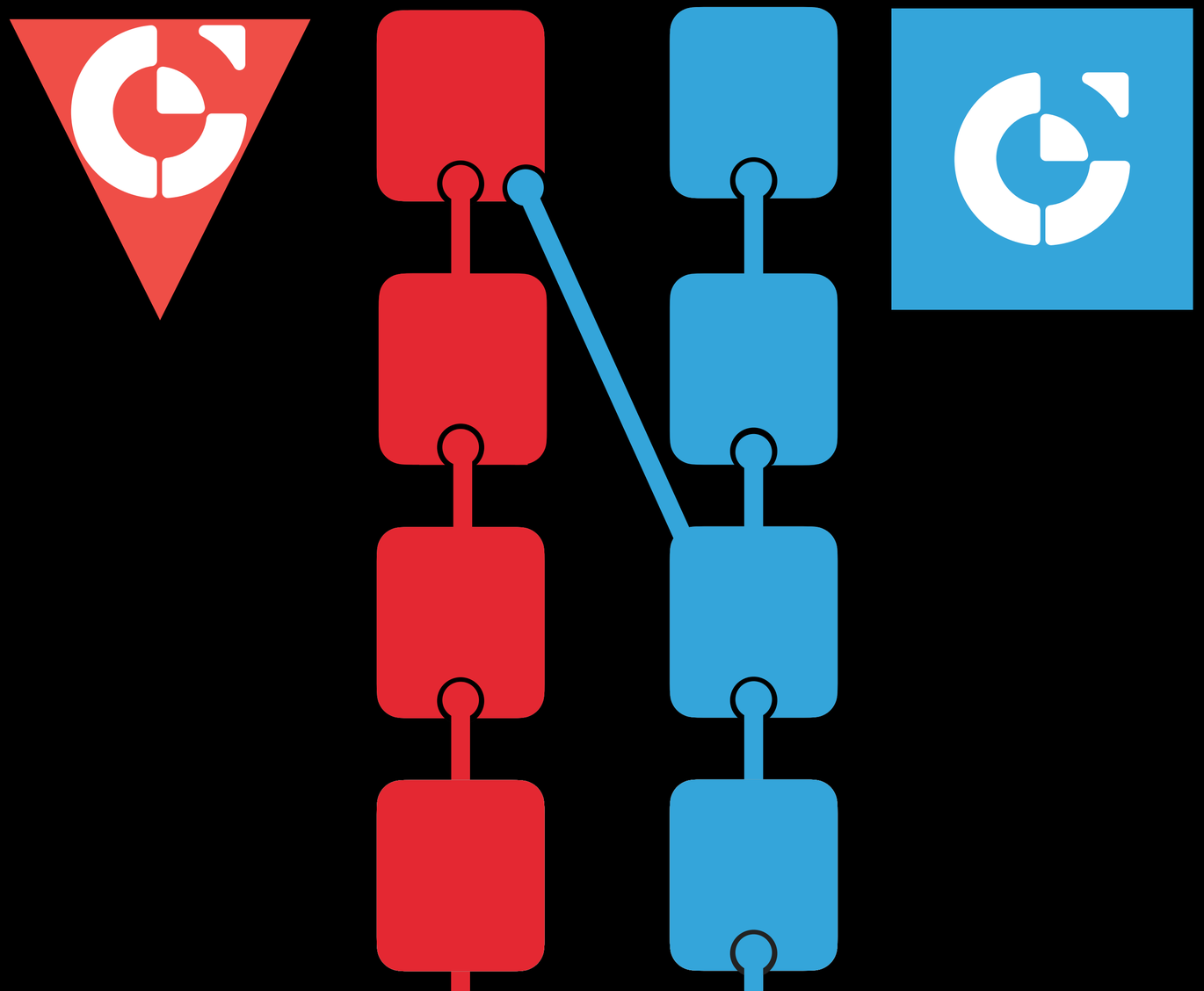
ATOMIC COMMITMENT ACROSS CHAINS

- Multiple chains
- Different validator machines



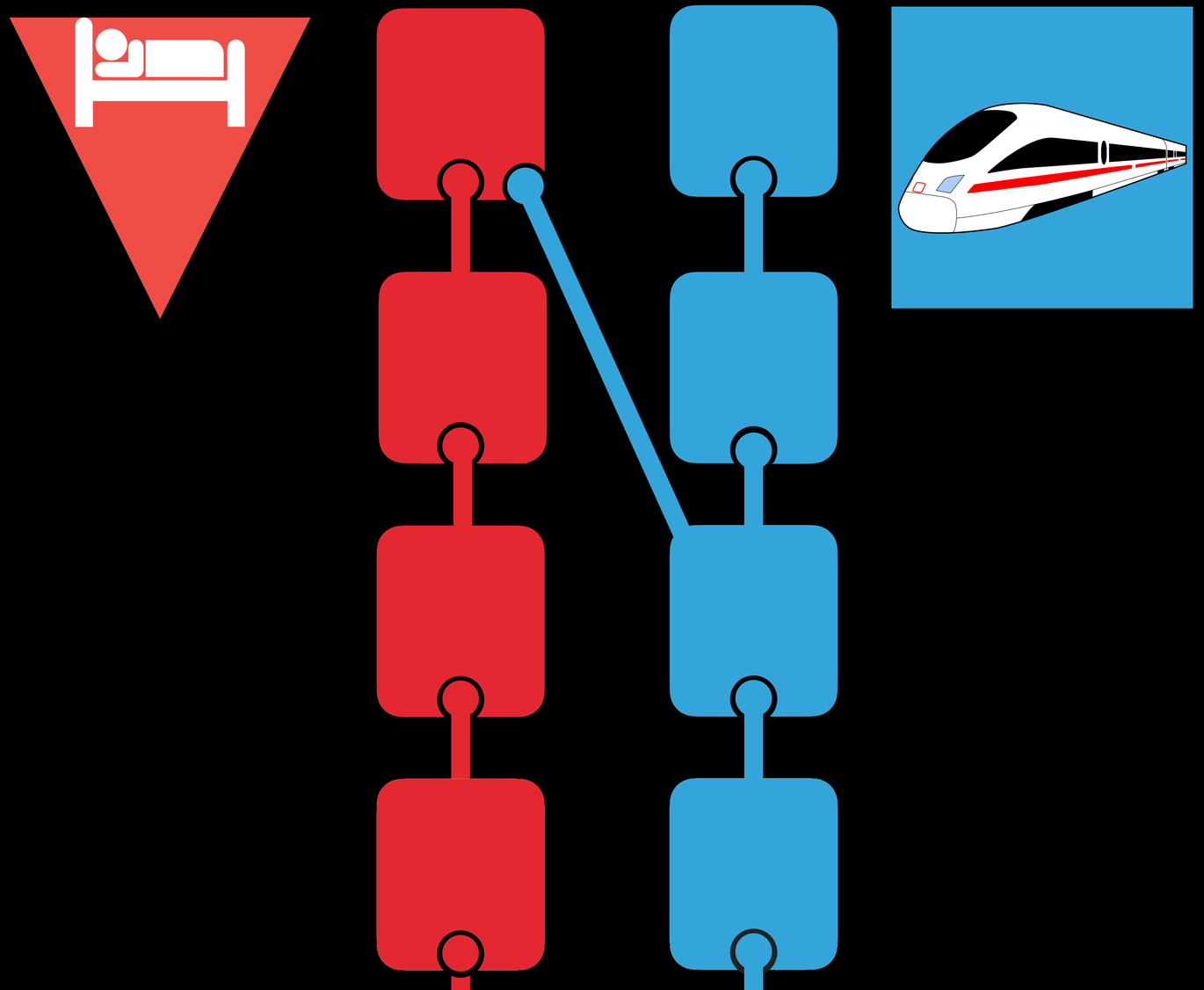
ATOMIC COMMITMENT ACROSS CHAINS

- Multiple chains
- Different validator machines
- IBC (ibcprotocol.org)



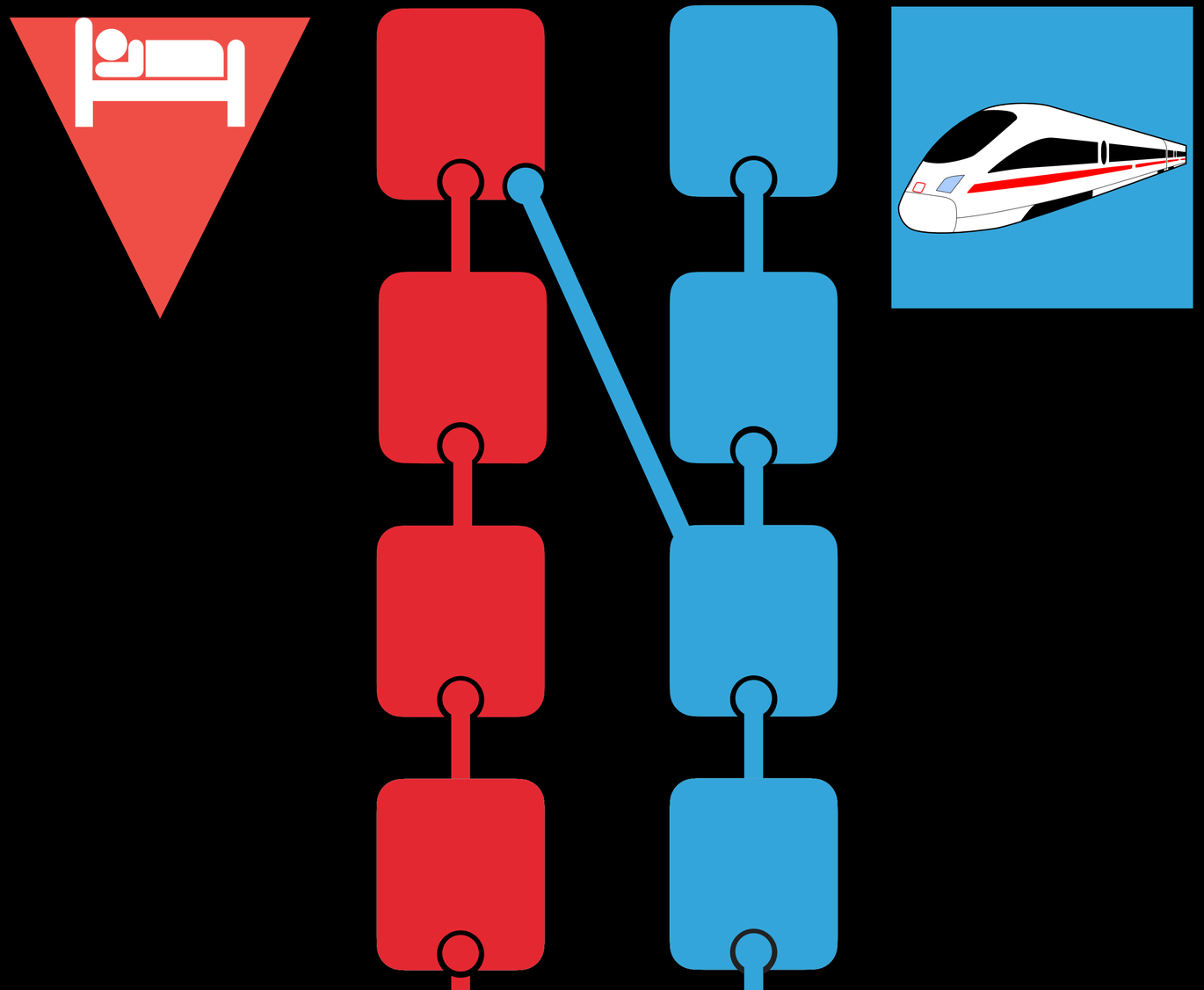
TRAIN & HOTEL PROBLEM

- Multiple chains
- Different validator machines
- IBC (ibcprotocol.org)
- Atomic commitment
  - Both or Neither:
    - Hotel Room
    - Train Ticket



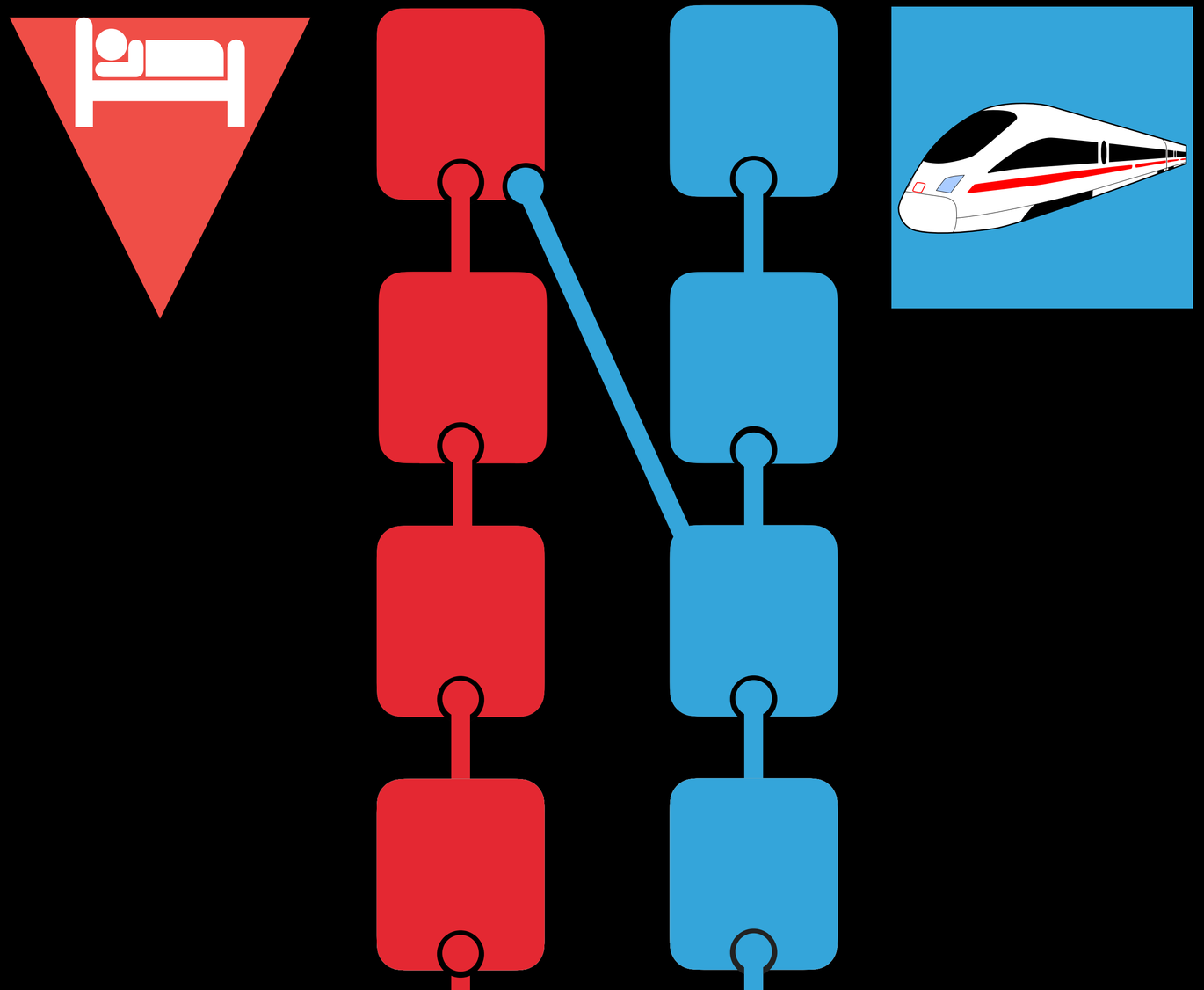
TRAIN & HOTEL PROBLEM

- Multiple chains
- Different validator machines
- IBC (ibcprotocol.org)
- Atomic commitment
  - Both or Neither:
    - Hotel Room
    - Train Ticket
- Shared Sequencers? (Espresso)

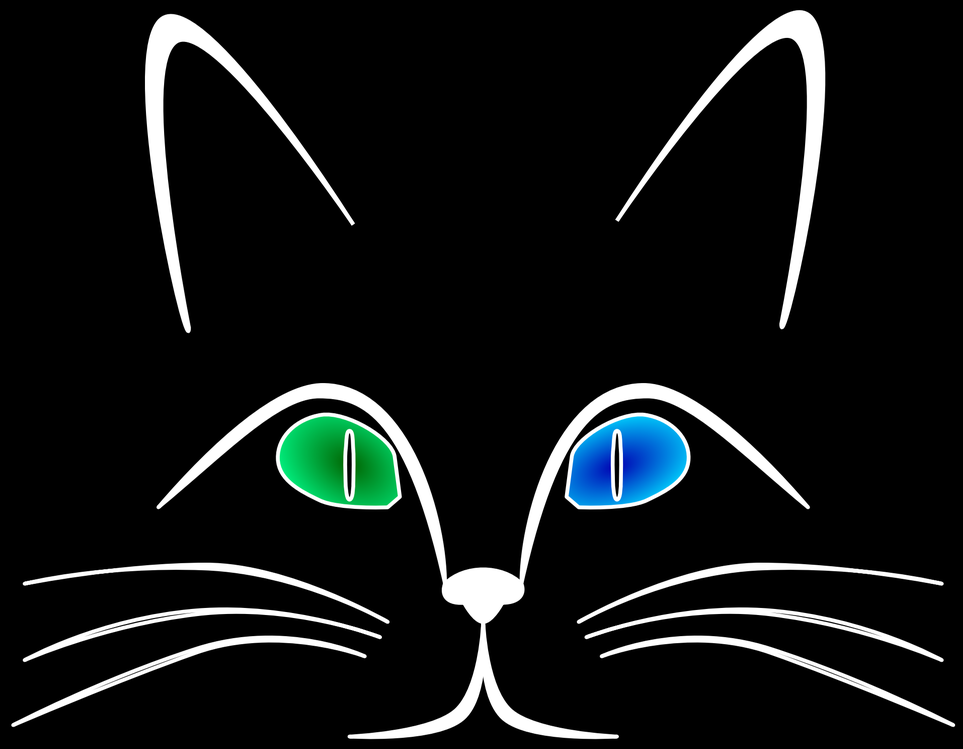


TRAIN & HOTEL PROBLEM

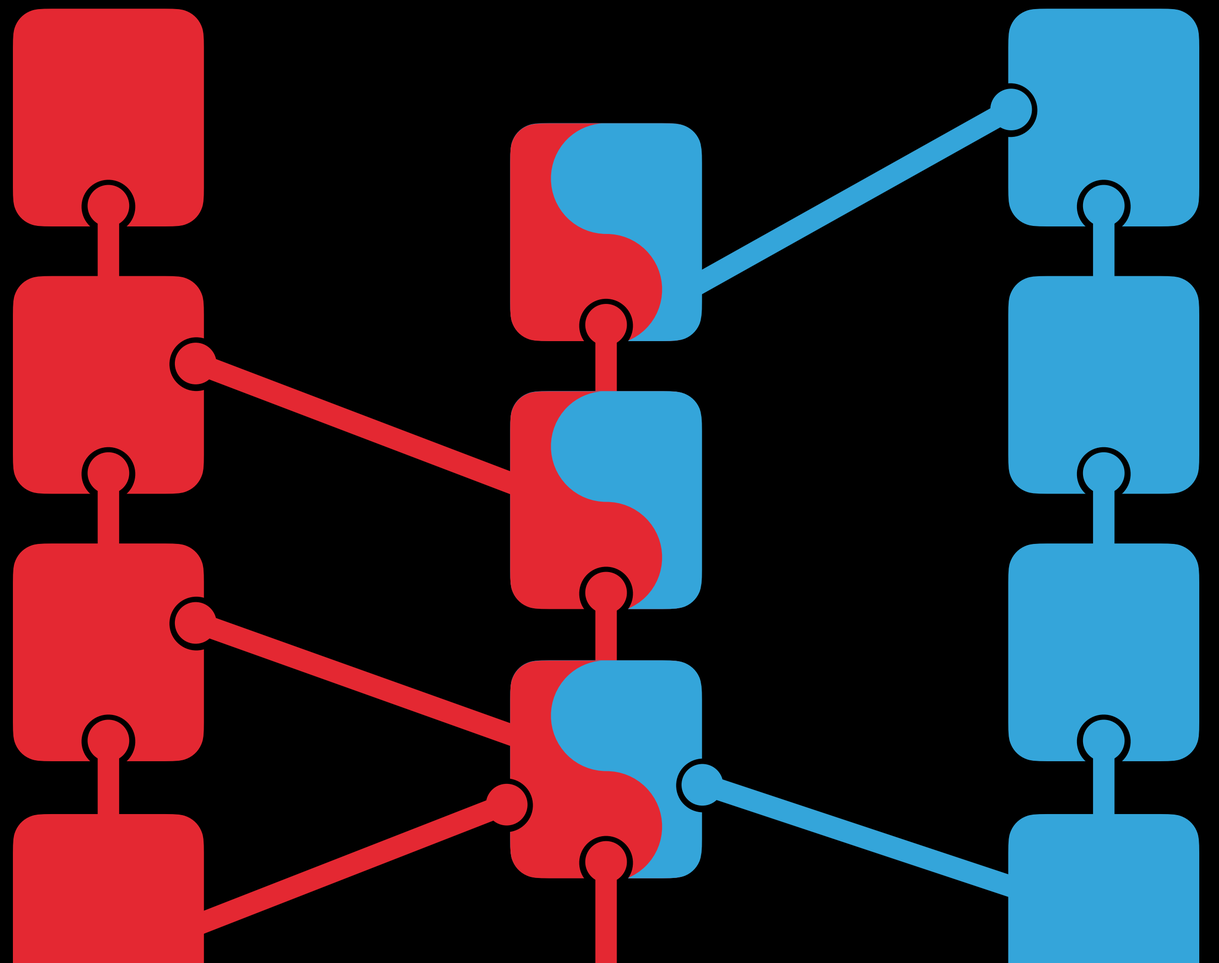
- Multiple chains
- Different validator machines
- IBC (ibcprotocol.org)
- Atomic commitment
  - Both or Neither:
    - Hotel Room
    - Train Ticket
- Multi-phase commit



MOTIVATION

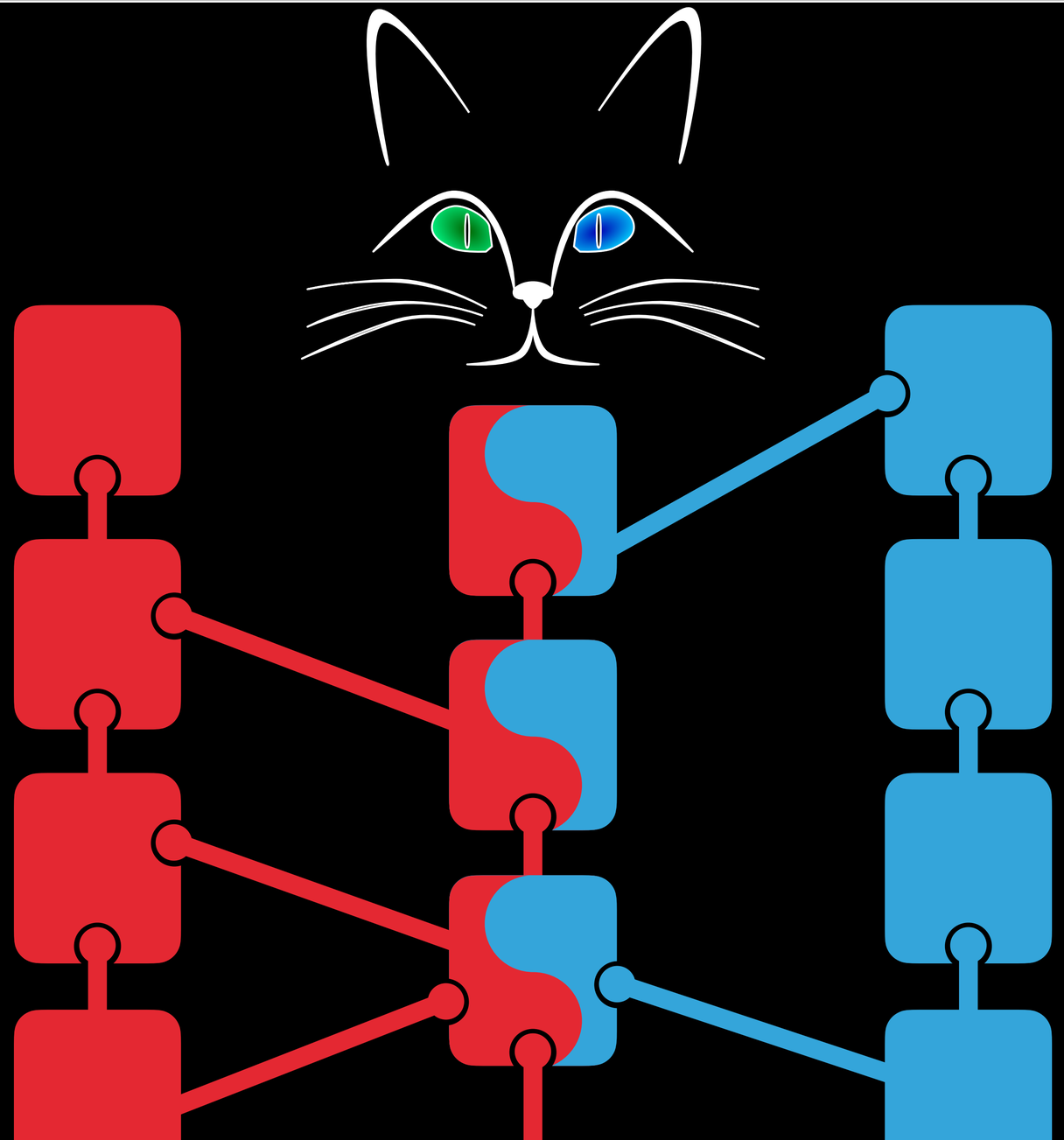


CHIMERA CHAINS



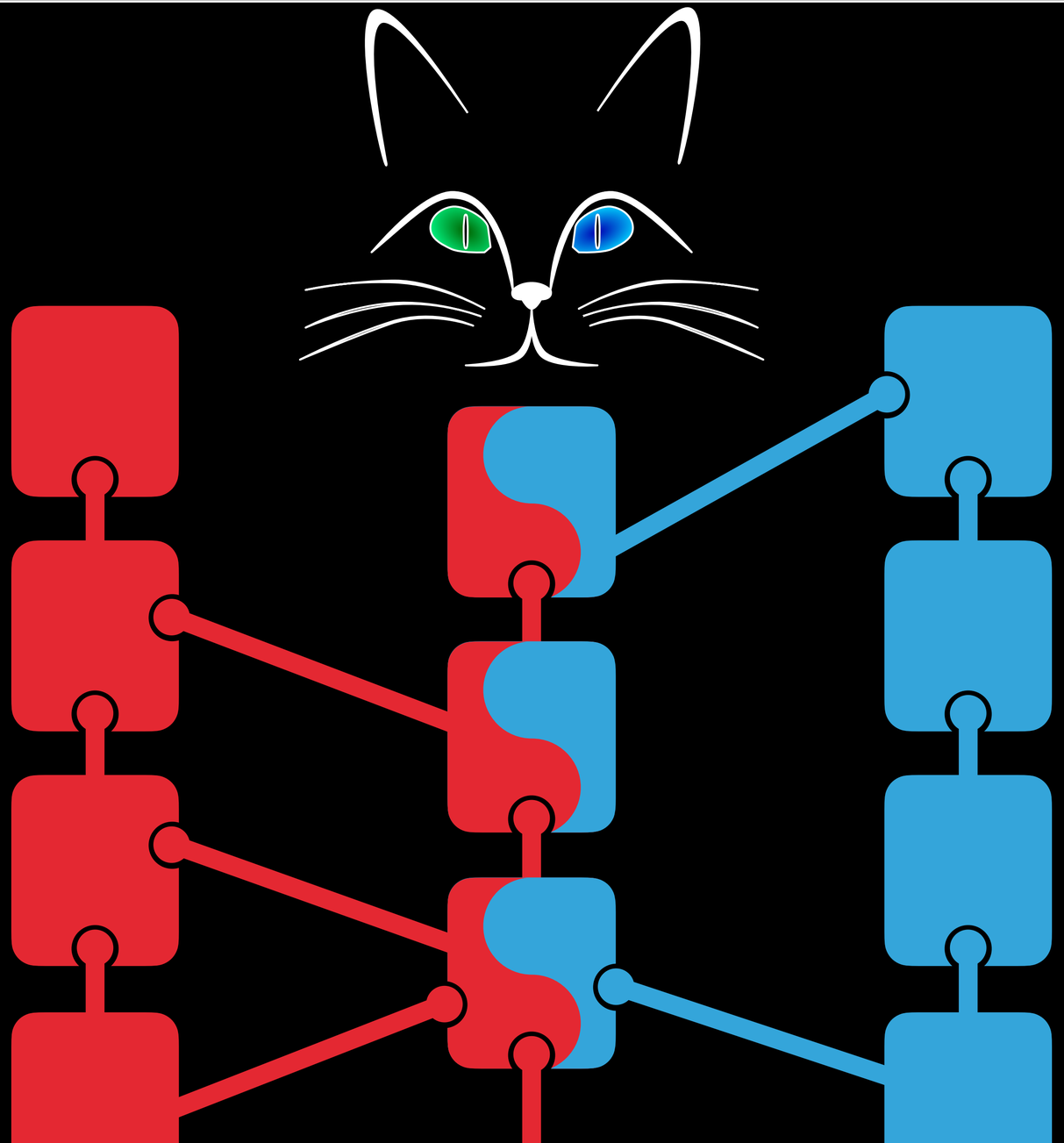
CHIMERA CHAINS

- Each chain liveness / integrity of its own consensus



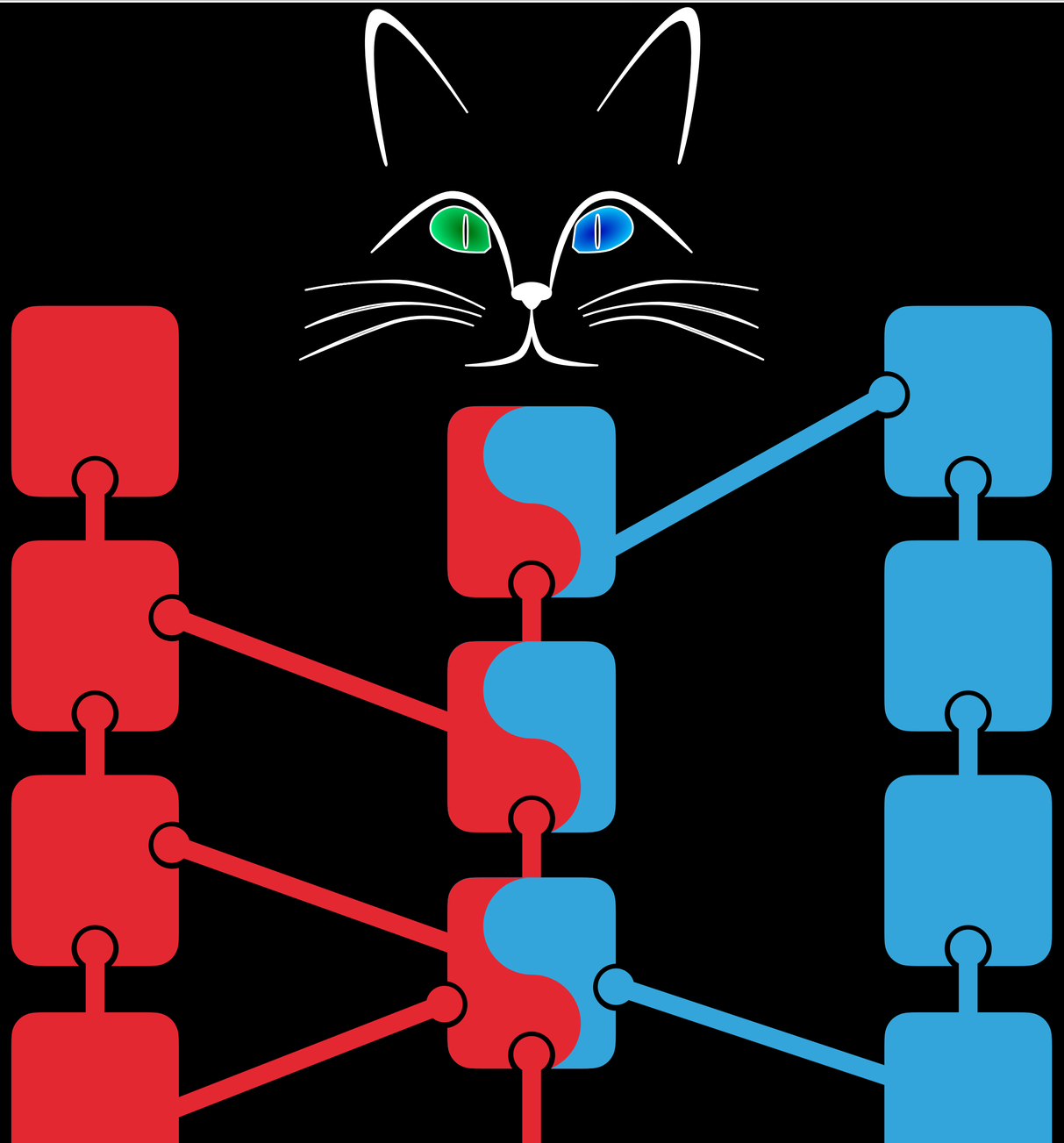
ATOMIC BATCHES

- Each chain liveness / integrity of its own consensus
- Atomic batches of "multi-chain" transactions that commit atomically (ALL or NONE)



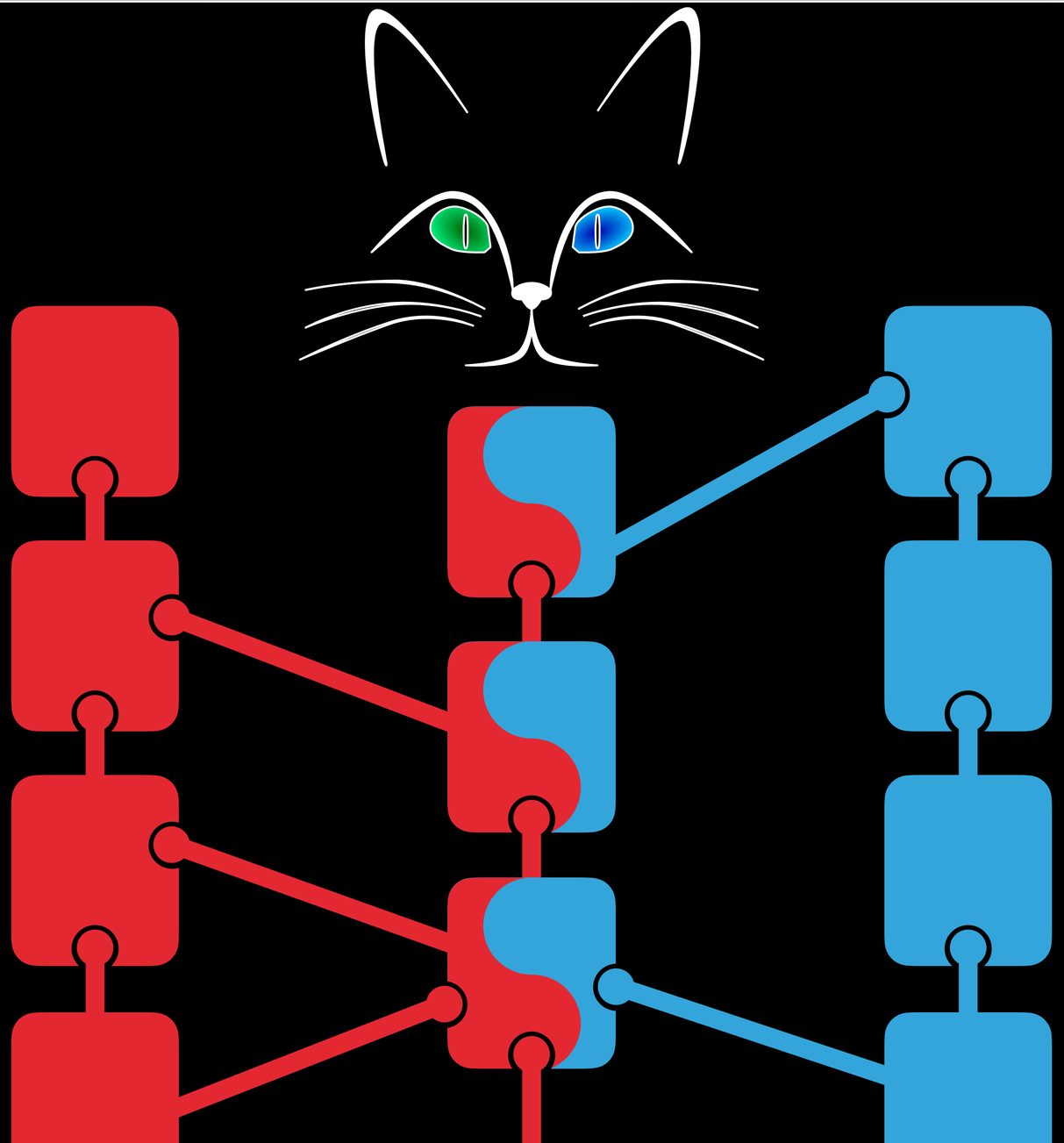
ATOMIC BATCHES

- Each chain liveness / integrity of its own consensus
- Atomic batches of "multi-chain" transactions that commit atomically (ALL or NONE)
- Heterogeneous Paxos (OPODIS 2020)



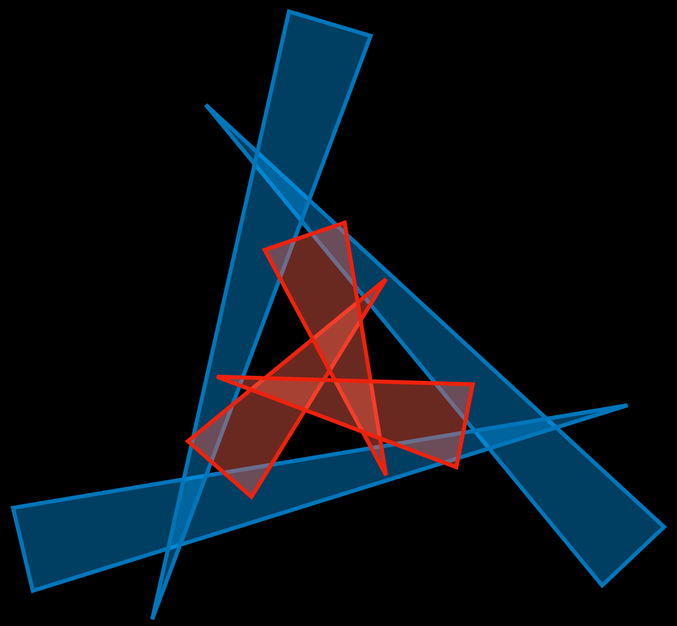
ATOMIC BATCHES

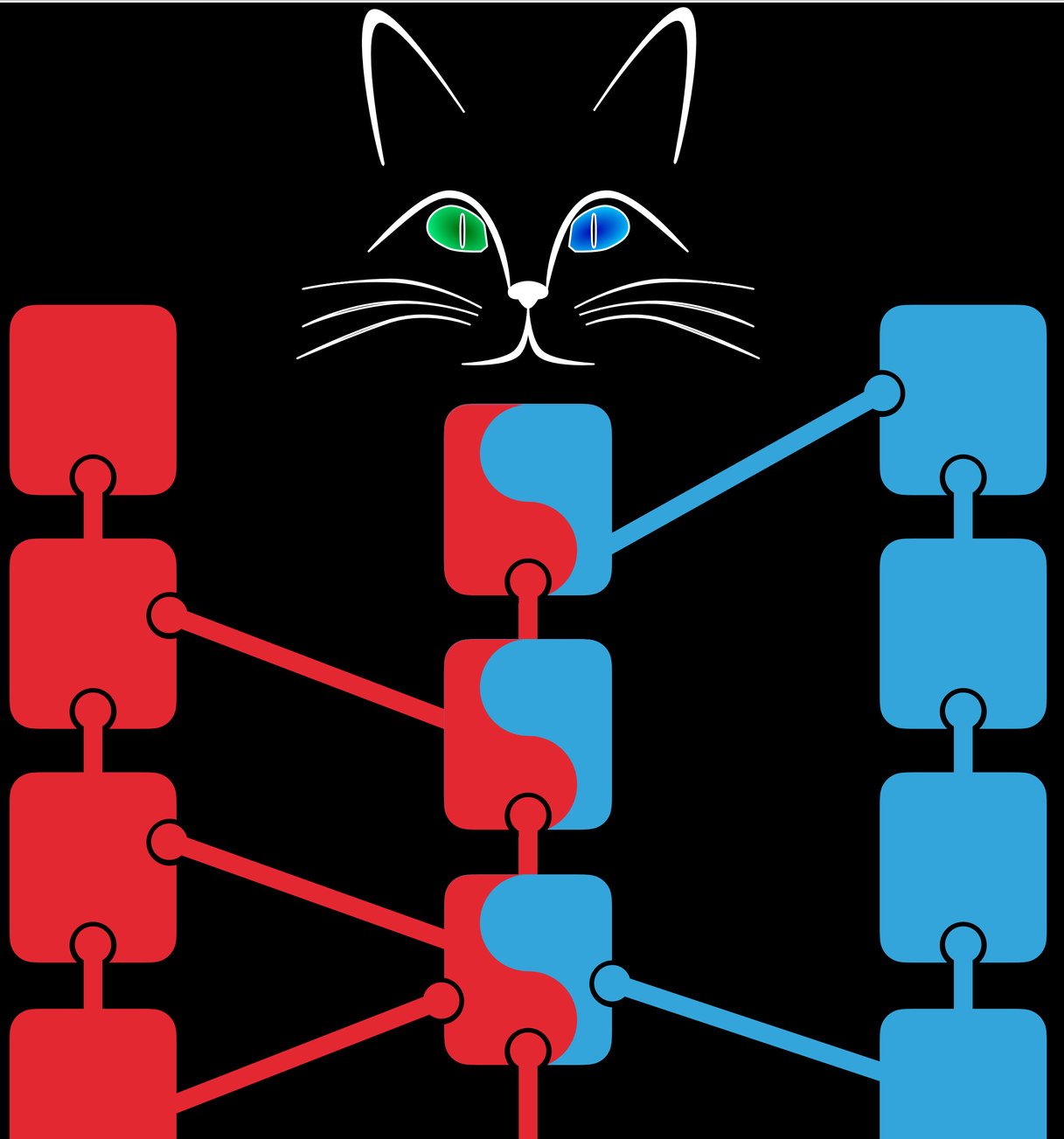
- Each chain liveness / integrity of its own consensus
- Atomic batches of "multi-chain" transactions that commit atomically (ALL or NONE)
- Heterogeneous Paxos (OPODIS 2020)
  - Atomicity guaranteed under certain conditions



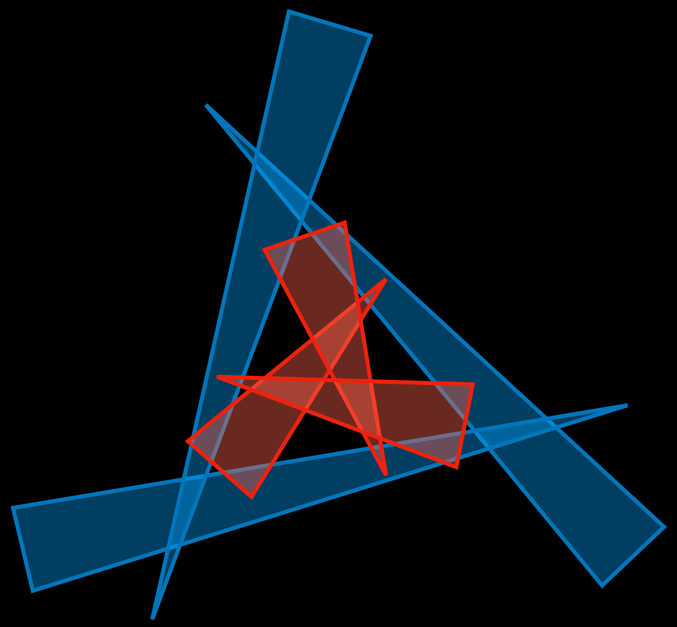
TRUST ASSUMPTIONS

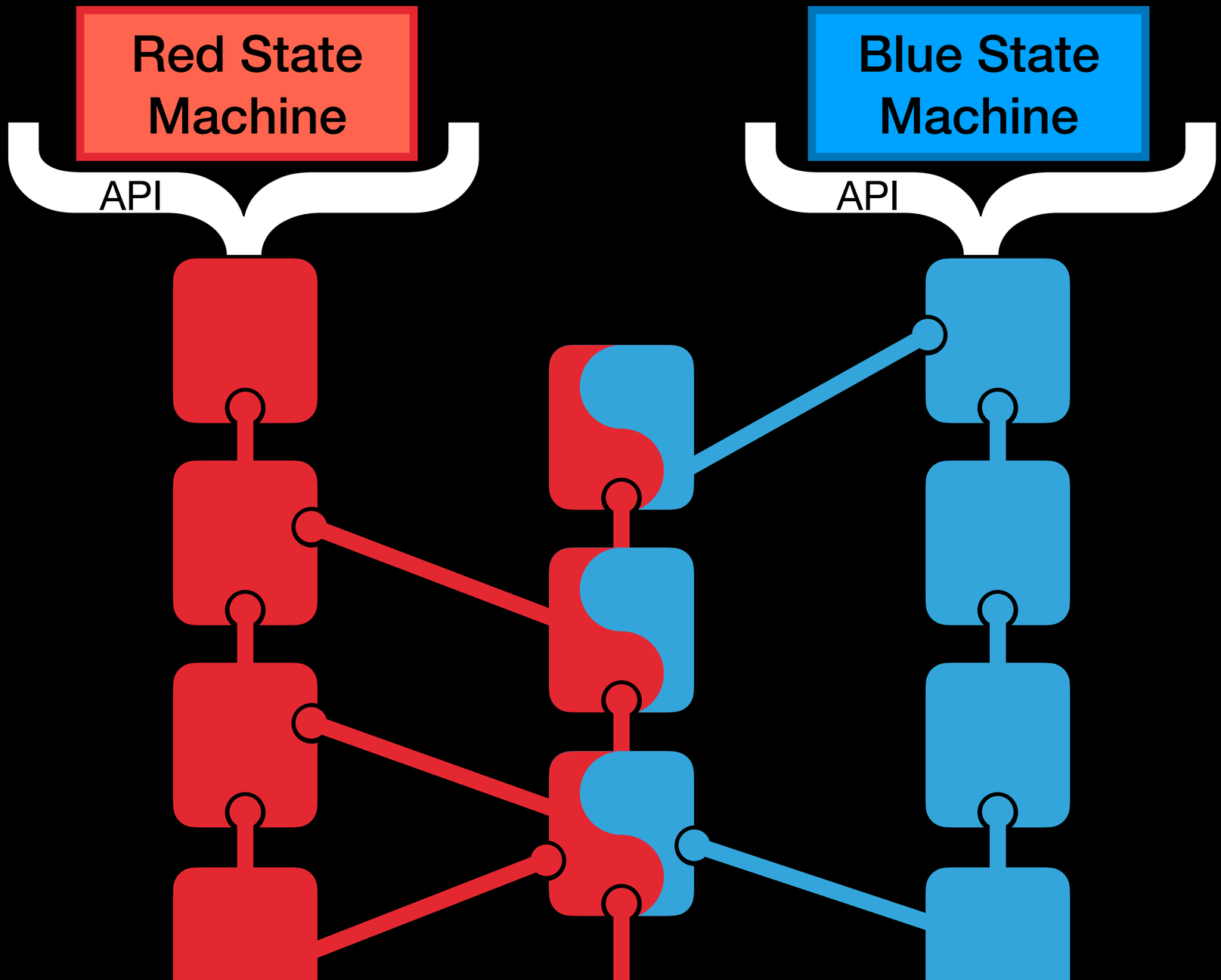
- Safety derives from validators common to multiple chains
- High validator overlap in practice





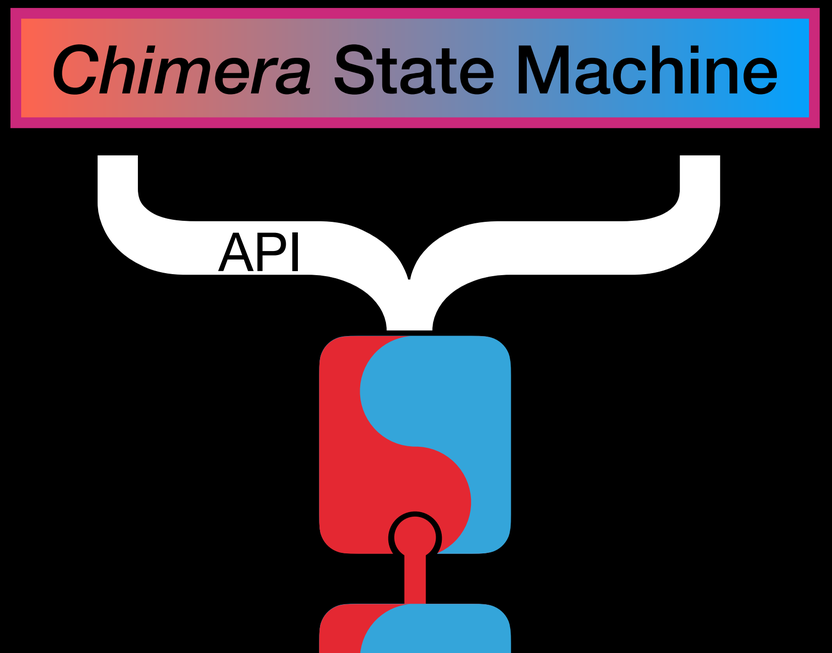
STATE MACHINE





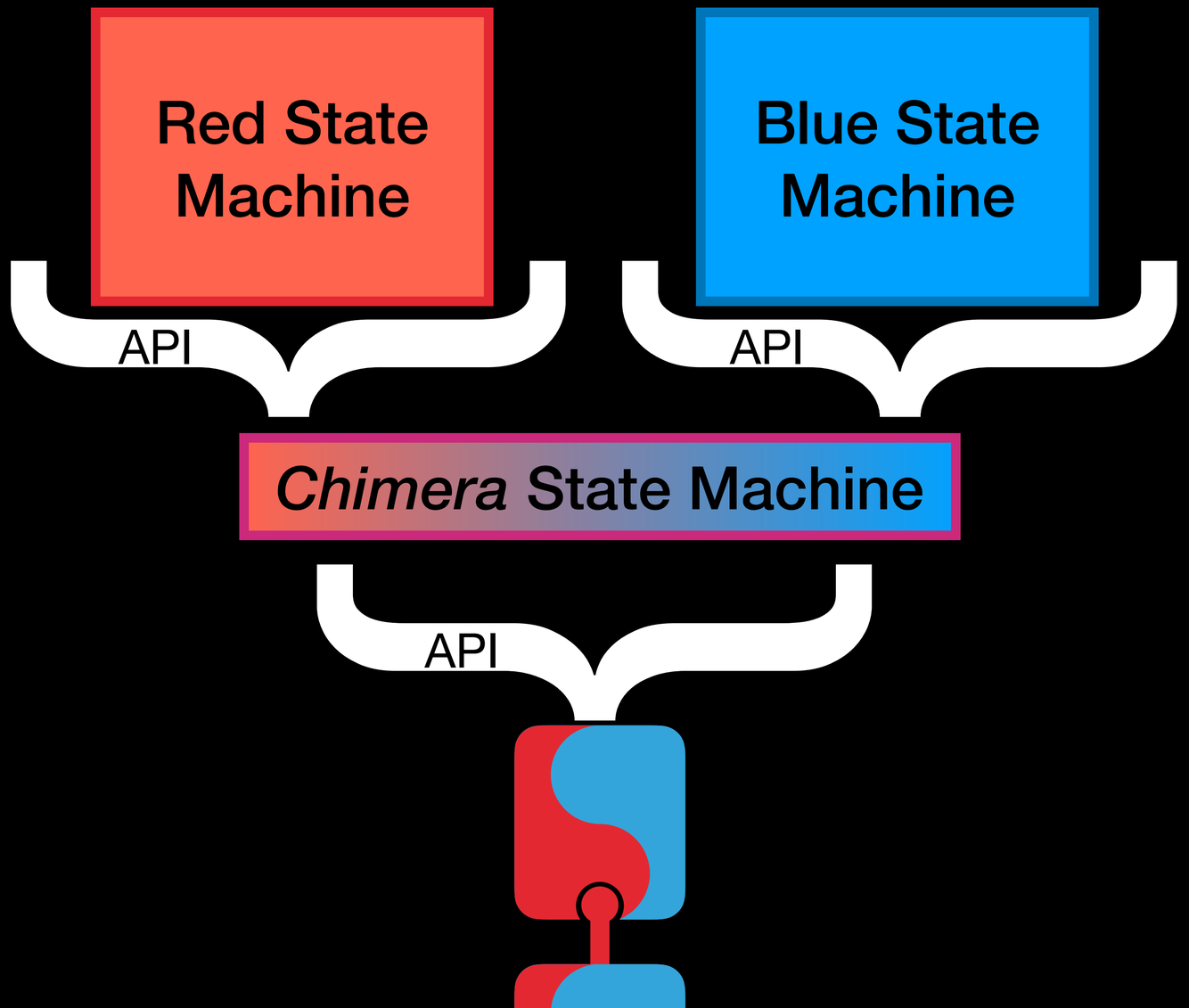
STATE MACHINE

- Over Chimera Chain



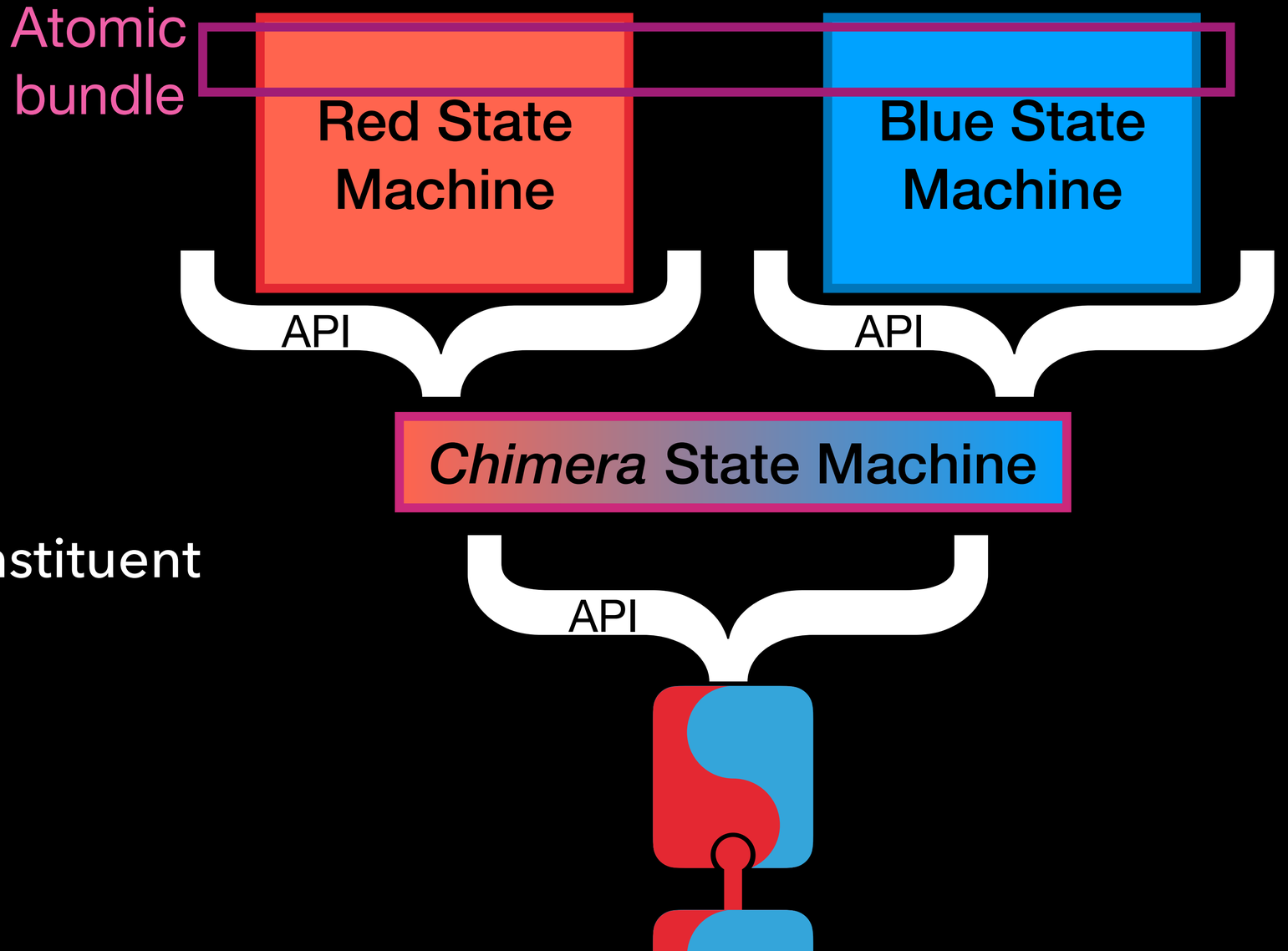
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines



