SAWTOOTH CONSENSUS ENGINES

ADAM LUDVIK

PRIOR WORK

- Current State:
  - 3 interfaces:
    - BlockPublisher
    - BlockVerifier
    - ForkResolver
  - Polling model