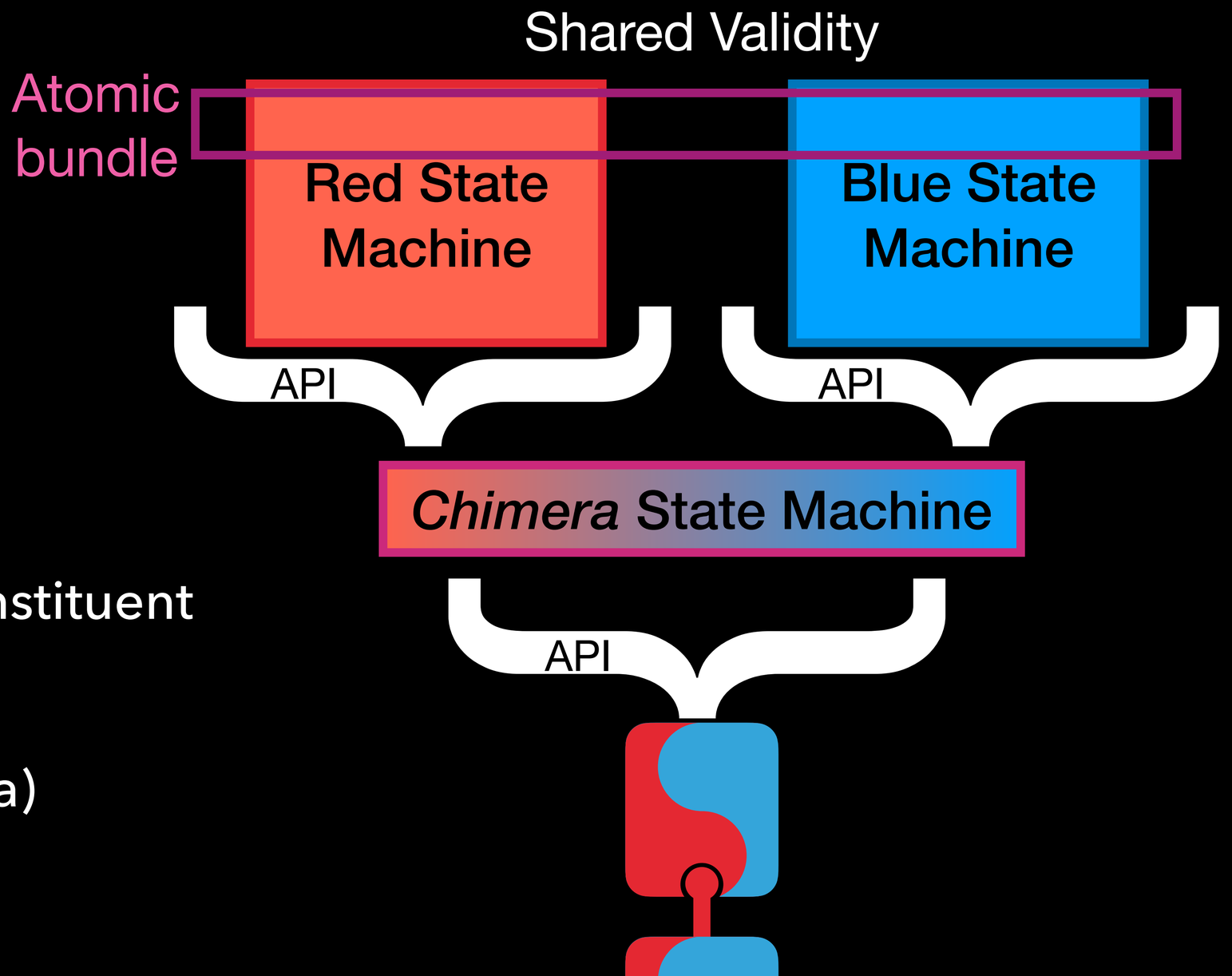
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions



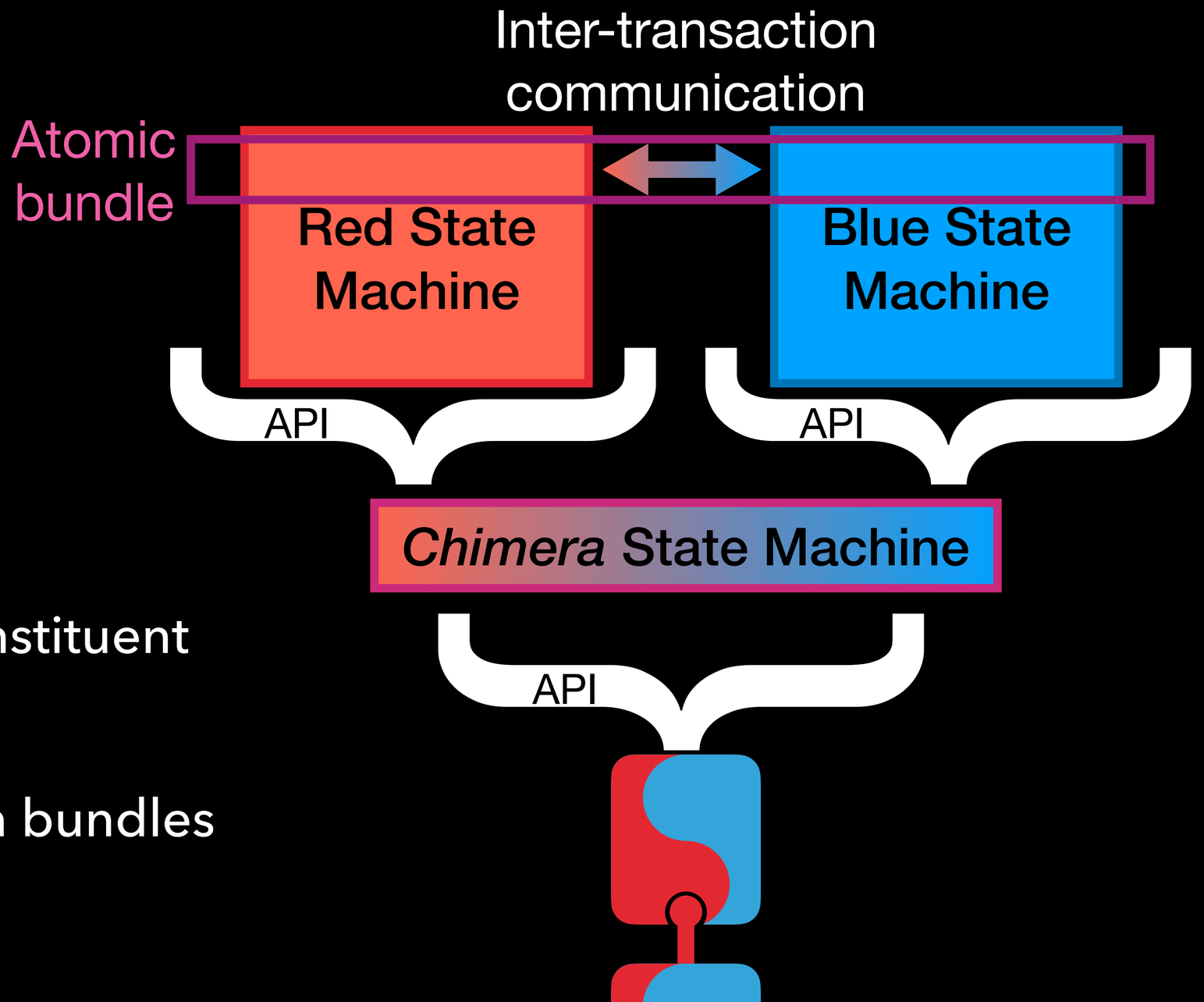
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions
  - Shared Validity (Umbra)



STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions
  - Communication within bundles



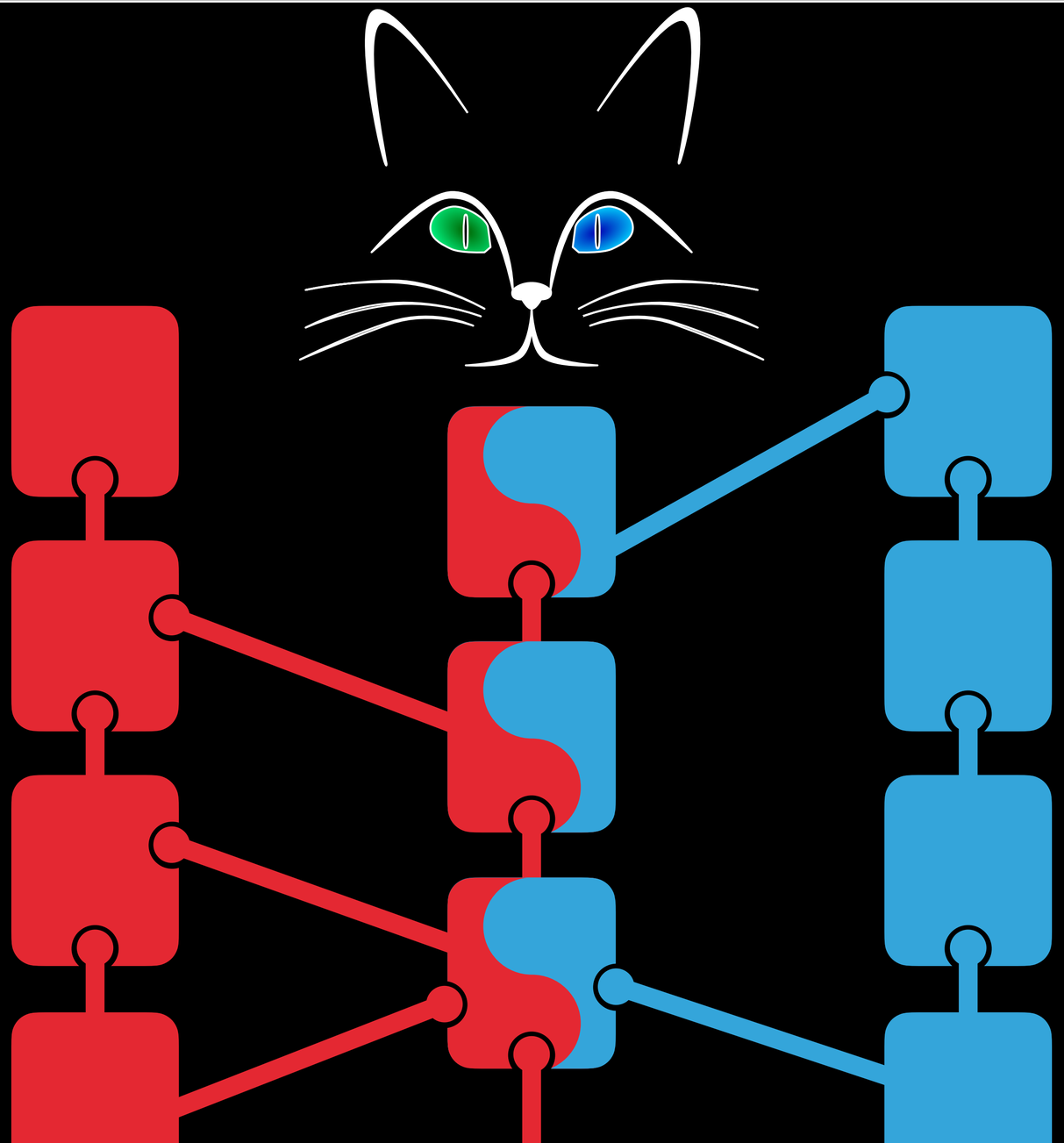
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions
  - Communication within bundles

Inter-transaction communication

CHIMERA CHAINS

- Each chain liveness / integrity of its own consensus
- Atomic batches of "multi-chain" transactions that commit atomically (ALL or NONE)
- Heterogeneous Paxos (OPODIS 2020)
  - Atomicity guaranteed under certain conditions



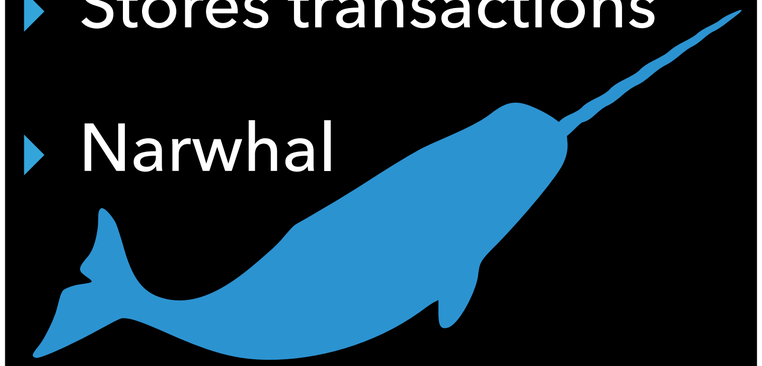
COMPONENTS

Cross-chain transactions

Post-ordering execution

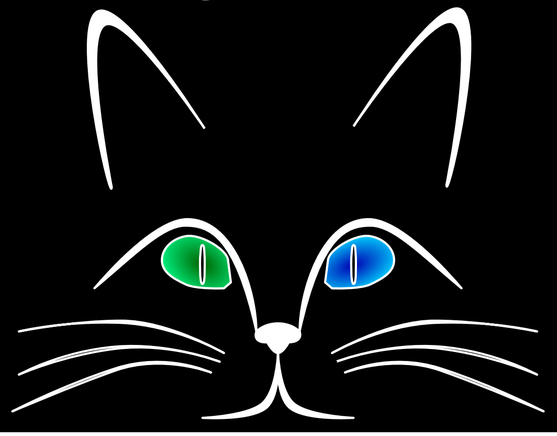
MEMPOOL

- Receives from clients / solvers
- Stores transactions
- Narwhal



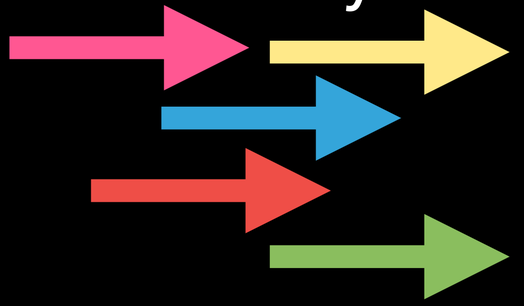
CONSENSUS

- Orders transactions
- Heterogeneous Paxos



EXECUTION

- State machine
- Client reads
- Concurrency



Shared P2P Layer

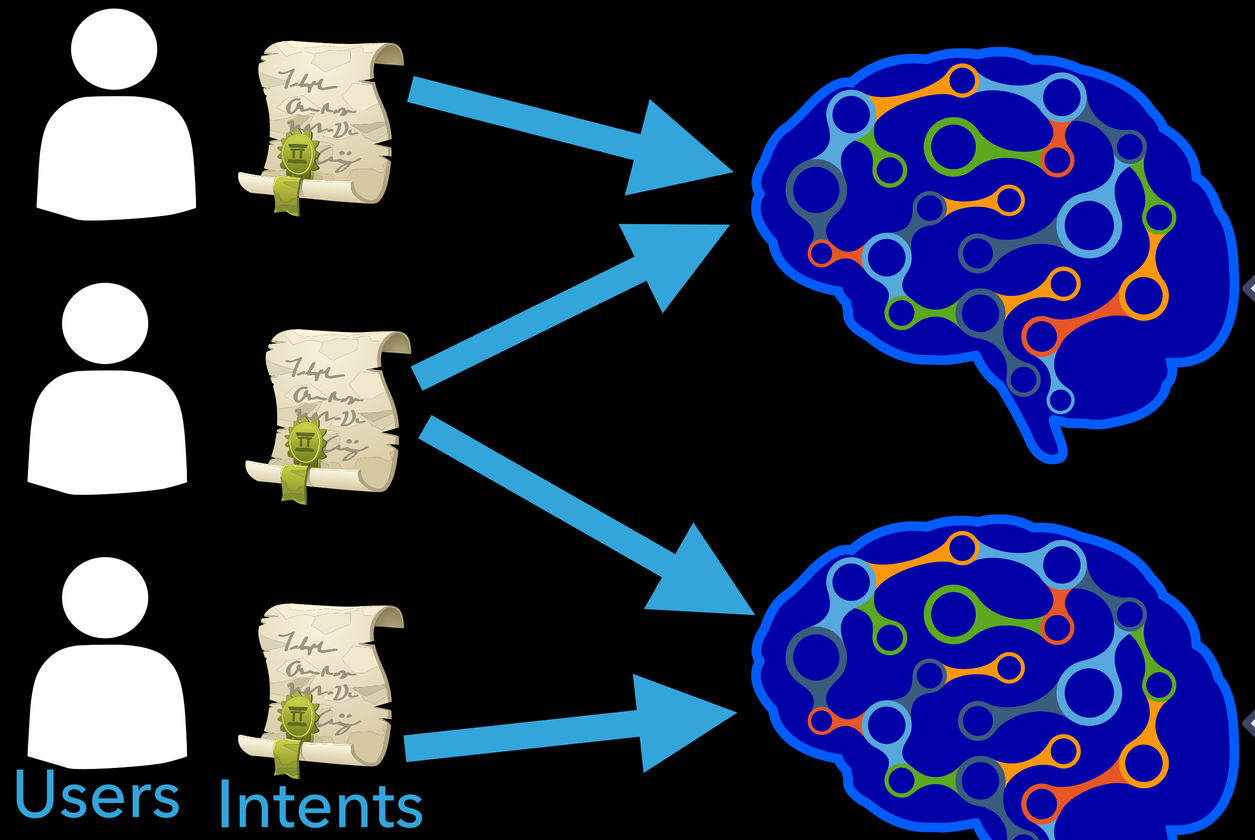
P2P

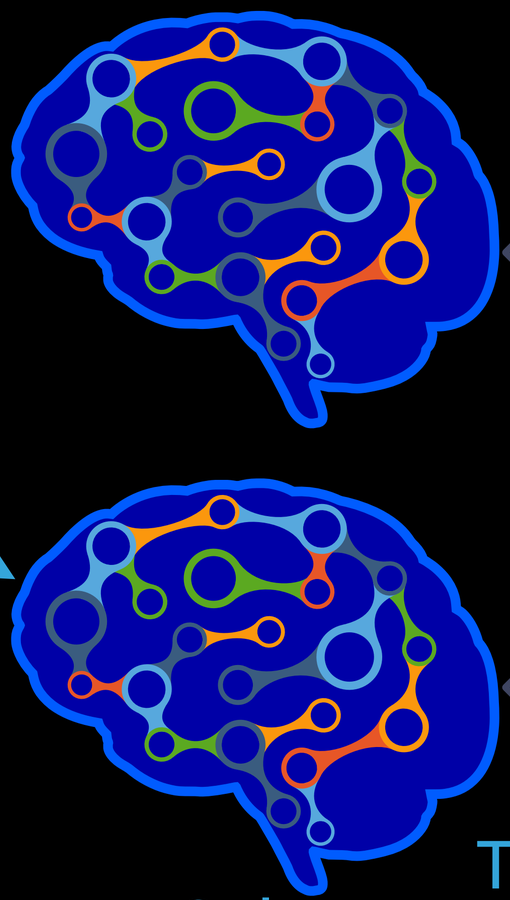
- Communication / Multicast
- P2P Overlay Domains with Sovereignty (PODS)

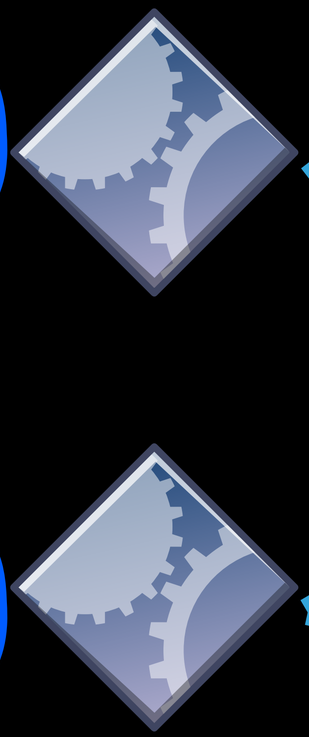
3 POINTS

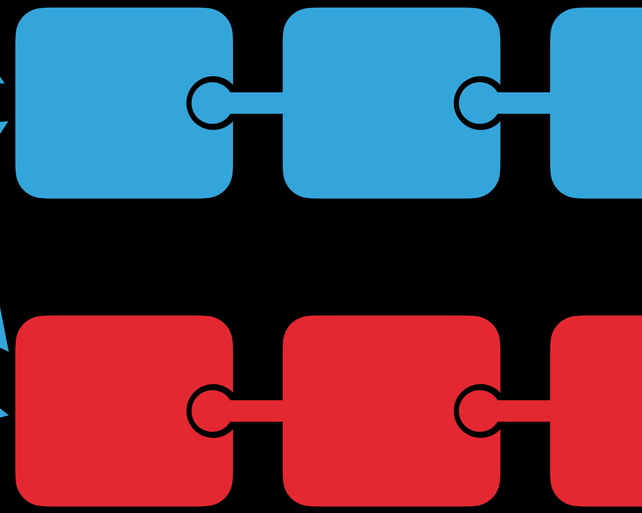
- Shared P2P Layer
- Post-ordering execution
- Multi-chain transactions

anoma









CONCLUSIONS

anoma will use TYPHON, which supports CHIMERA CHAINS

- PODS: https://arxiv.org/abs/2306.16153
- Full spec proposal coming soon!
- github.com/anoma/typhon

anoma will use TYPHON, which supports CHIMERA CHAINS

- PODS: https://arxiv.org/abs/2306.16153
- Full spec proposal coming soon!
- github.com/anoma/typhon

- Formal specification & proofs
  - New heterogeneous protocols
- Communication language within atomic bundles
- Share Components
- Practical problems encountered

TYPHON OVERVIEW

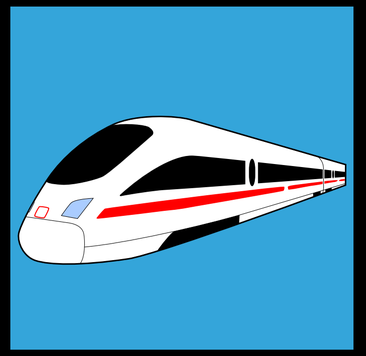
BONUS SLIDES

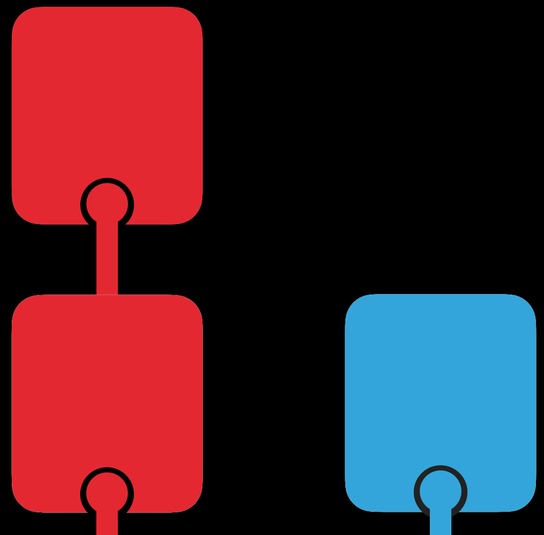
TYPHON OVERVIEW

2 PHASE

ATOMIC COMMITMENT ACROSS CHAINS

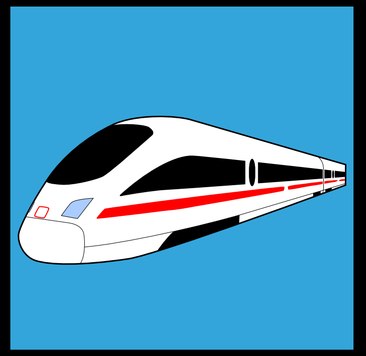
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit

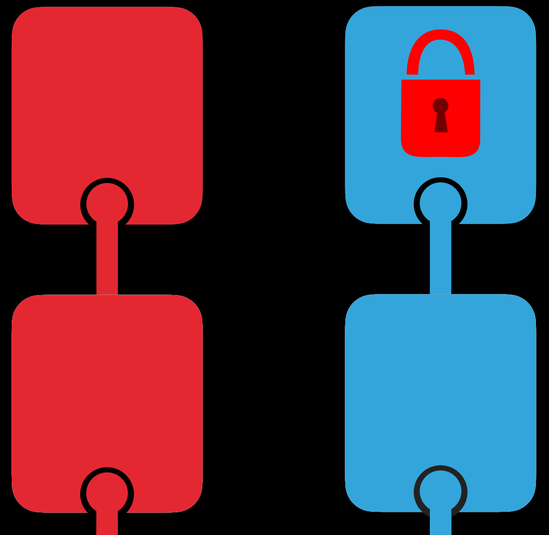




ATOMIC COMMITMENT ACROSS CHAINS

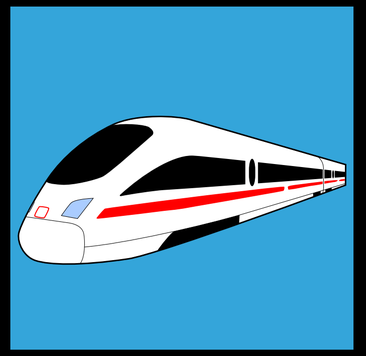
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Each chain locks

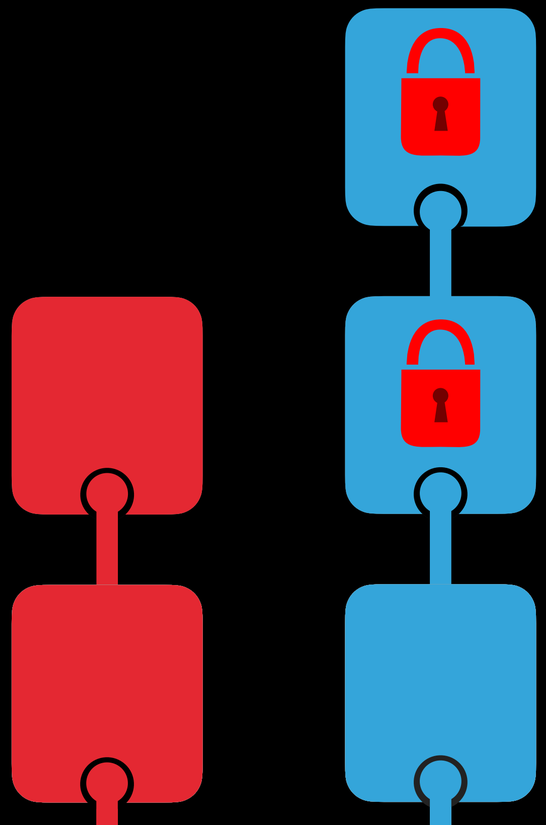




ATOMIC COMMITMENT ACROSS CHAINS

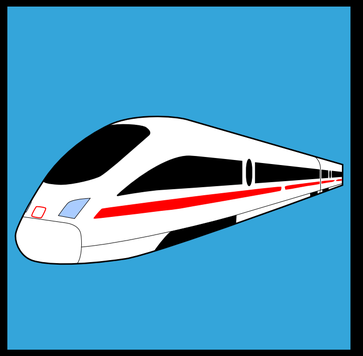
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Each chain locks
    - And stays locked

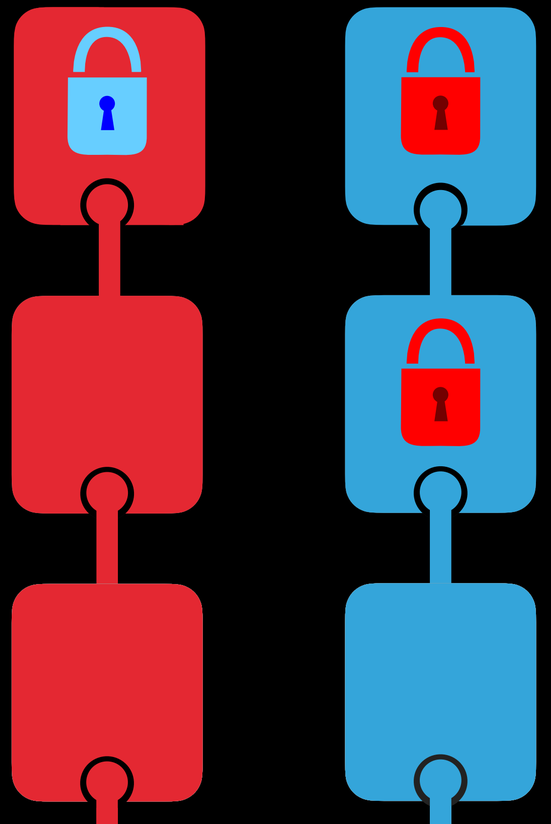




ATOMIC COMMITMENT ACROSS CHAINS

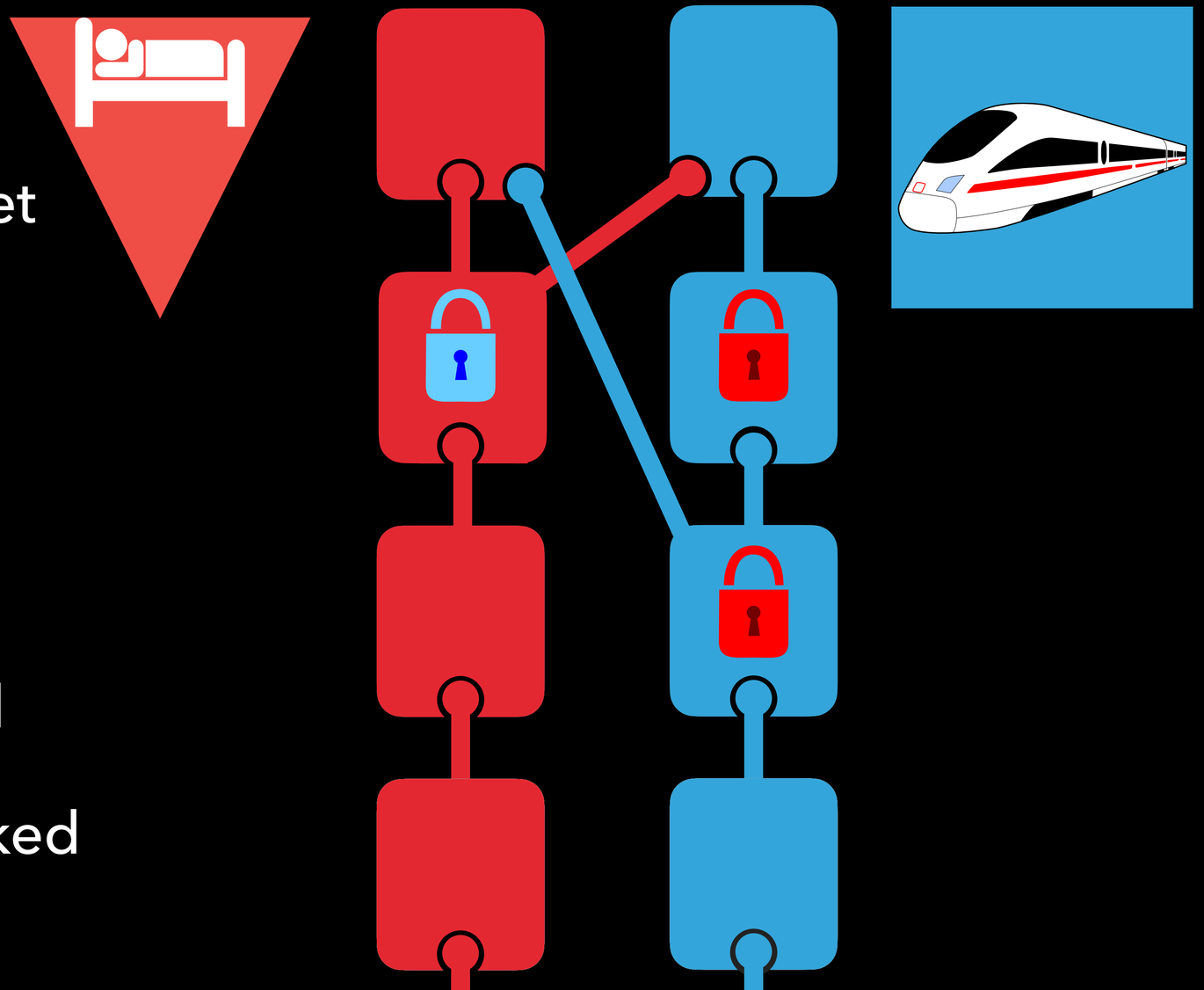
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Each chain locks
    - And stays locked
    - Until both chains are locked





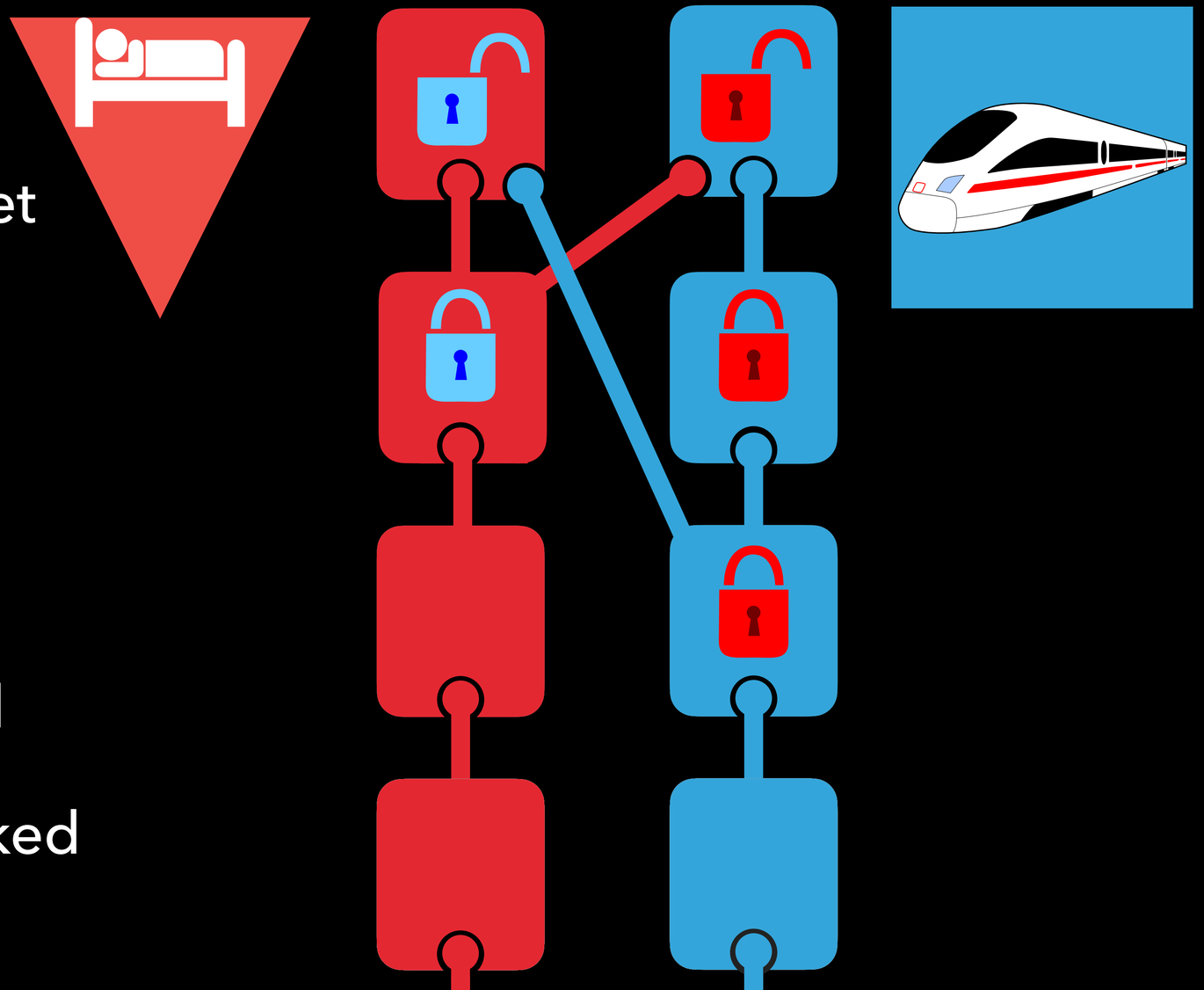
ATOMIC COMMITMENT ACROSS CHAINS

- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Each chain locks
    - And stays locked
    - Until both chains are locked
  - Verifies other chains have locked



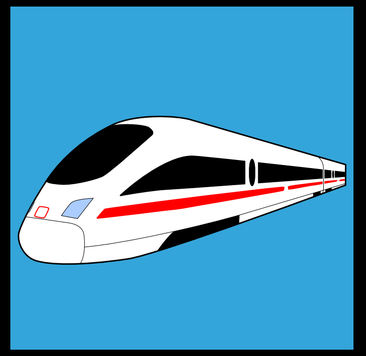
ATOMIC COMMITMENT ACROSS CHAINS

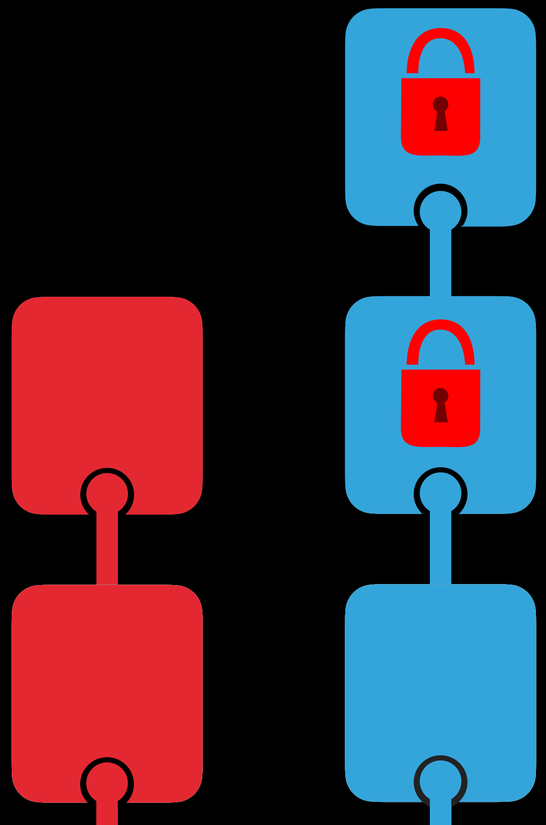
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Each chain locks
    - And stays locked
    - Until both chains are locked
  - Verifies other chains have locked
    - Unlocks



ATOMIC COMMITMENT ACROSS CHAINS

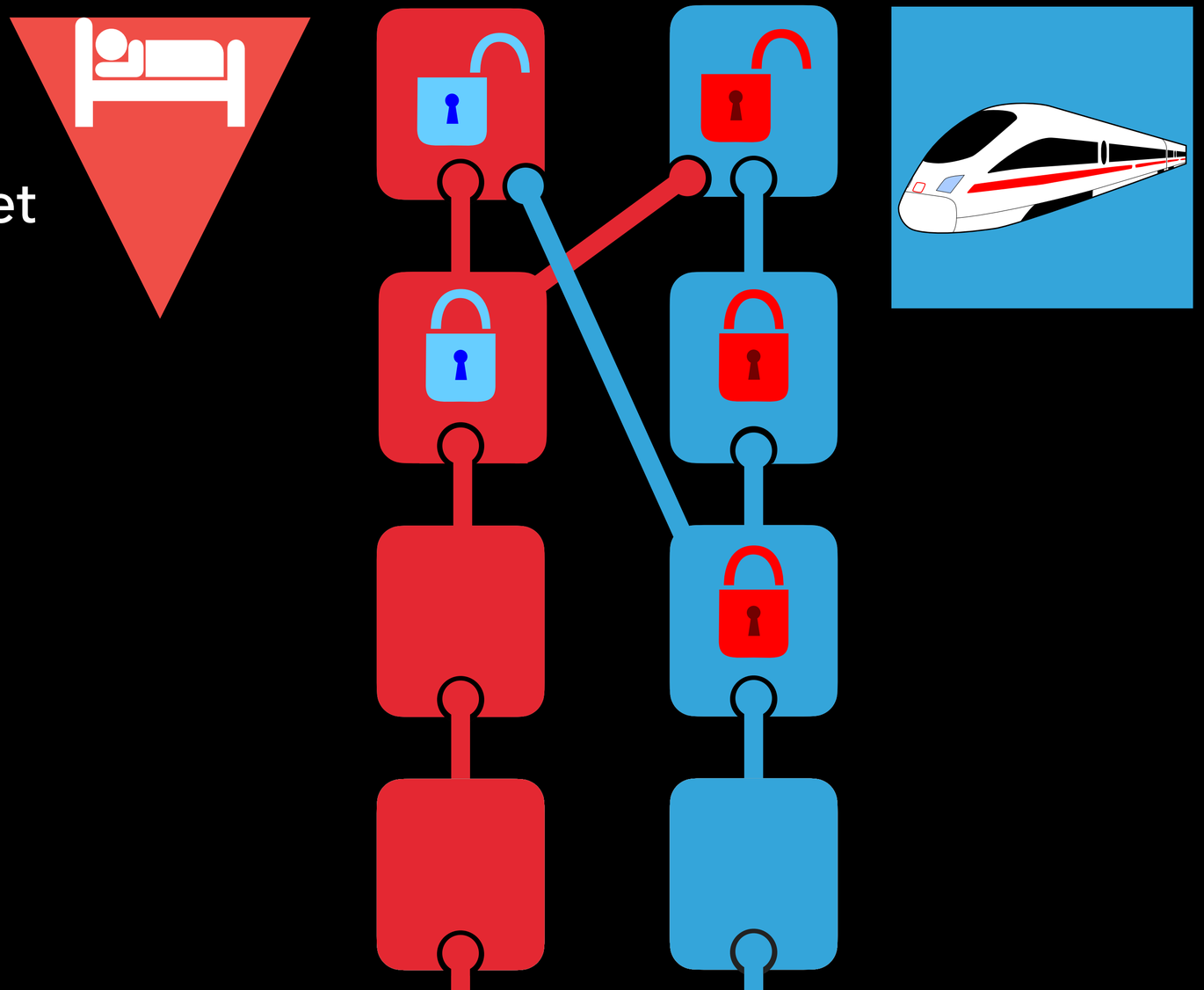
- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Liveness





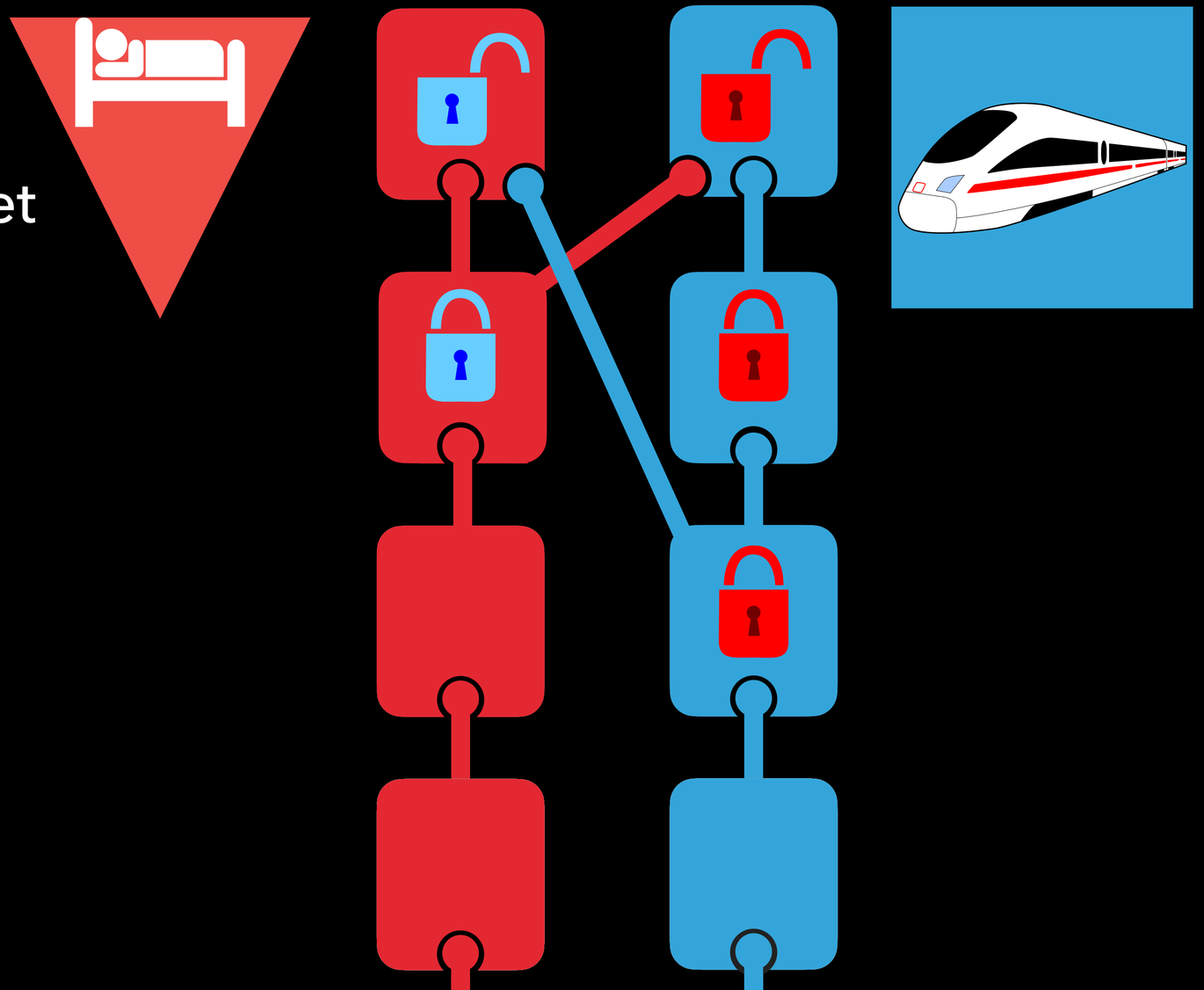
ATOMIC COMMITMENT ACROSS CHAINS

- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Liveness
  - Multiple Rounds



ATOMIC COMMITMENT ACROSS CHAINS

- Atomic commitment
  - Both or Neither: Room & Ticket
- Multi-Phase Commit
  - Liveness
  - Multiple Rounds
  - Free Option

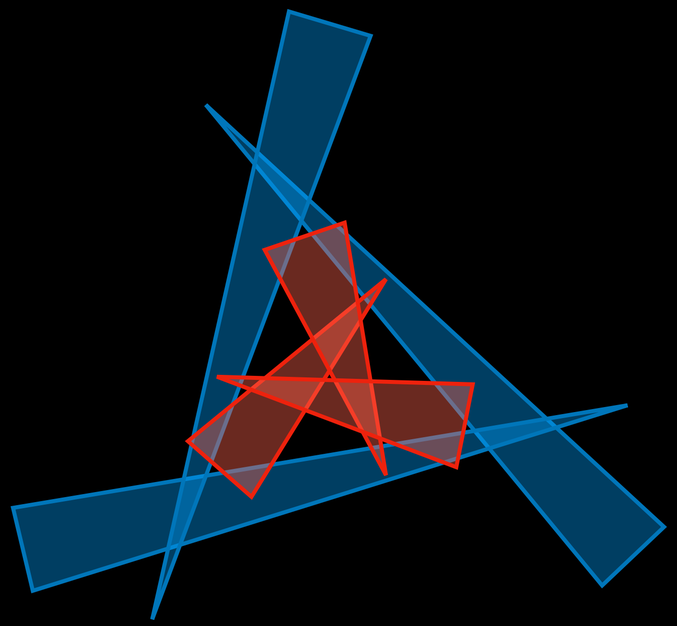


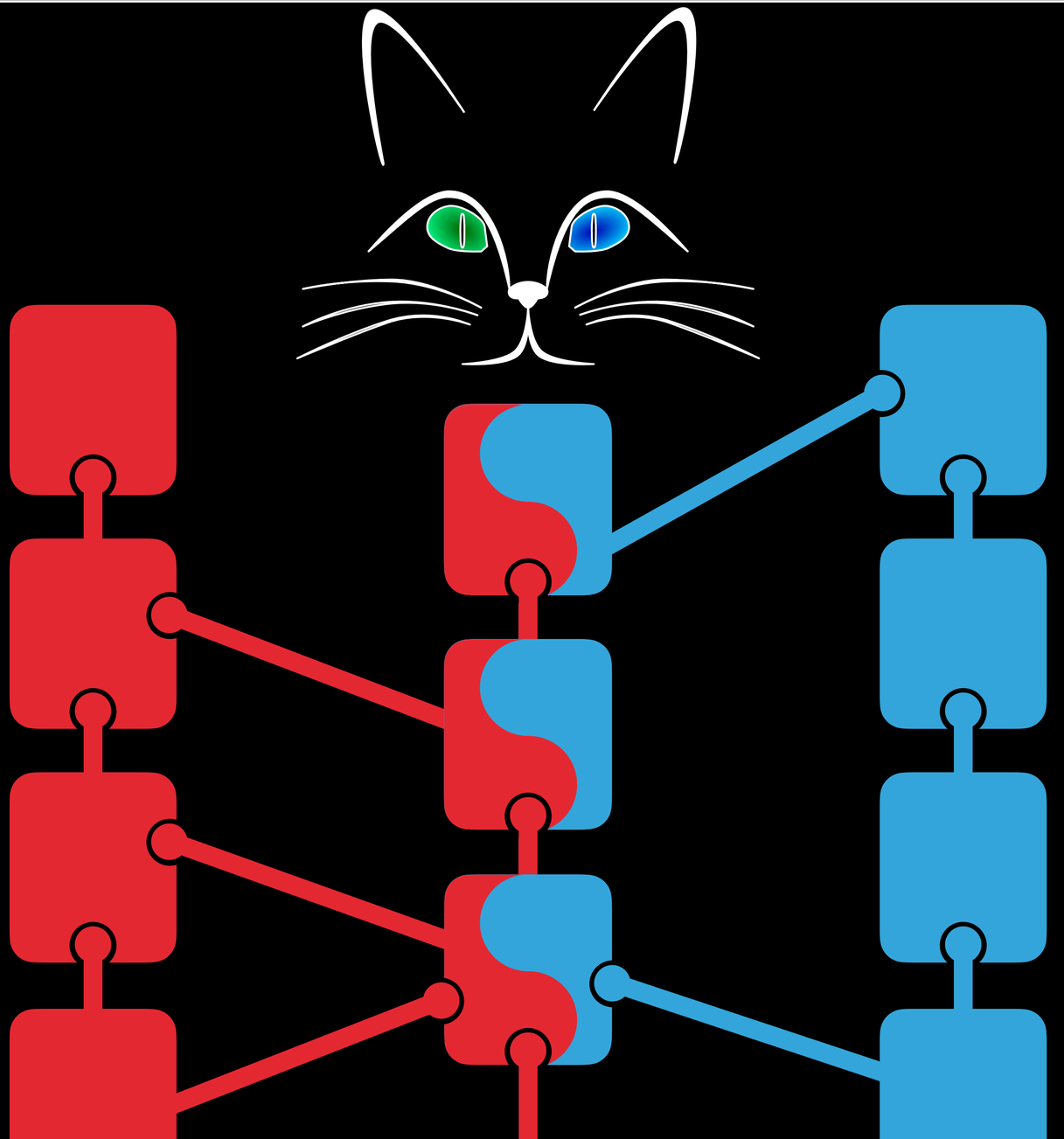
TYPHON OVERVIEW

LOSS OF ATOMICITY

TRUST ASSUMPTIONS

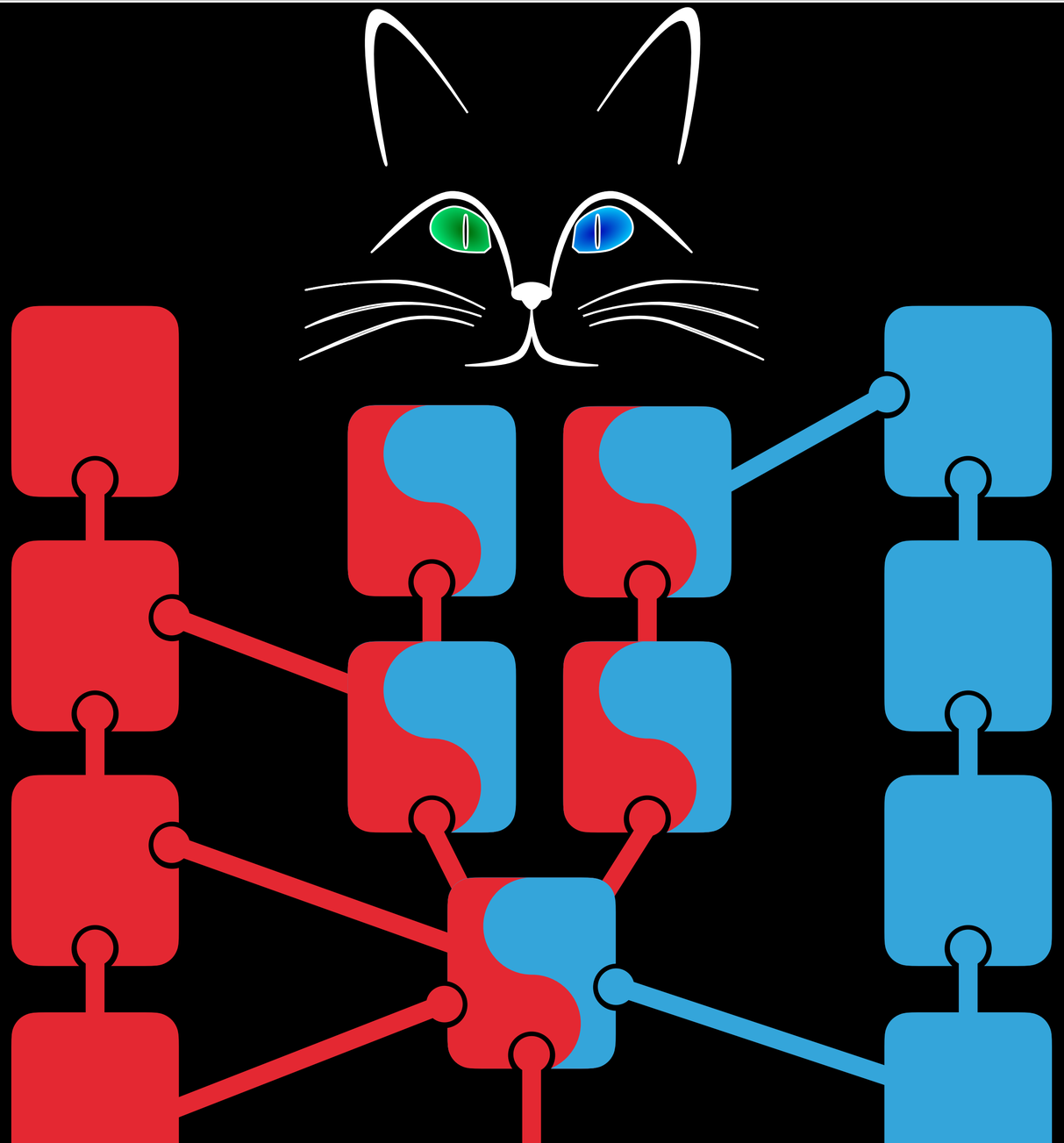
- Safety derives from validators common to multiple chains
- High validator overlap in practice





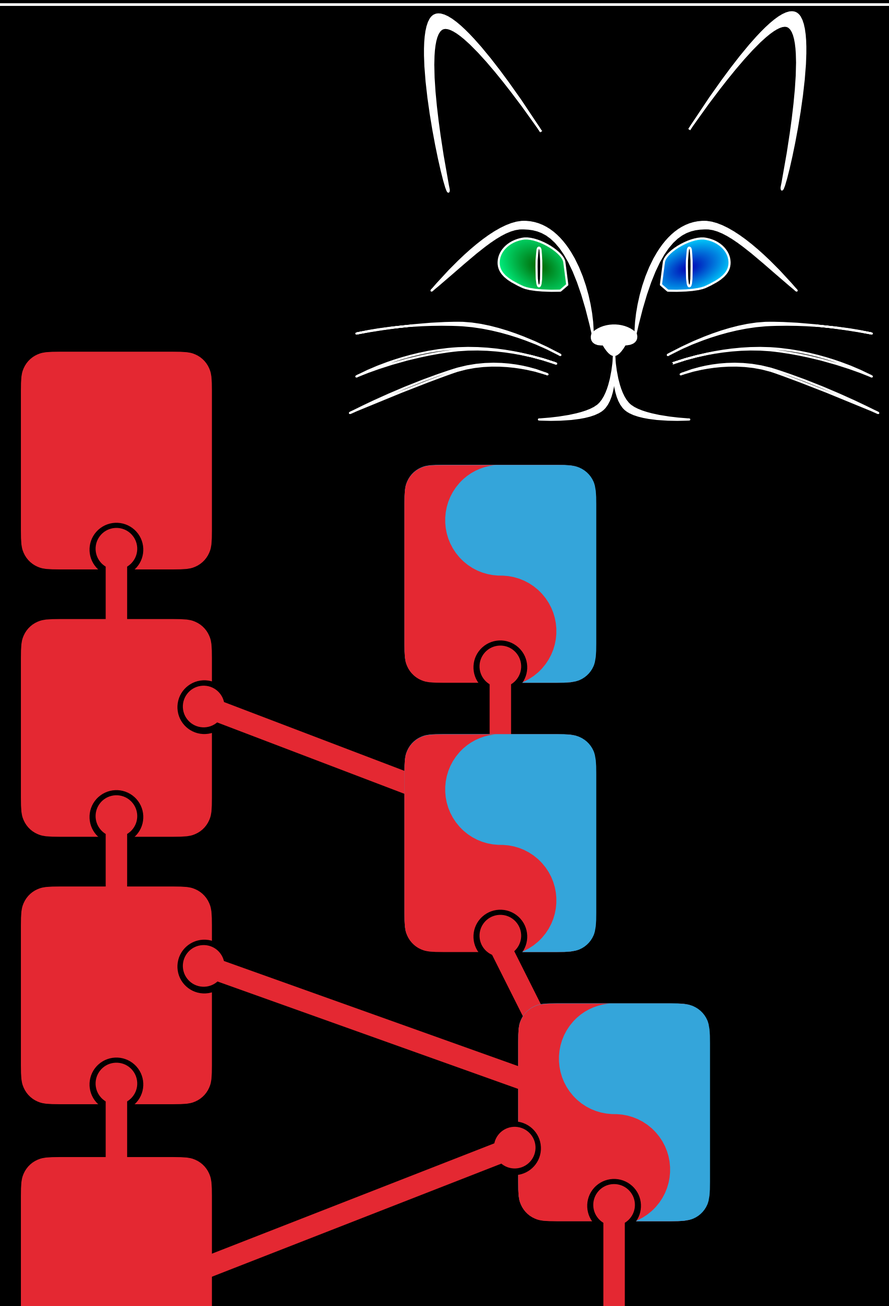
WHEN ATOMICITY FAILS

- Each chain liveness / integrity of its own consensus



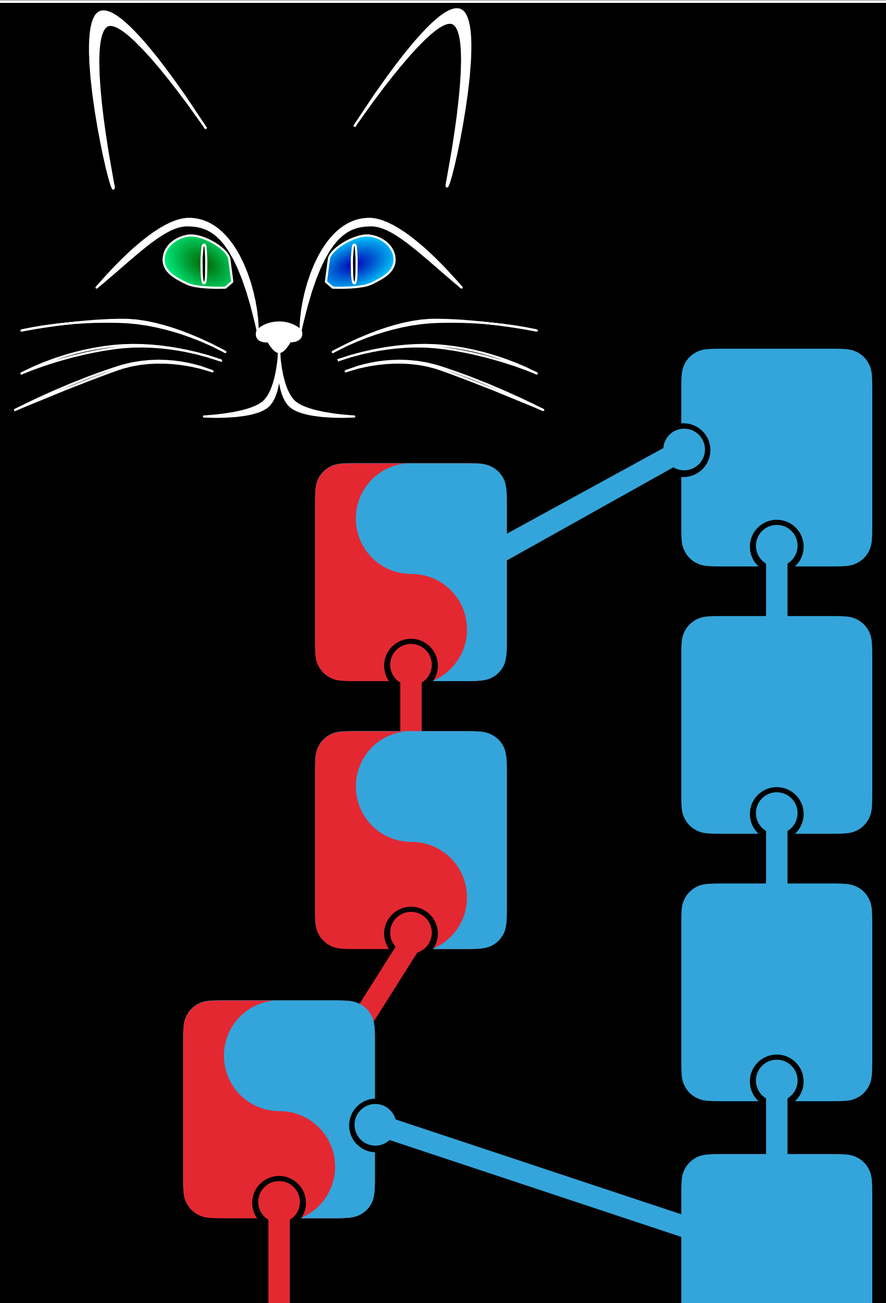
WHEN ATOMICITY FAILS

- Each chain liveness / integrity of its own consensus
- Red Chain remains consistent



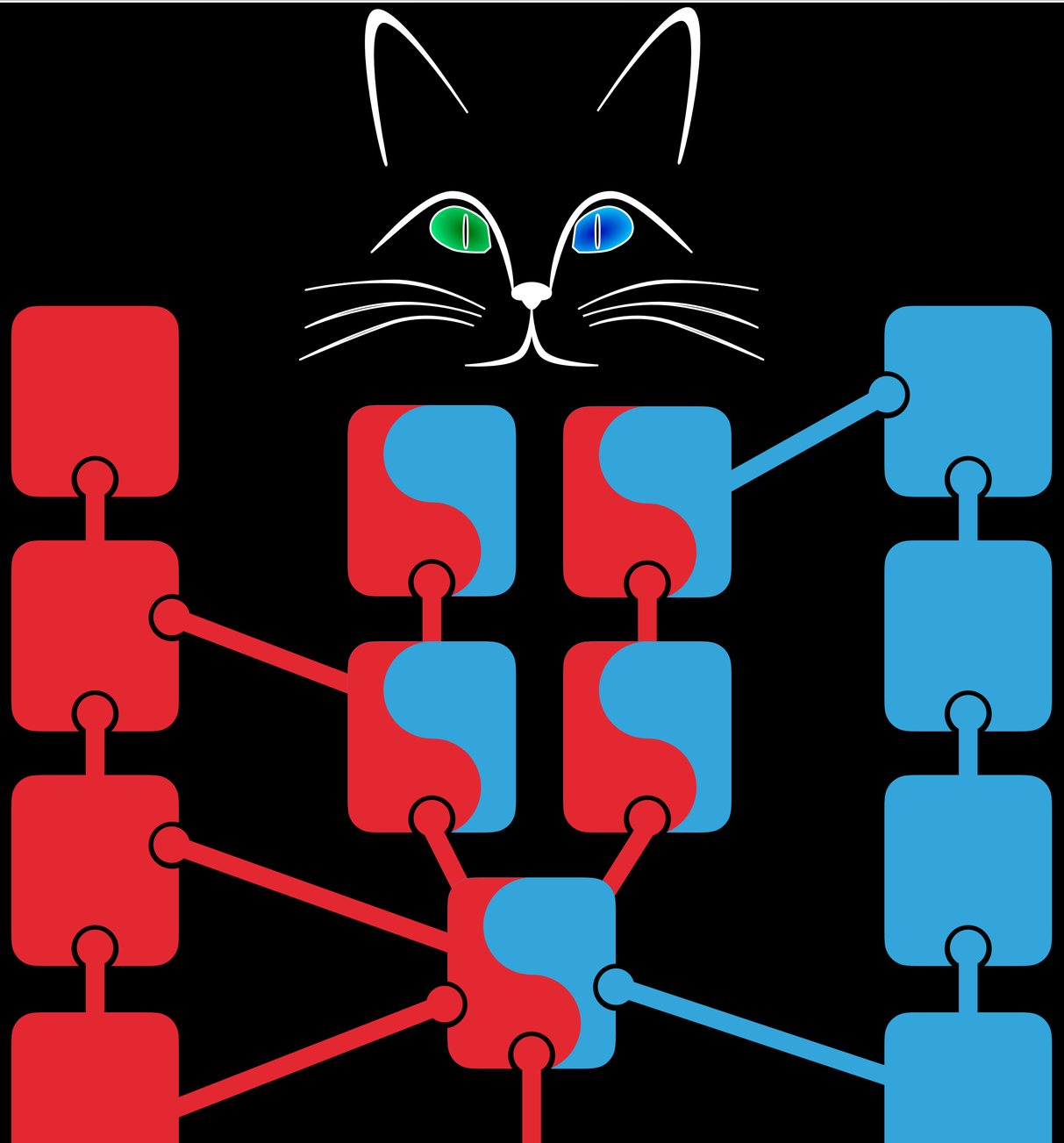
WHEN ATOMICITY FAILS

- Each chain liveness / integrity of its own consensus
- Red Chain remains consistent
- Blue Chain remains consistent



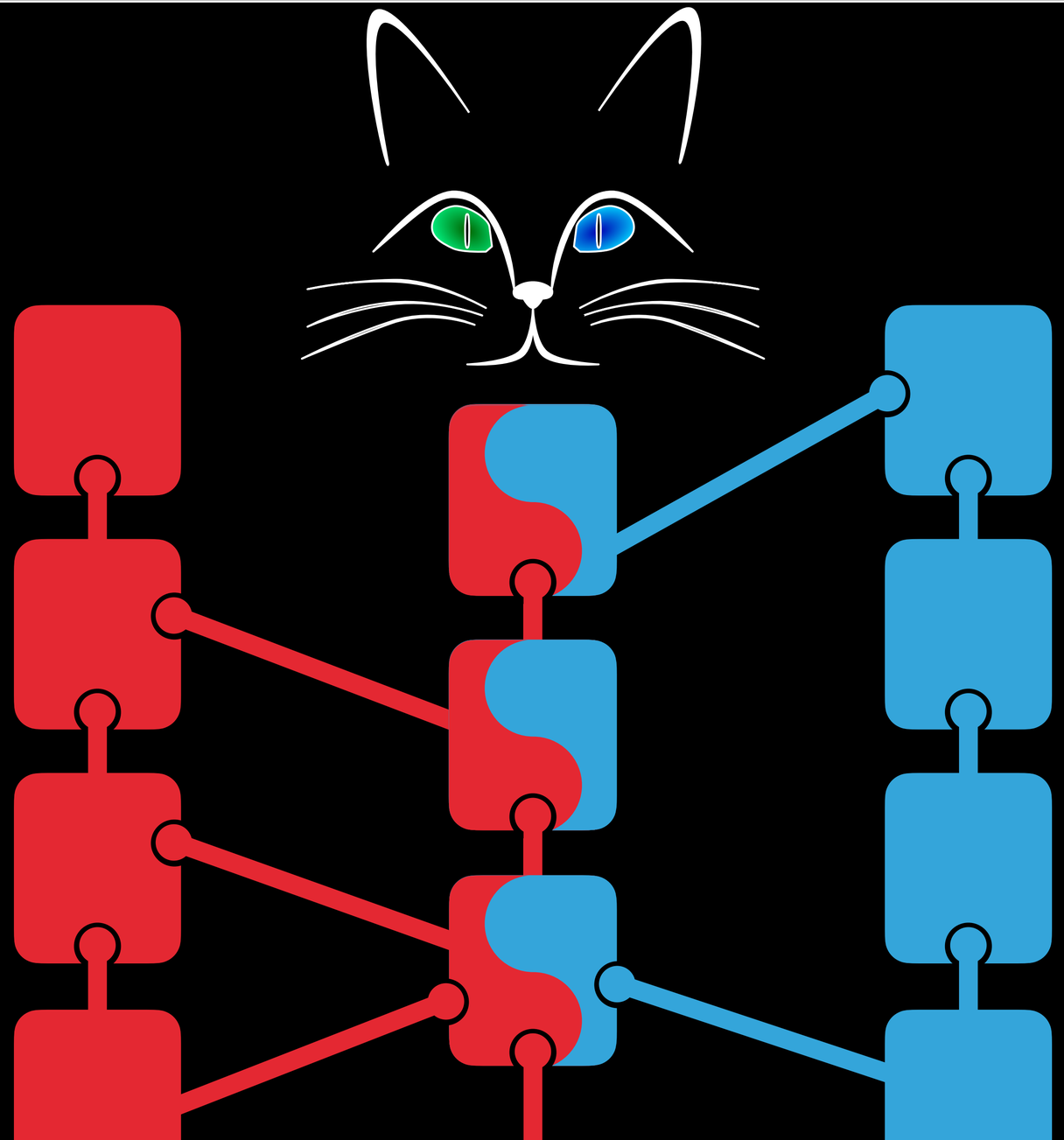
WHEN ATOMICITY FAILS

- Each chain liveness / integrity of its own consensus
- Red Chain remains consistent
- Blue Chain remains consistent



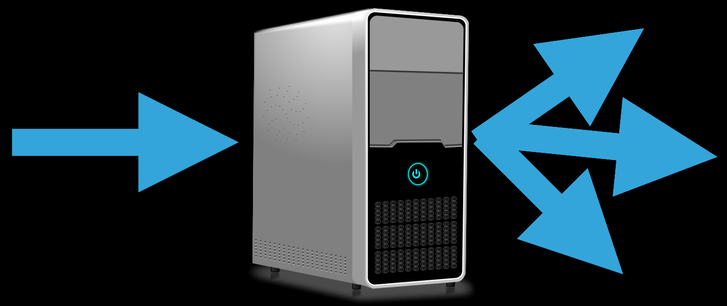
WHEN ATOMICITY FAILS

- Each chain liveness / integrity of its own consensus
- Red Chain remains consistent
- Blue Chain remains consistent



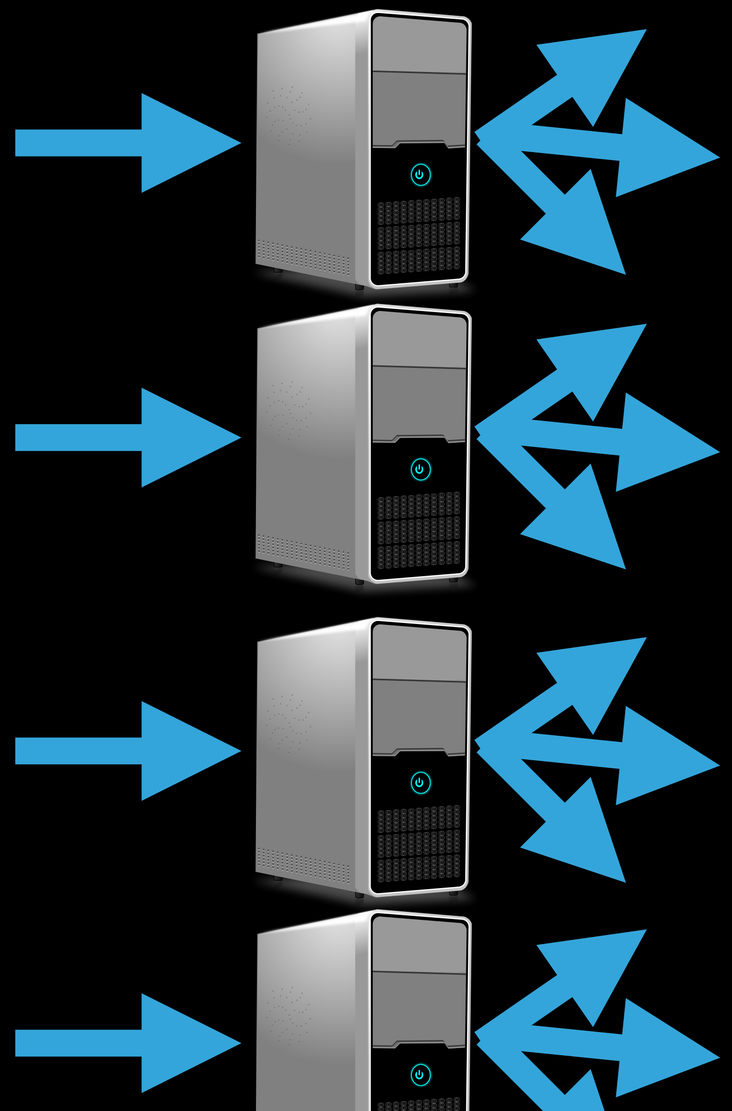
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store



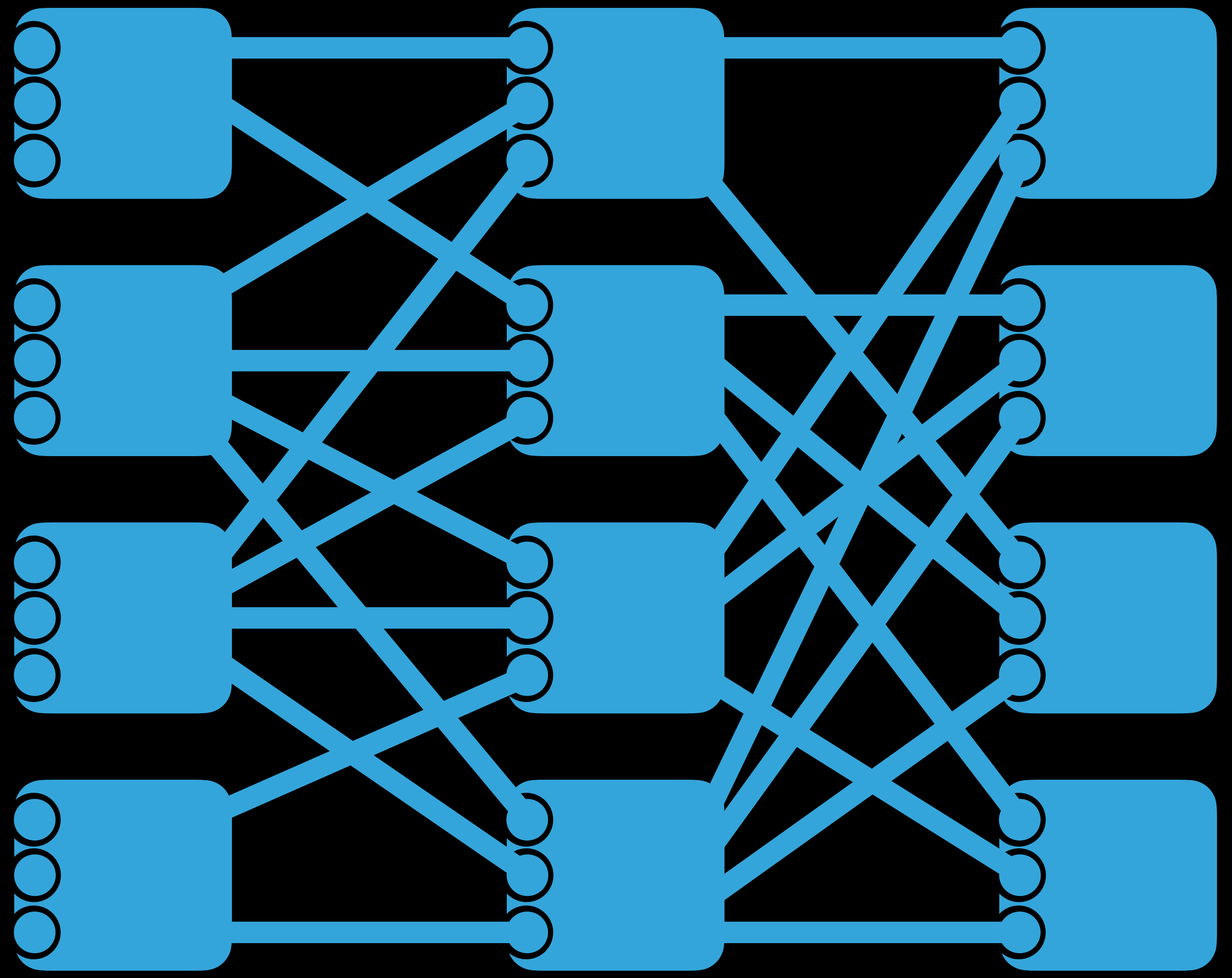
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator



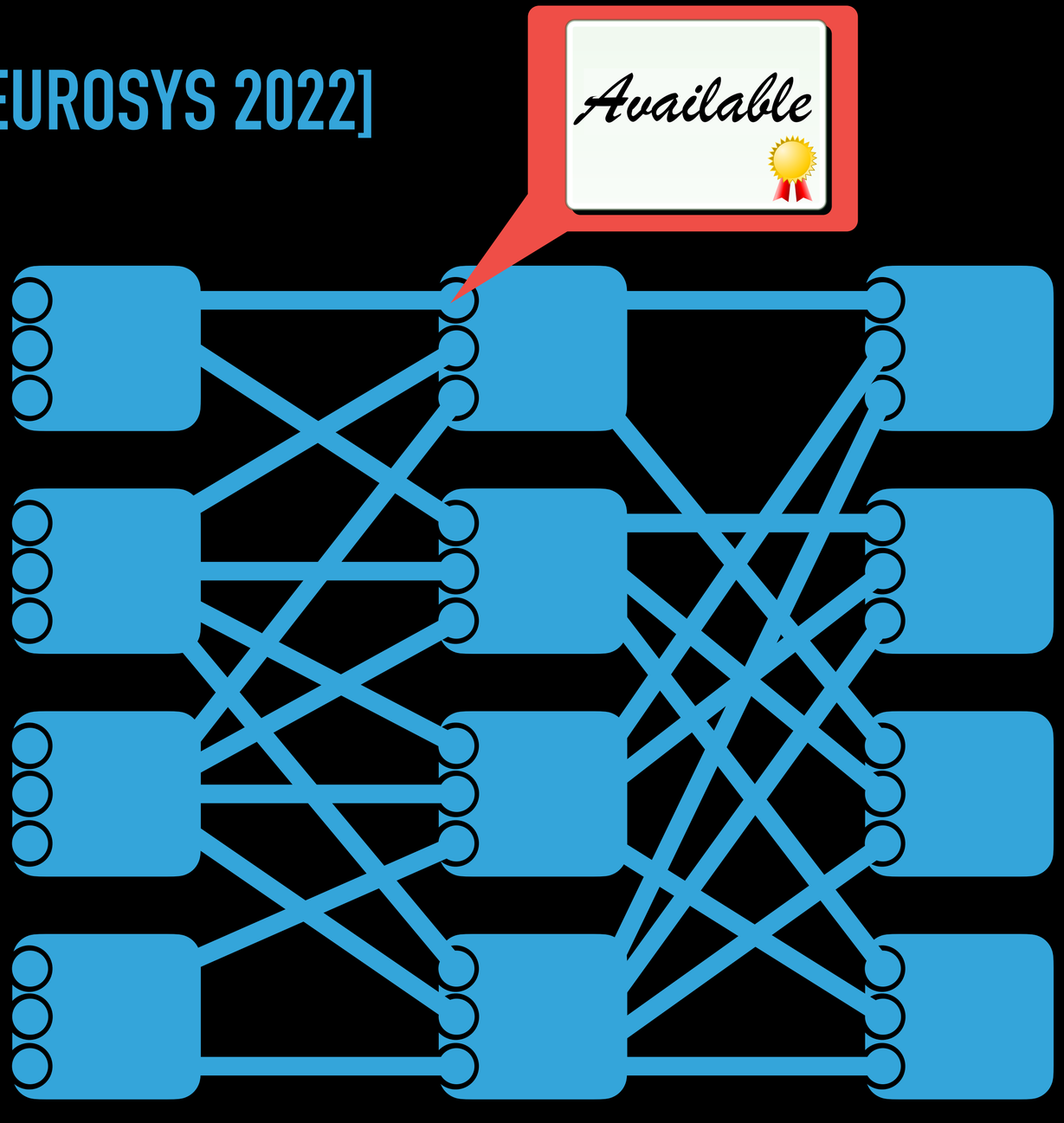
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks



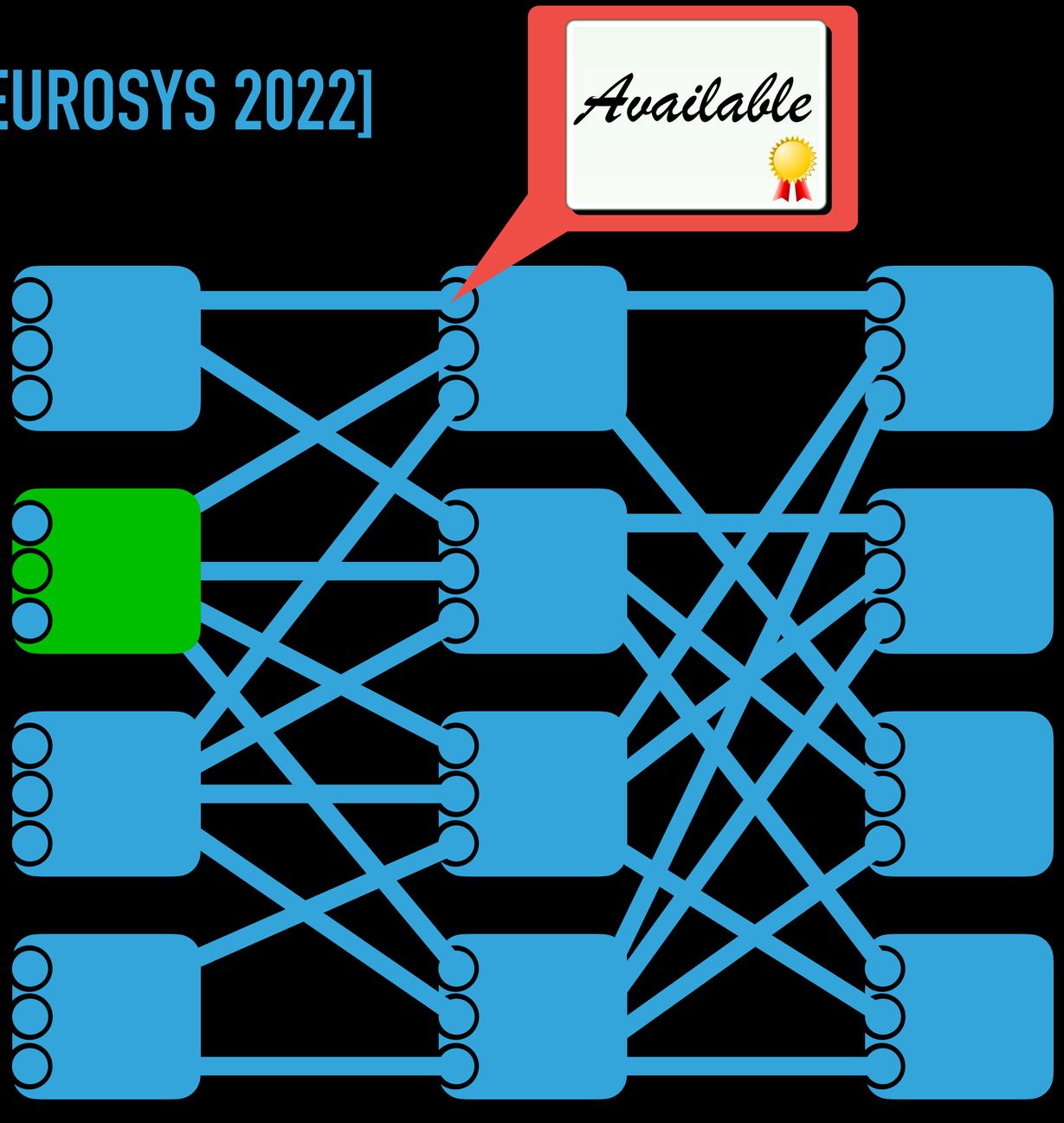
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order



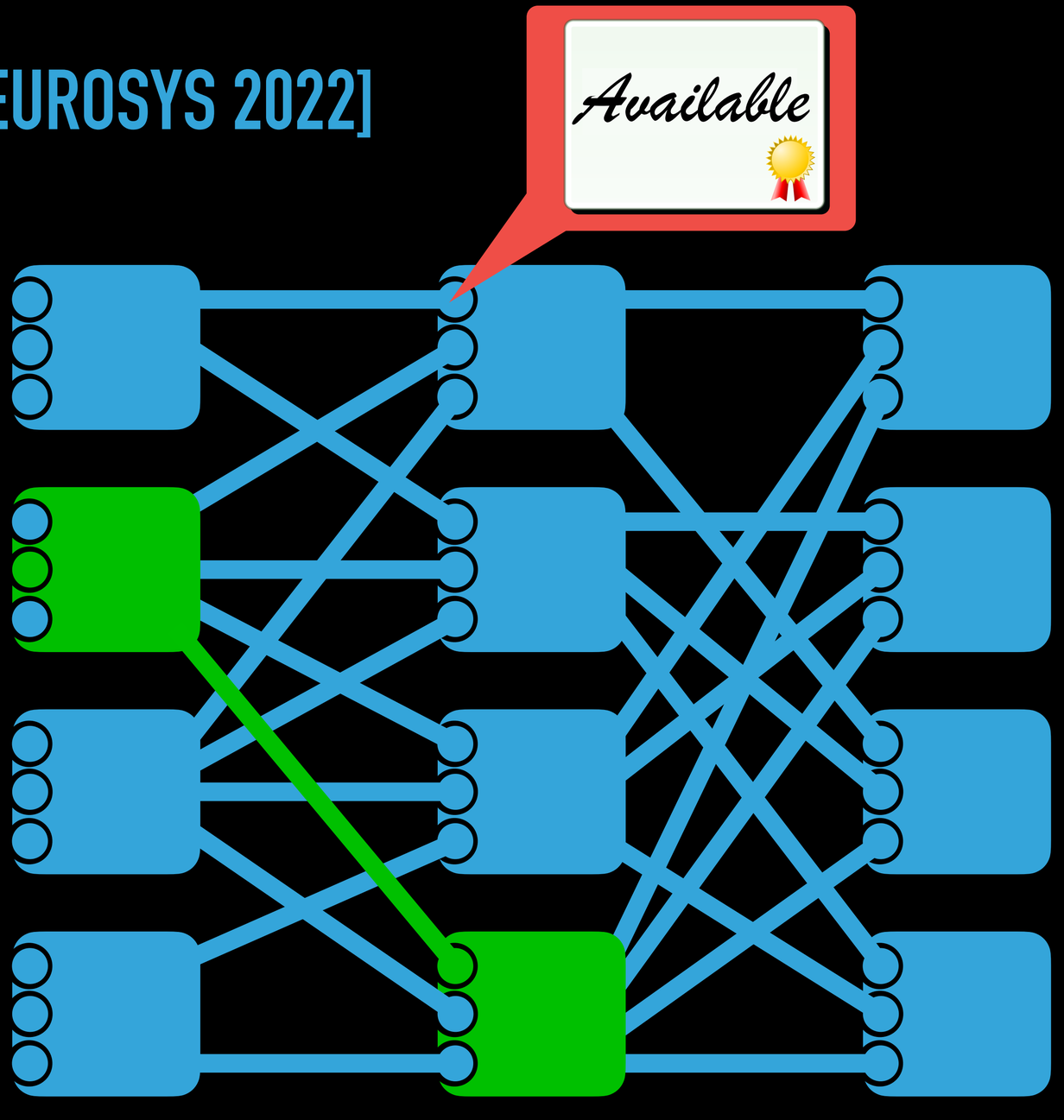
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order



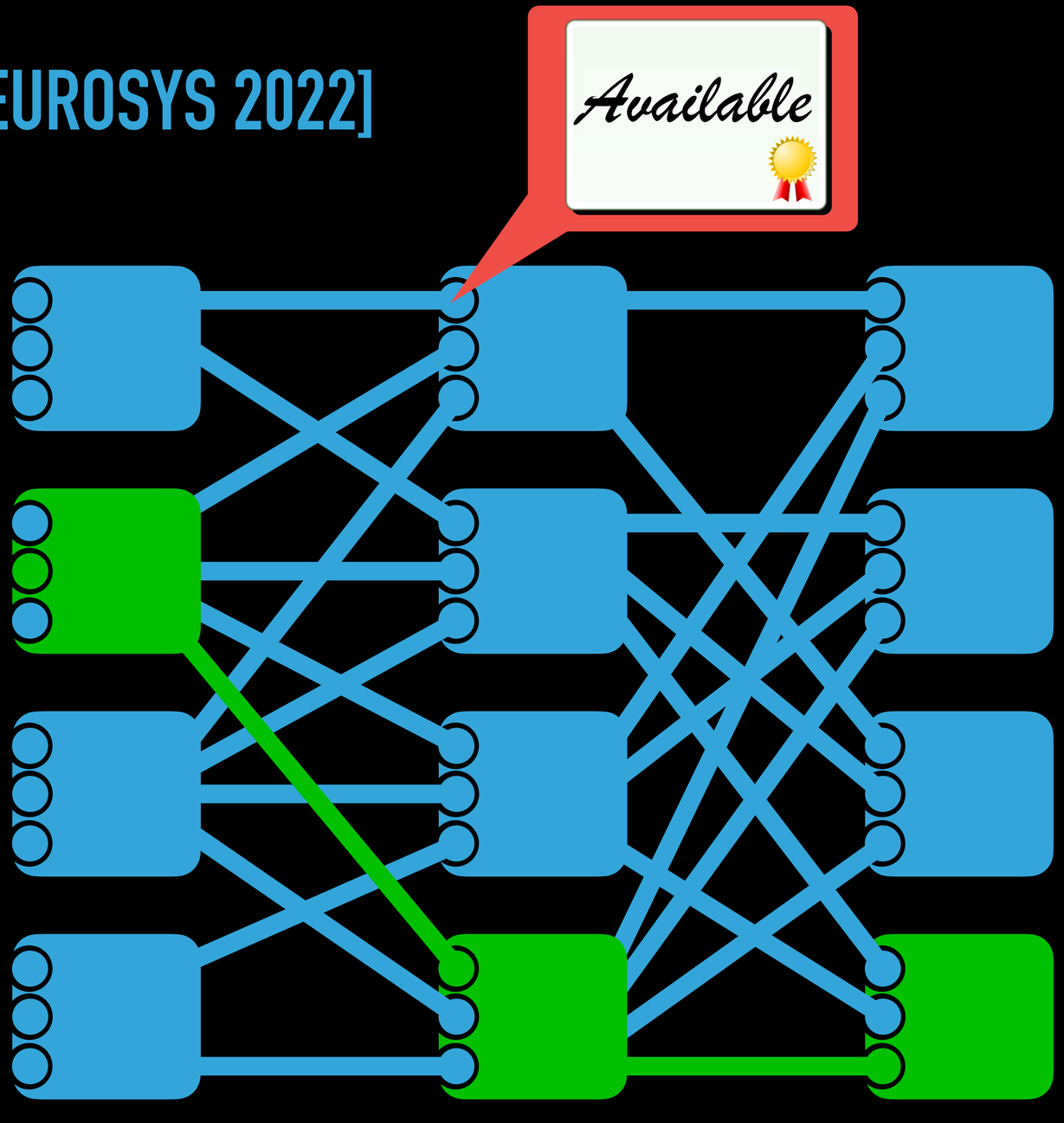
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order



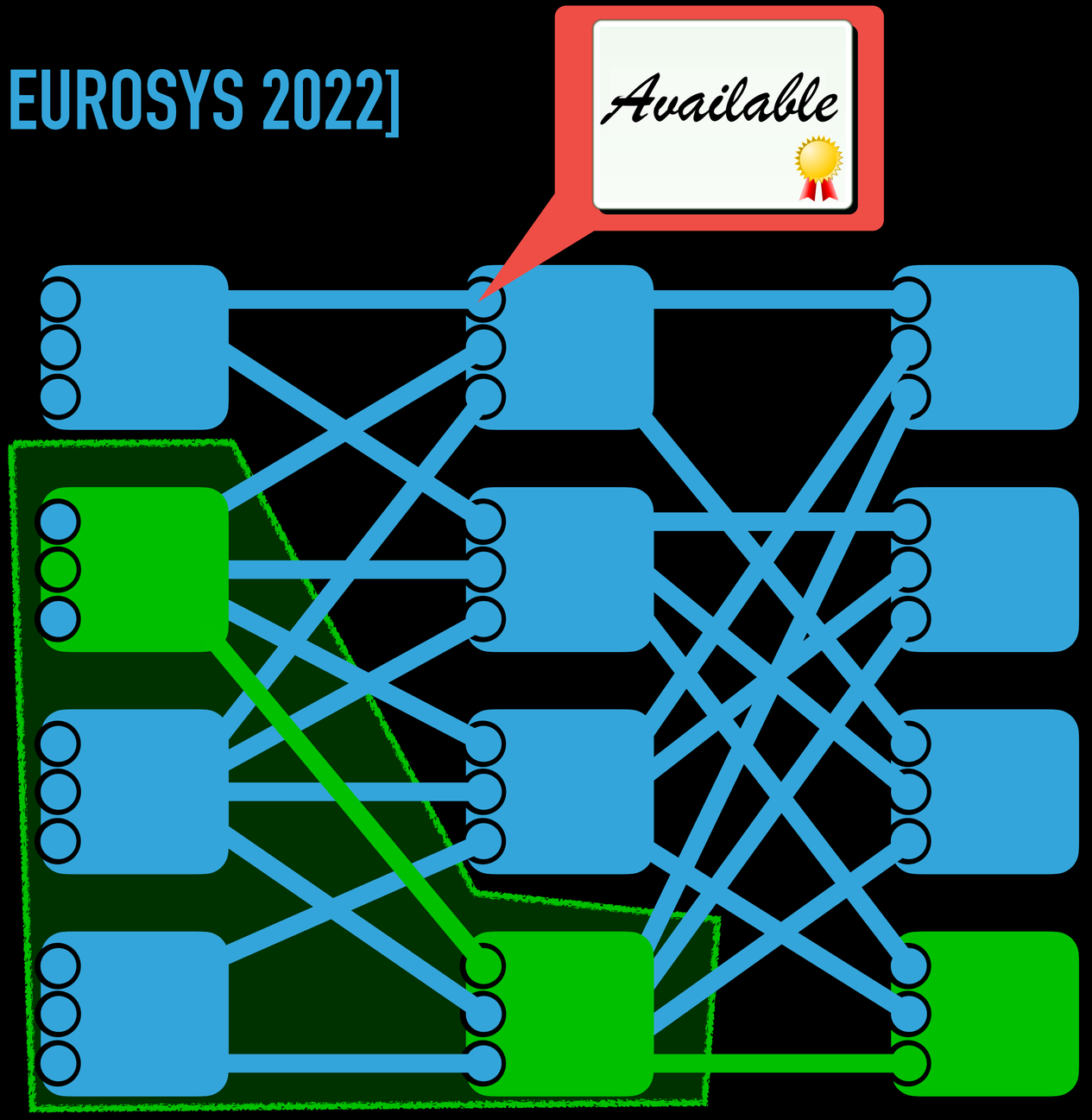
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order



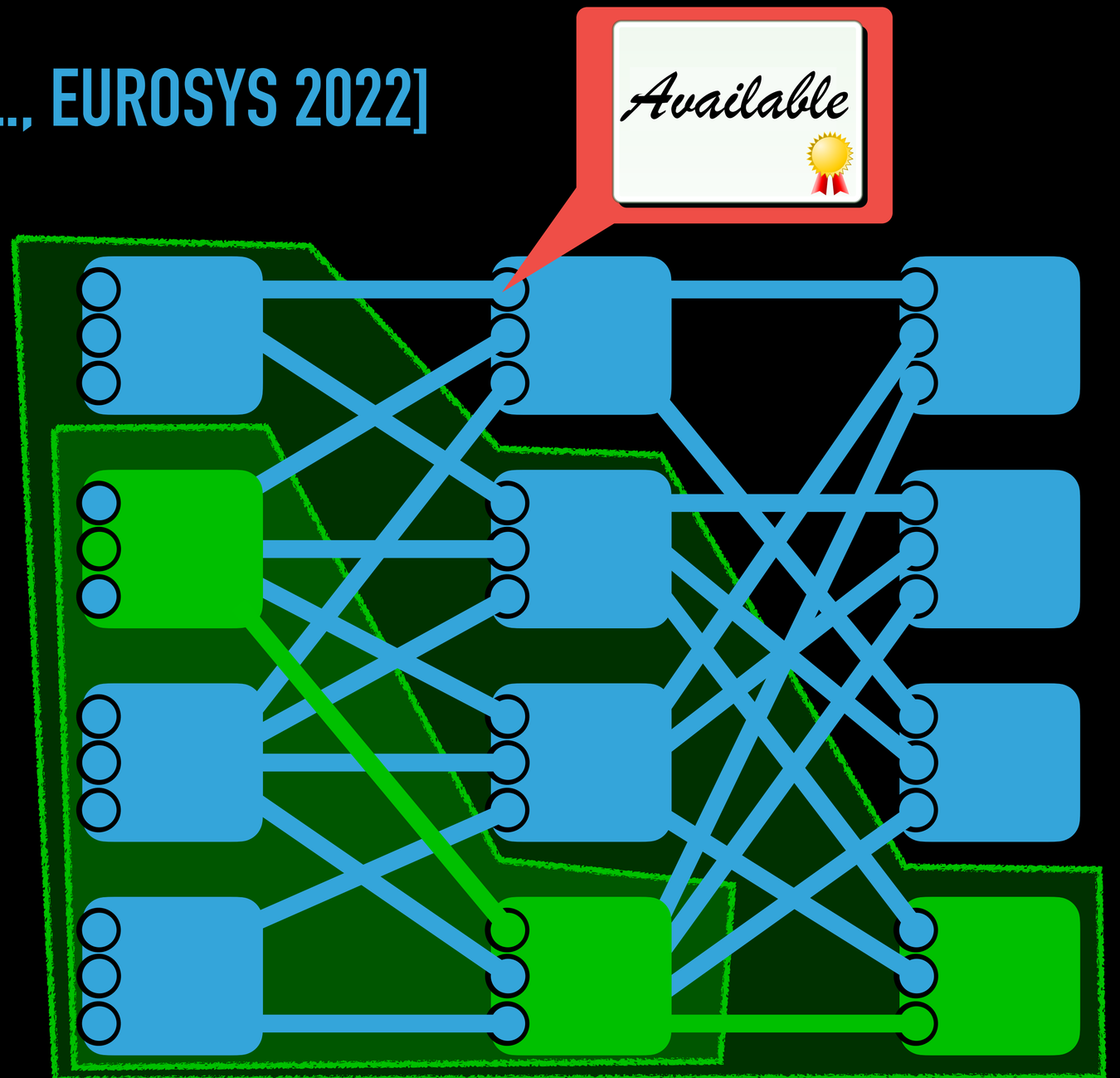
NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order

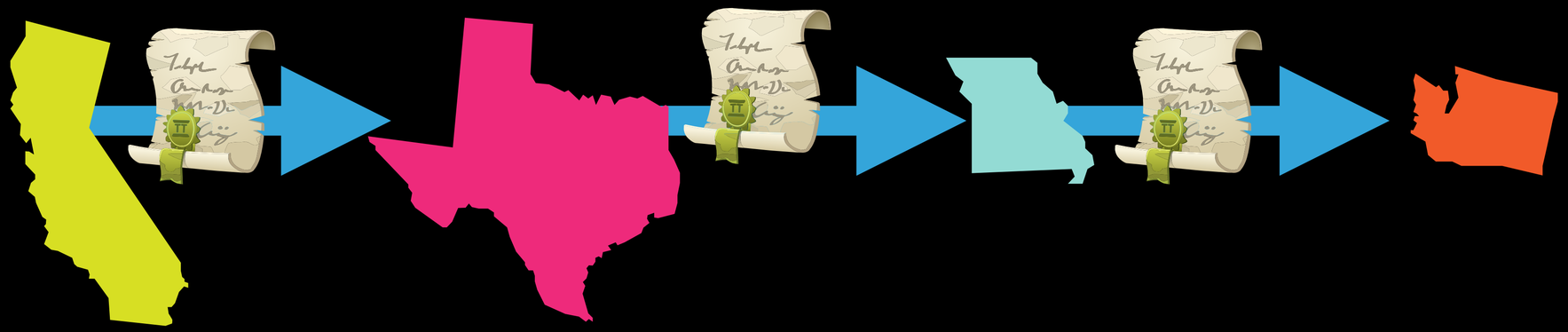


NARWHAL MEMPOOL [DANZENIS ET. AL., EUROSYS 2022]

- Validators
  - Receive transactions from clients
  - Replicate and store
- Many workers per validator
- DAG of Mempool blocks
  - Certificates of Availability
  - Consensus chooses total order



COMET

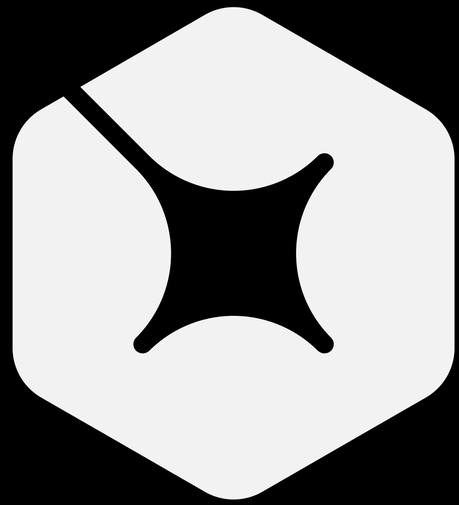


- State Machine
  - Sub-state with well-defined permissions
- High availability
- ~~High Throughput~~
- High Integrity
  - "Everyone" agrees

Serialized execution

Block proposal bottleneck

Cross-chain transactions



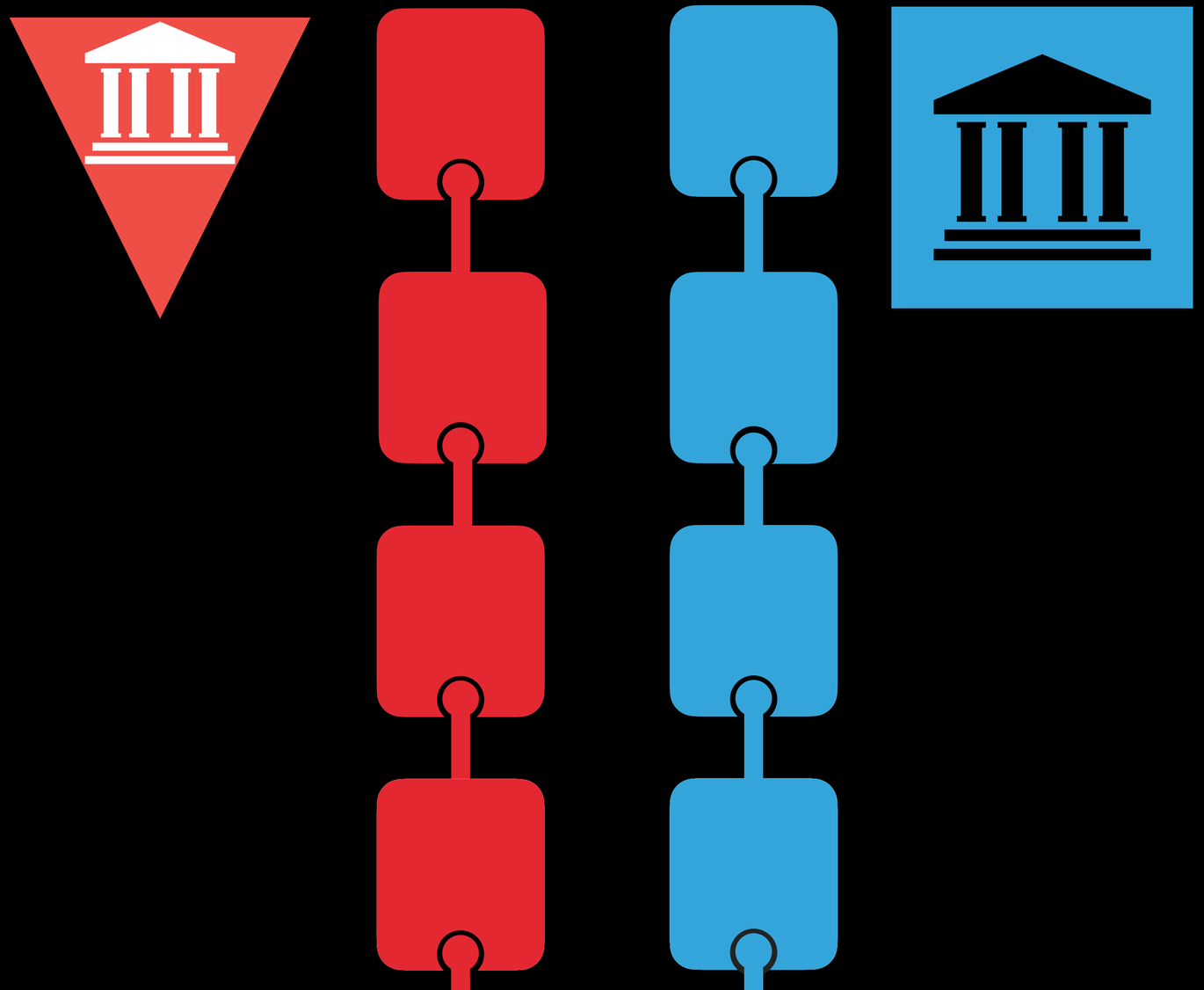
IEVS

VOCABULARY

State Machine Replication	Blockchain
BFT Replicated State Machine System	Chain
State Machine	State Machine
State Transition / Transaction	Transaction
Log	Ledger
Object	Smart Contract
Batch of Transactions	Block
Replica / Learner	Full Node
Acceptor	Validator / Voter / Miner
Slot / Instance of Consensus	Height

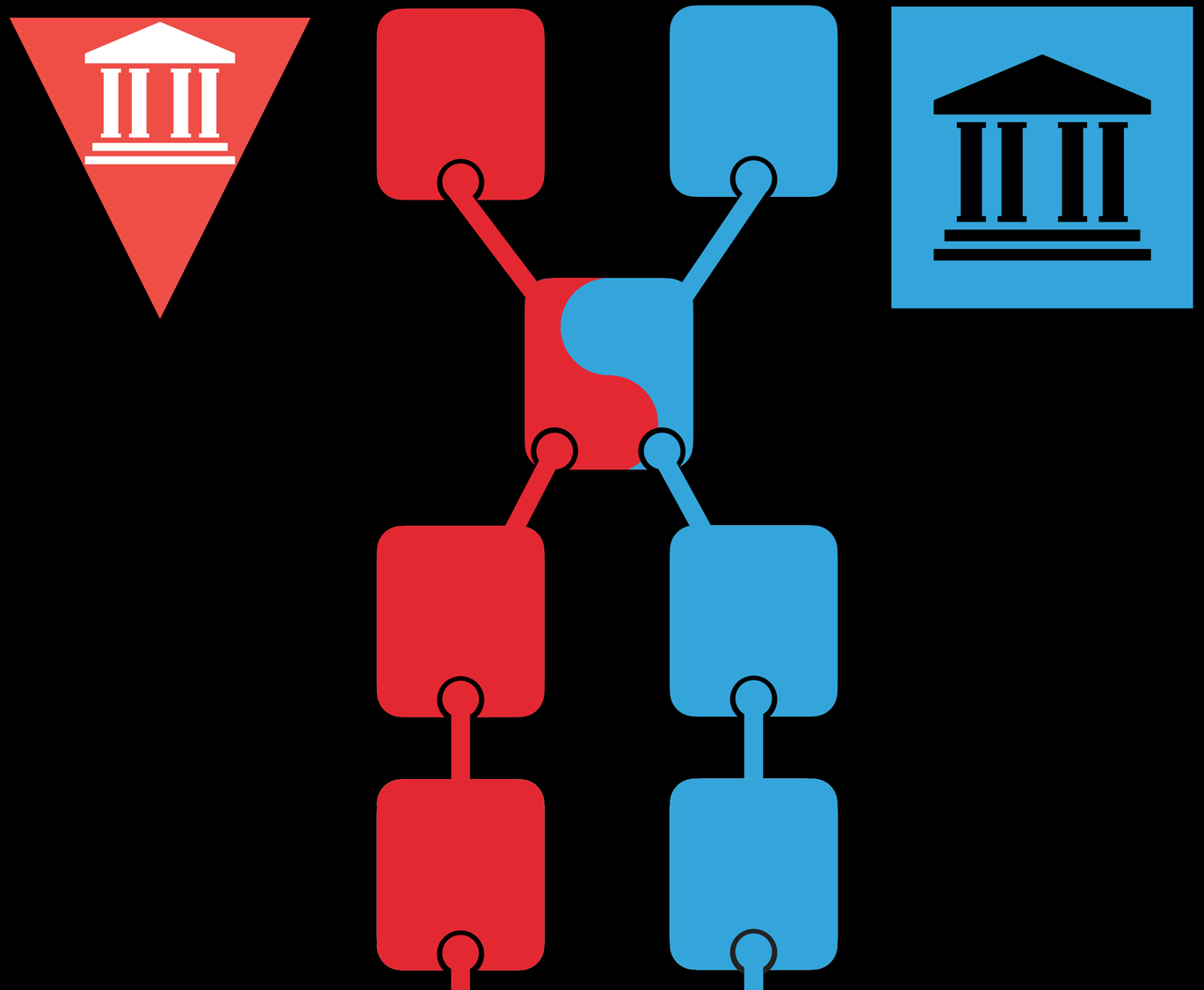
ATOMIC COMMITMENT ACROSS CHAINS

- 2 chains (with finality)
  - Different maintainers

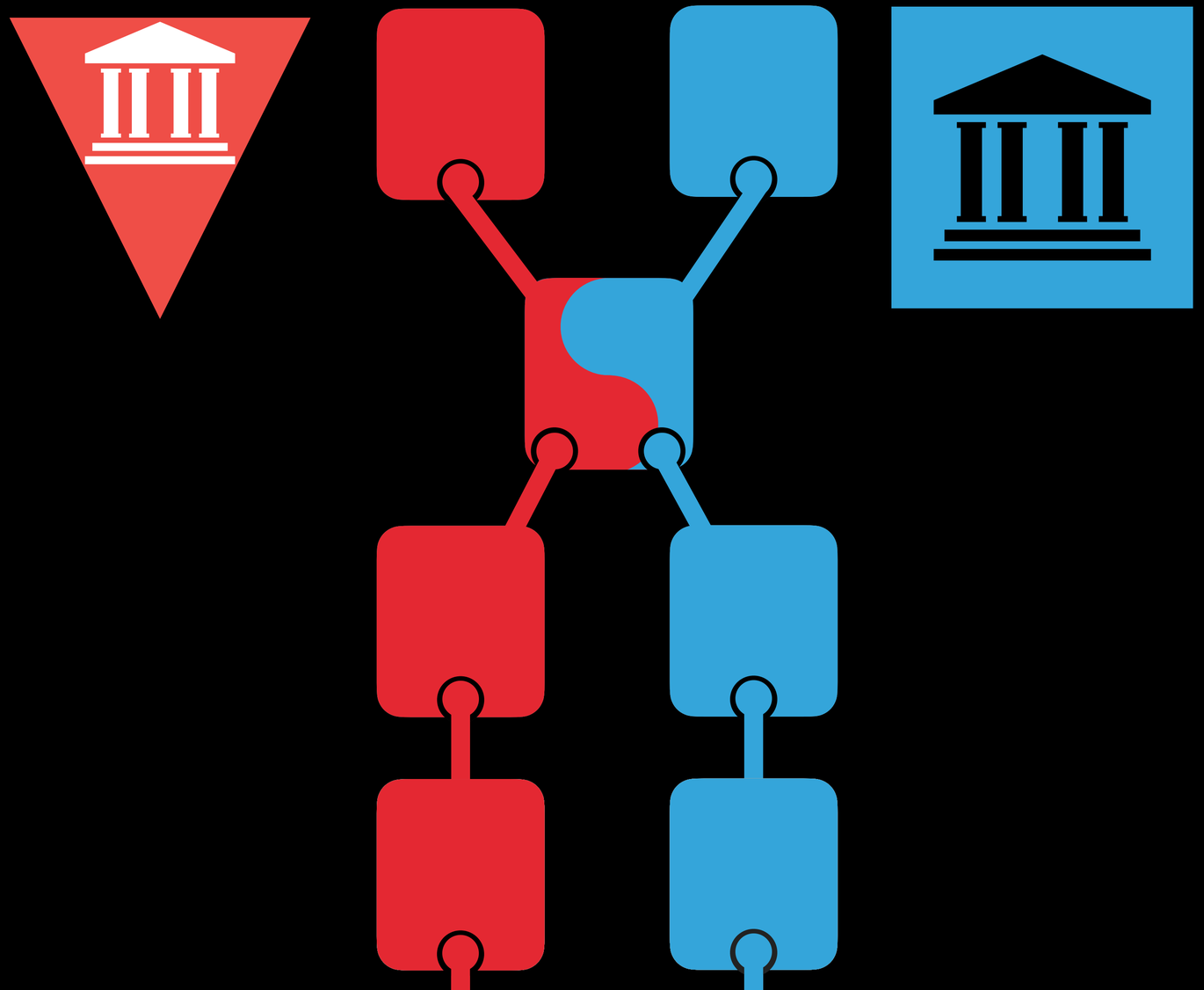


ATOMIC COMMITMENT ACROSS CHAINS

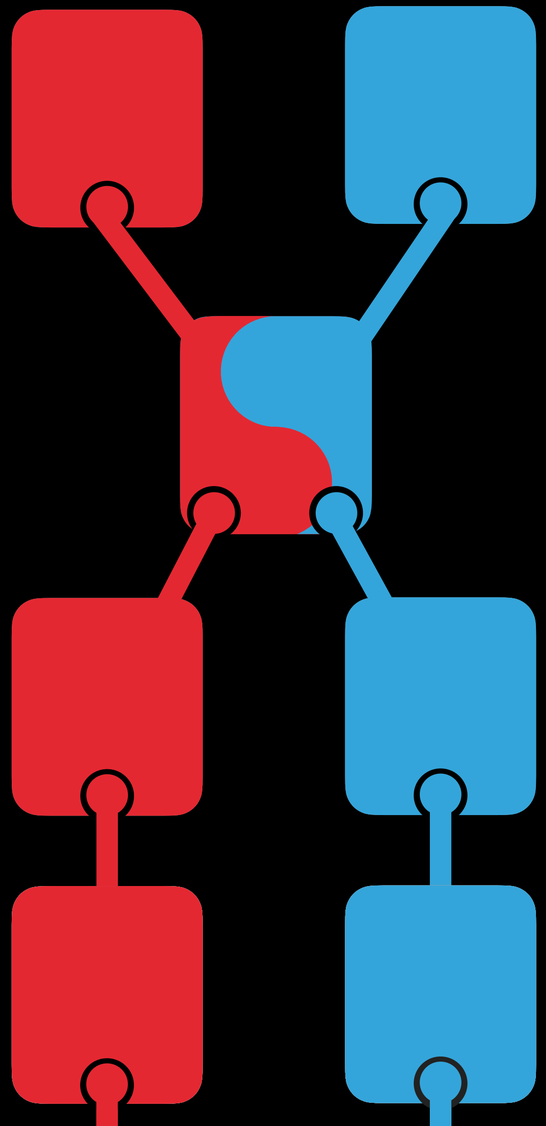
- 2 chains (with finality)
  - Different maintainers
- One block for both chains



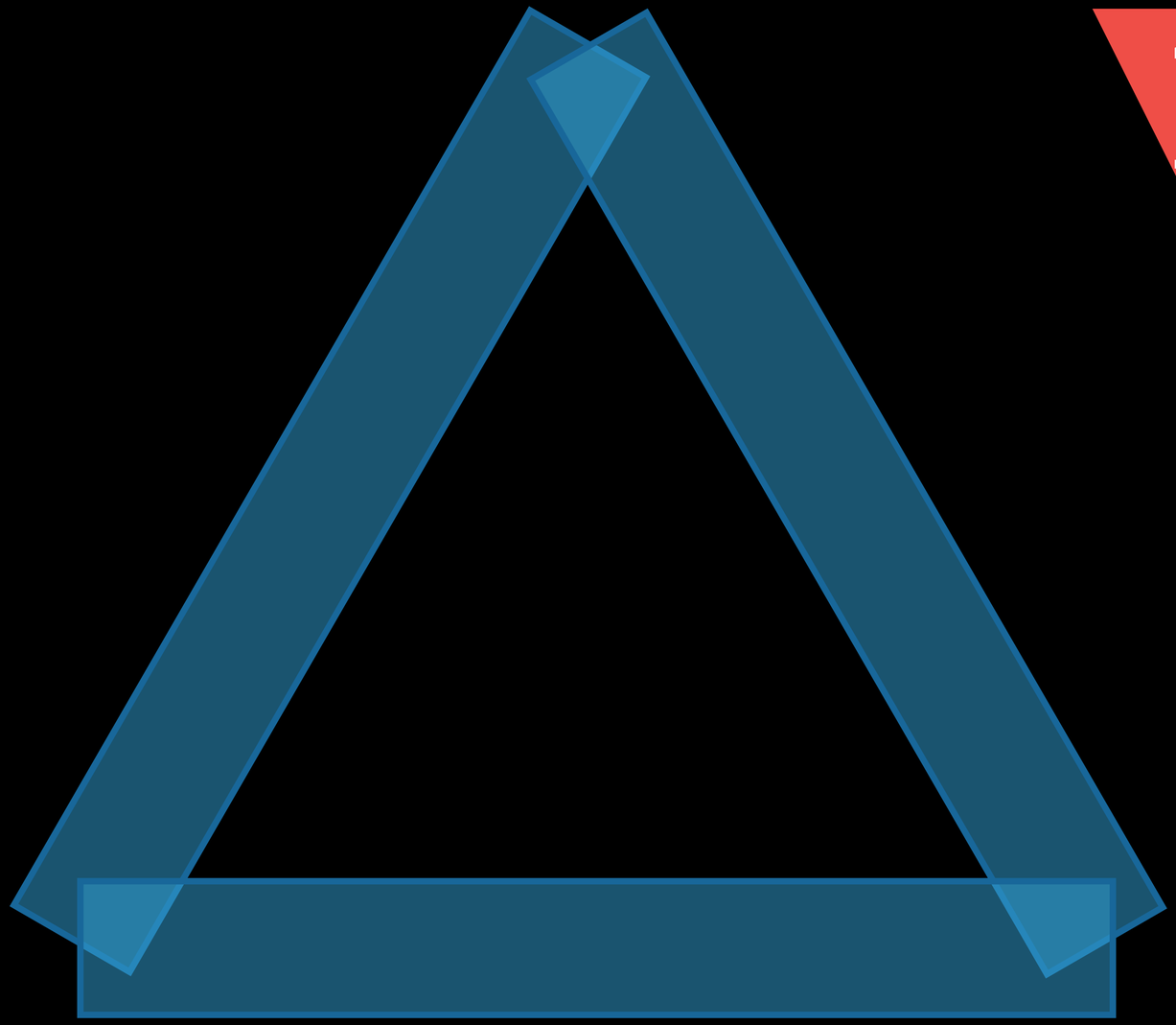
HETEROGENEOUS PAXOS

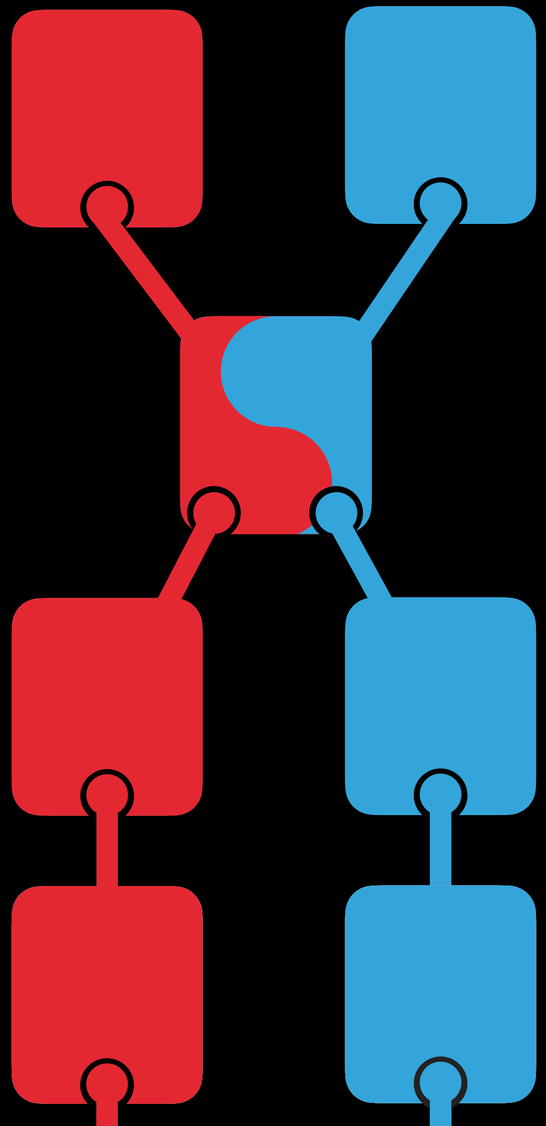


HETEROGENEOUS PAXOS

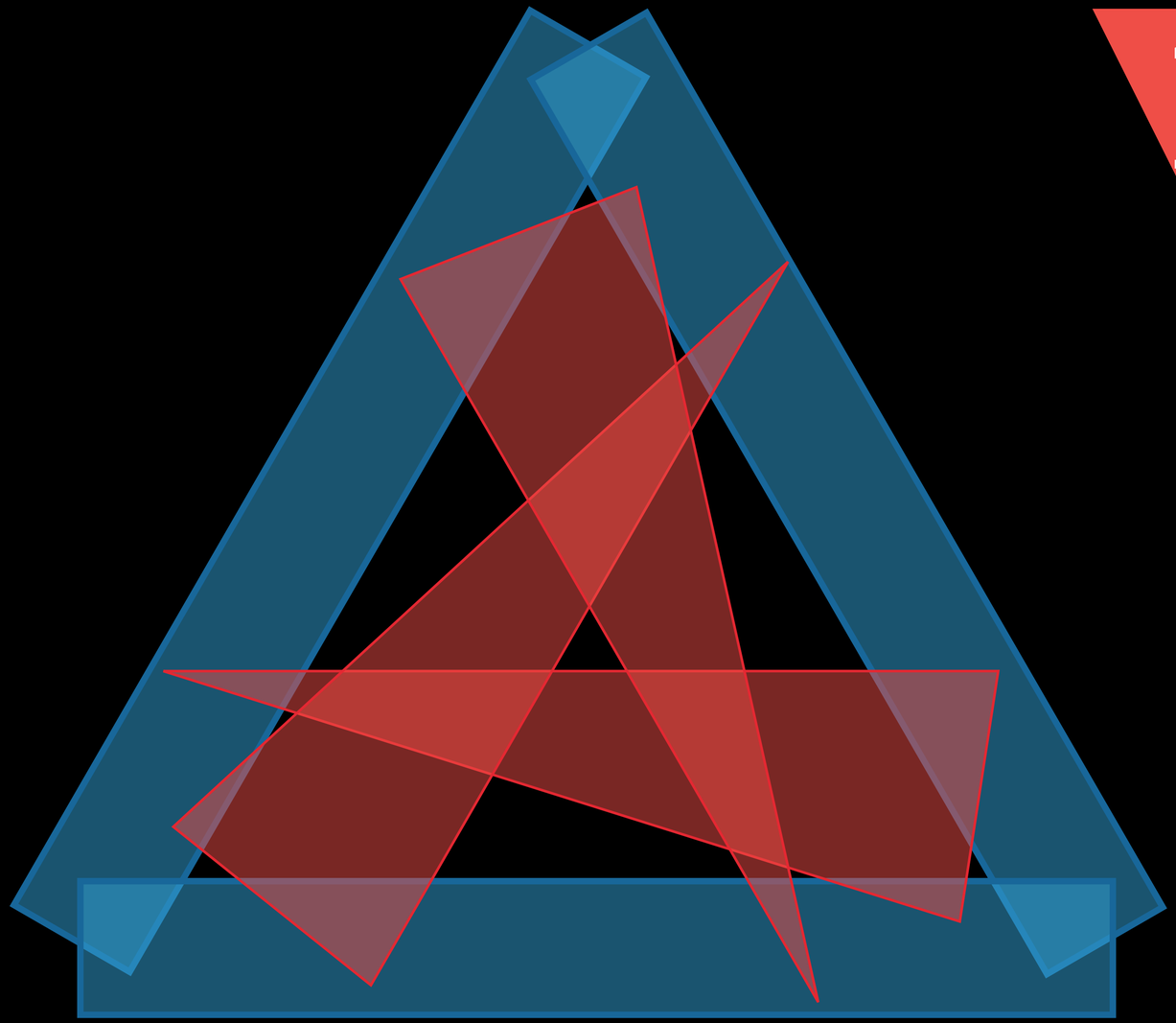


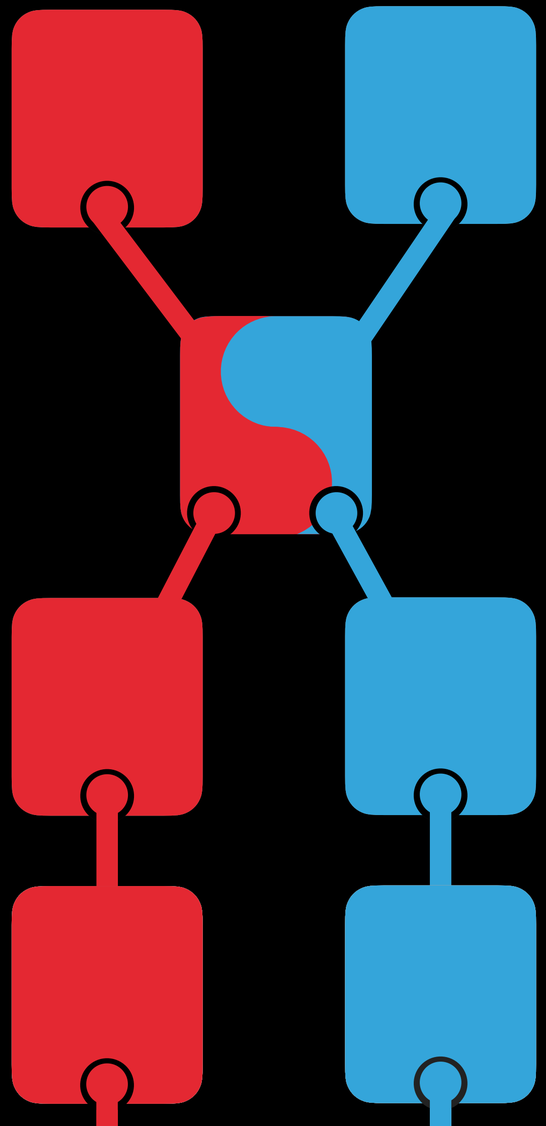
HETEROGENEOUS PAXOS



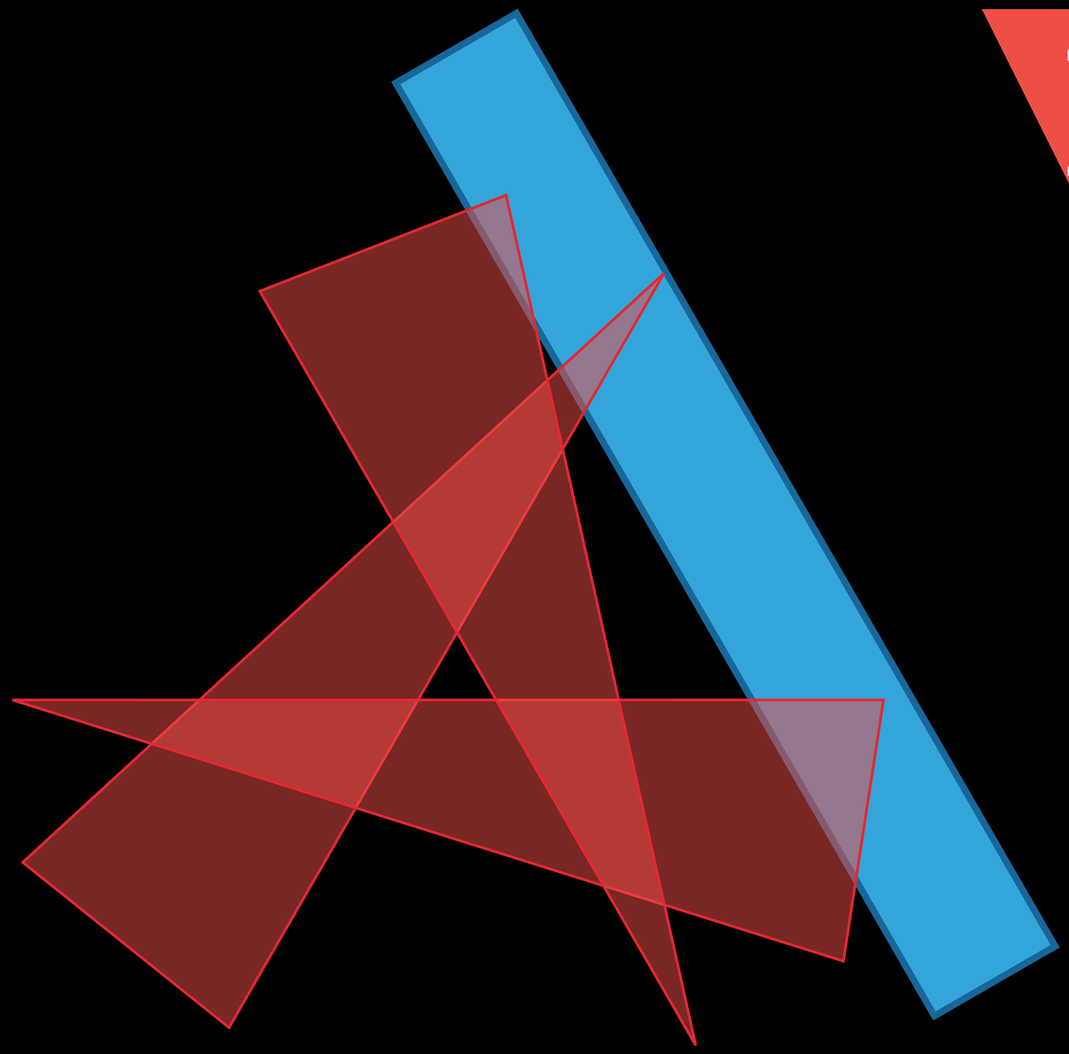


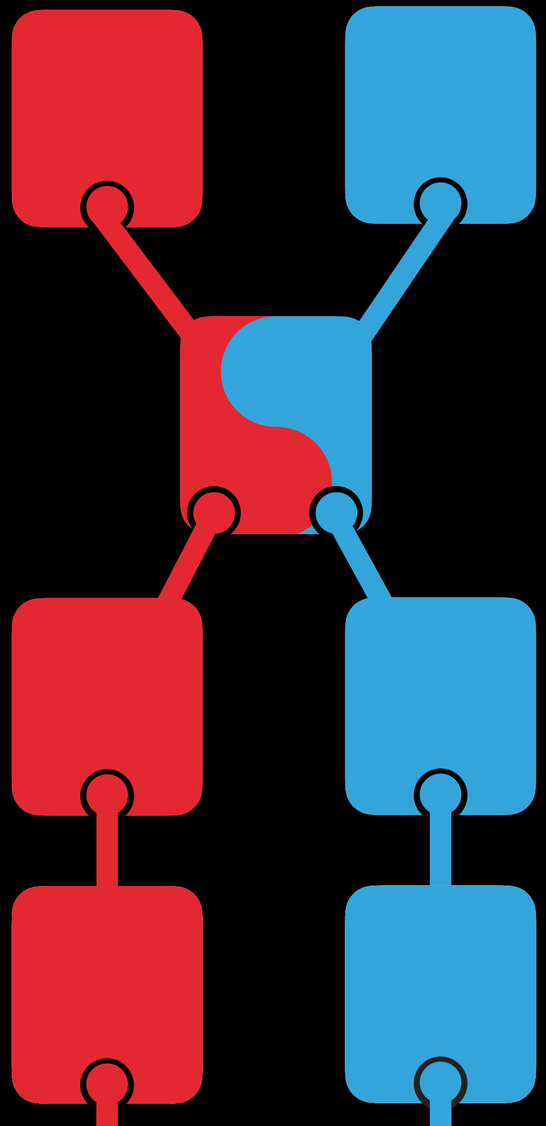
HETEROGENEOUS PAXOS



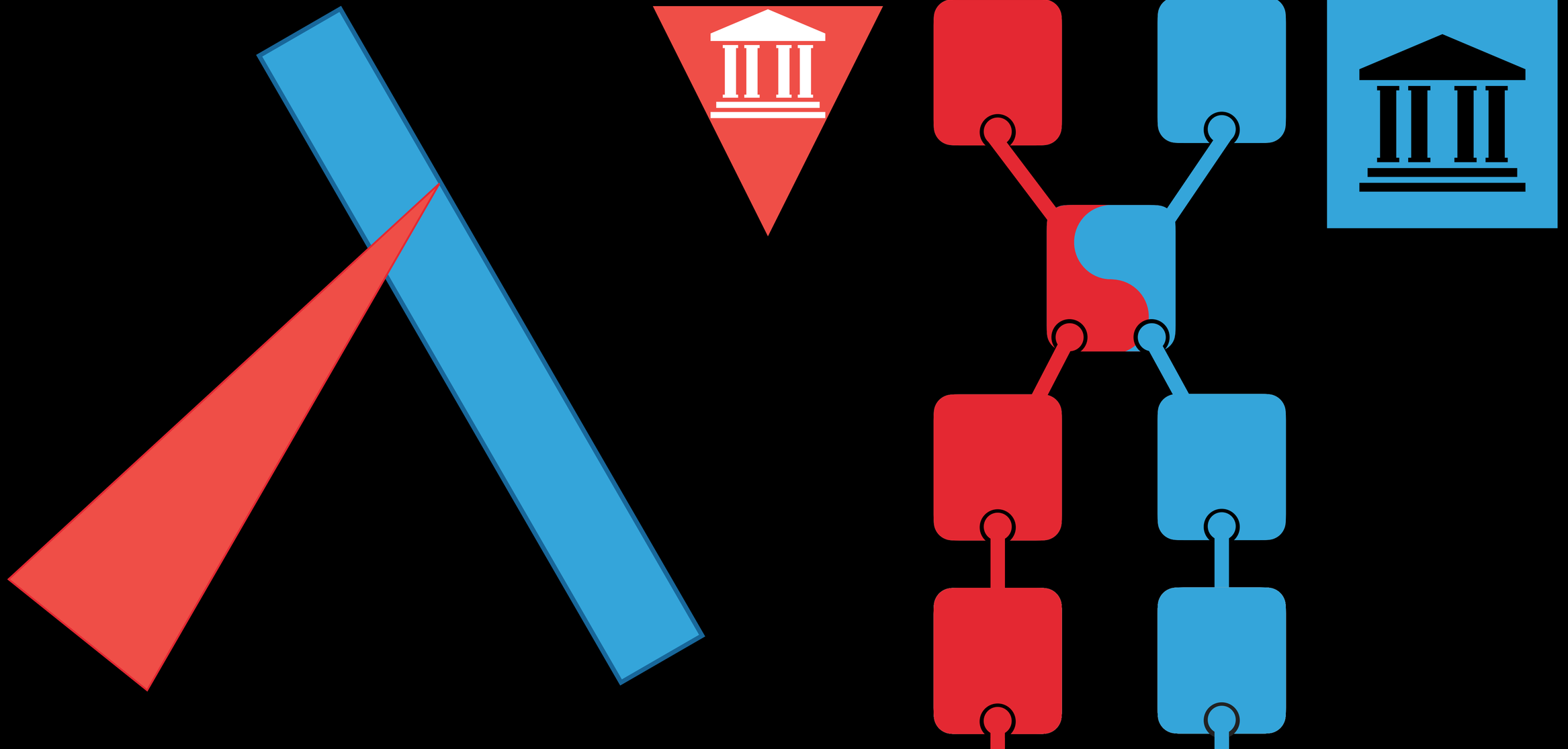


HETEROGENEOUS PAXOS

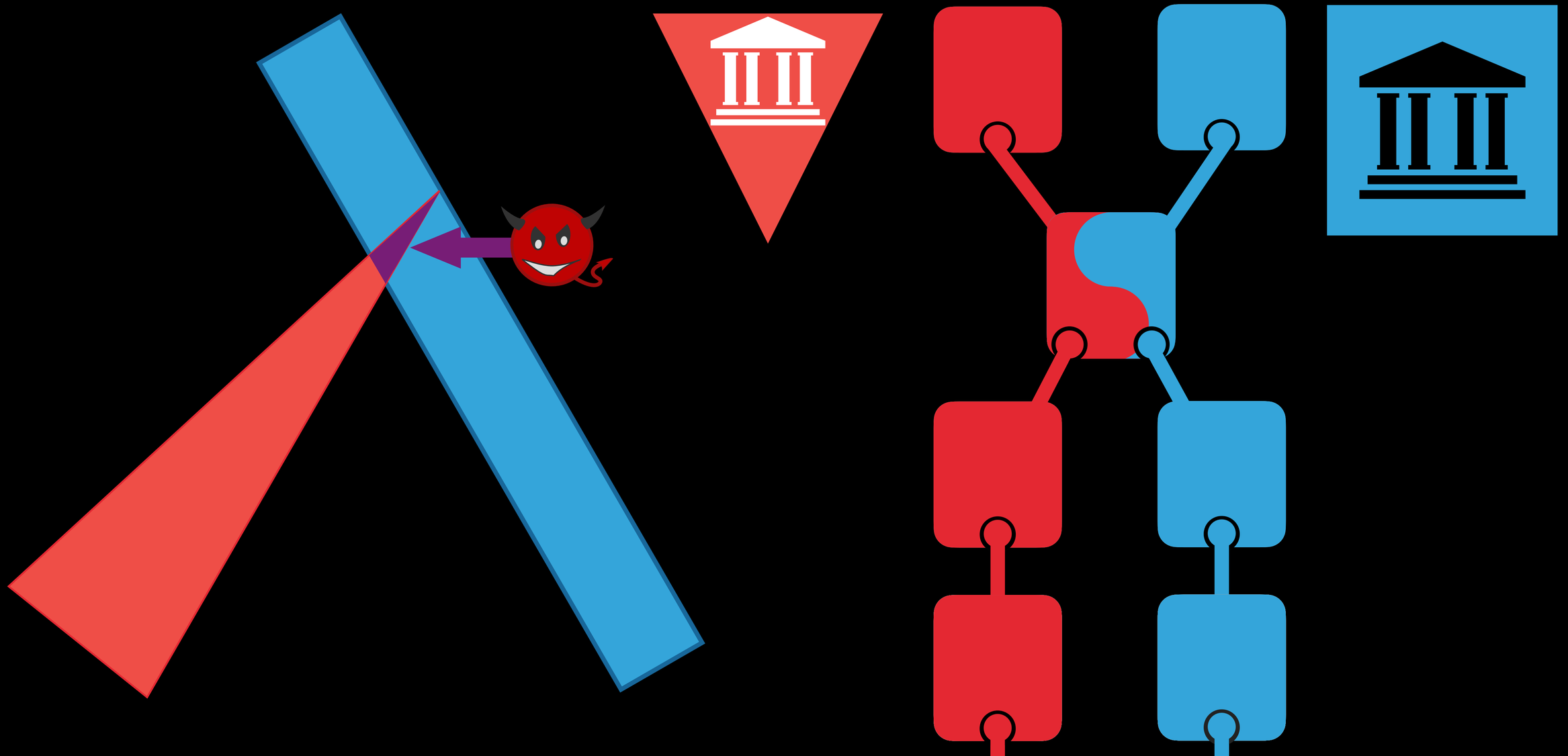




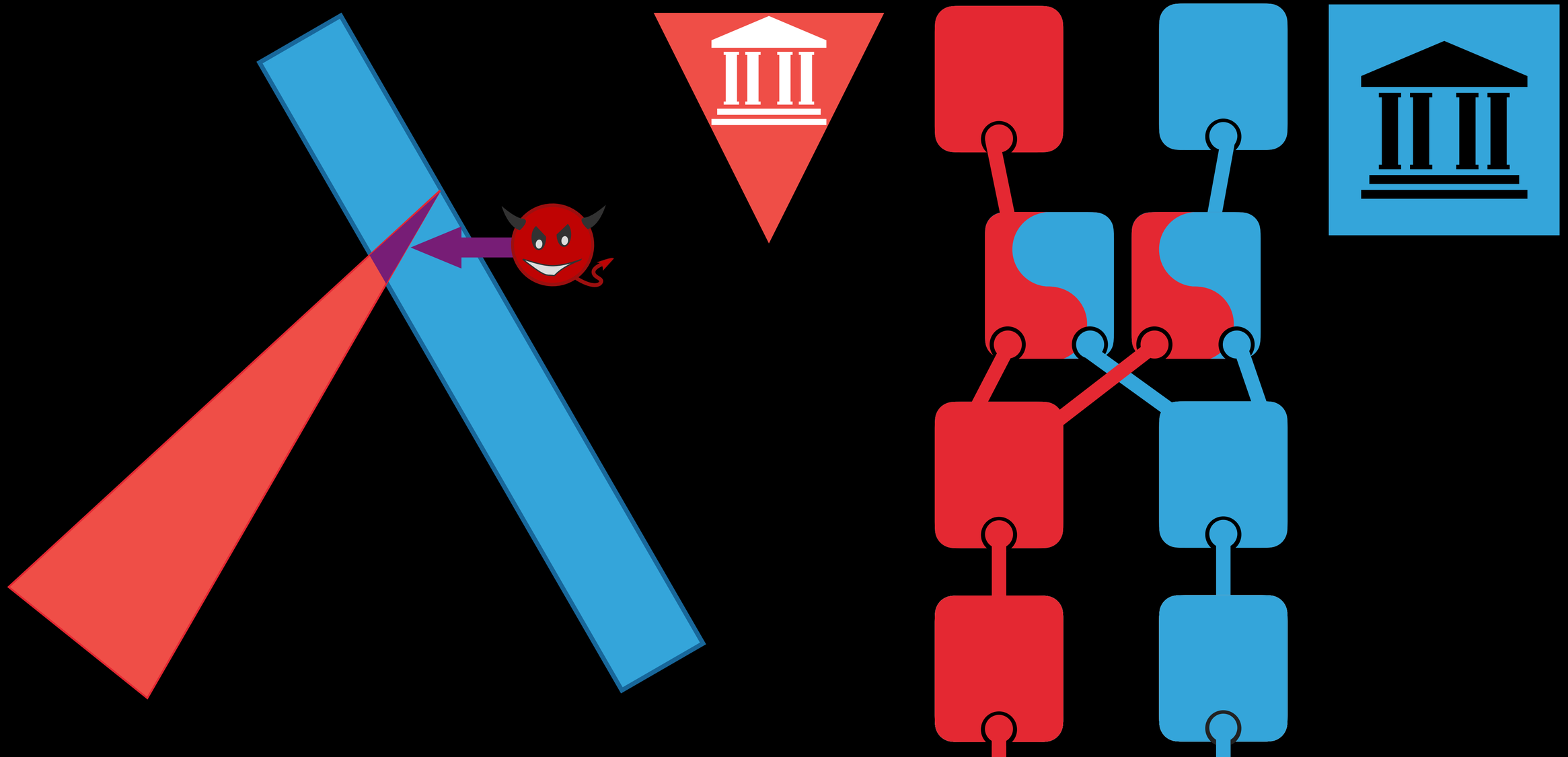
HETEROGENEOUS PAXOS



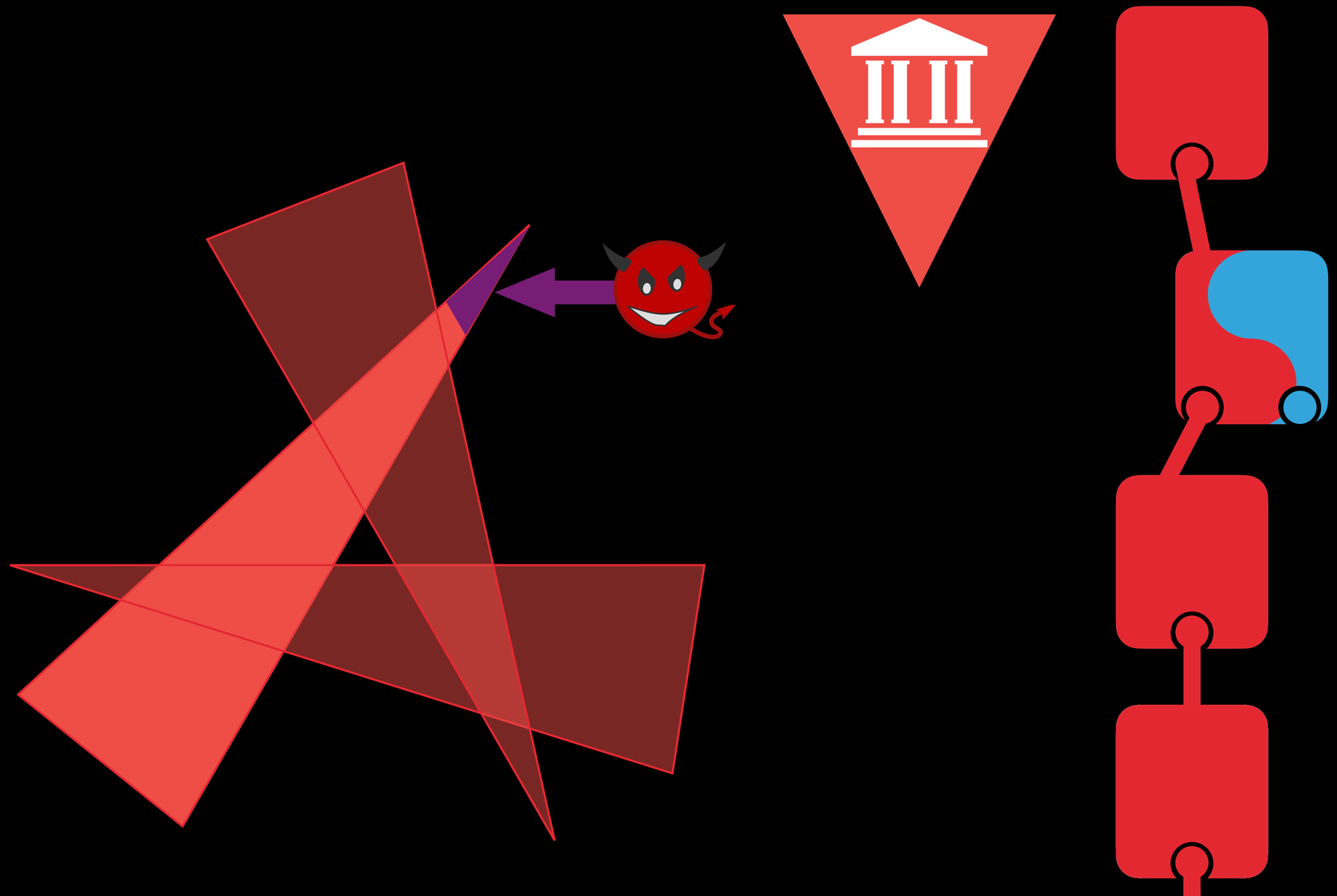
HETEROGENEOUS PAXOS



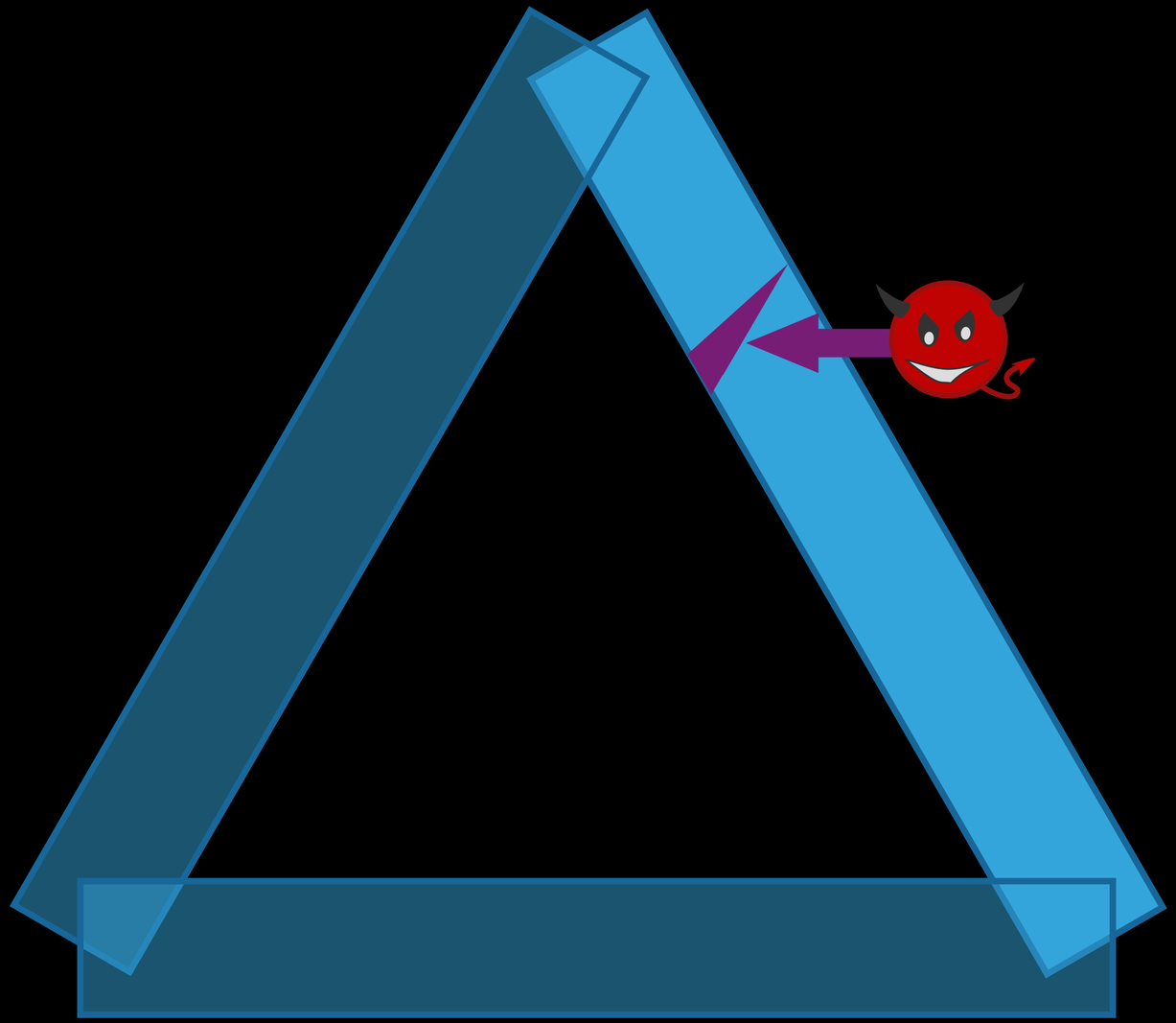
HETEROGENEOUS PAXOS

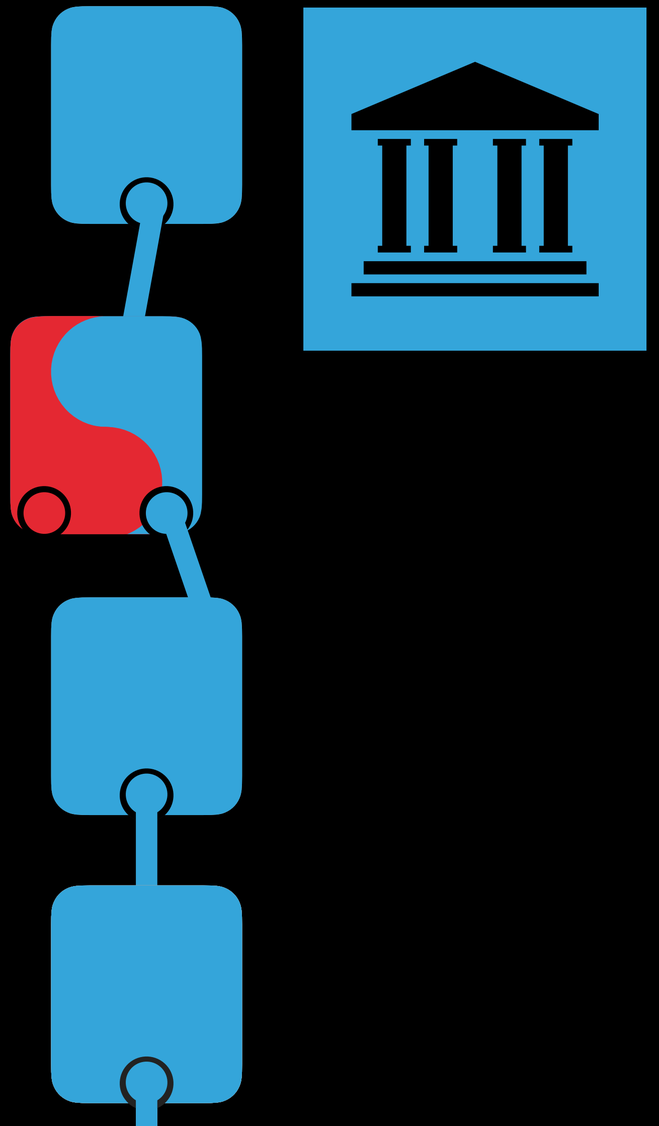


HETEROGENEOUS PAXOS

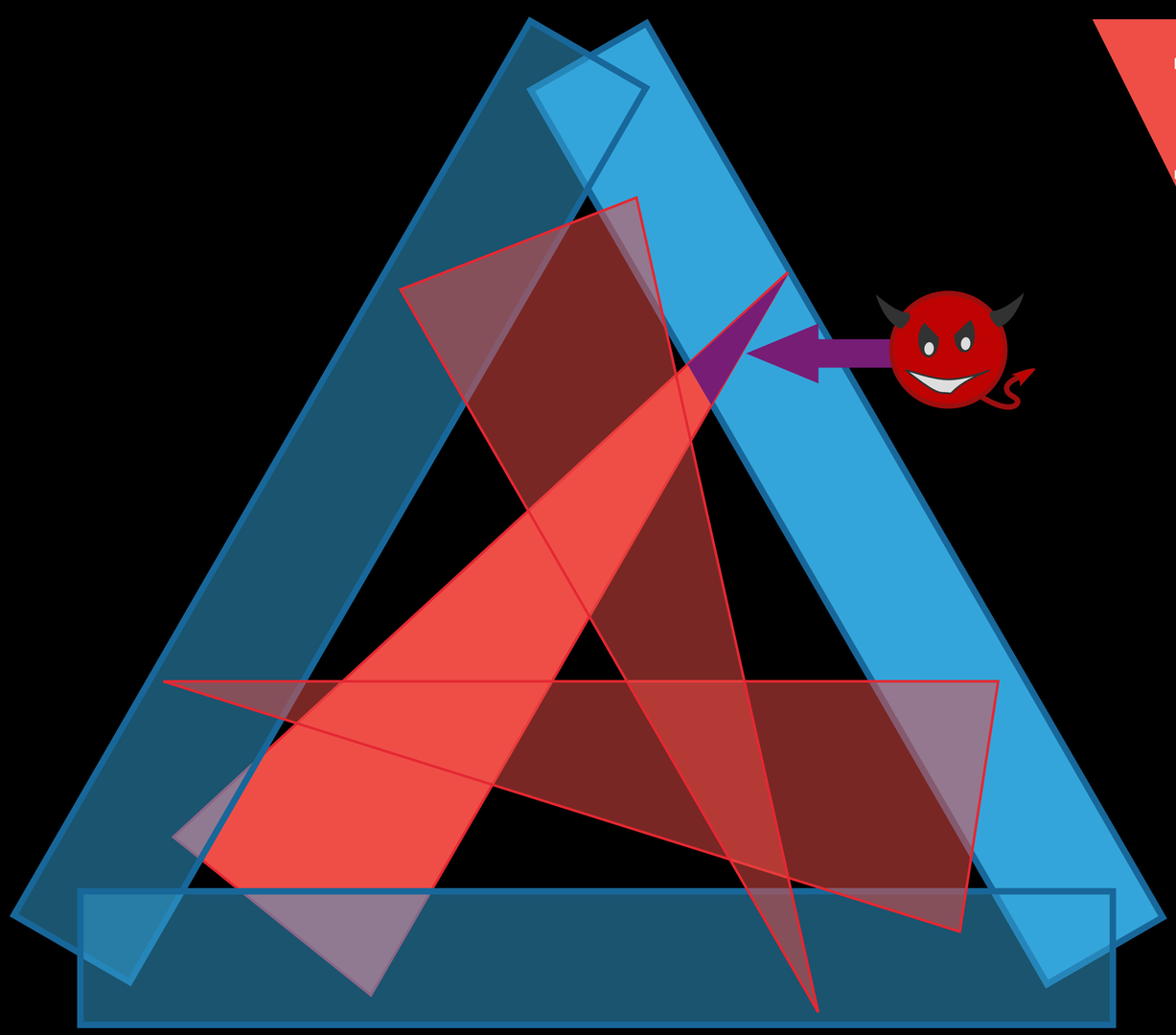


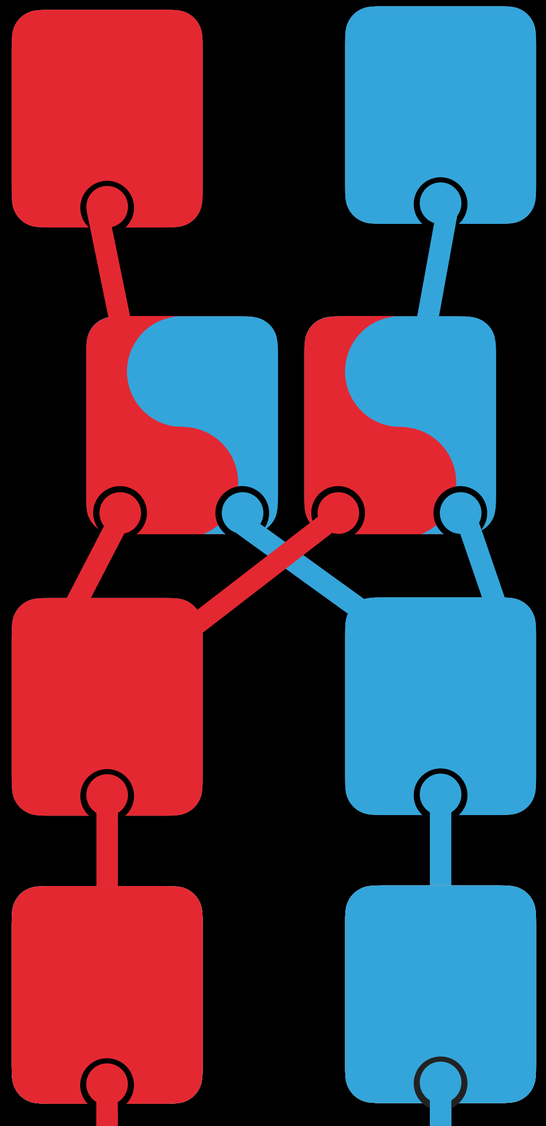
HETEROGENEOUS PAXOS



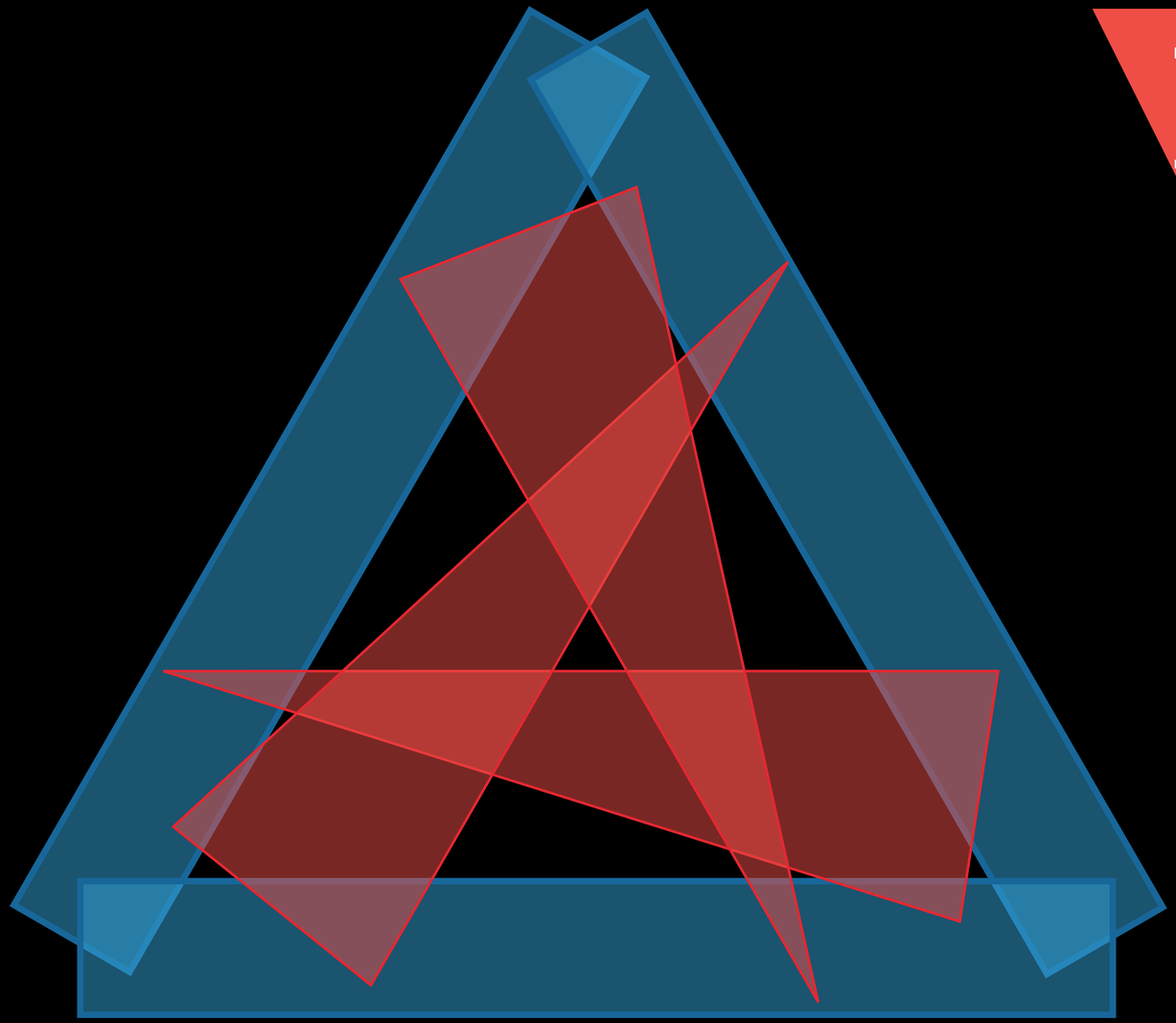


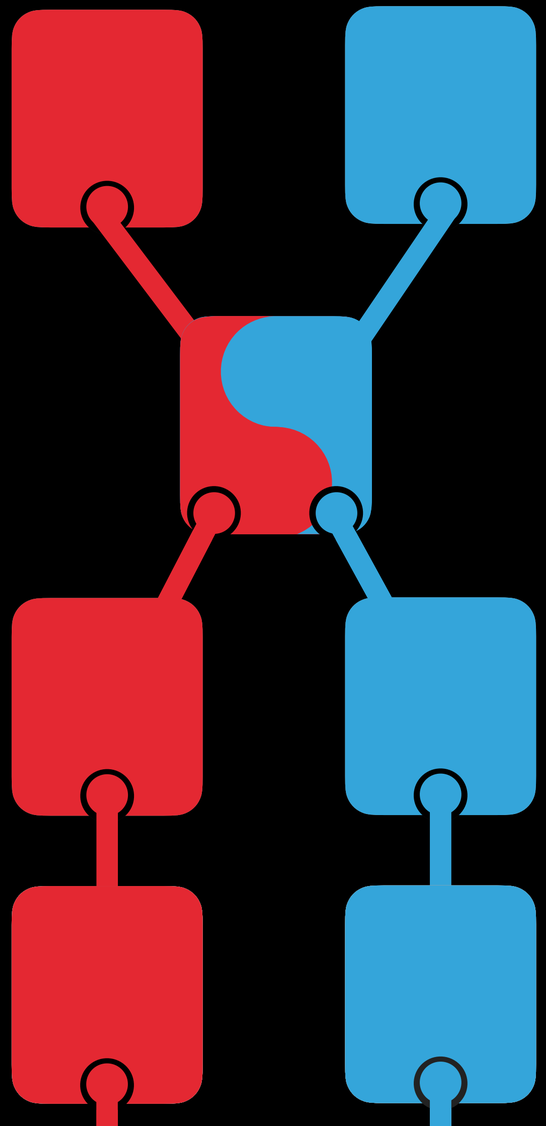
HETEROGENEOUS PAXOS



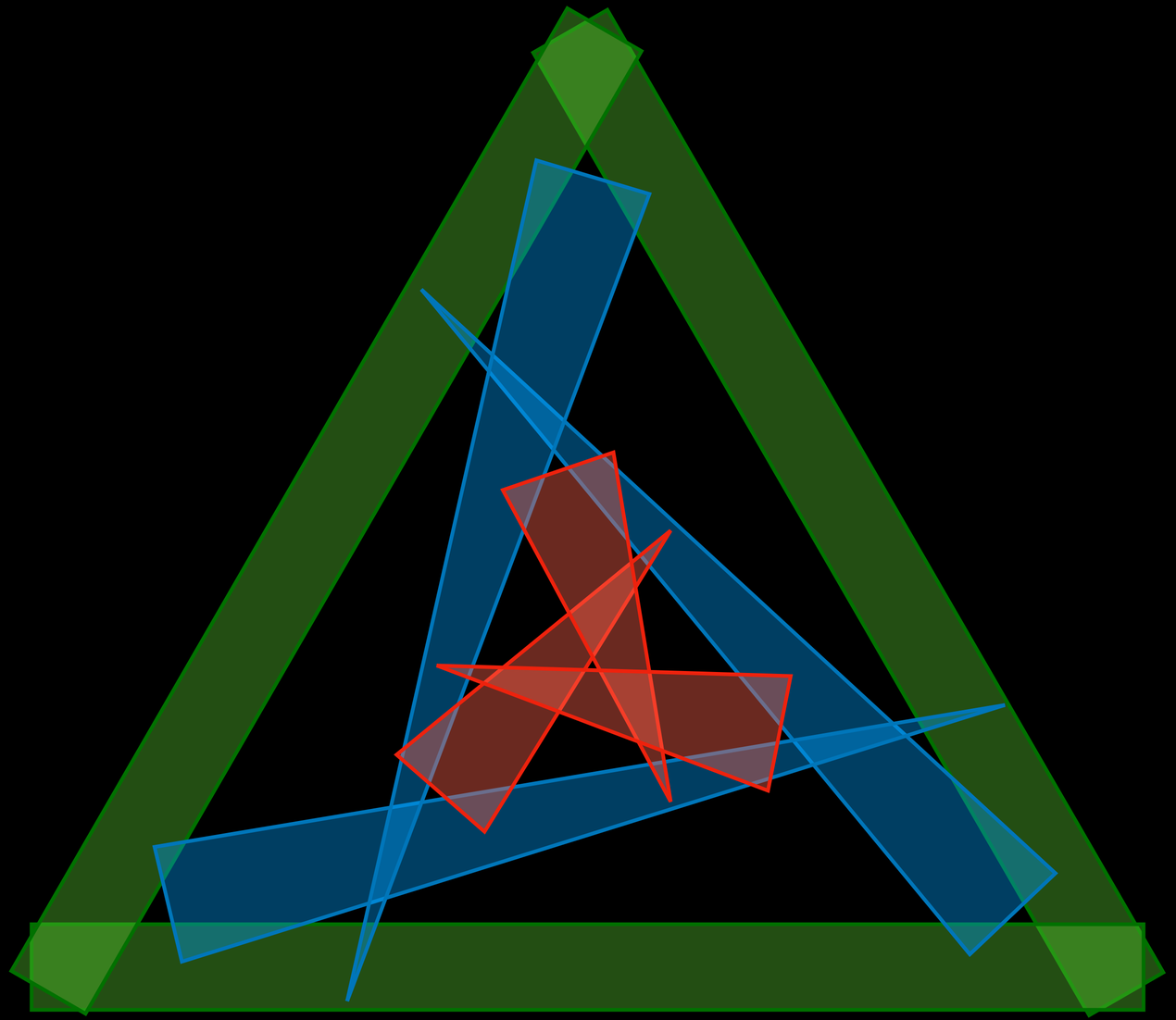


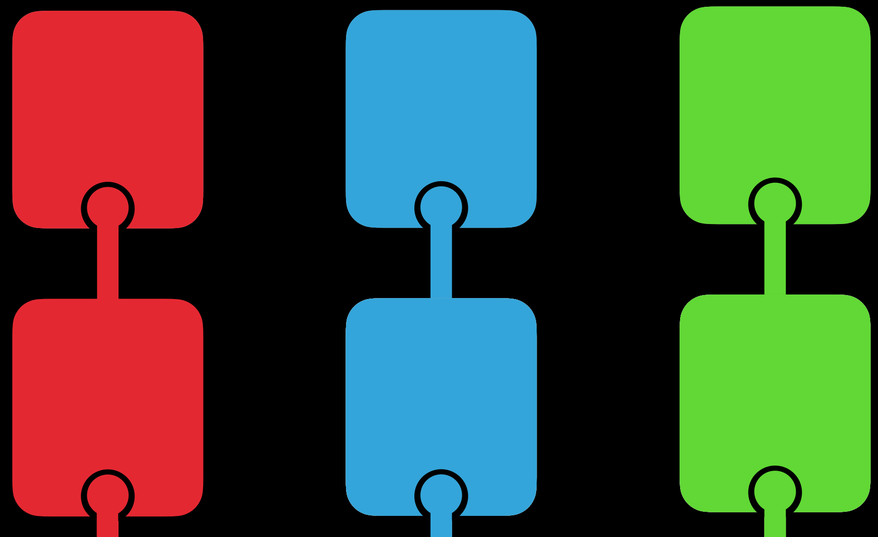
HETEROGENEOUS PAXOS



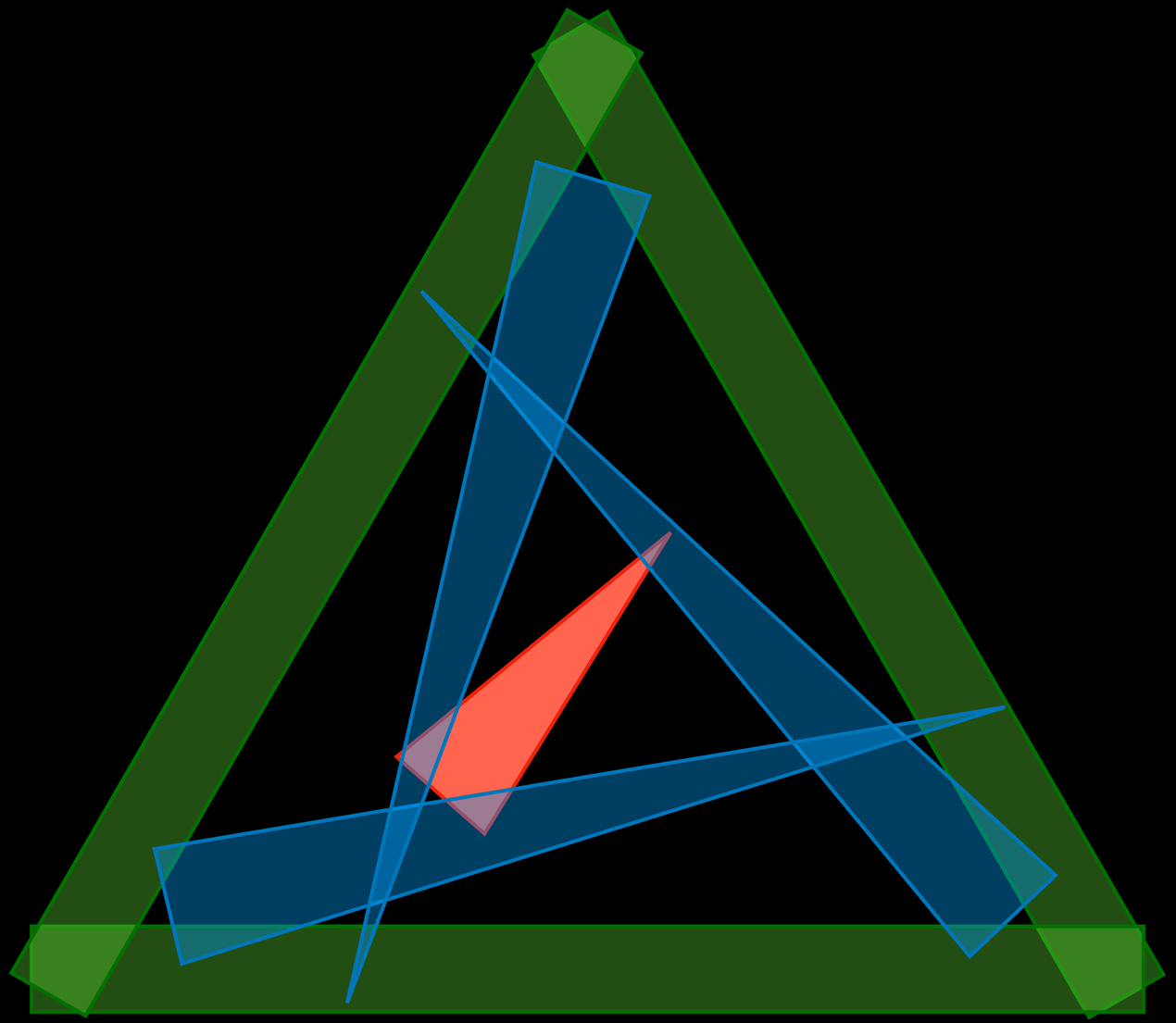


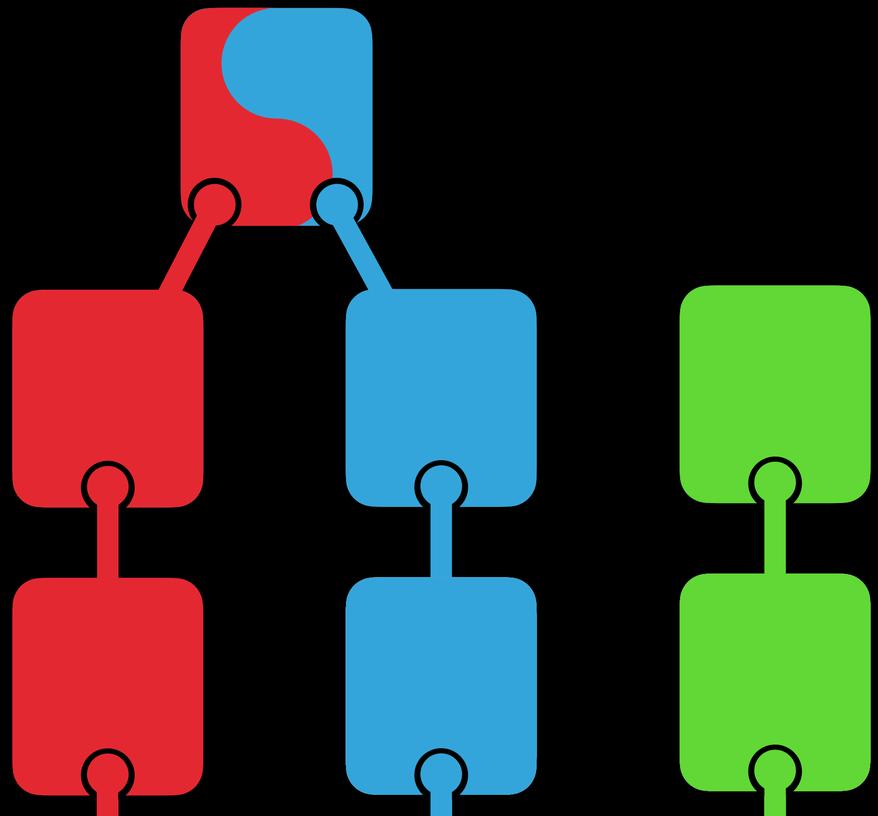
WHICH CONSENSUS WHEN?



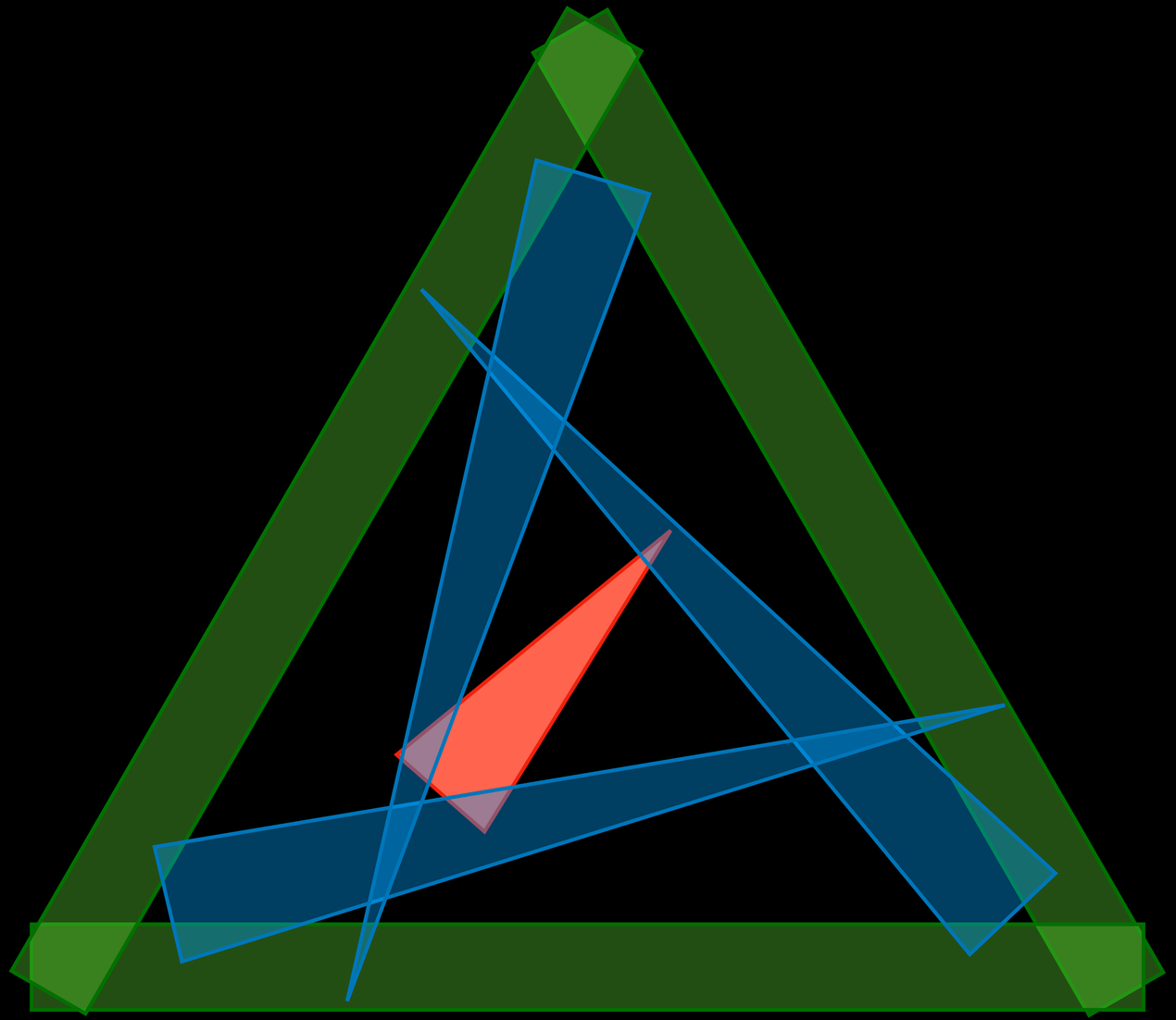


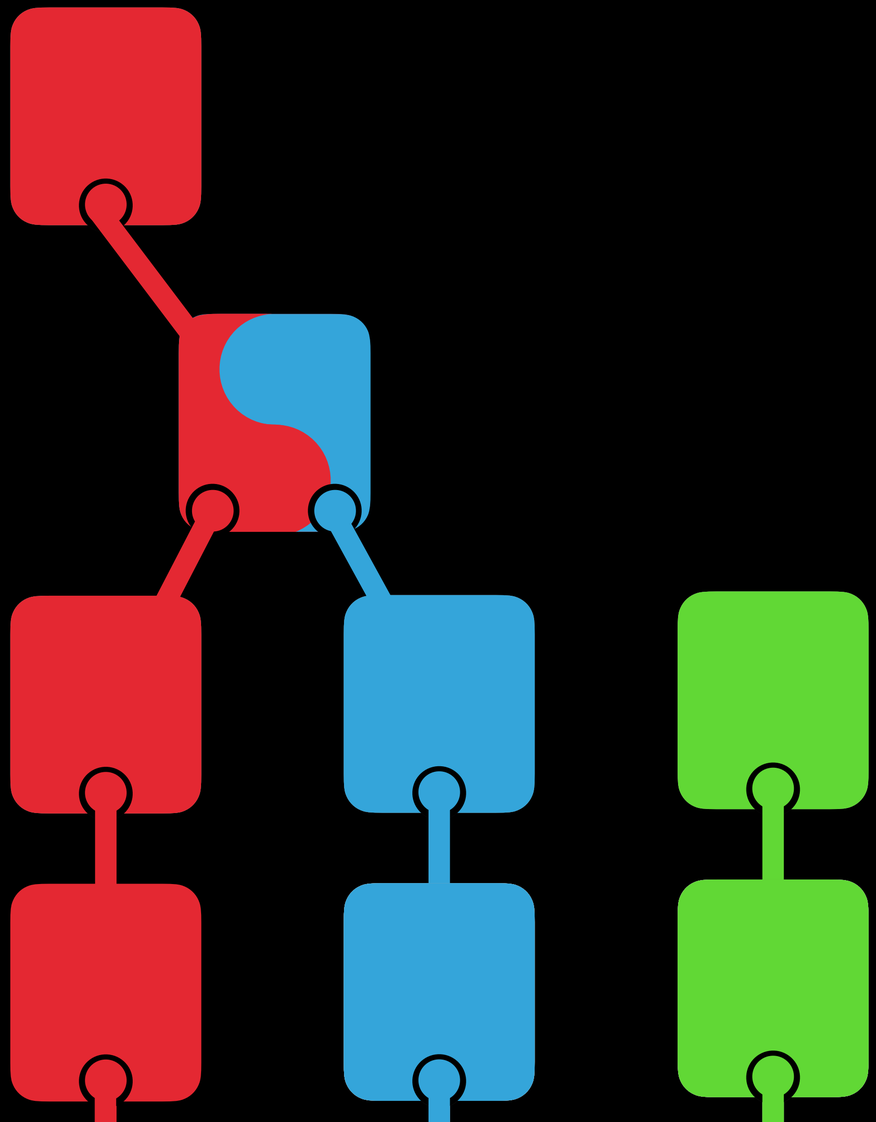
WHICH CONSENSUS WHEN?



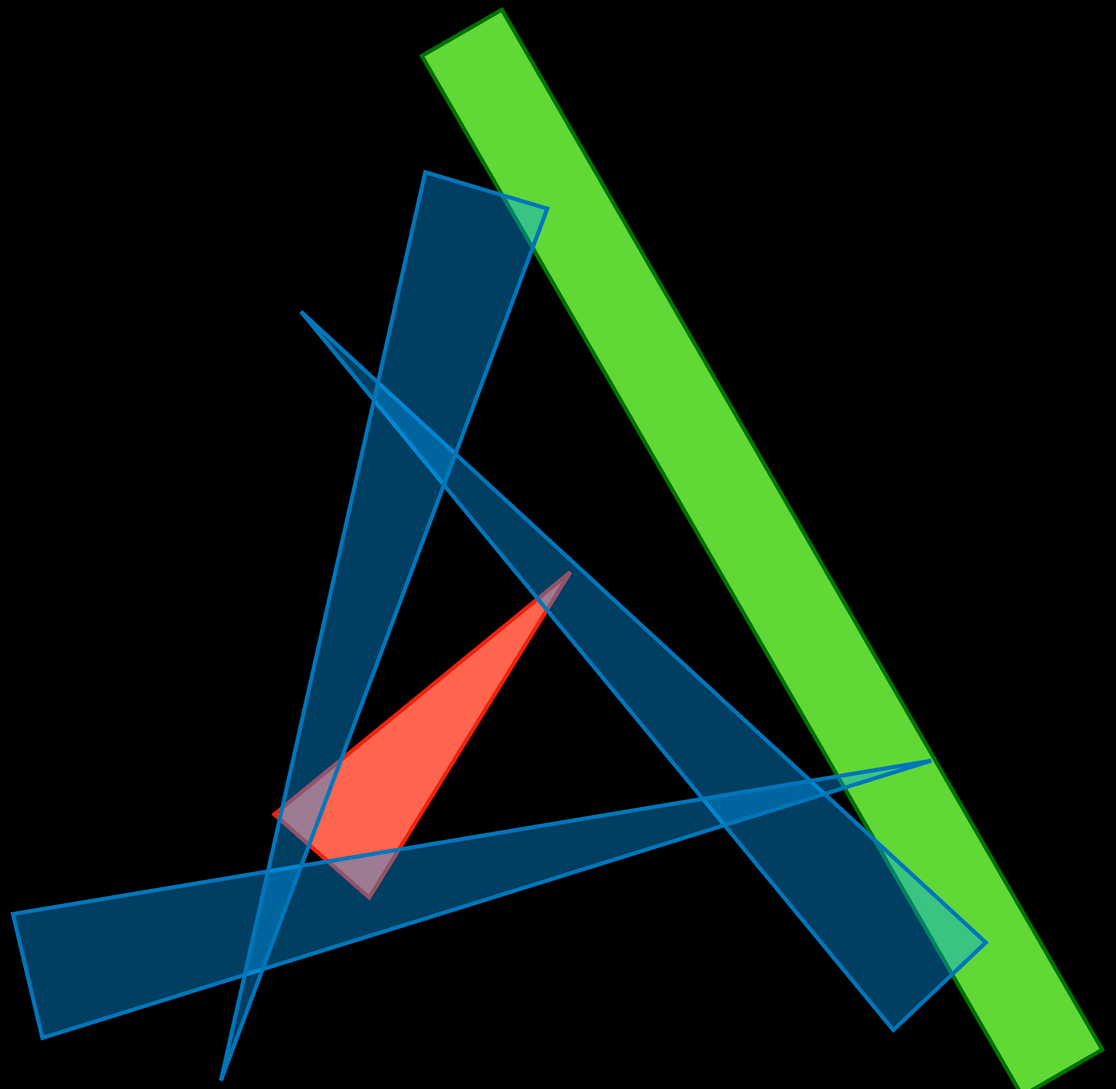


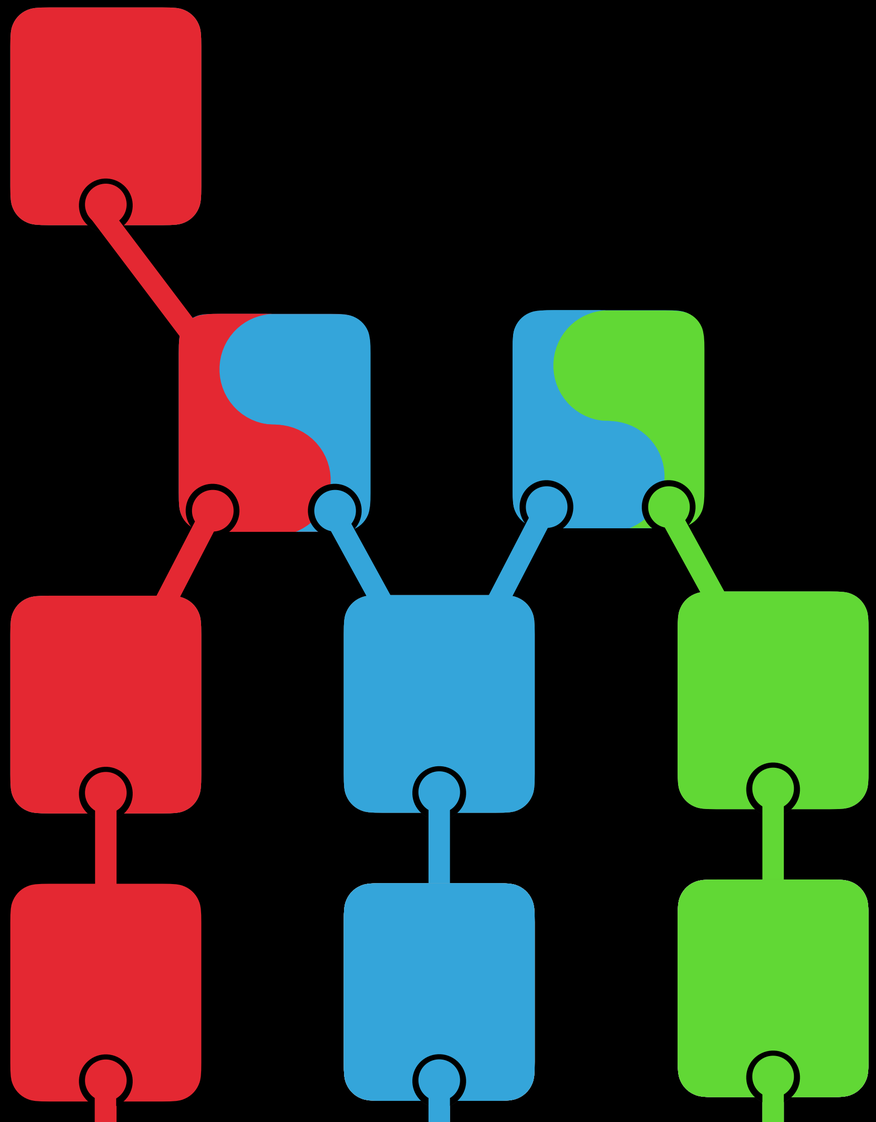
WHICH CONSENSUS WHEN?



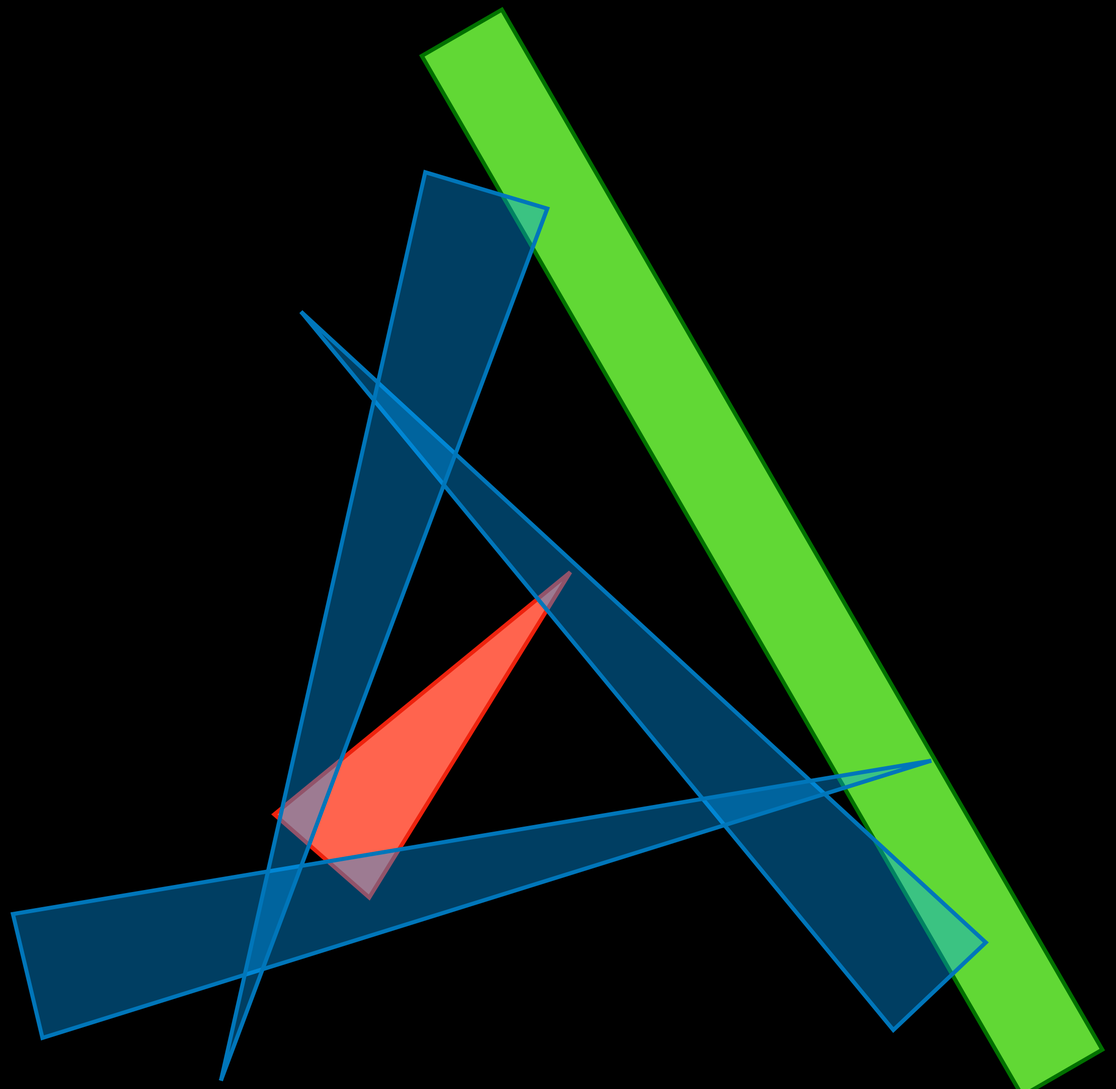


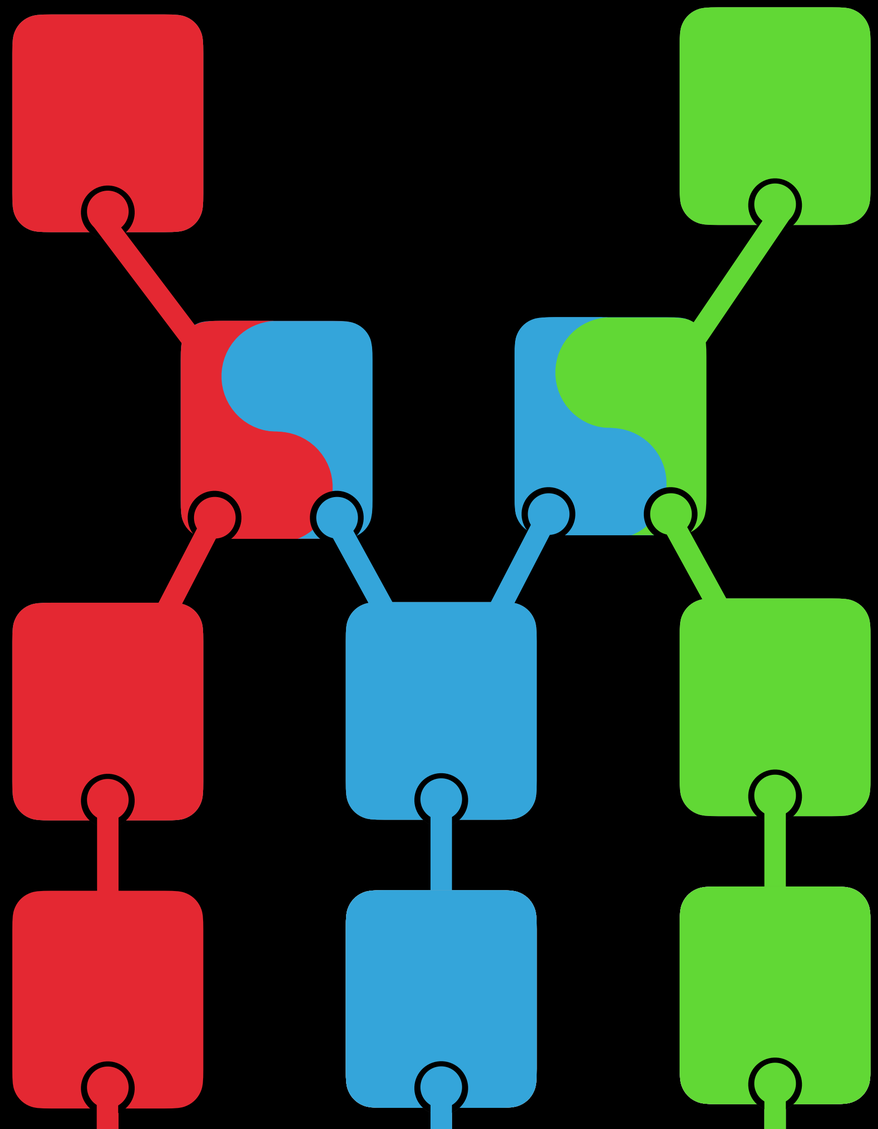
WHICH CONSENSUS WHEN?



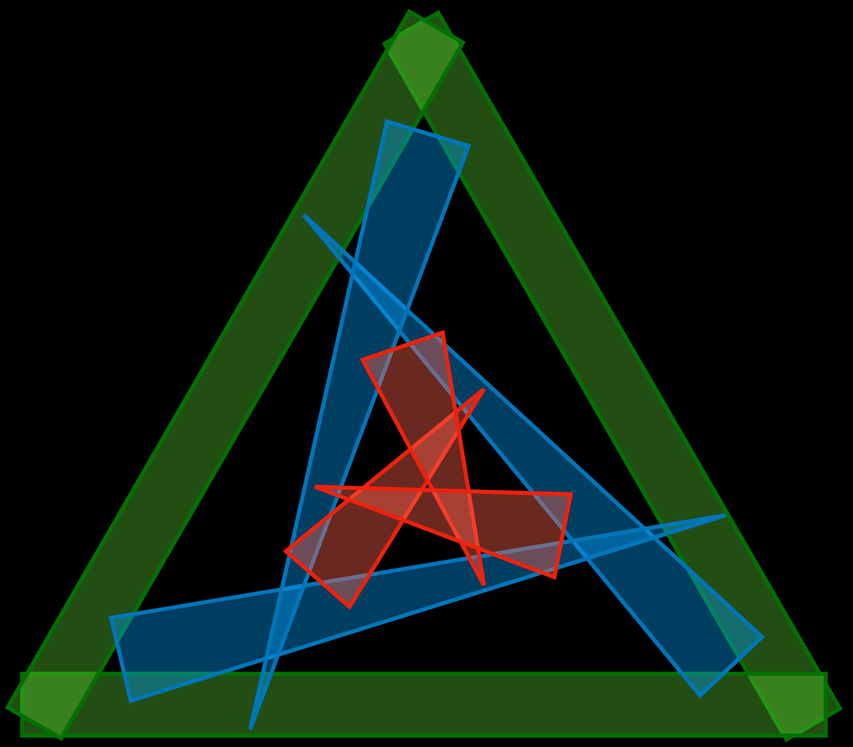


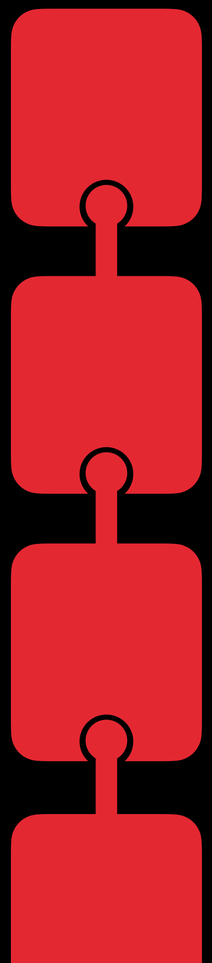
WHICH CONSENSUS WHEN?

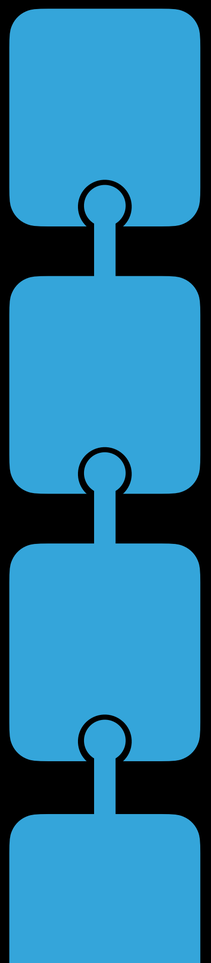


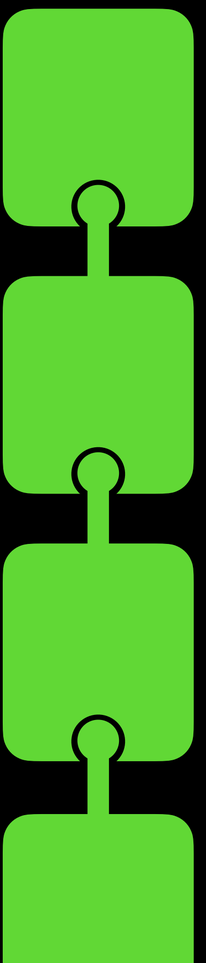


CHIMERA CHAINS



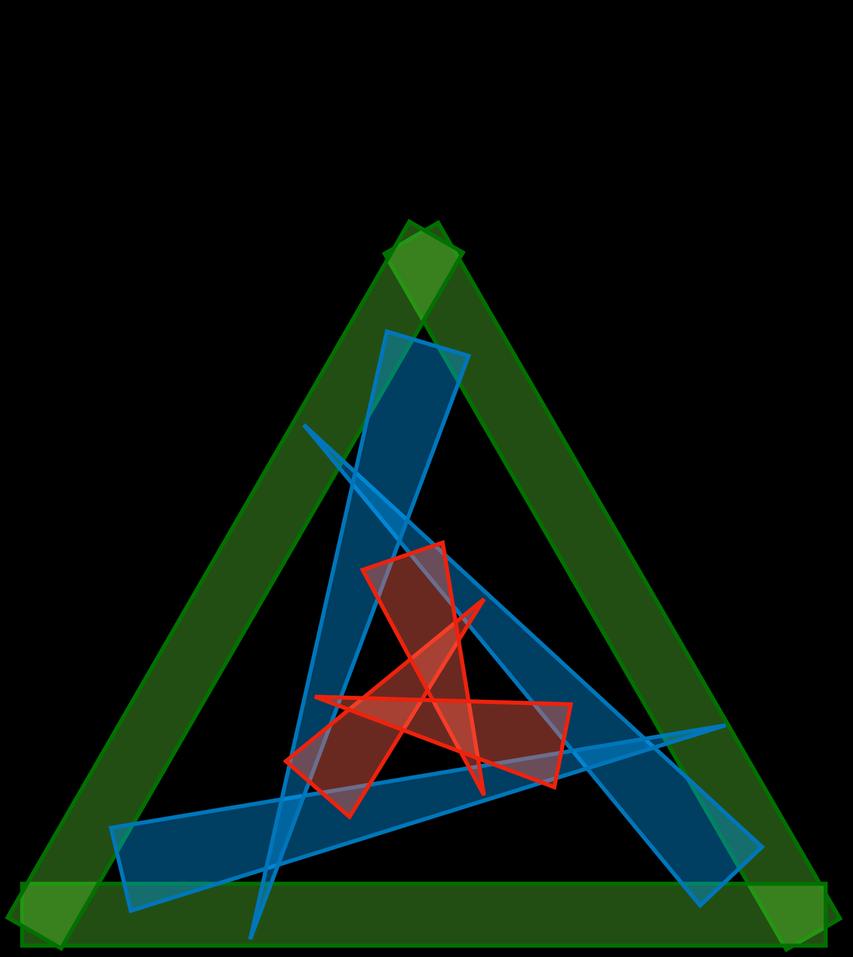


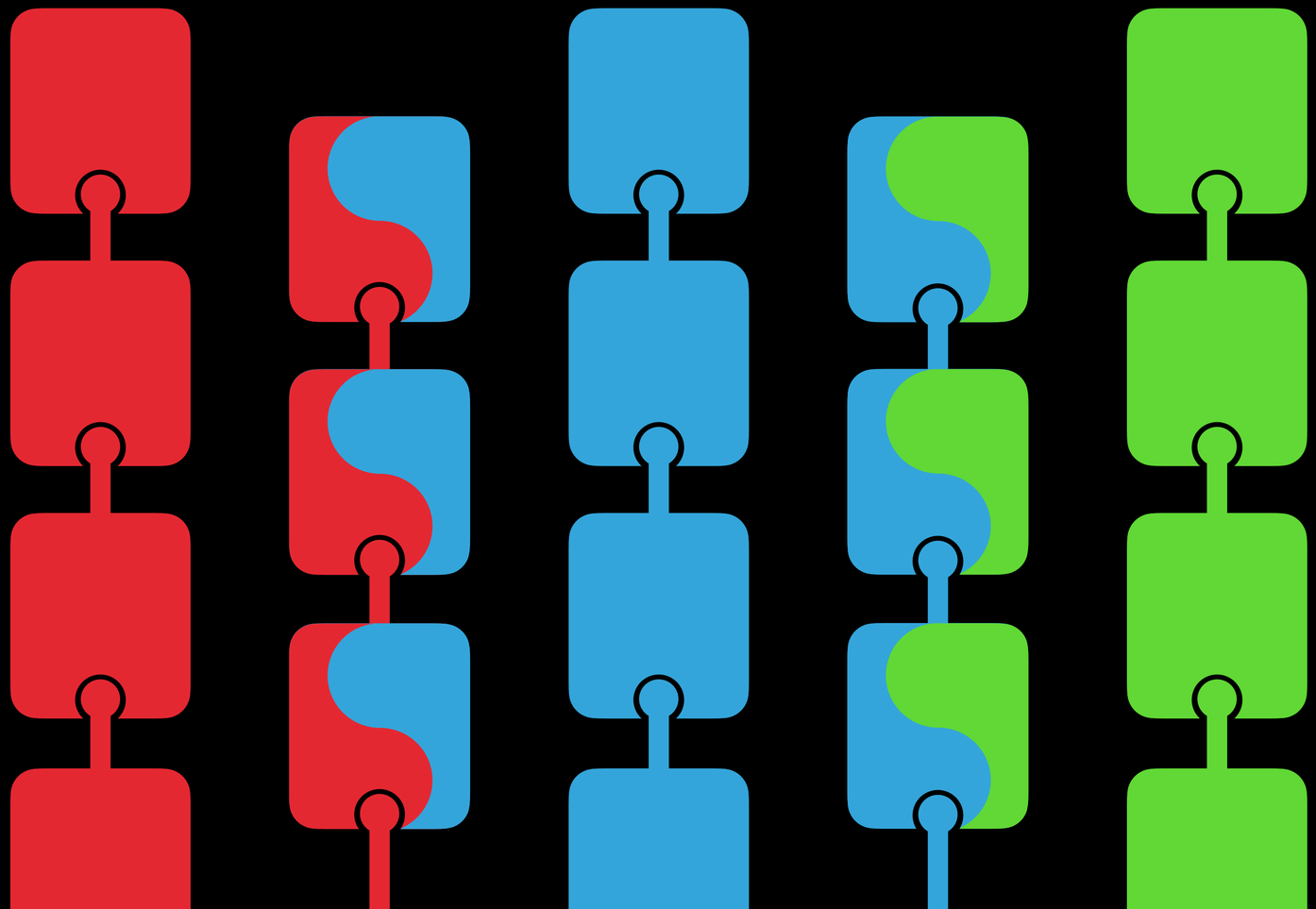




CHIMERA CHAINS

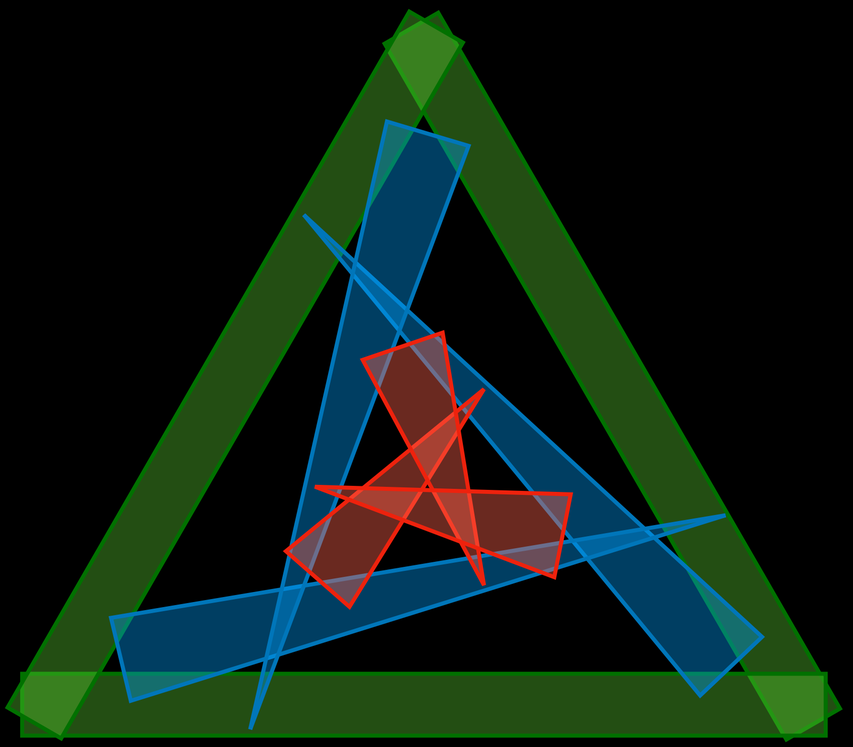
- A chain for each possible consensus

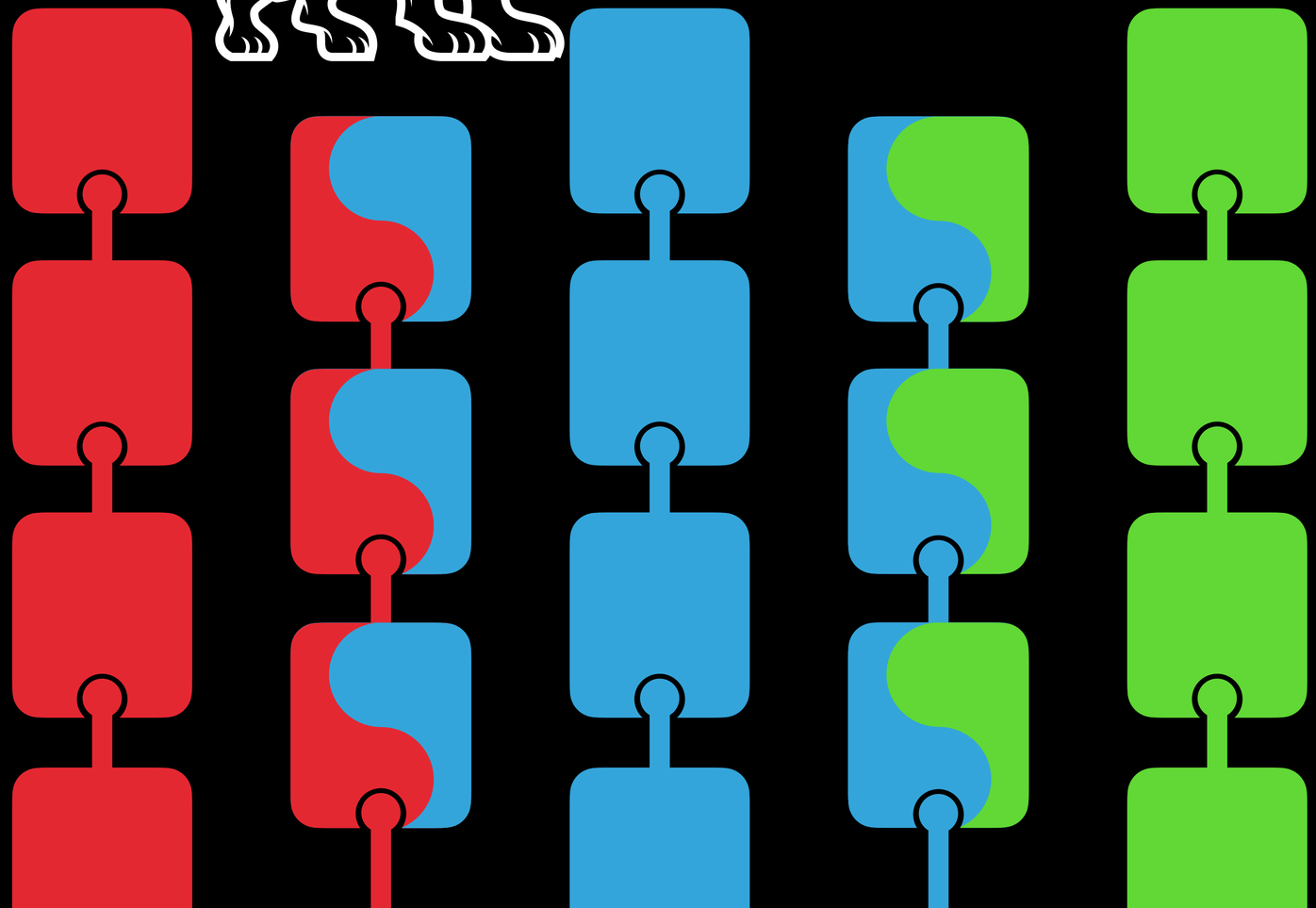




CHIMERA CHAINS

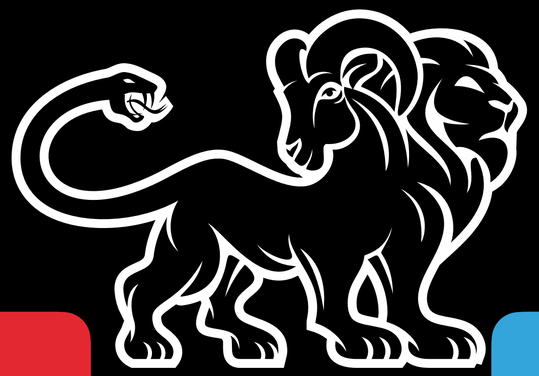
- A chain for each possible consensus

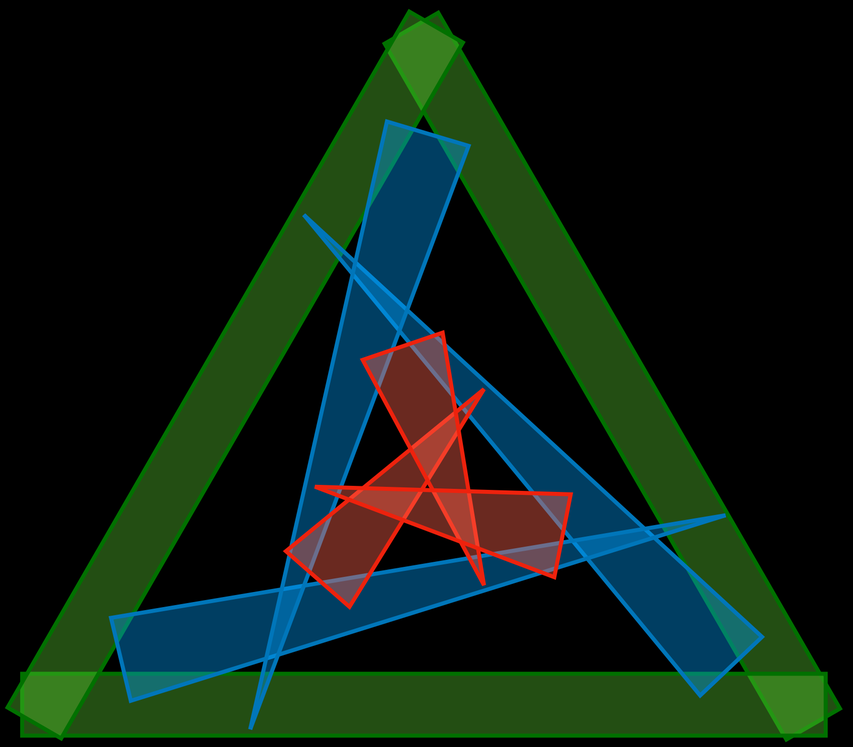


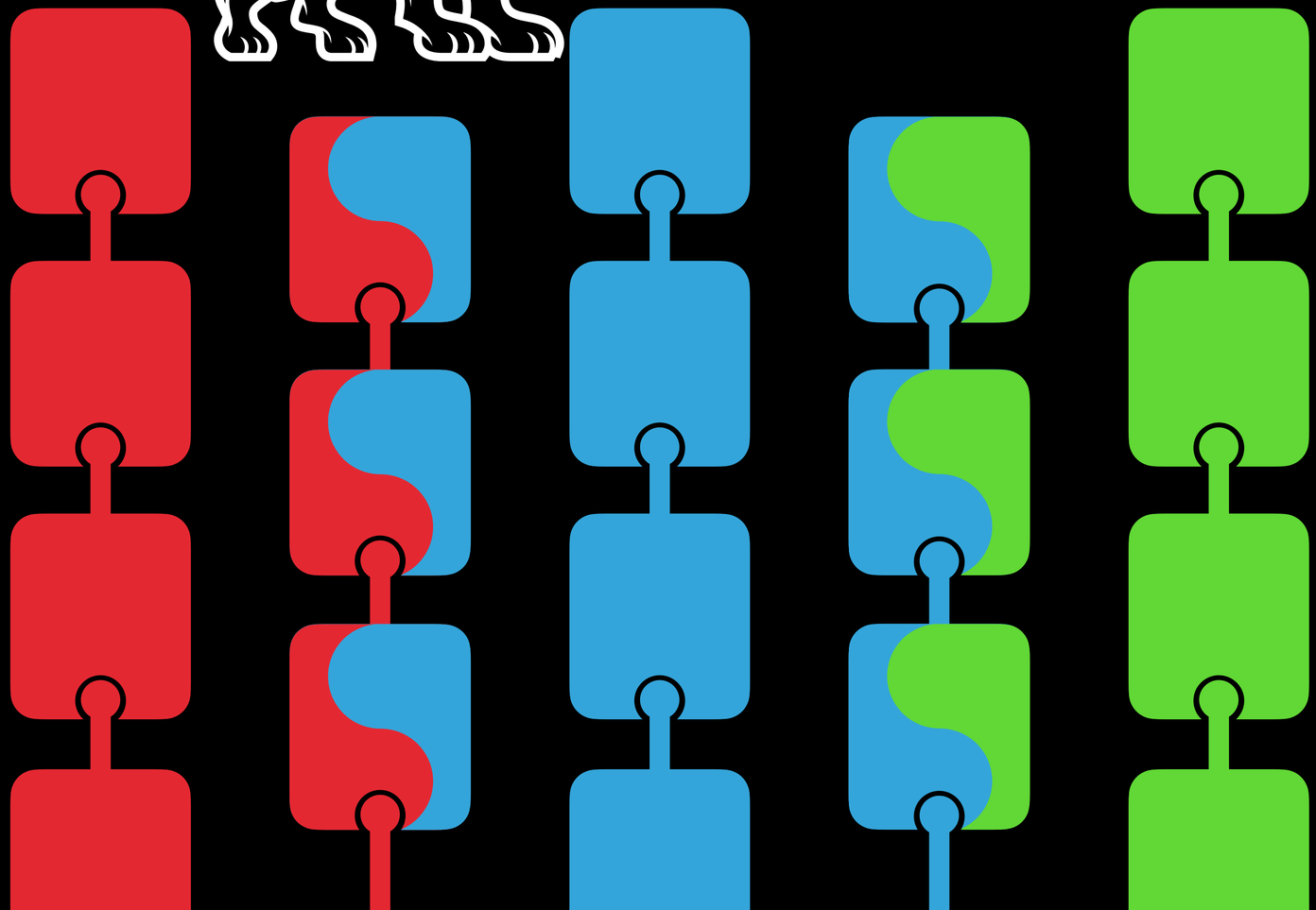


CHIMERA CHAINS

- A chain for each possible consensus

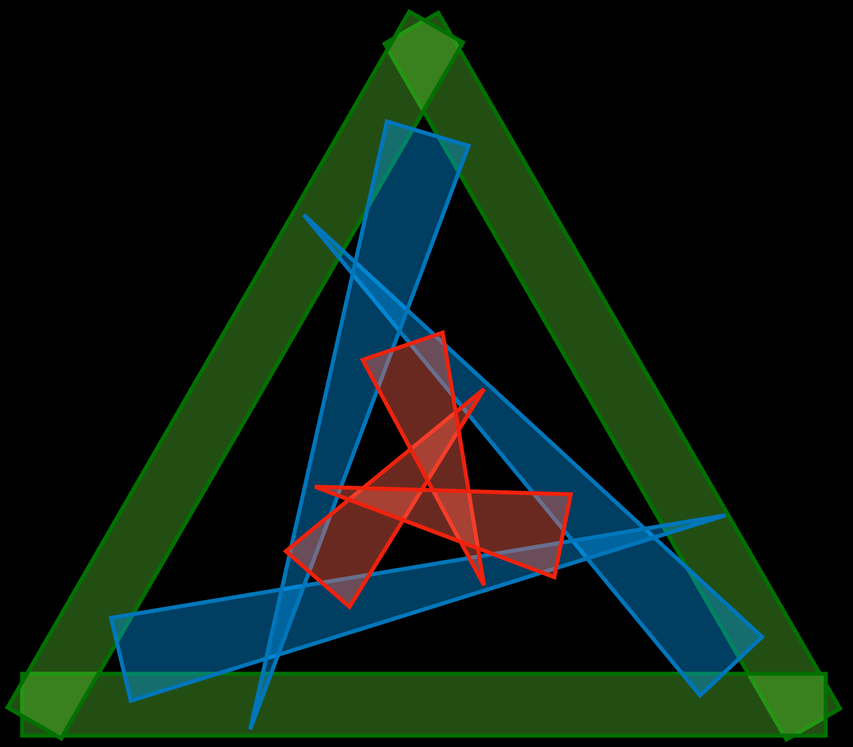


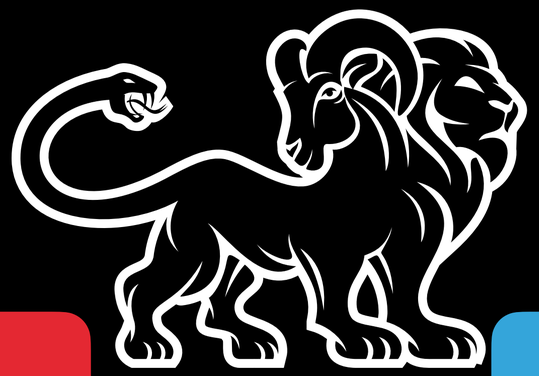


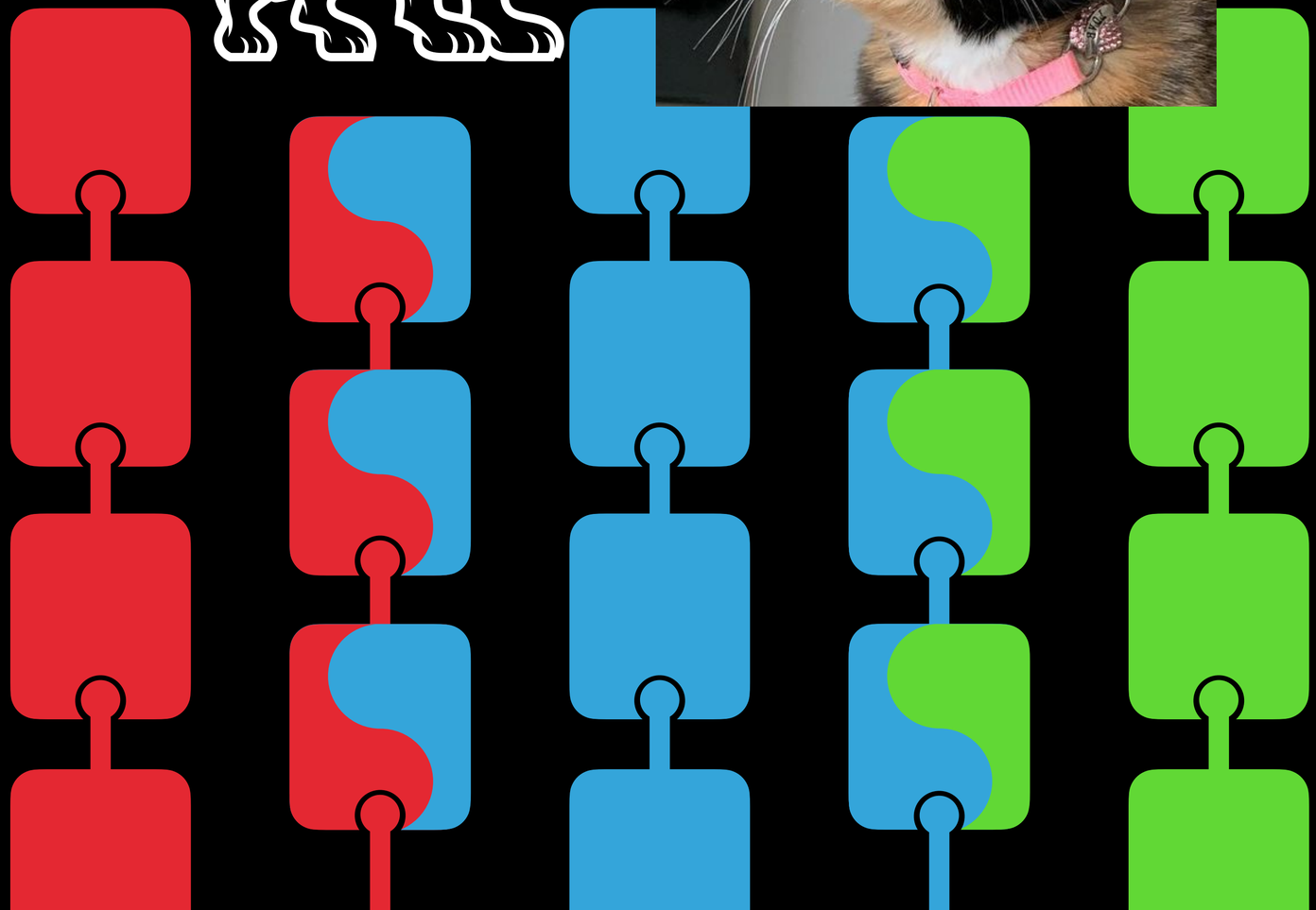


CHIMERA CHAINS

- A chain for each possible consensus

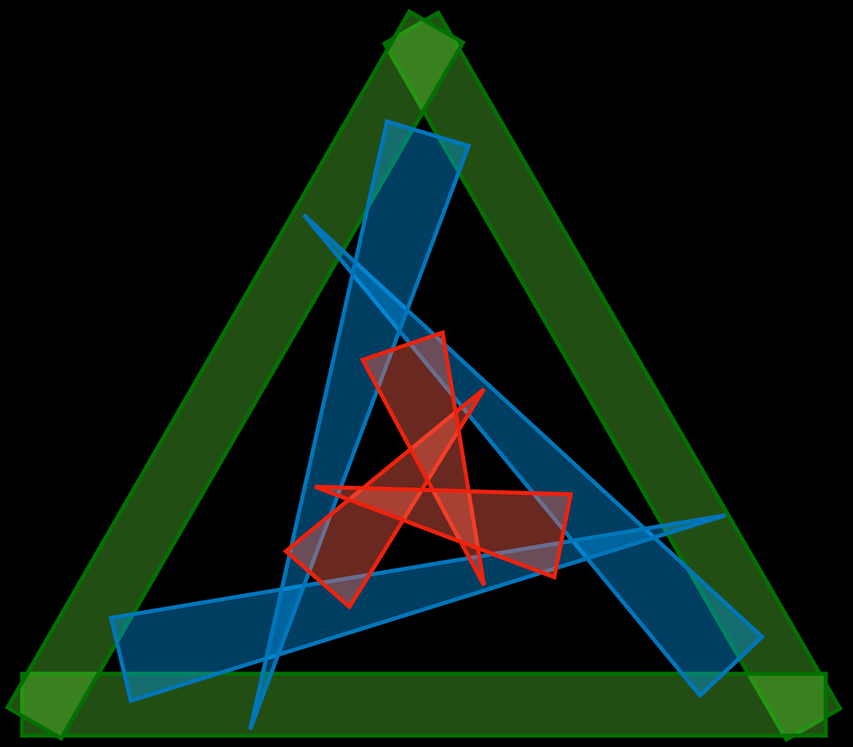


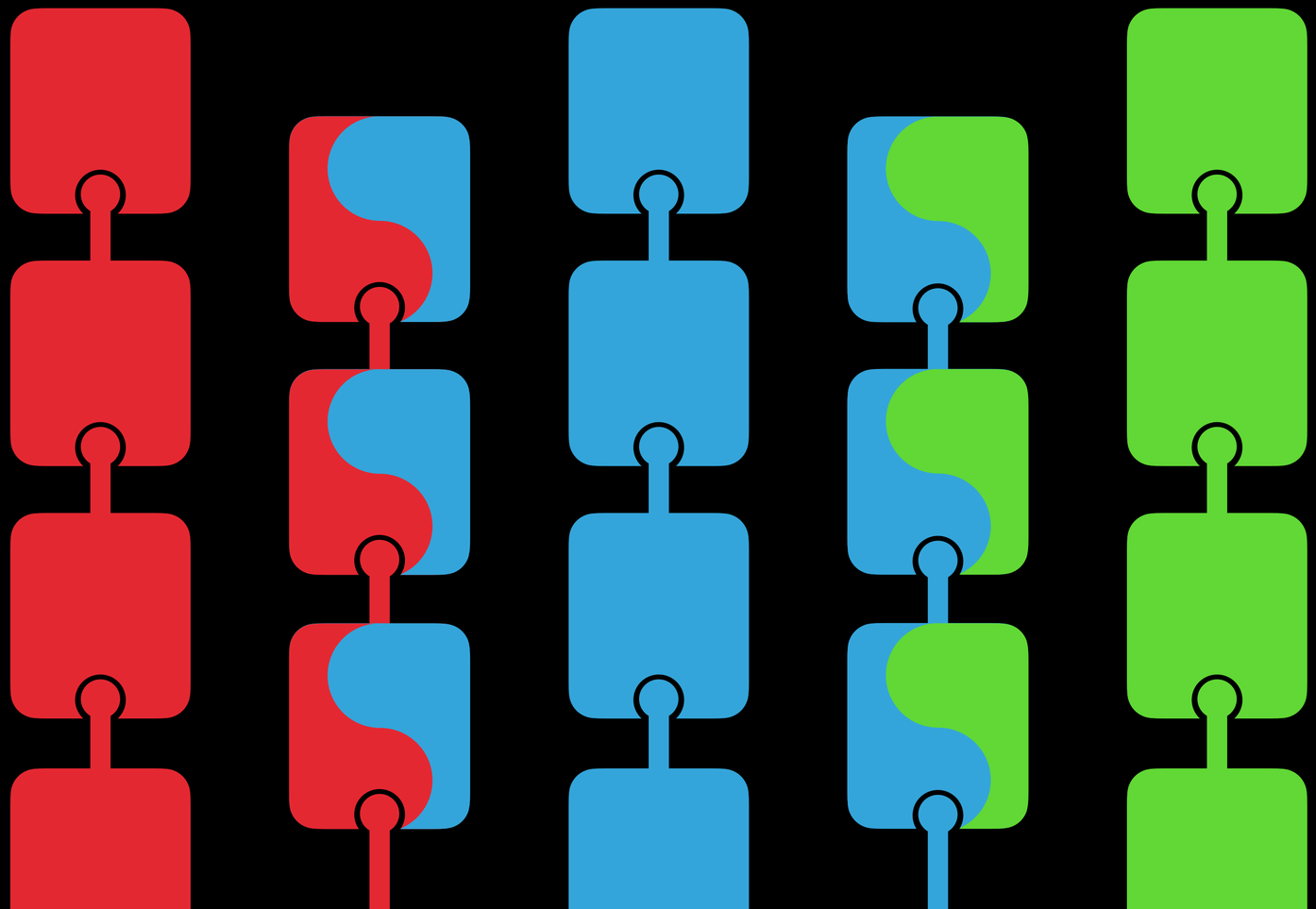




CHIMERA CHAINS

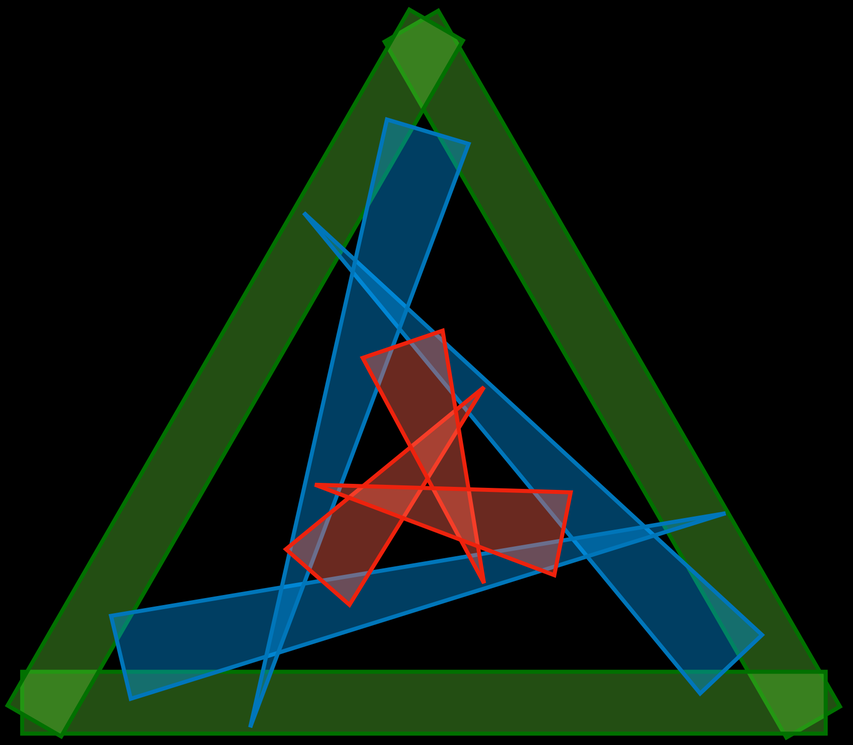
- A chain for each possible consensus
  - On-demand

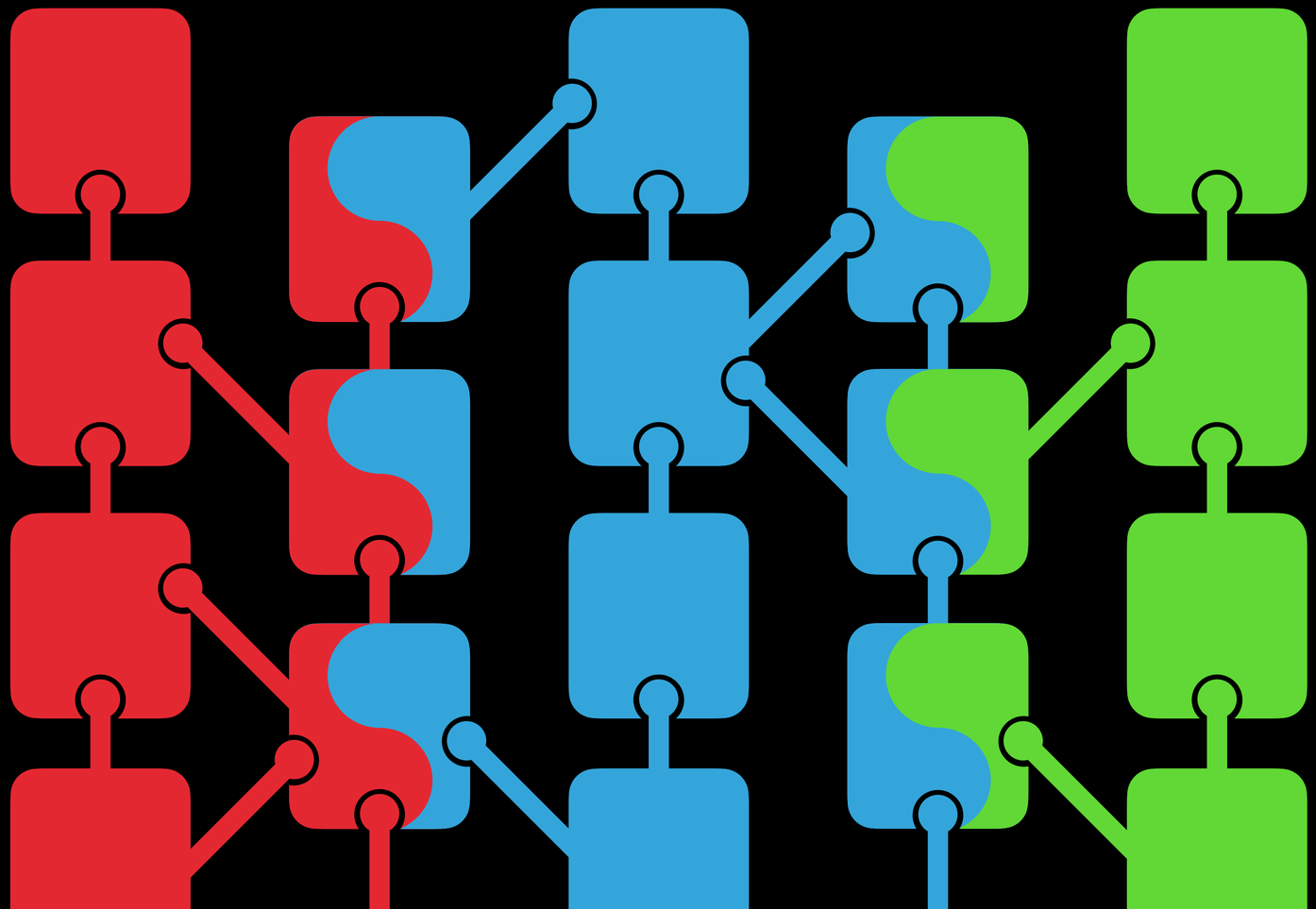




CHIMERA CHAINS

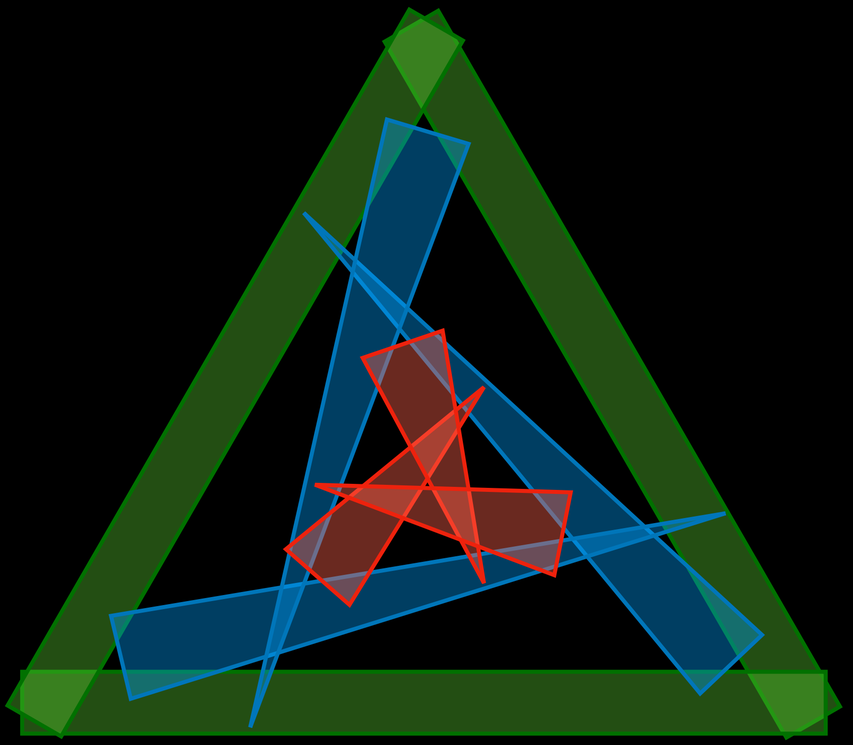
- A chain for each possible consensus
  - On-demand
- Inter-Chain Communication

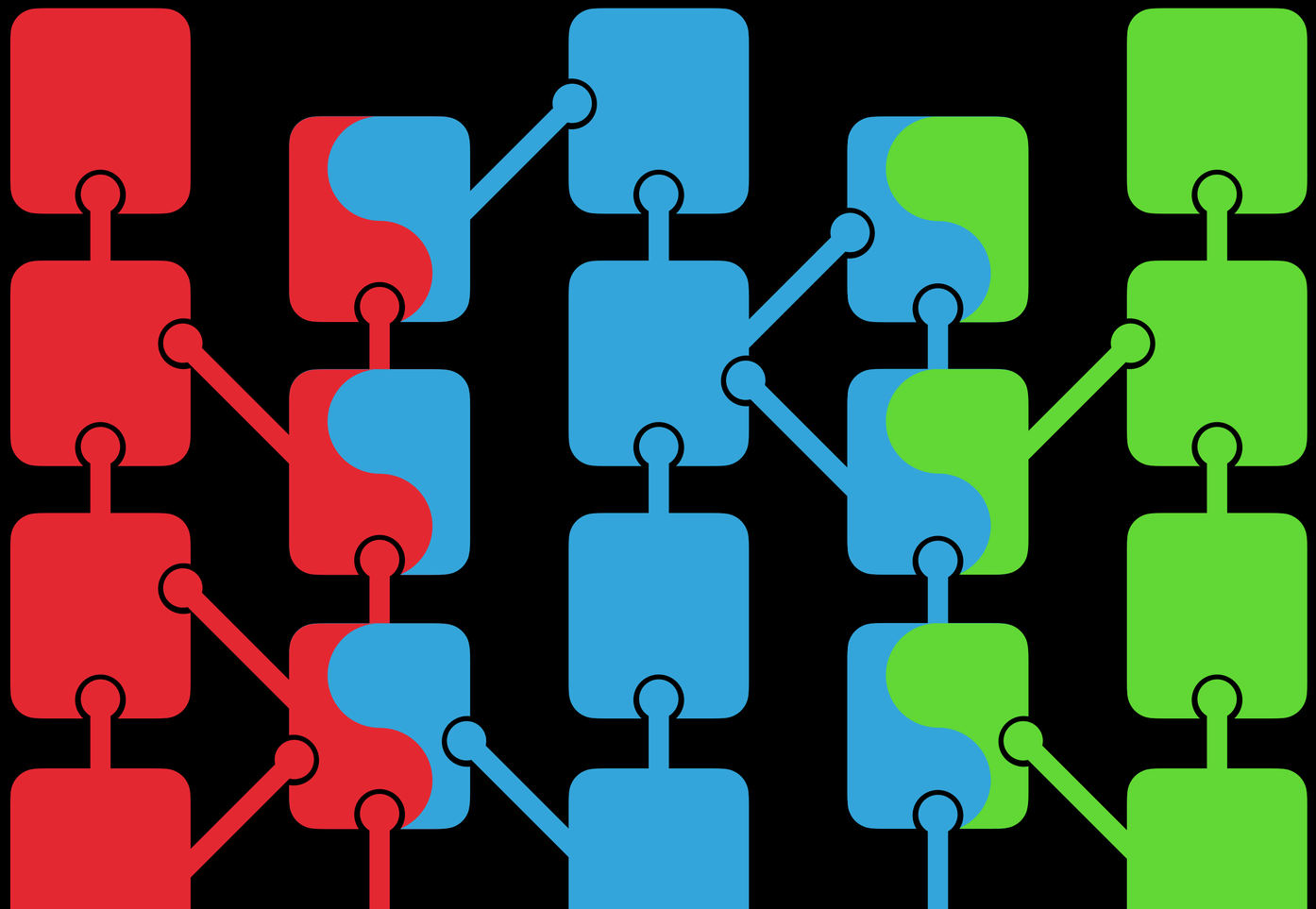




CHIMERA CHAINS

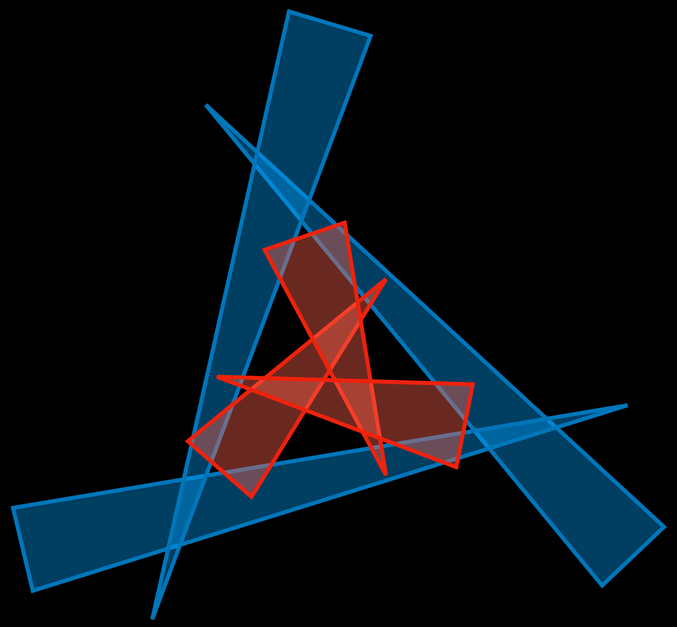
- A chain for each possible consensus
  - On-demand
- Inter-Chain Communication

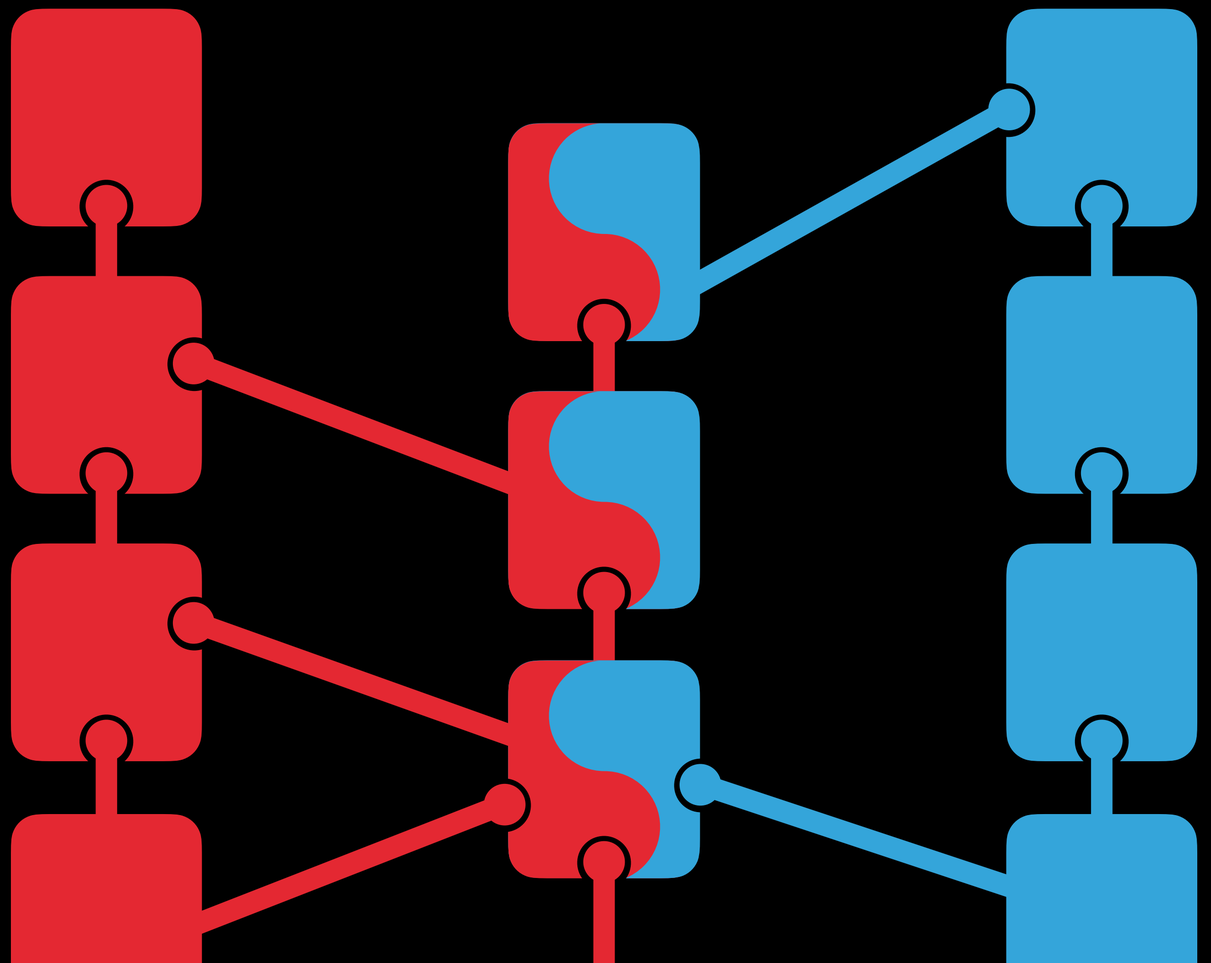




CHIMERA CHAINS

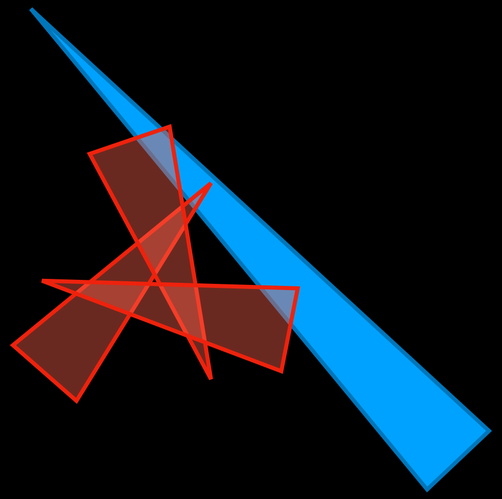
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

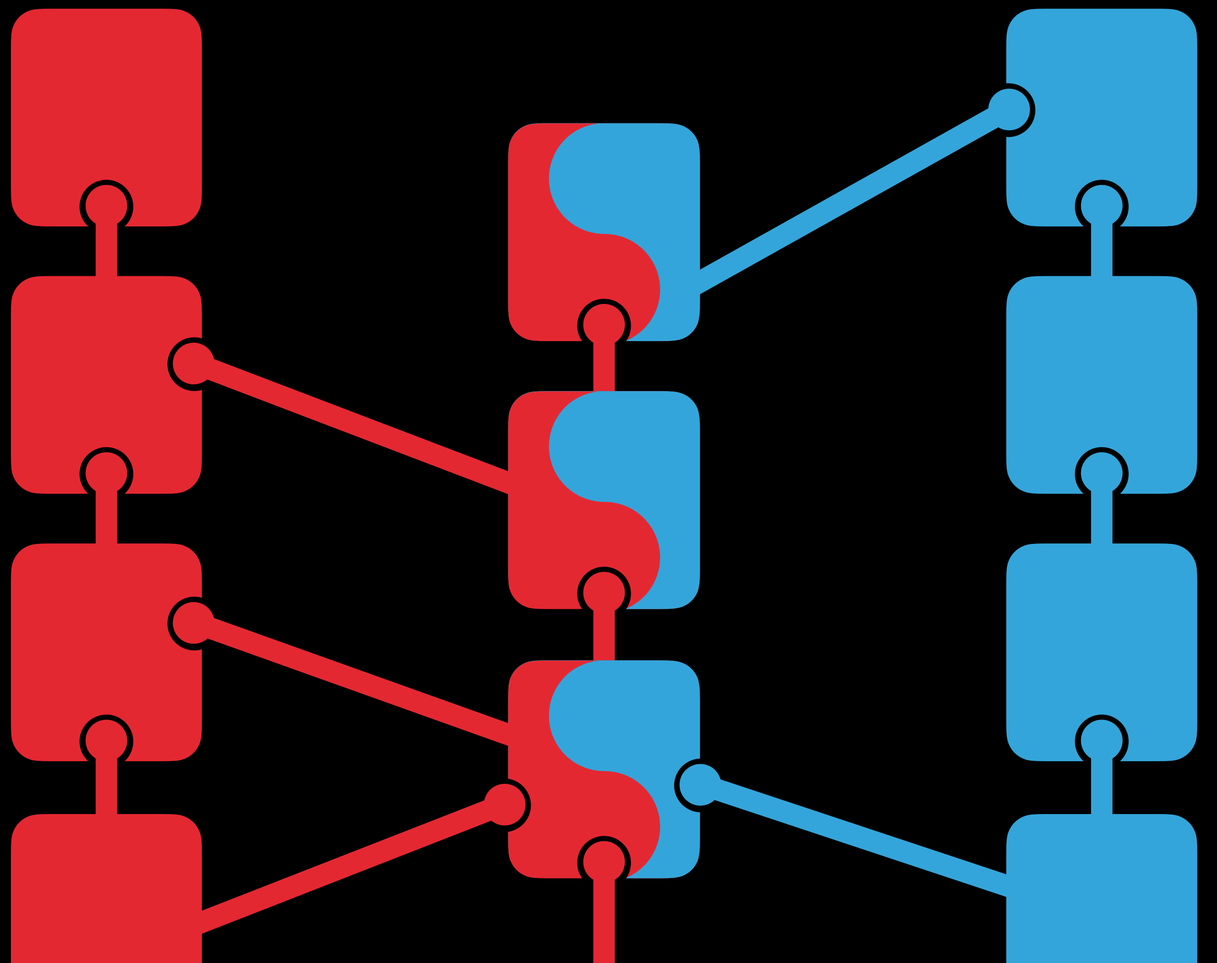




CHIMERA CHAINS

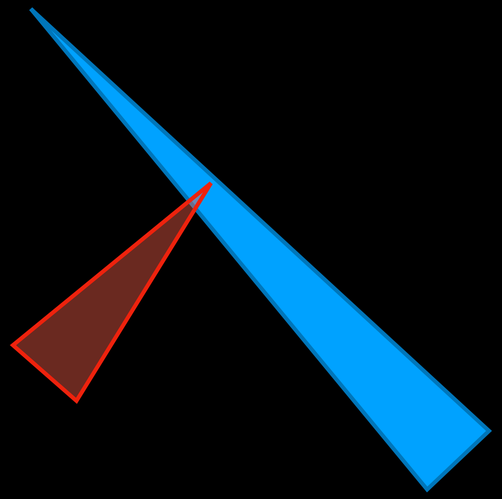
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

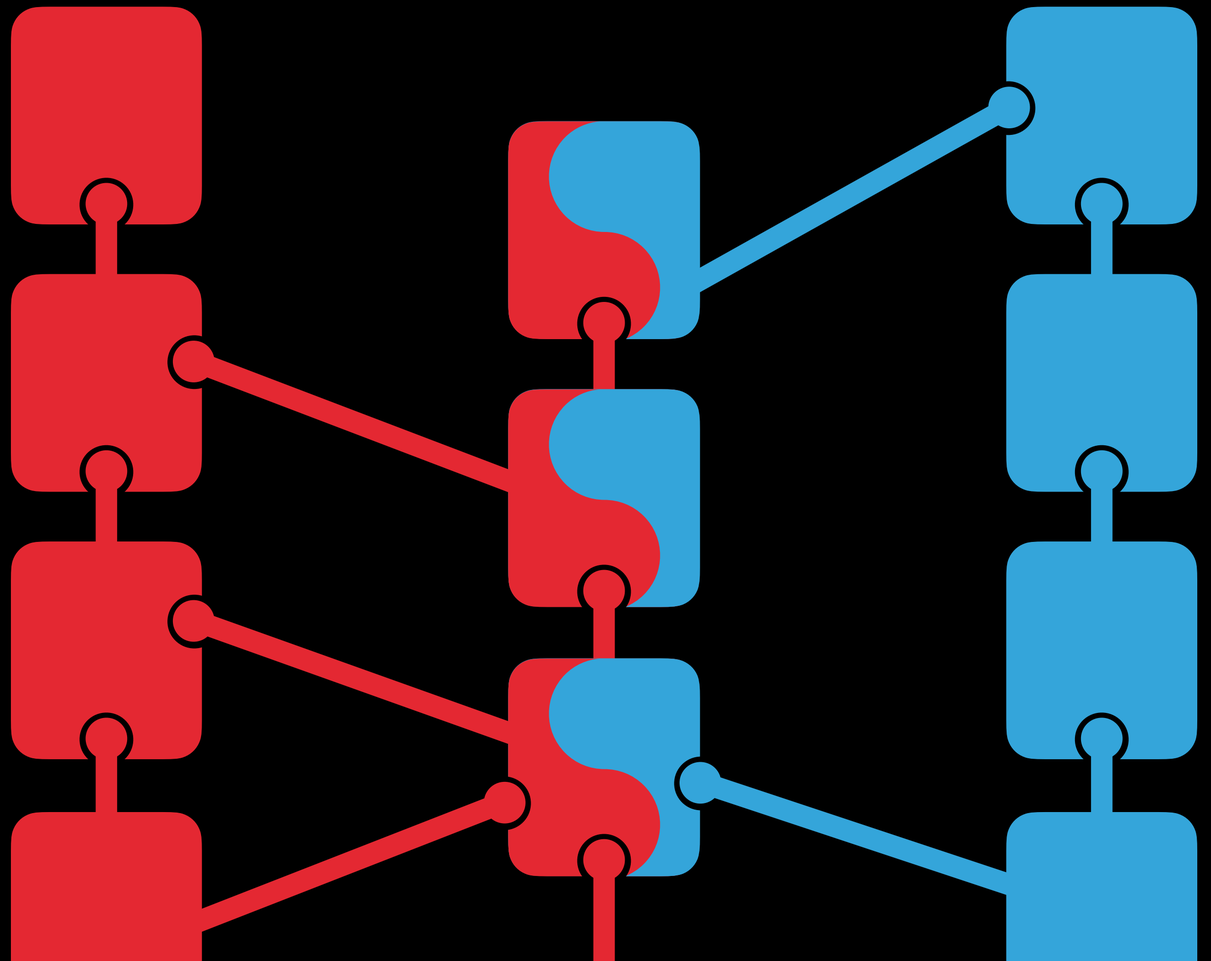




CHIMERA CHAINS

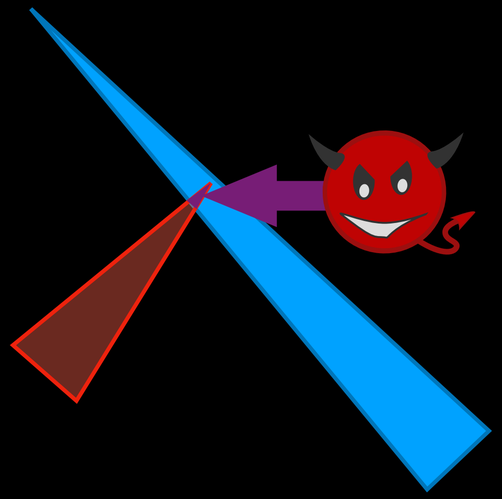
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

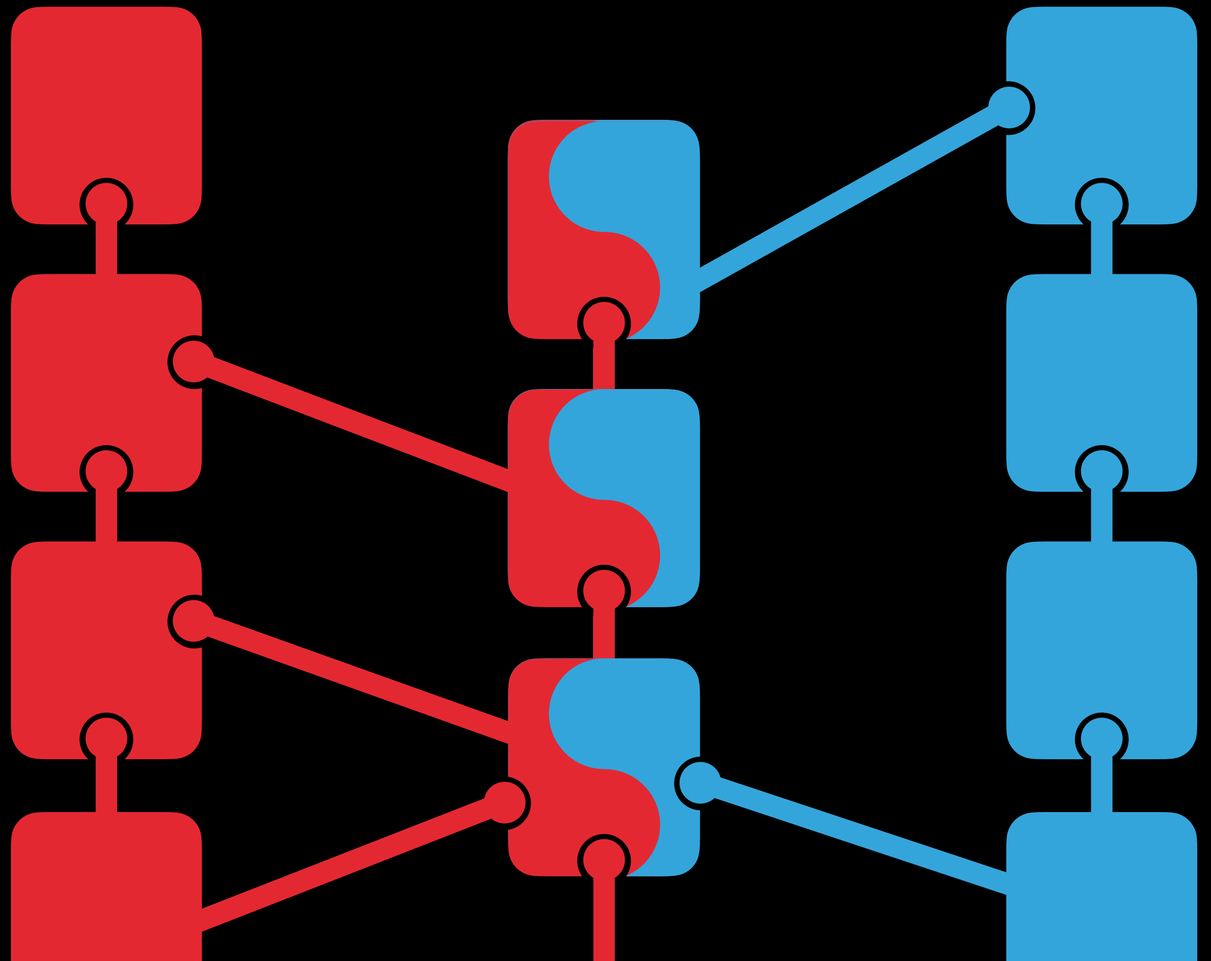




CHIMERA CHAINS

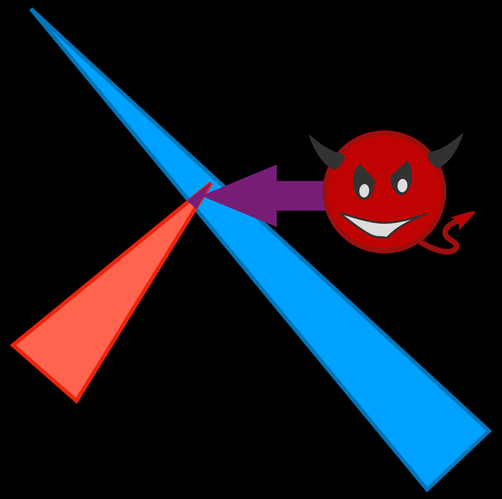
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

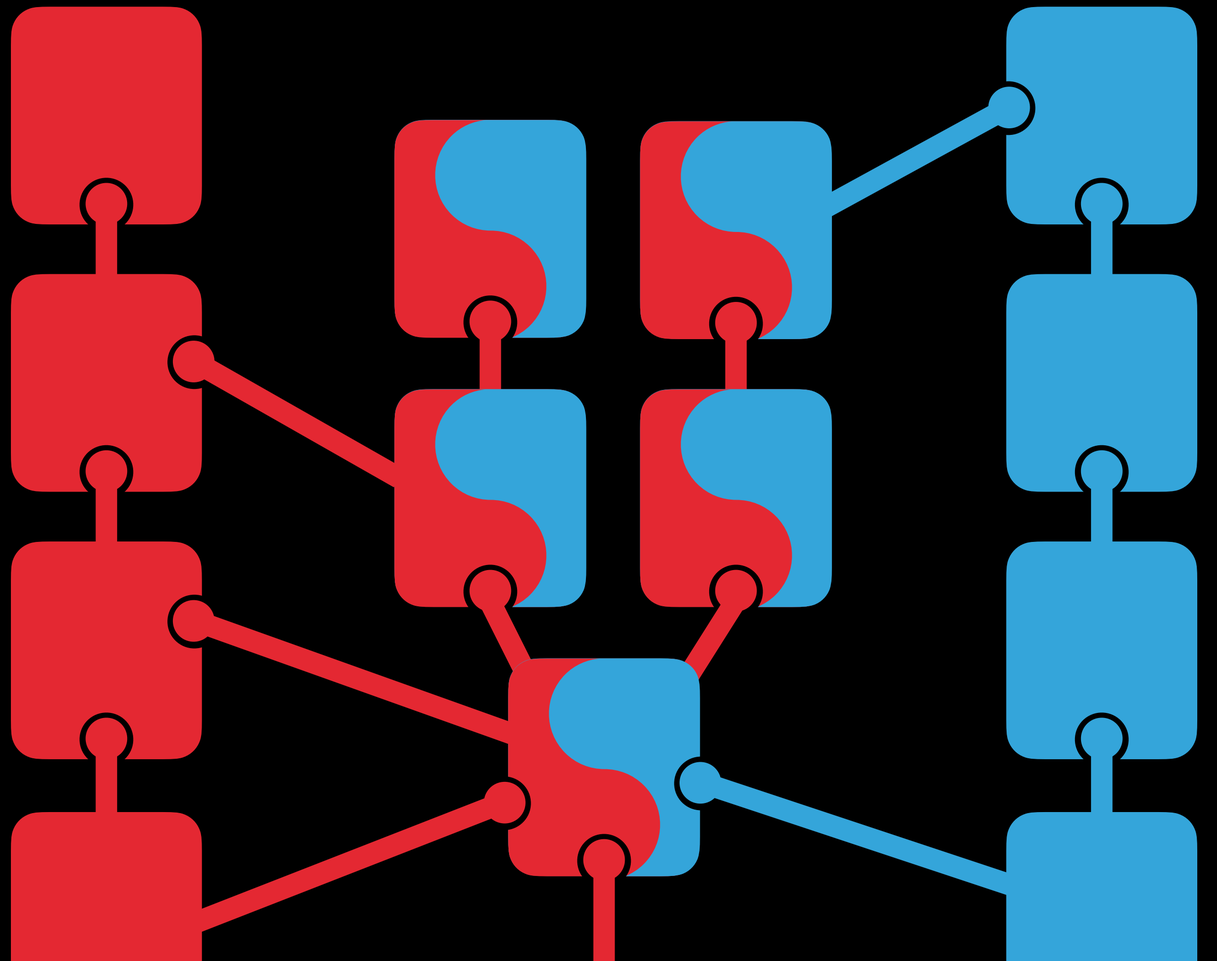




CHIMERA CHAINS

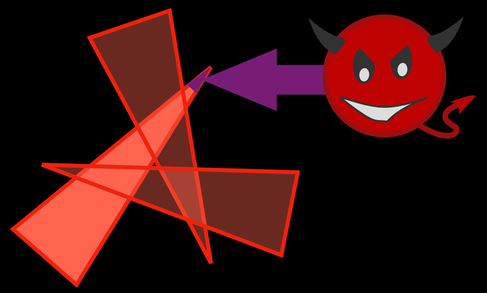
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

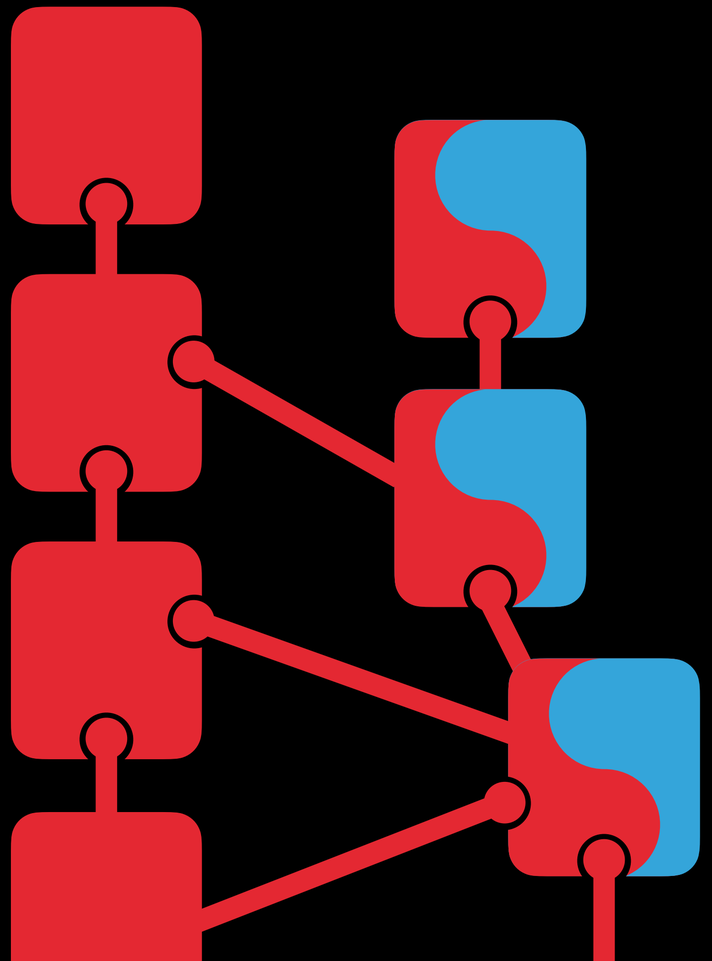




CHIMERA CHAINS

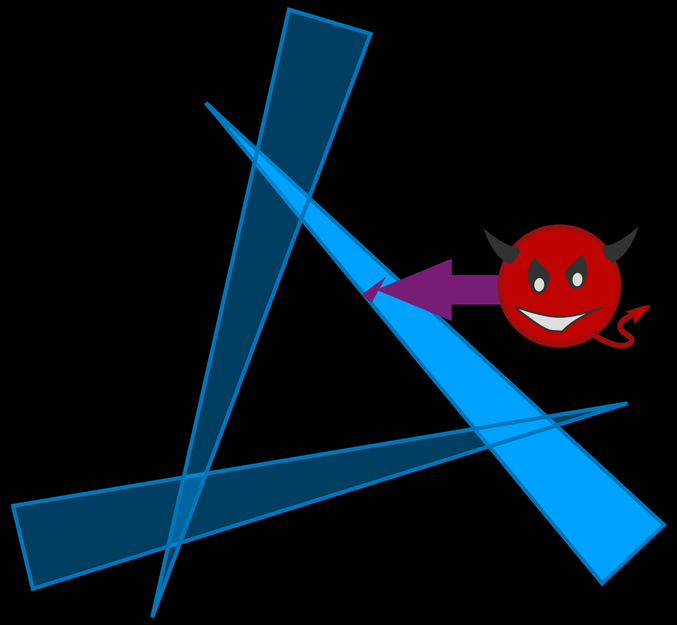
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

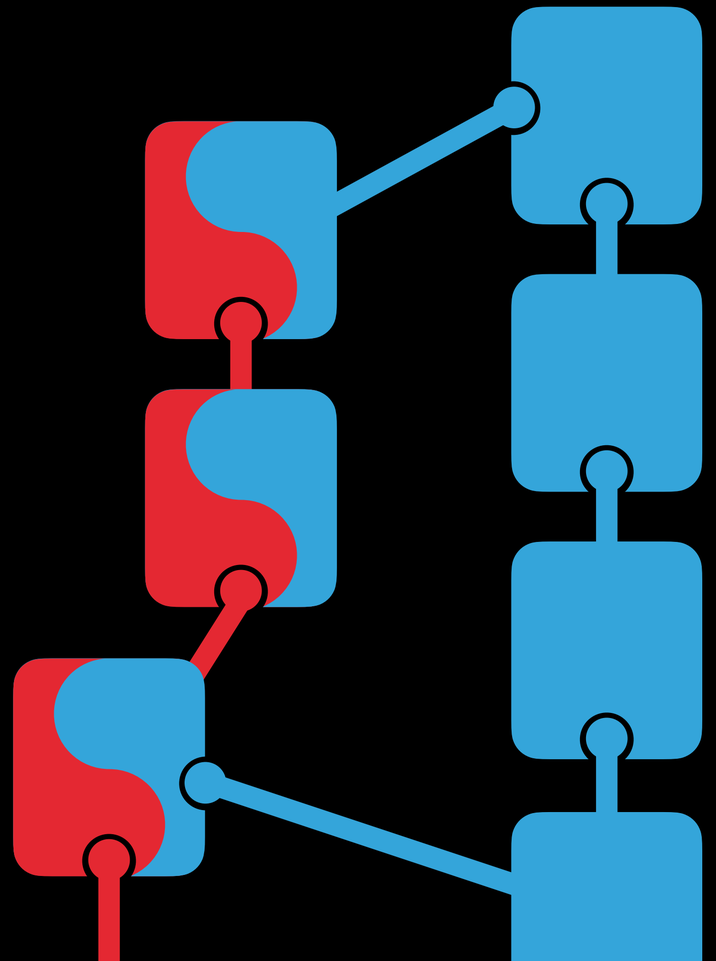




CHIMERA CHAINS

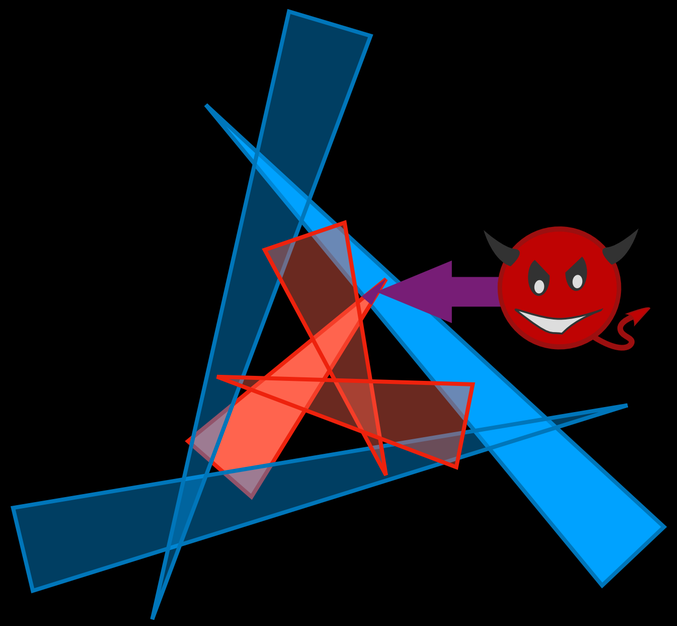
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

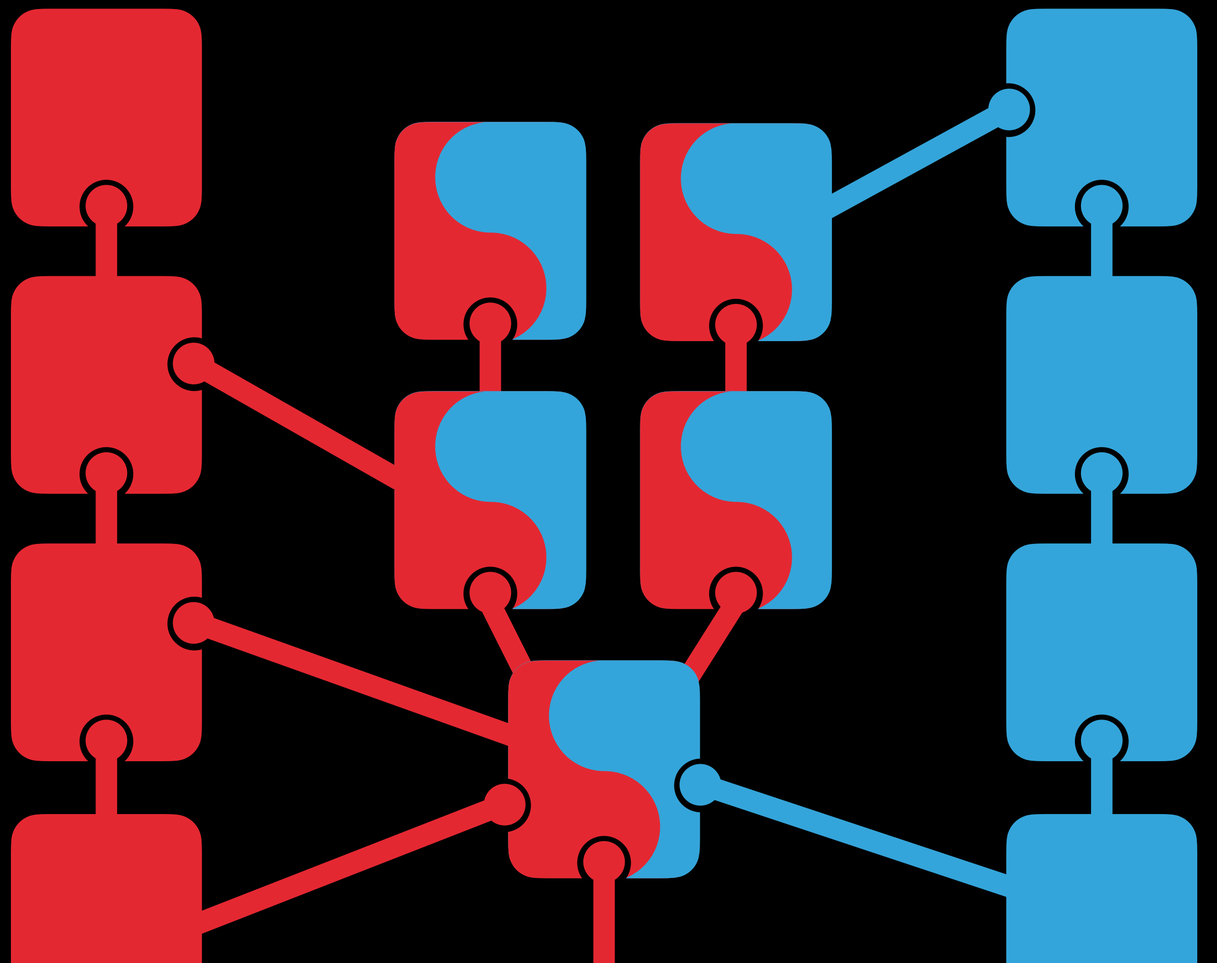




CHIMERA CHAINS

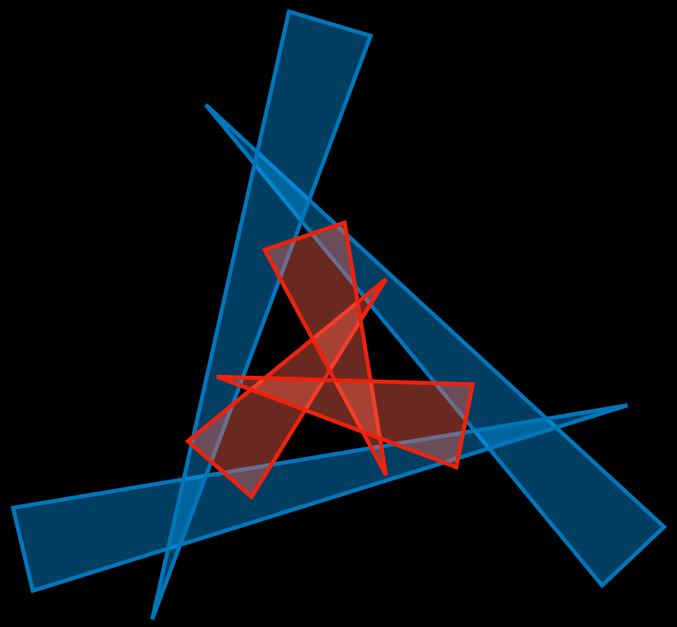
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

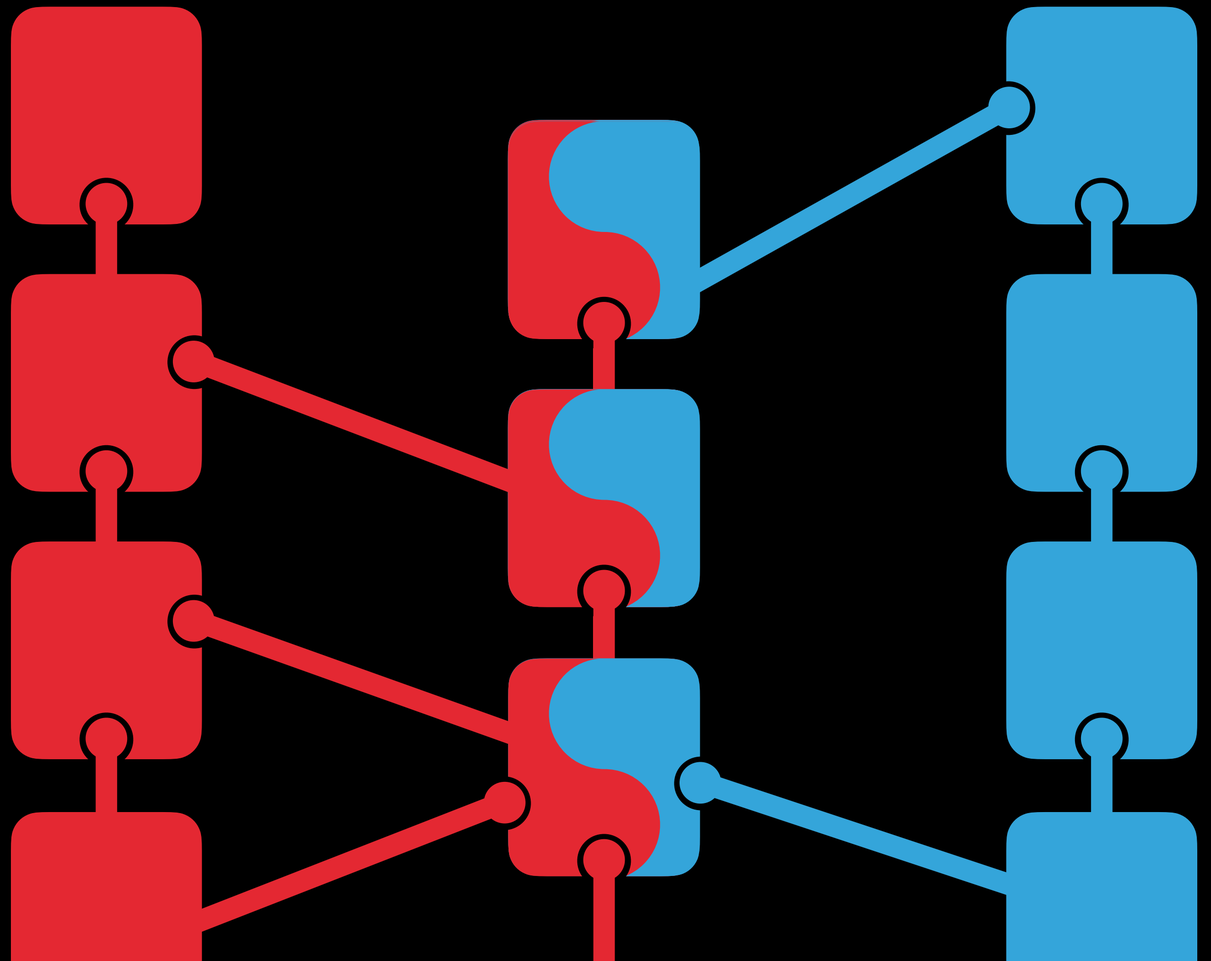




CHIMERA CHAINS

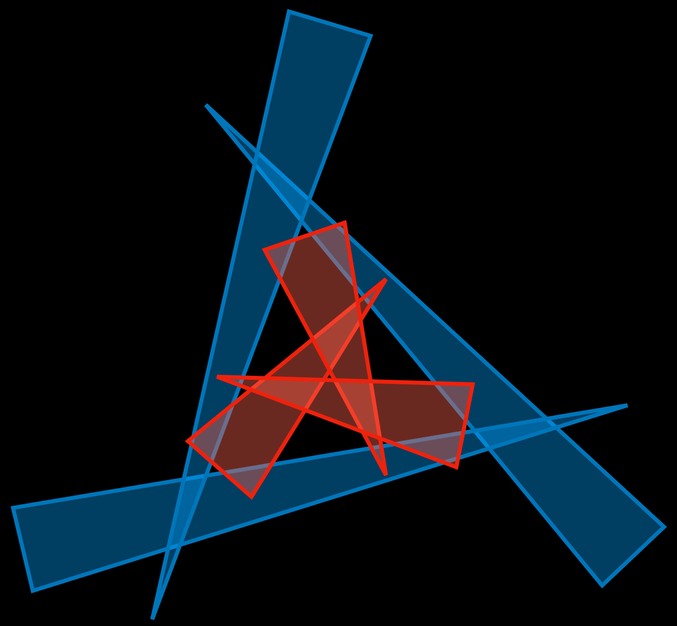
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

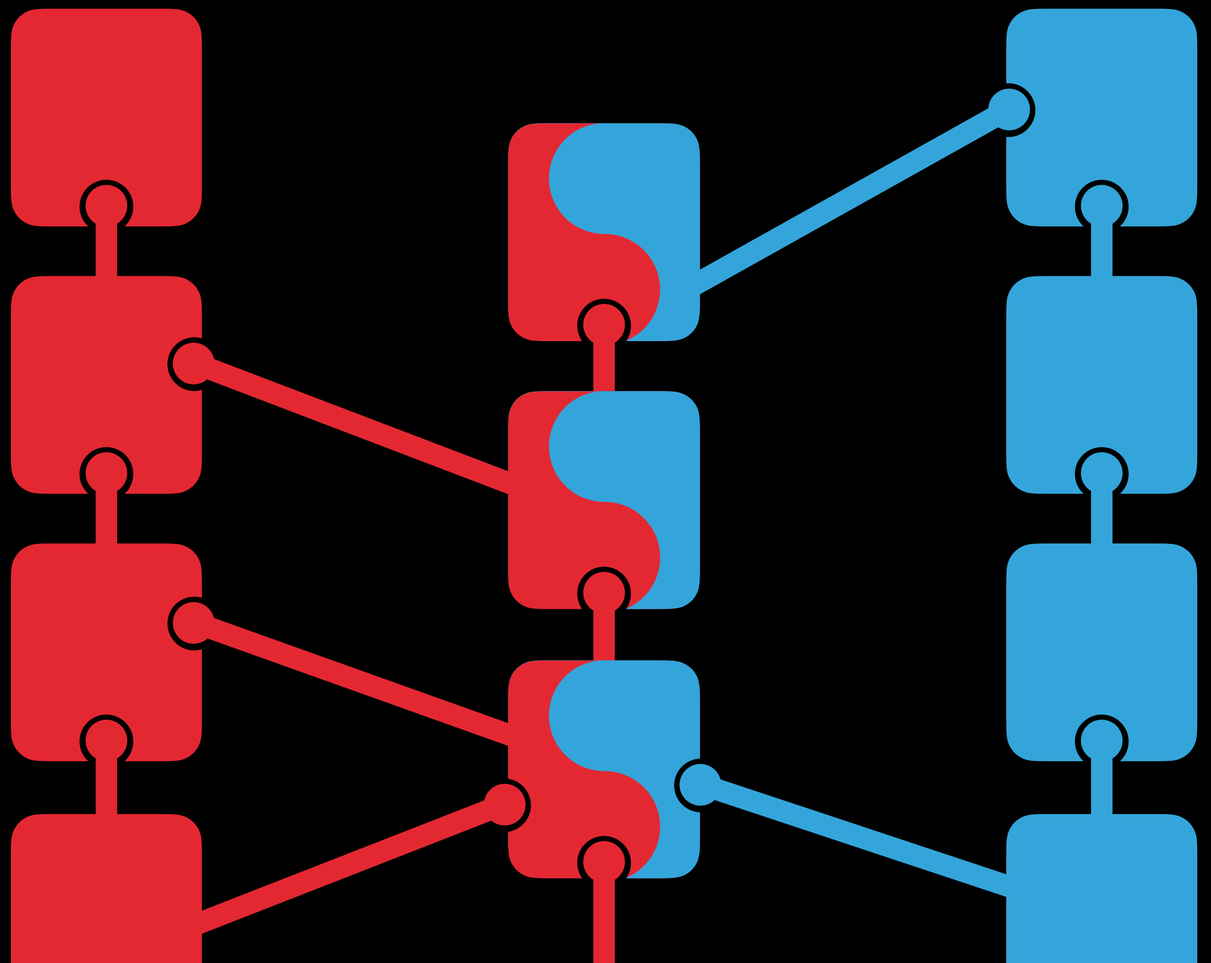




CHIMERA CHAINS

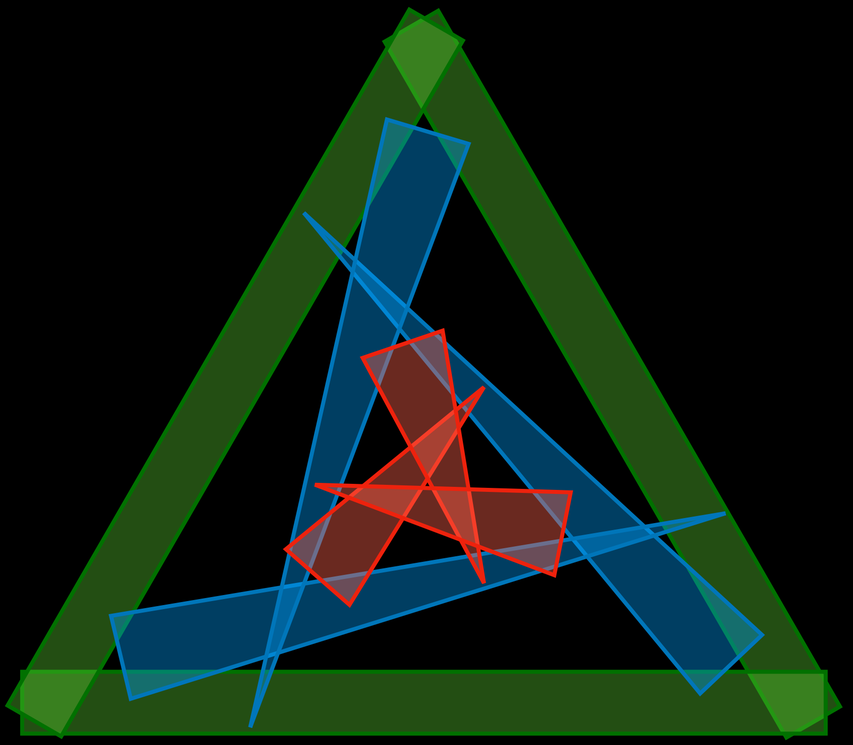
- Each chain liveness / integrity of its own quorums
- Inter-chain transaction atomicity when quorum intersections all contain a safe node

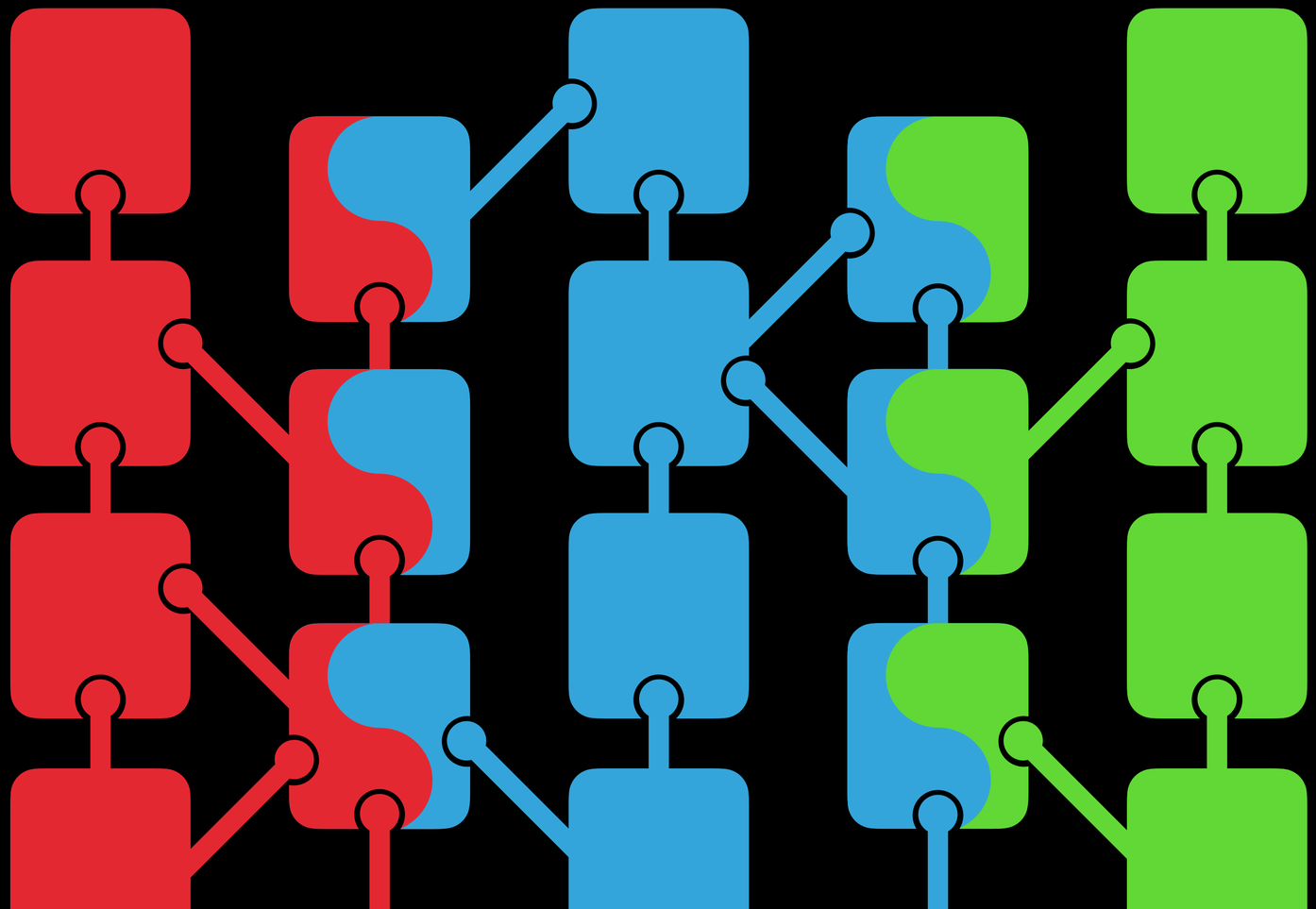




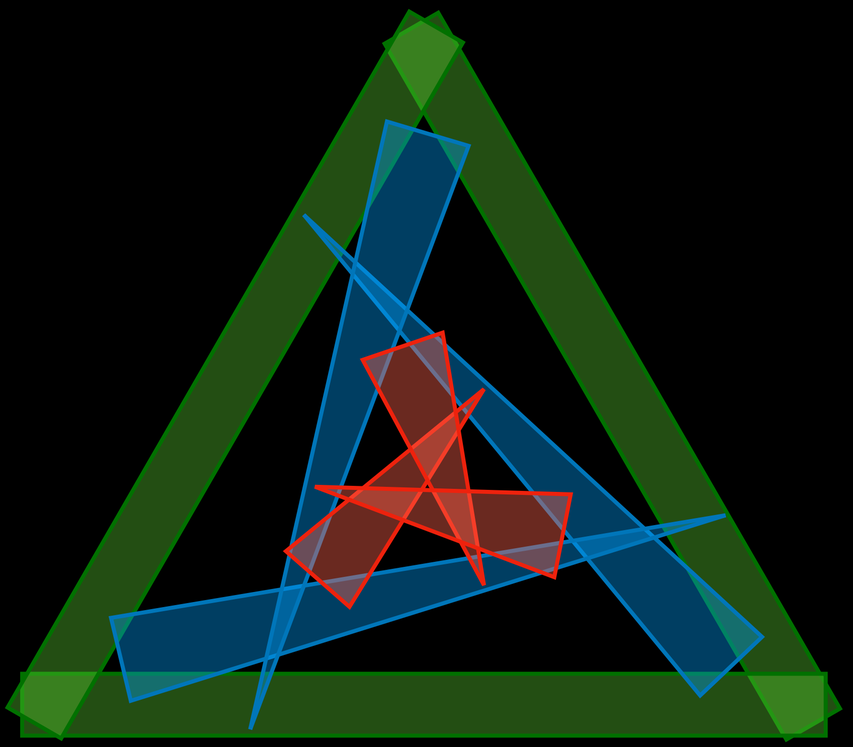
CHIMERA CHAINS

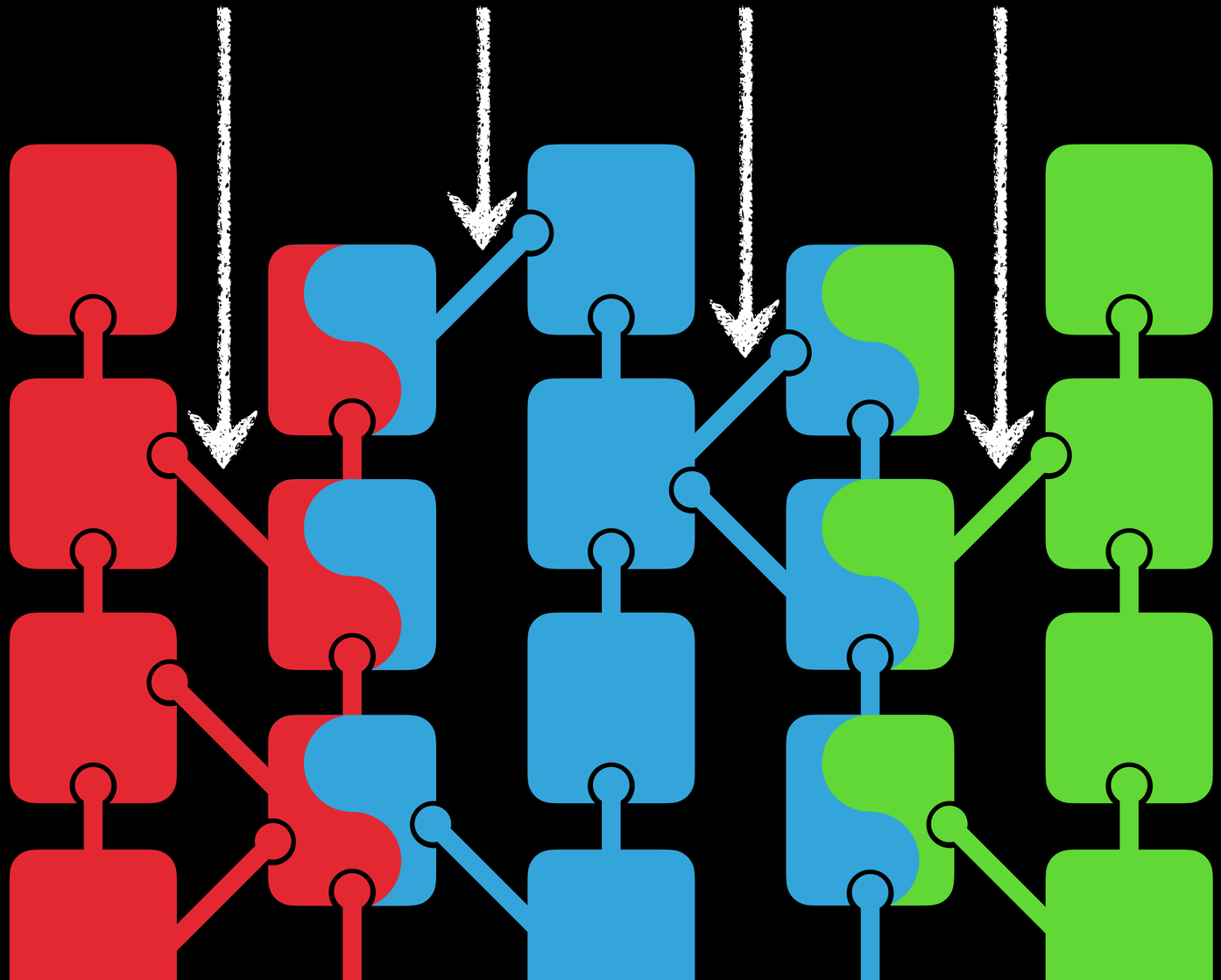
- A chain for each possible consensus
  - On-demand
- Inter-Chain Communication





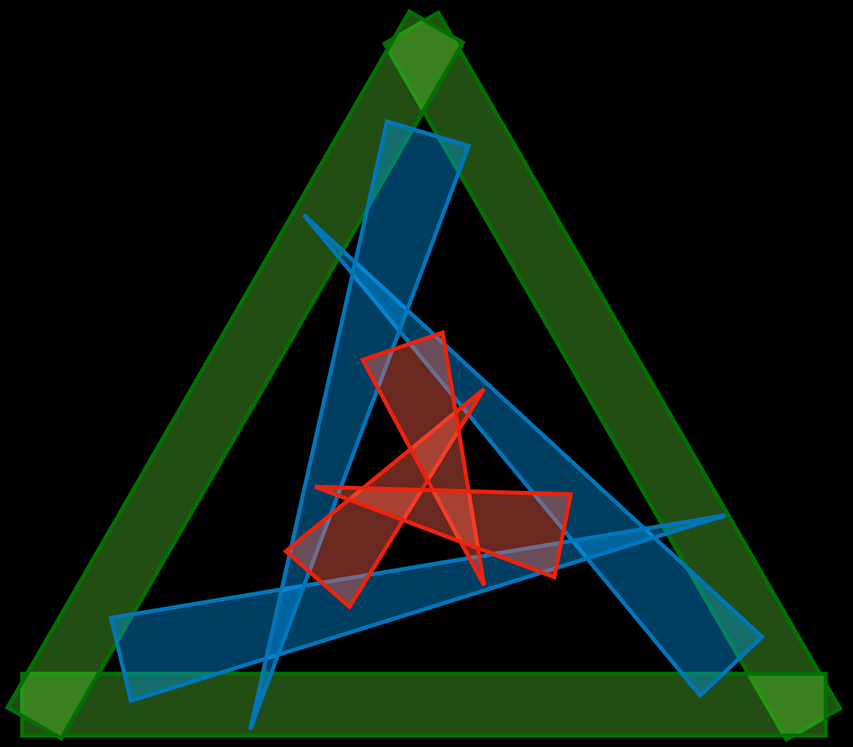
INTER-CHAIN COMMUNICATION

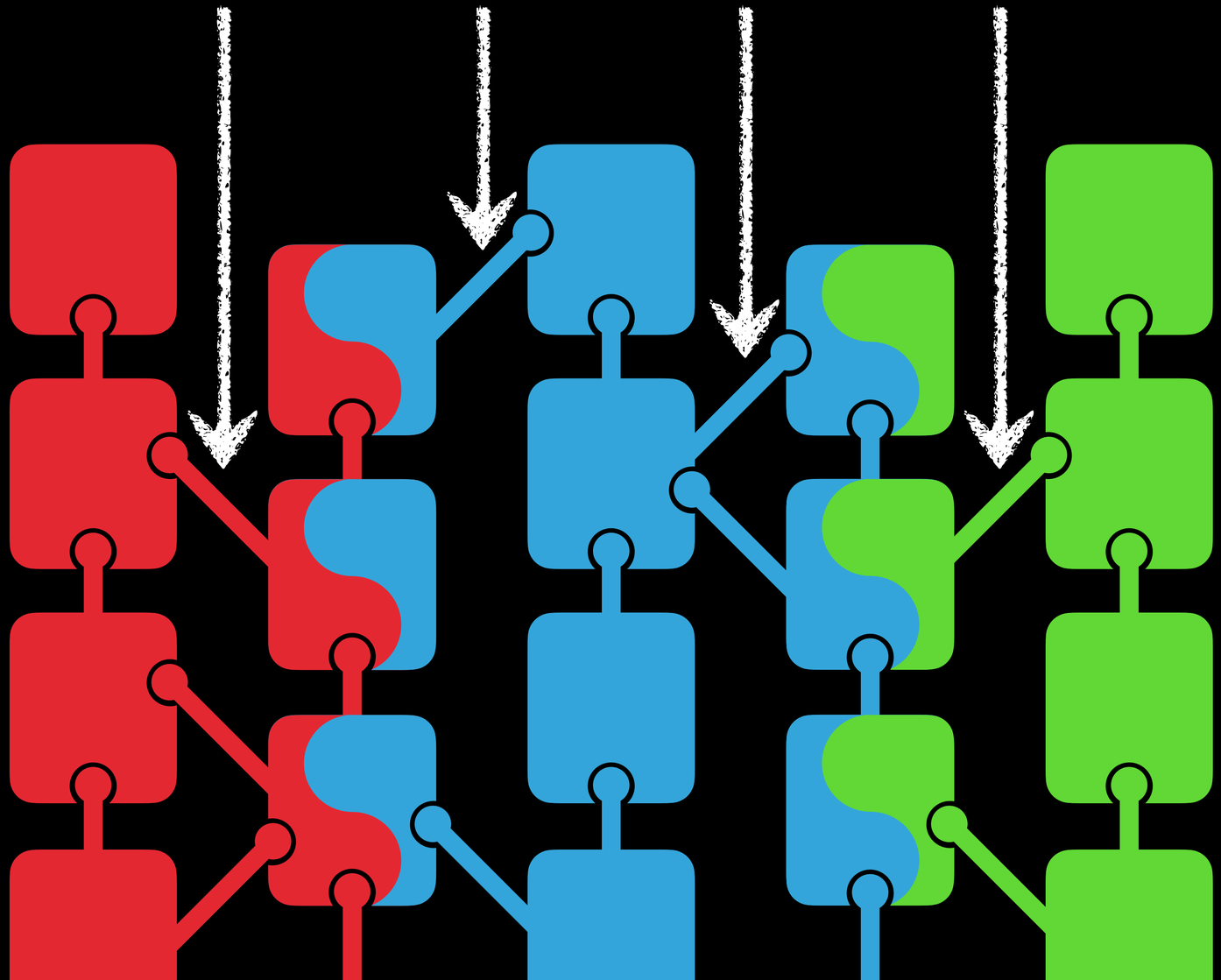




INTER-CHAIN COMMUNICATION

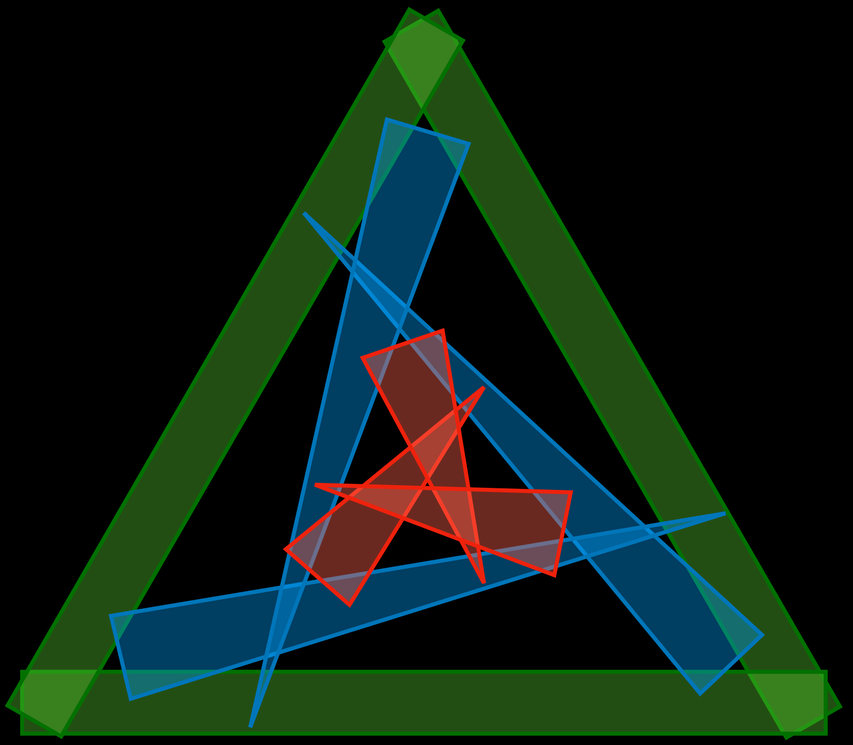
- IBC? [ibcprotocol.org]

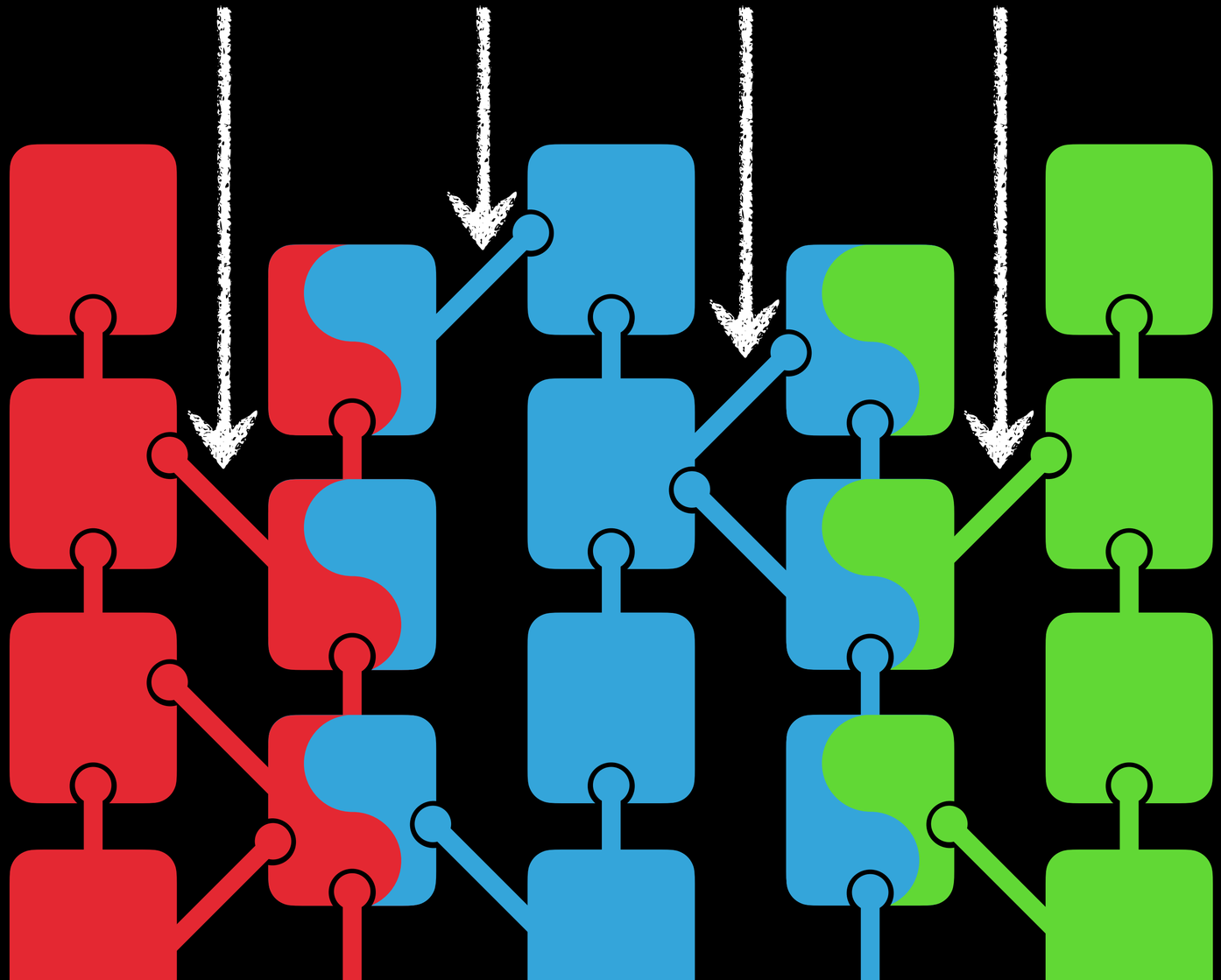




INTER-CHAIN COMMUNICATION

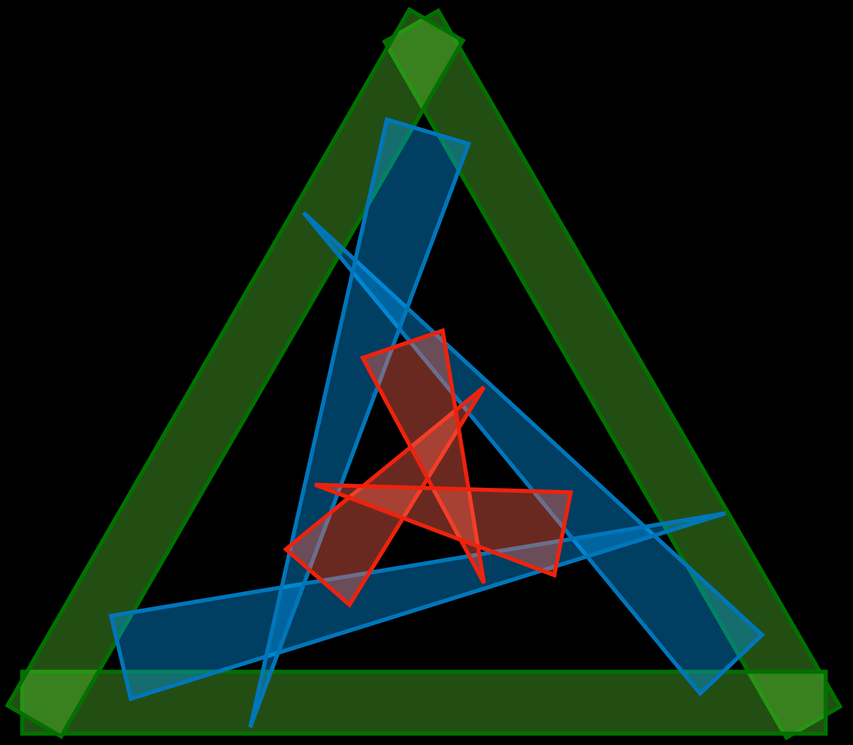
- IBC? [ibcprotocol.org]
- Do we need Proofs?

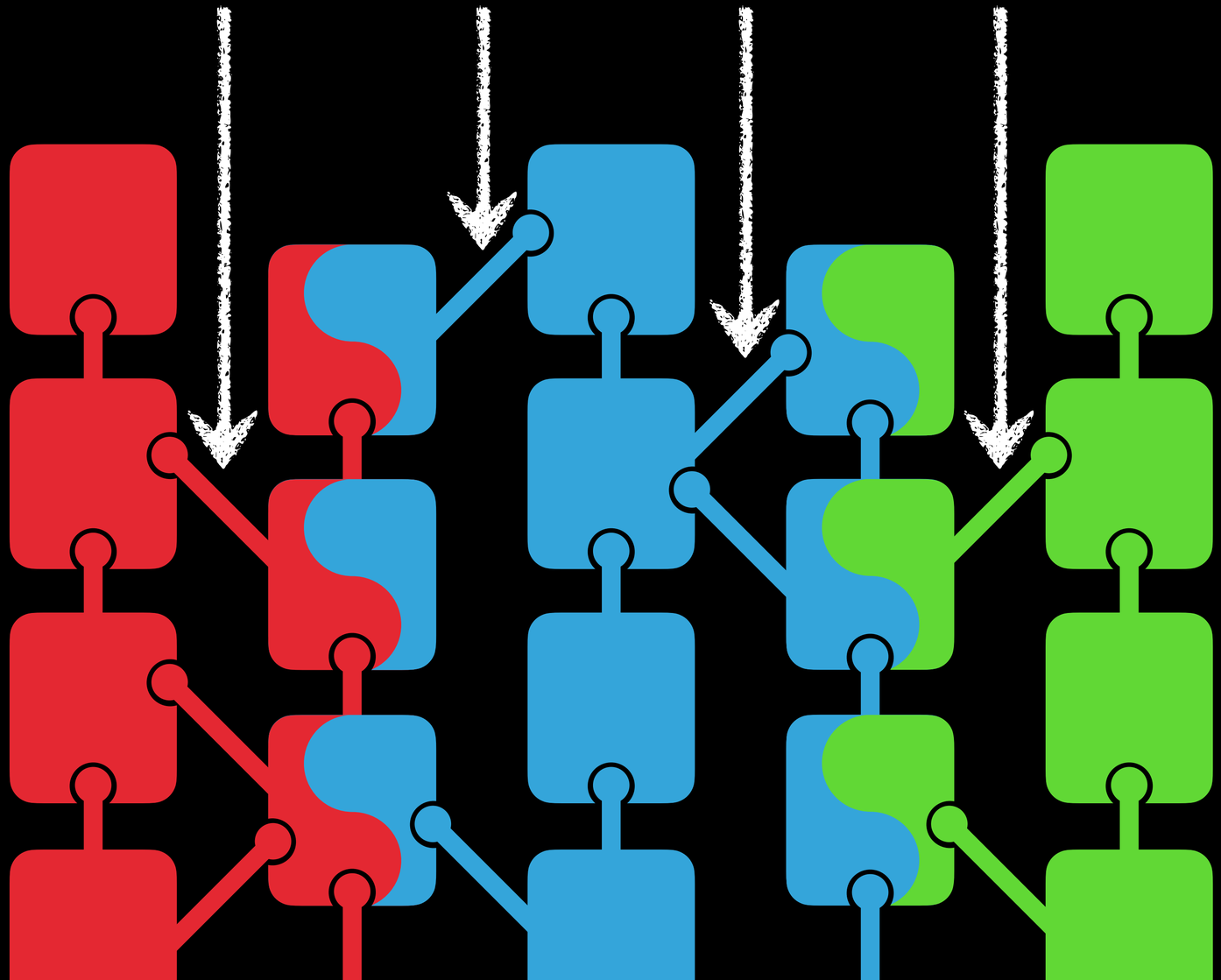




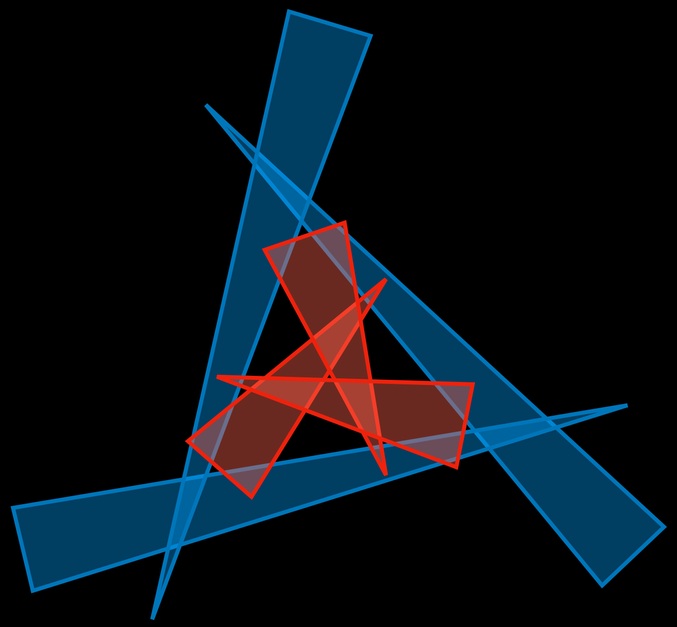
INTER-CHAIN COMMUNICATION

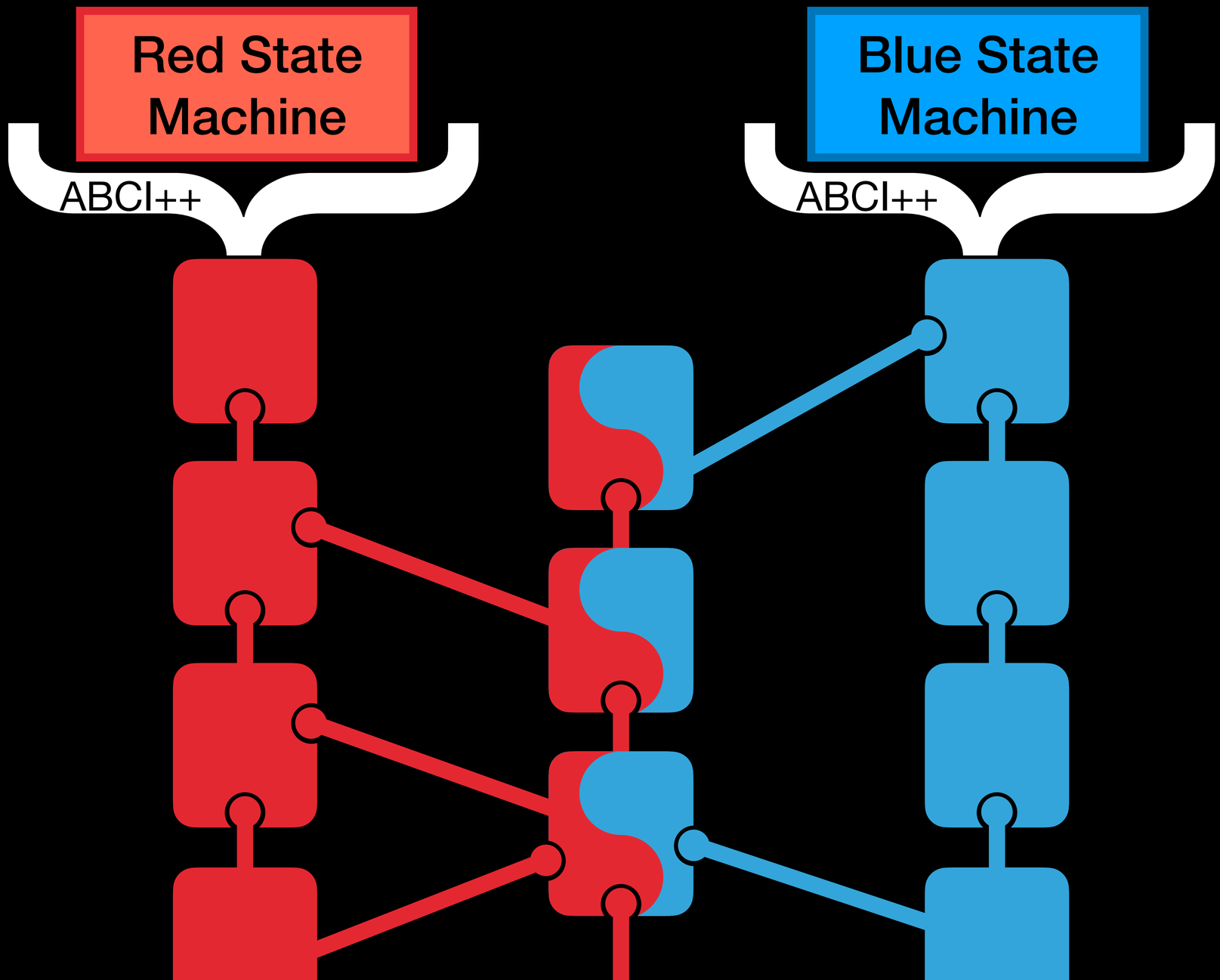
- IBC? [ibcprotocol.org]
- Do we need Proofs?
- Synchrony (in blocks)?





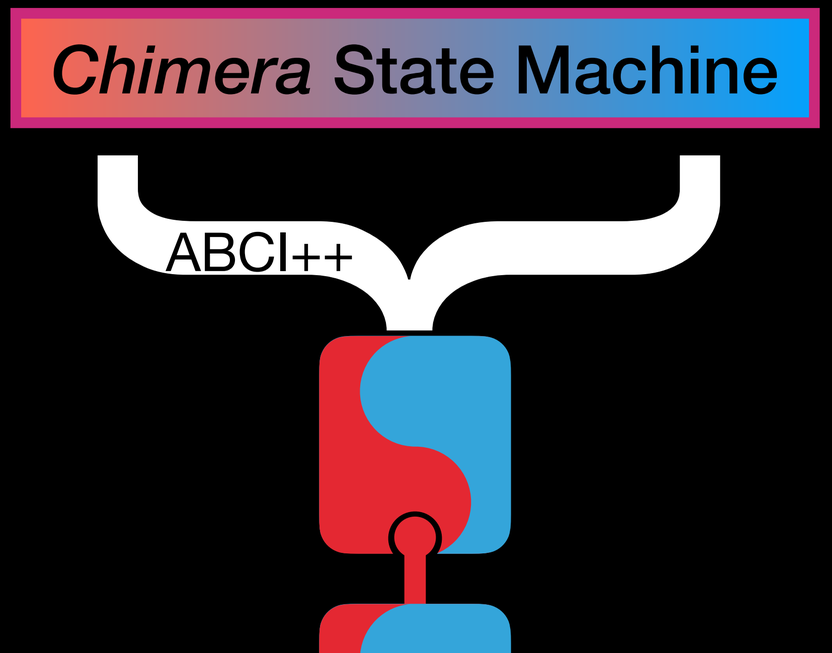
STATE MACHINE





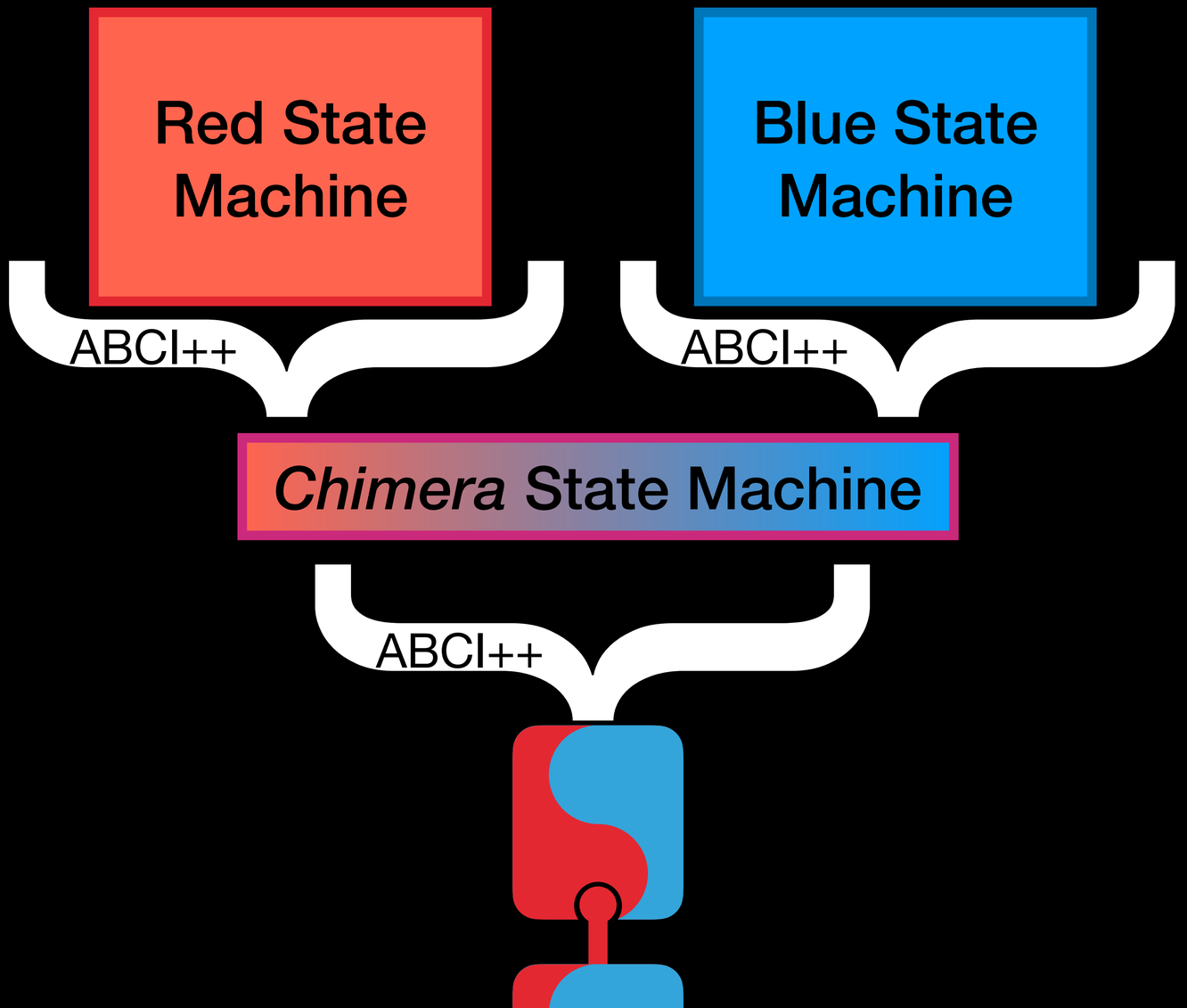
STATE MACHINE

- Over Chimera Chain



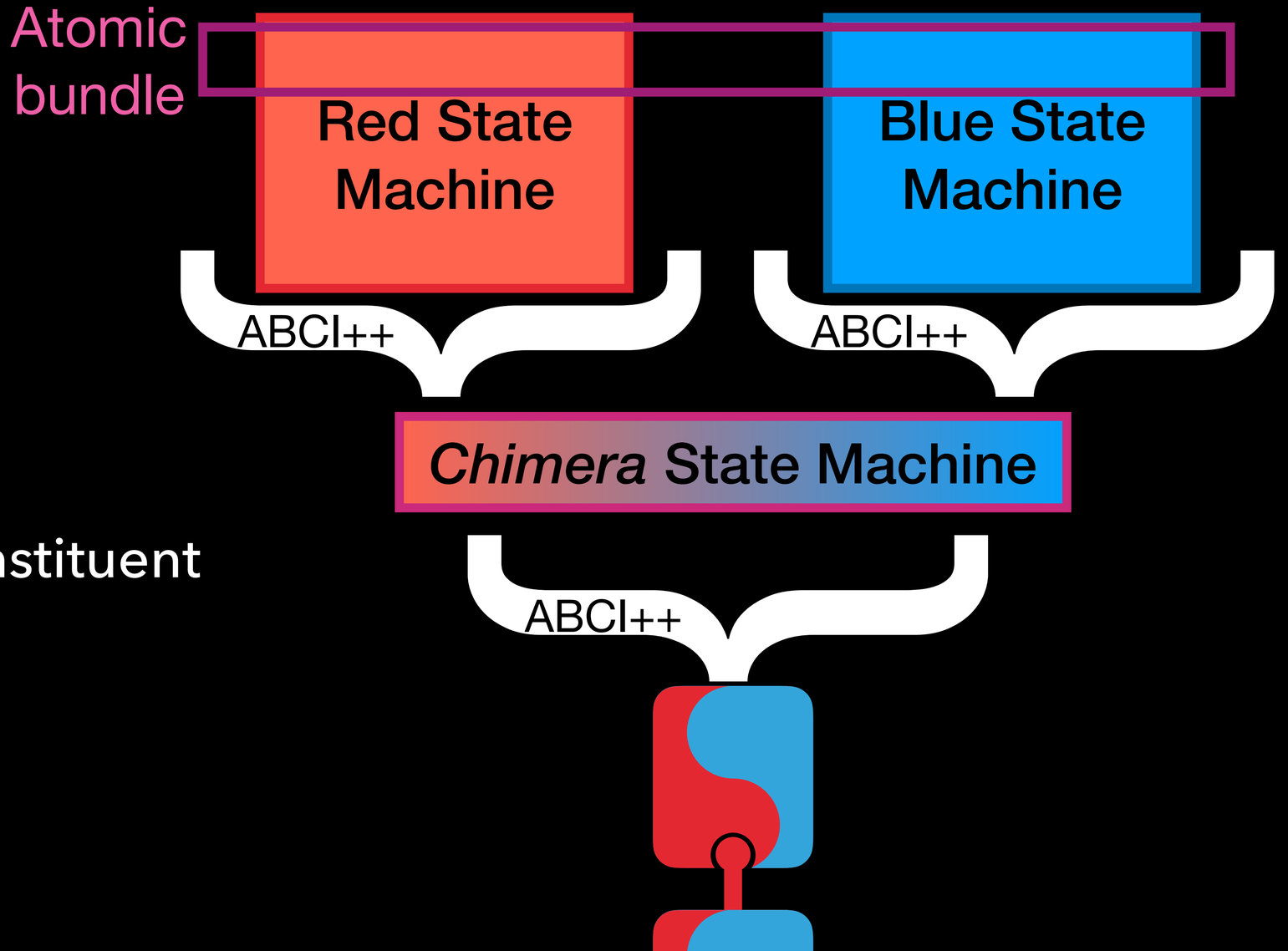
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines



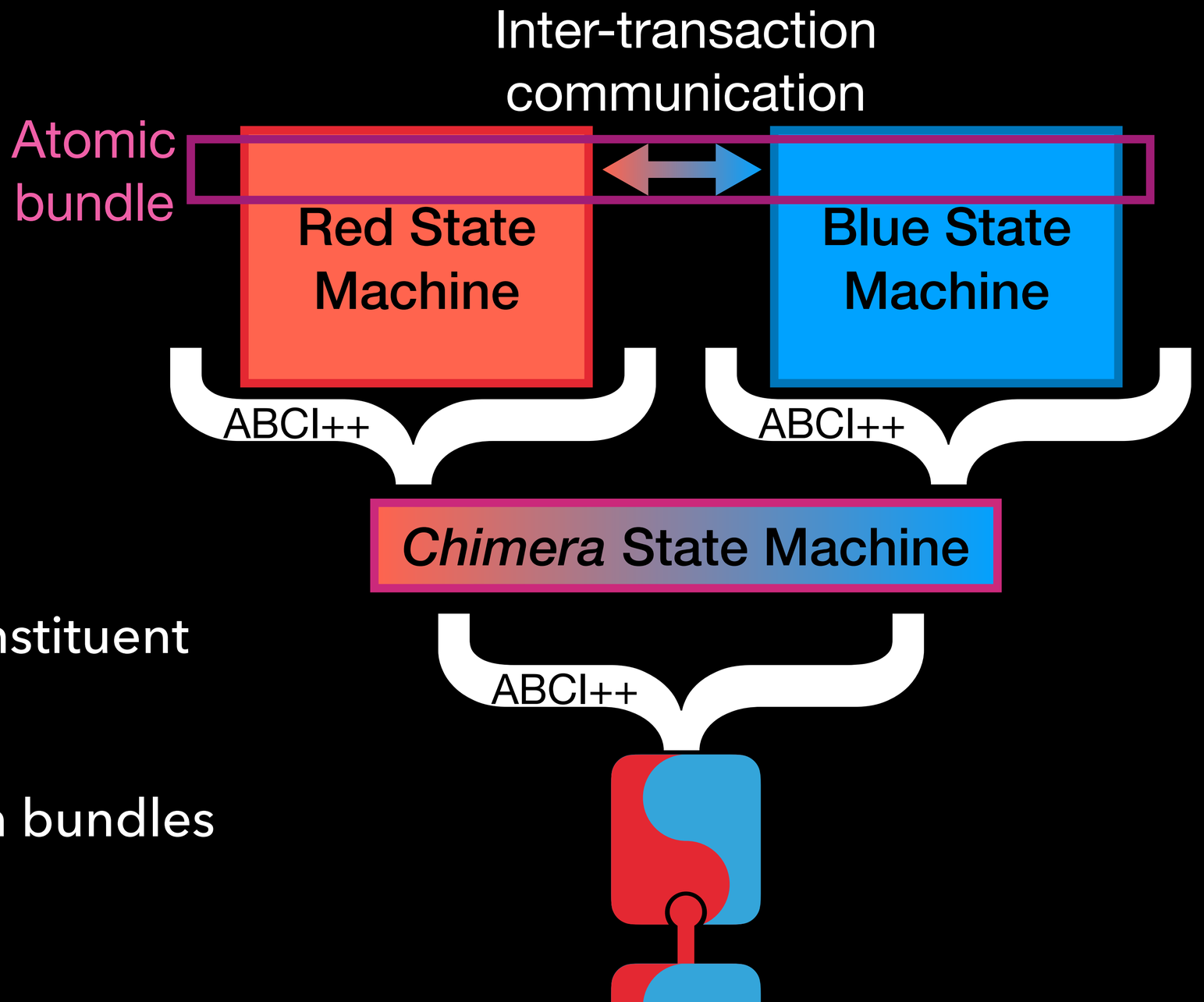
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions



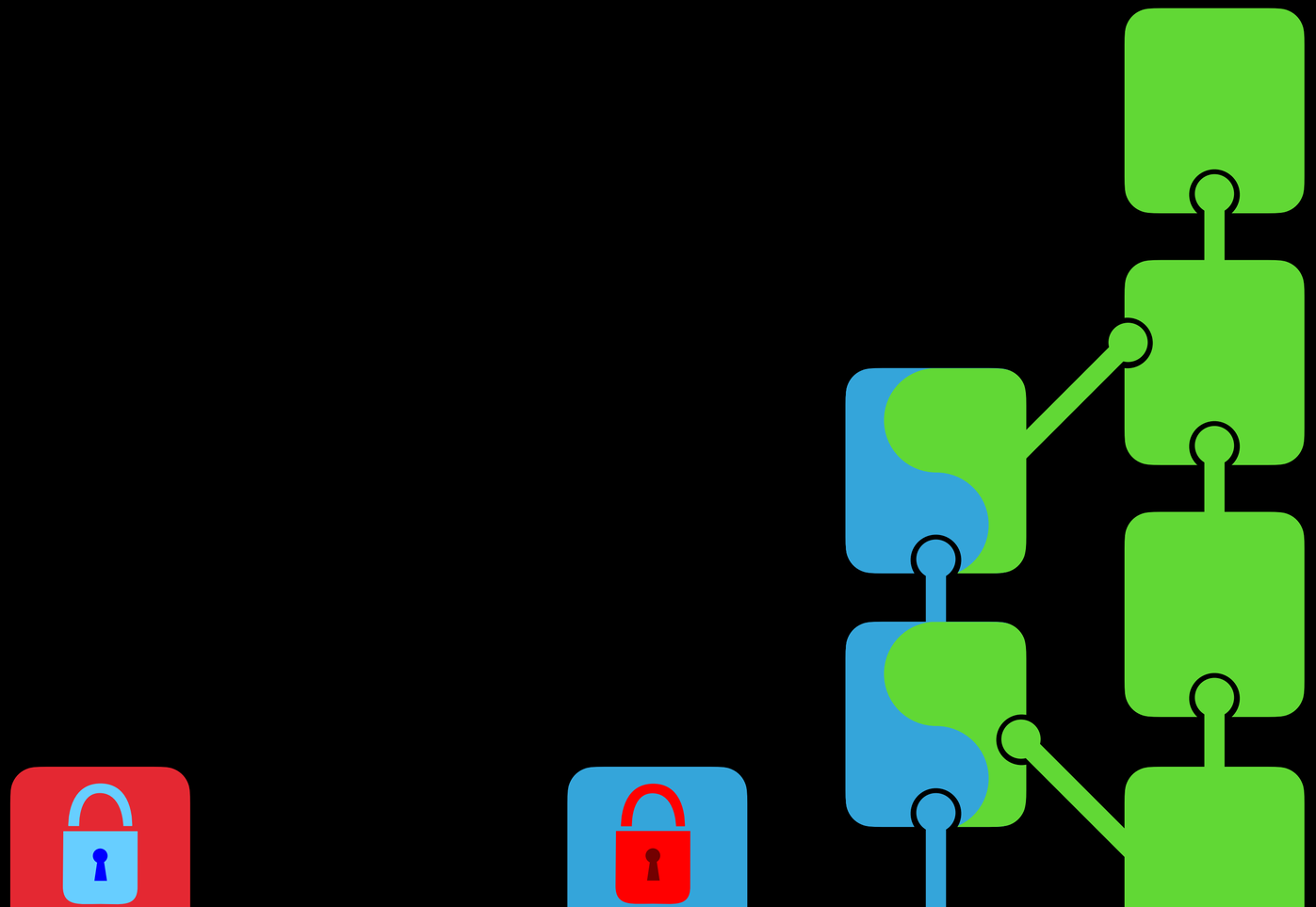
STATE MACHINE

- Over Chimera Chain
- Instances of constituent chain state machines
- Transactions:
  - Atomic bundles of constituent chain transactions
  - Communication within bundles



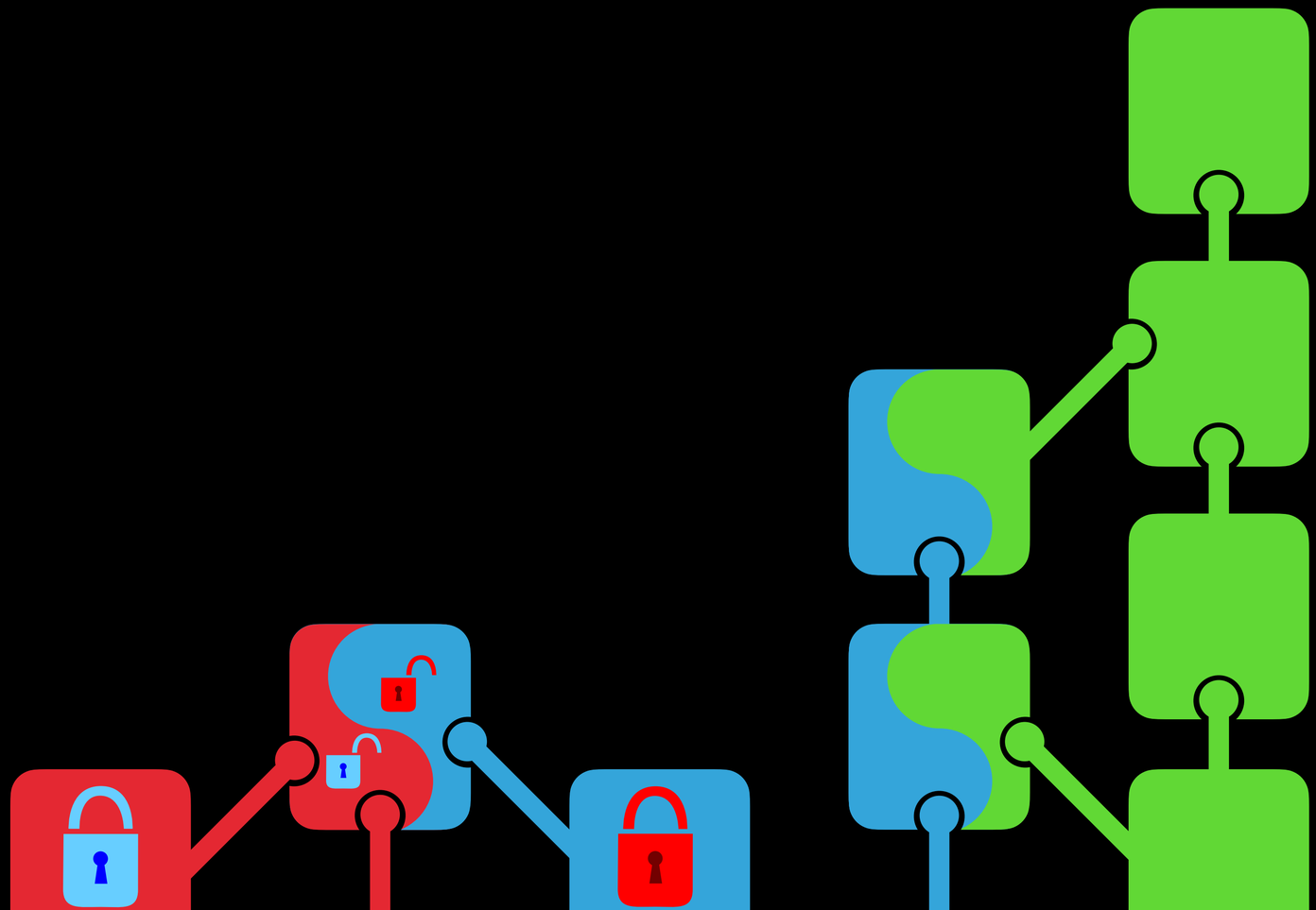
PROGRAMMING MODEL

- Locking State



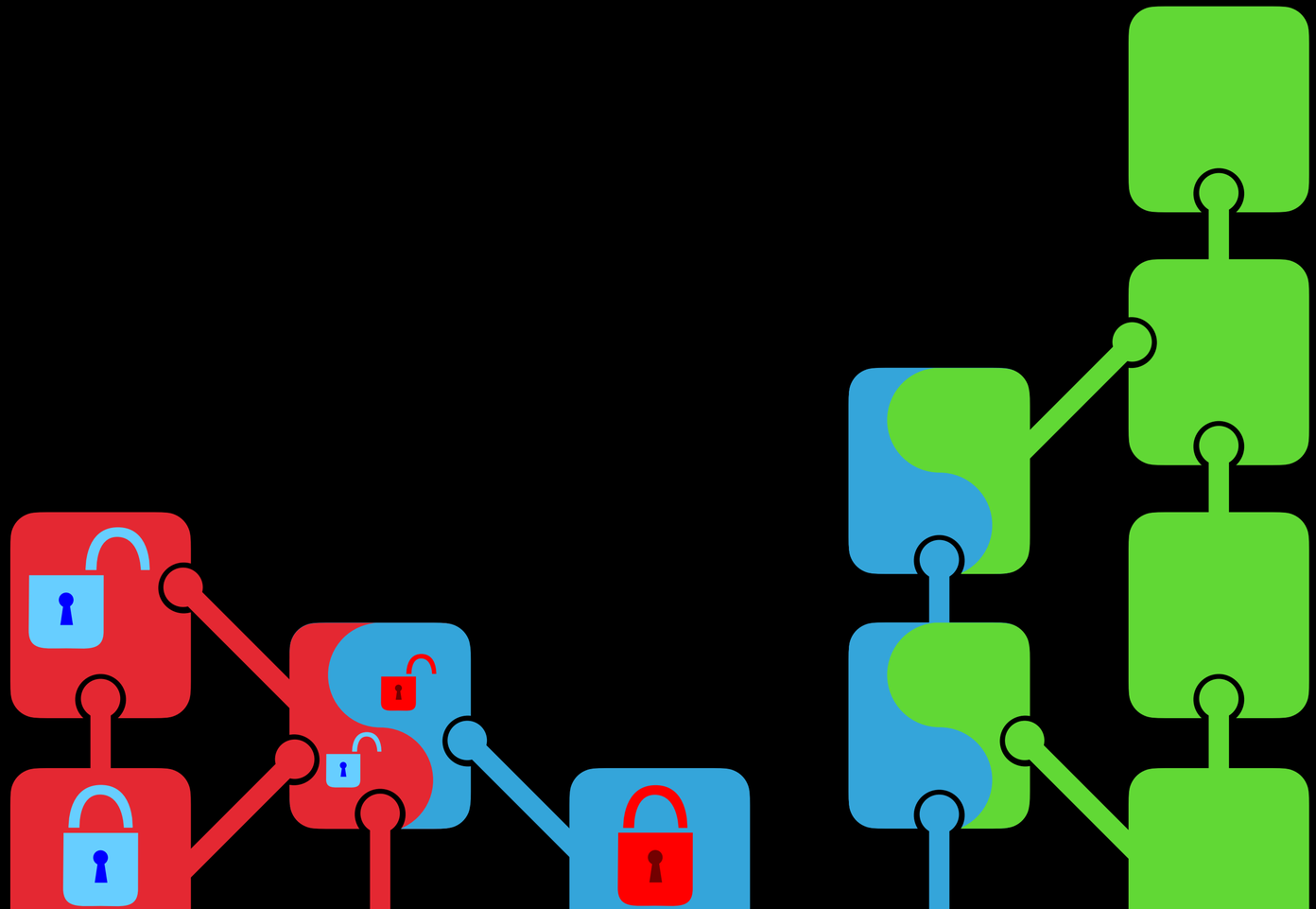
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain



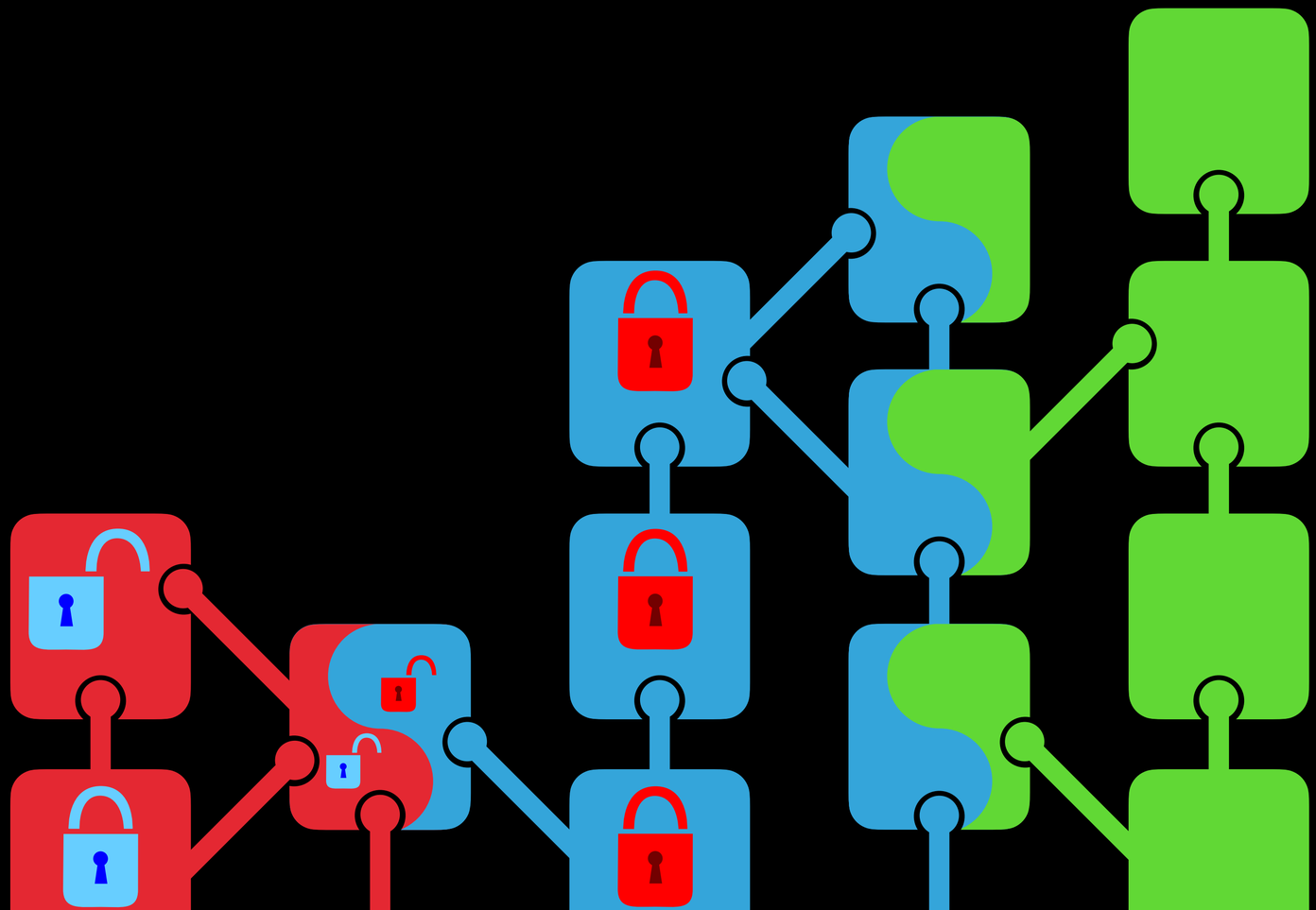
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain



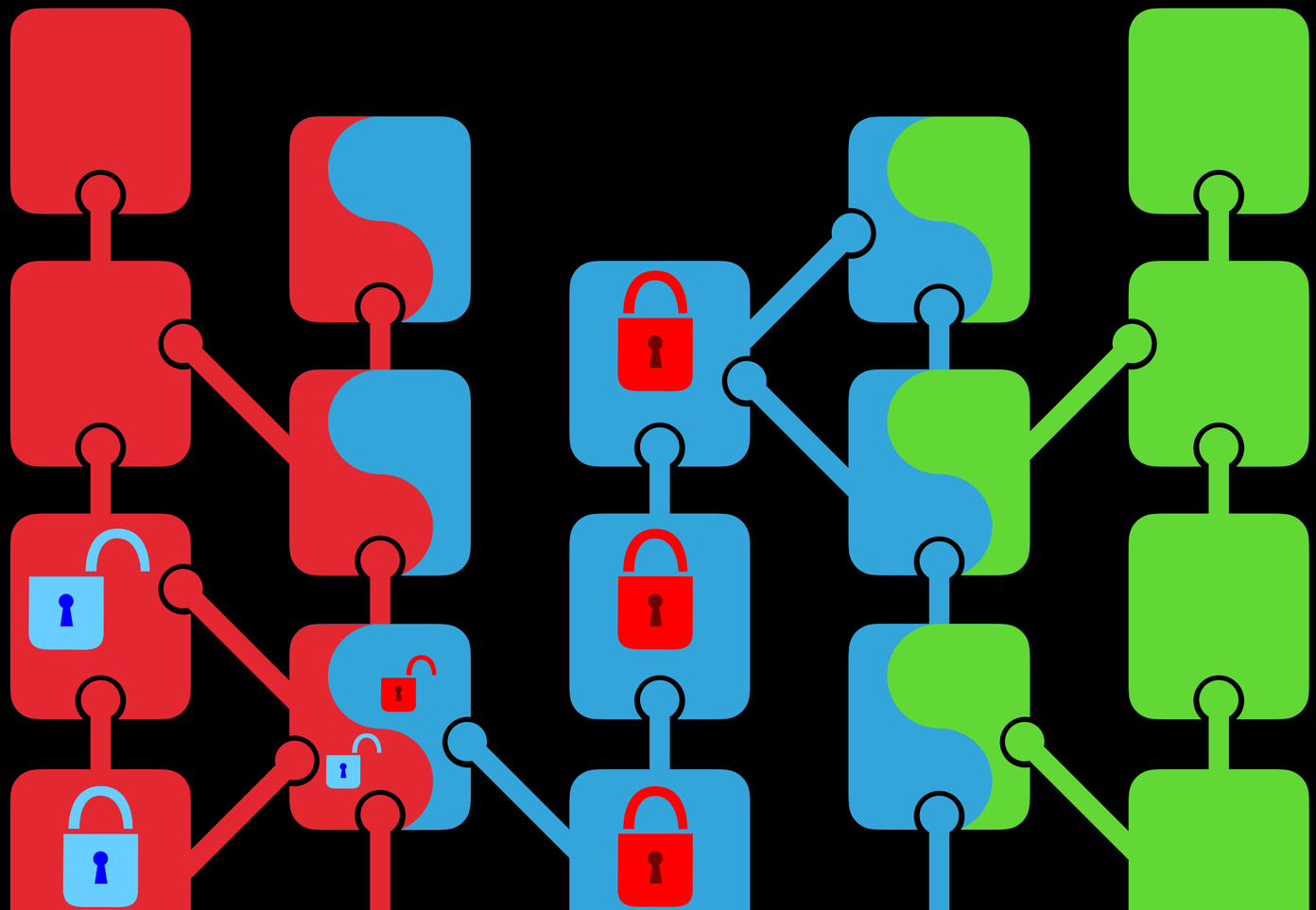
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain



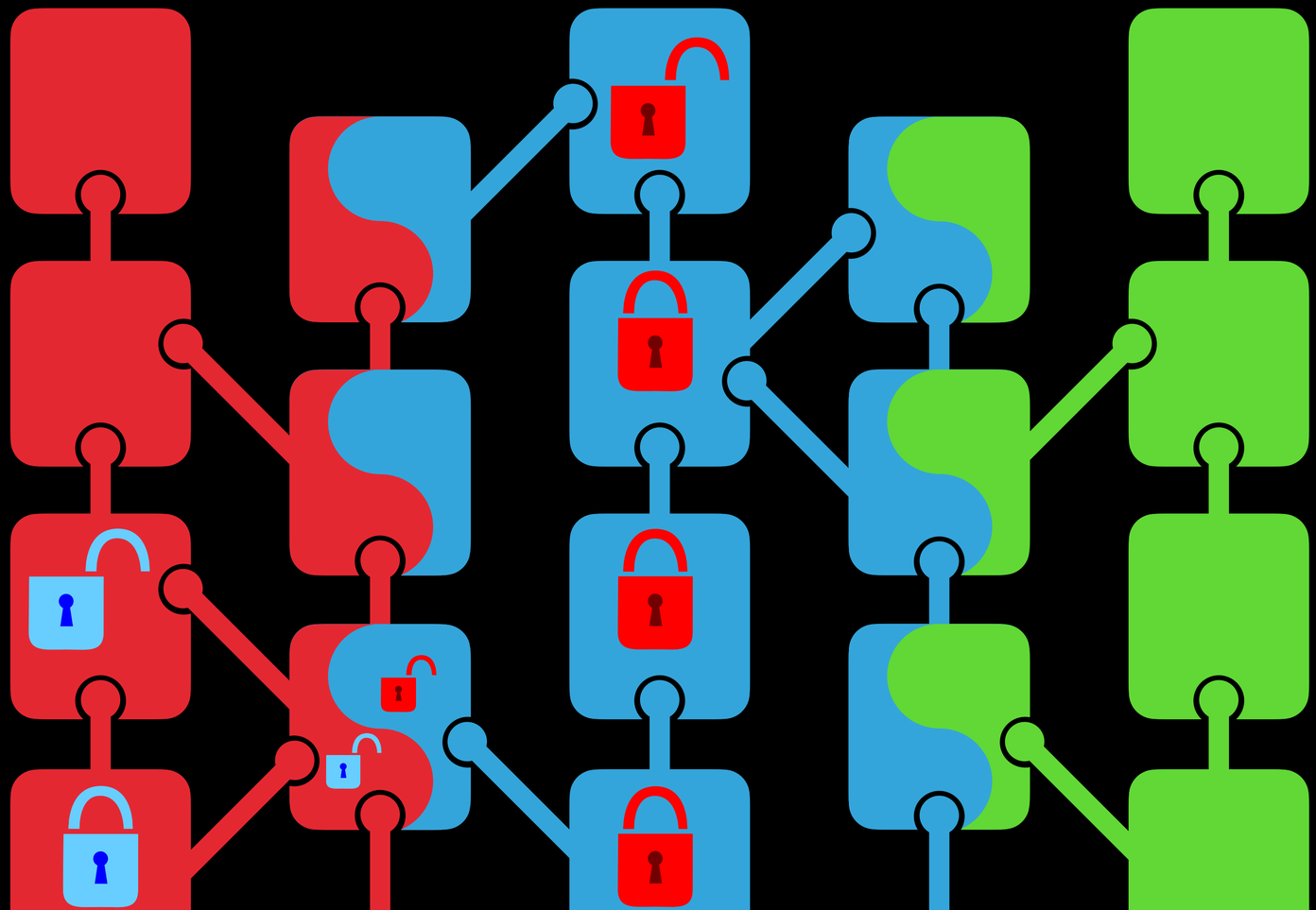
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain



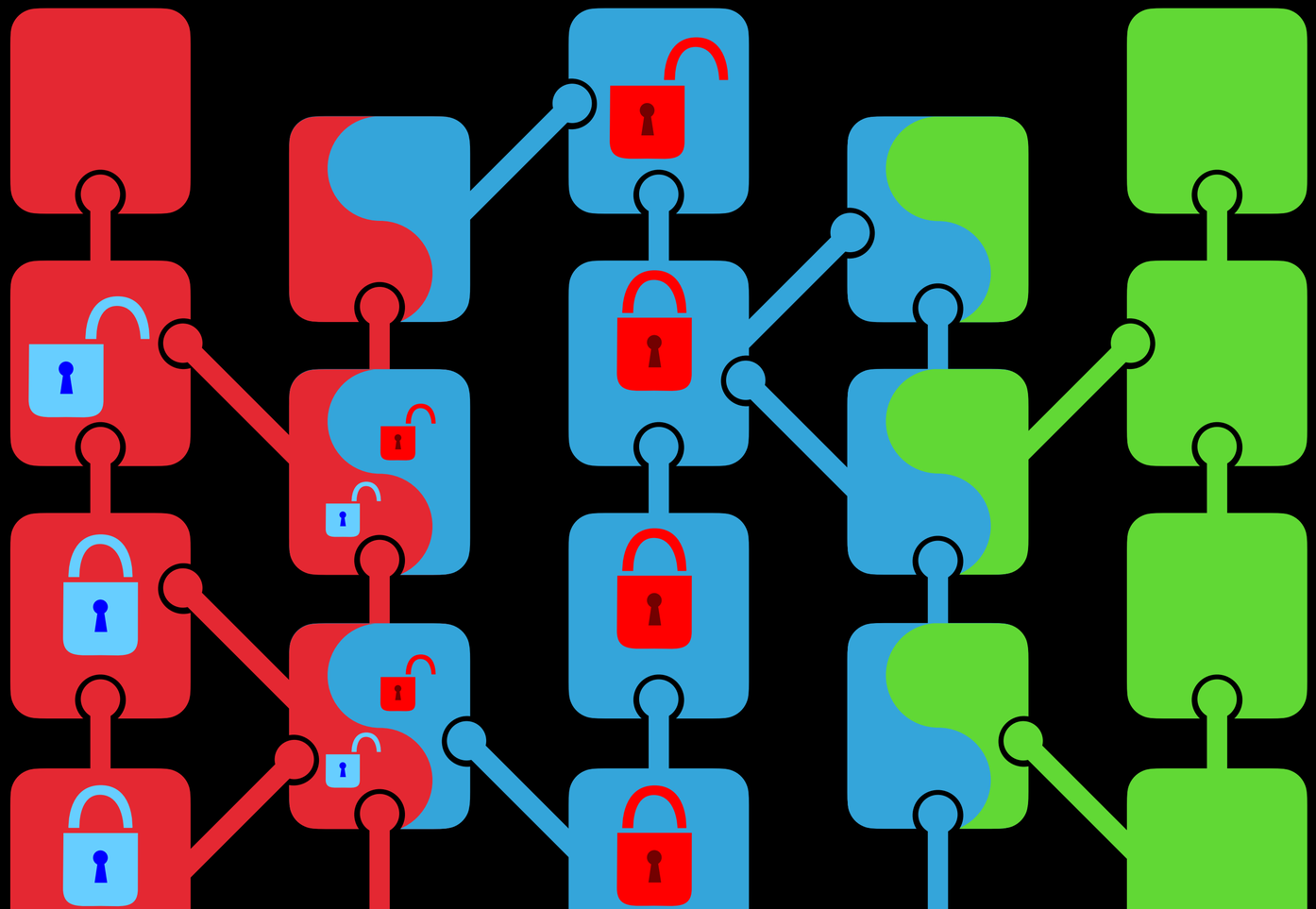
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain
  - Maintains liveness



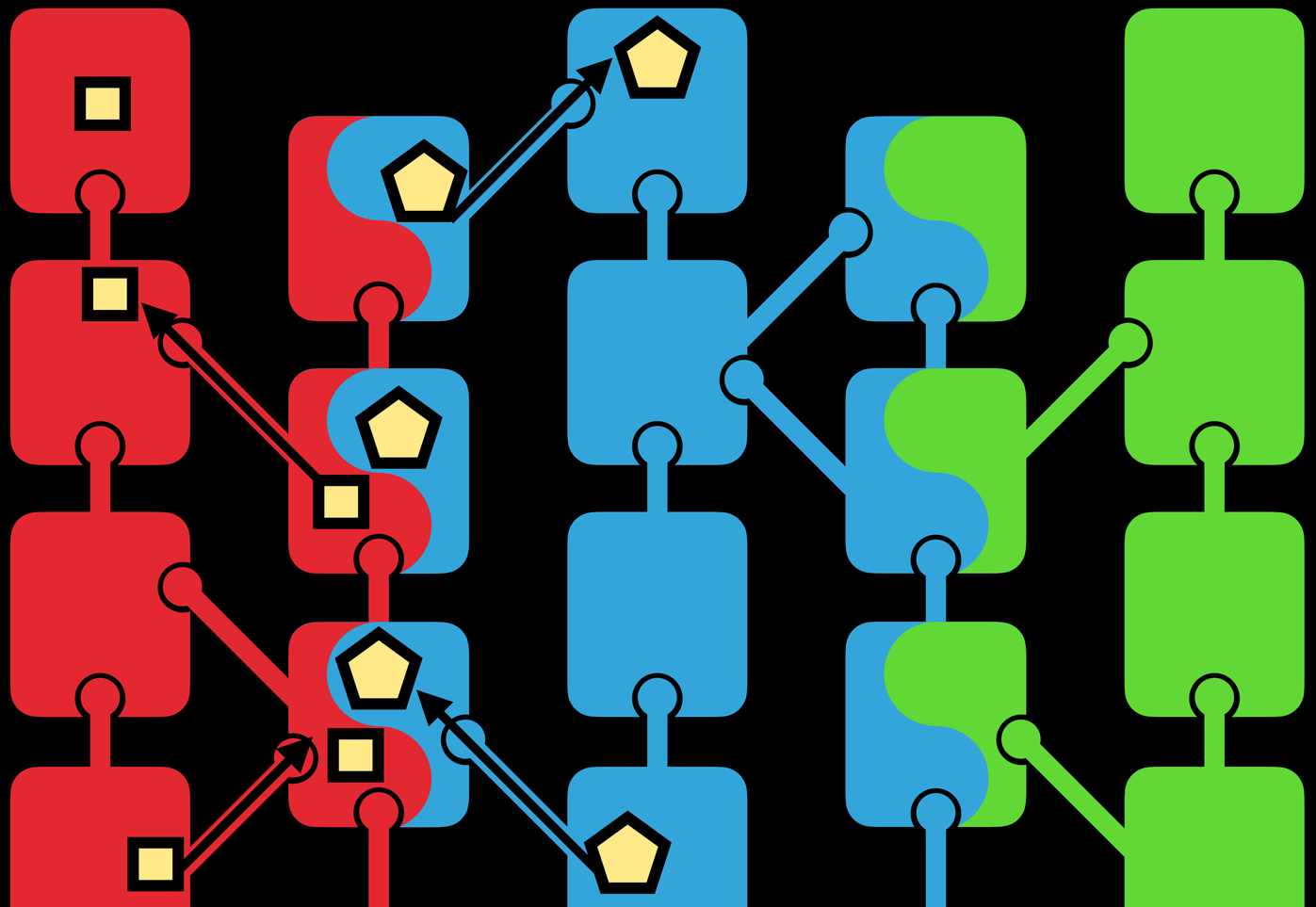
PROGRAMMING MODEL

- Locking State
  - Locks held by chimera chain
  - Maintains liveness
  - Re-usable



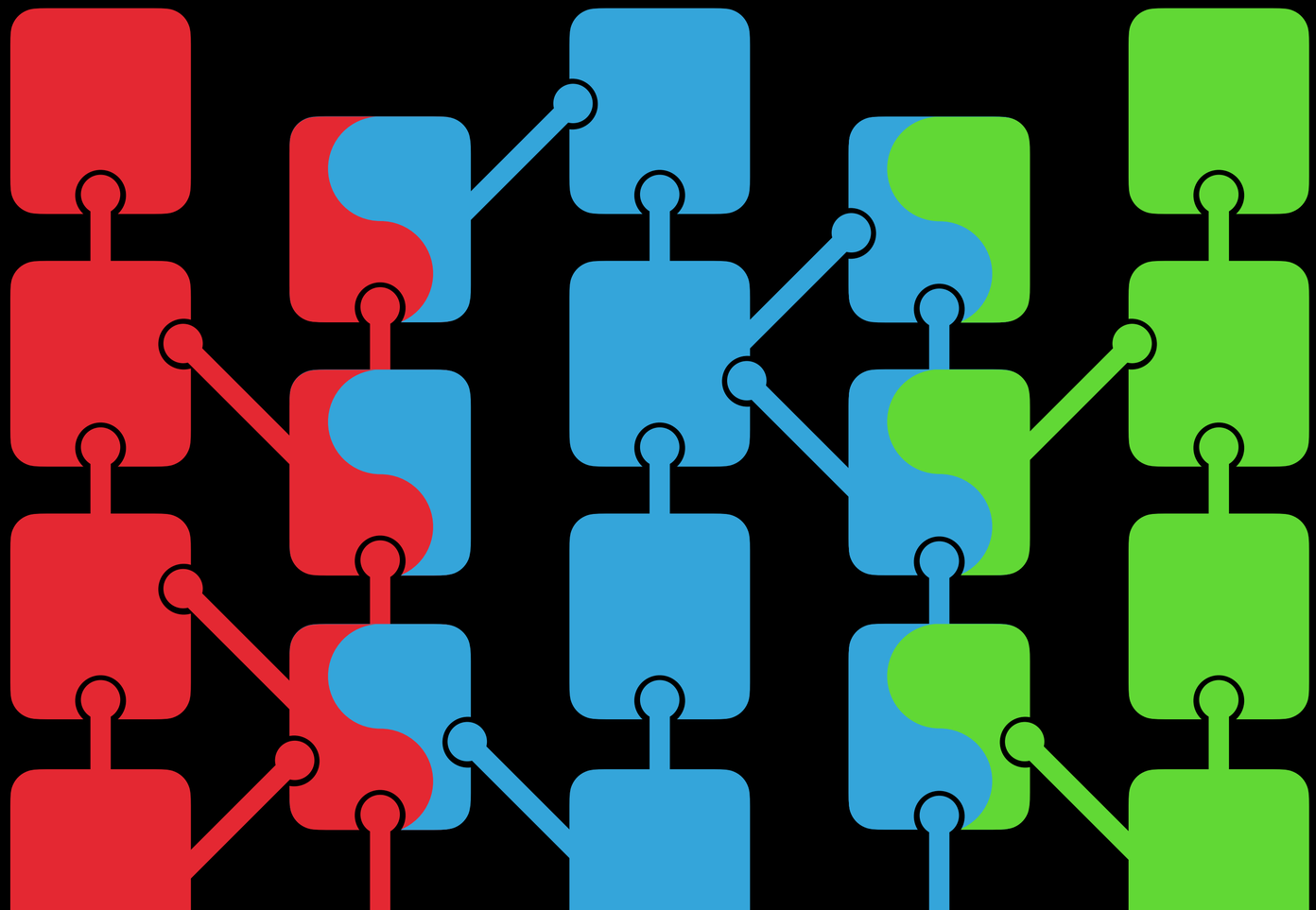
PROGRAMMING MODEL

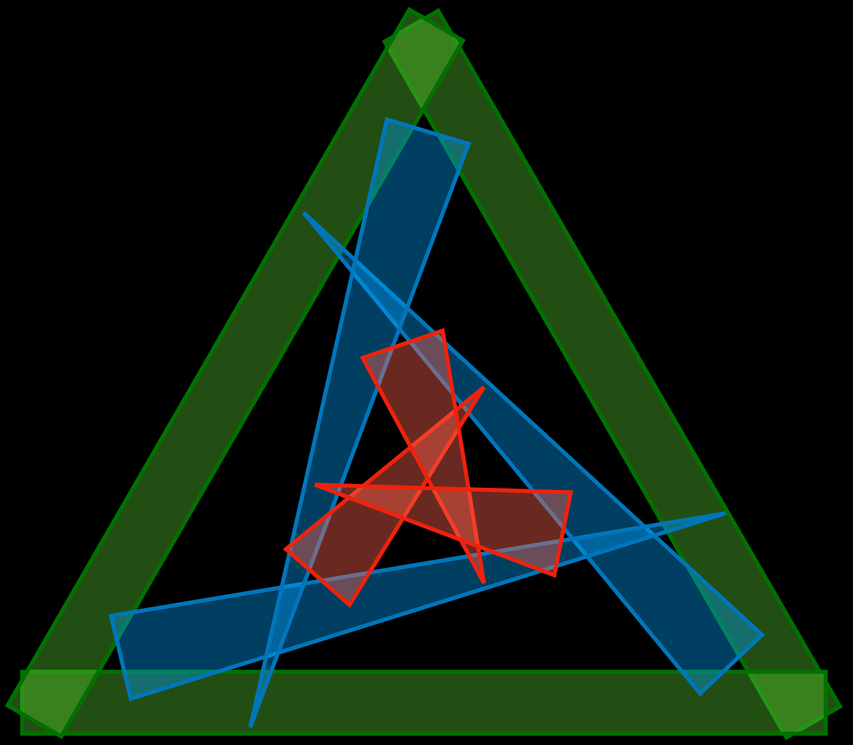
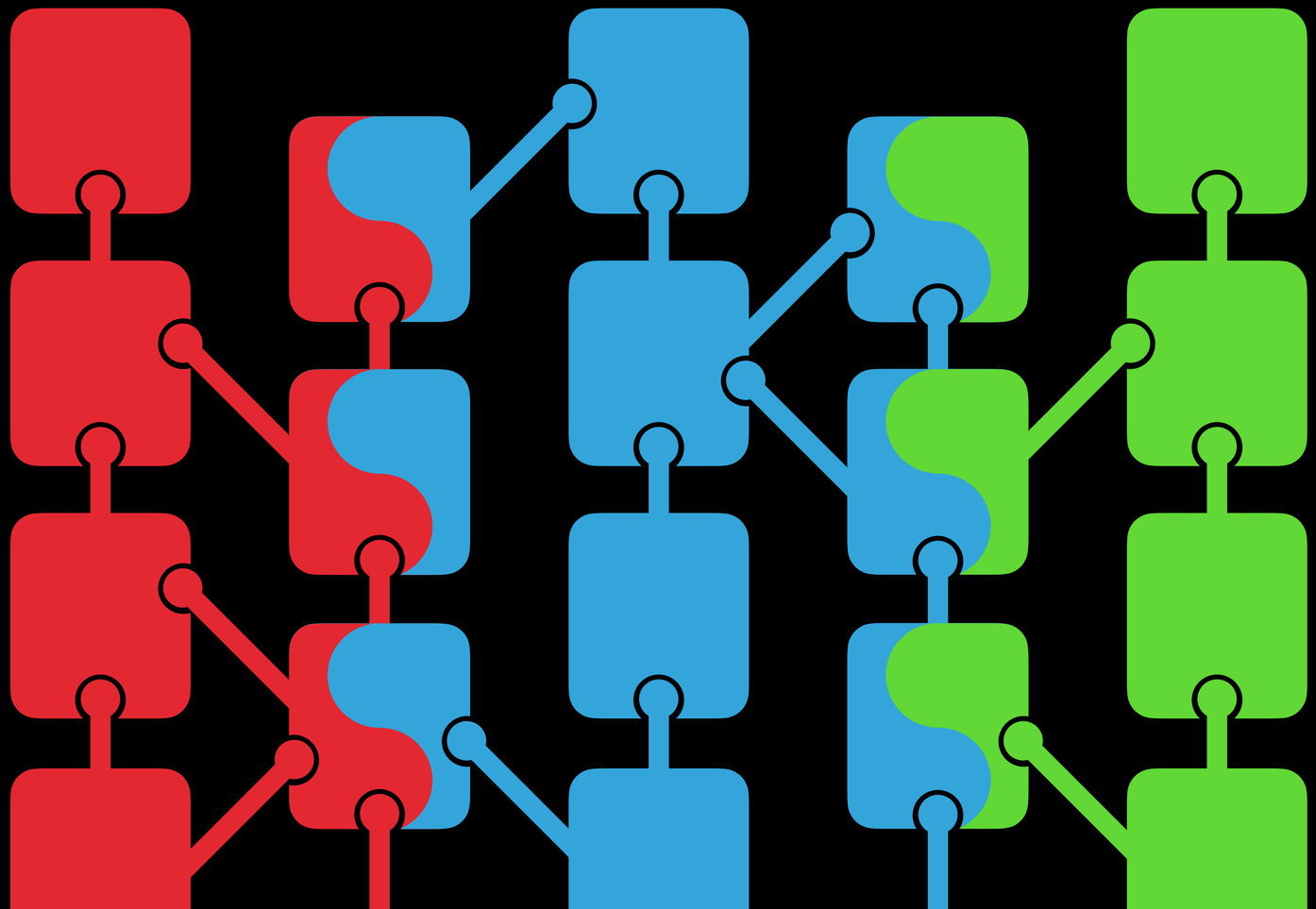
- Locking State
  - Locks held by chimera chain
  - Maintains liveness
  - Re-usable
- Moving Objects
  - Between state machines with same quorums
  - Synchronously (in blocks)



PRACTICAL QUESTIONS

- How to start an on-demand chain?
- Partially synchronous consensus on demand
- Gossiping and assembling atomic transaction bundles



CHIMERA CHAINS: MULTI-BLOCKCHAIN ATOMIC TRANSACTIONS

- No loss of liveness or integrity
- No global ordering
- No global integrity mechanism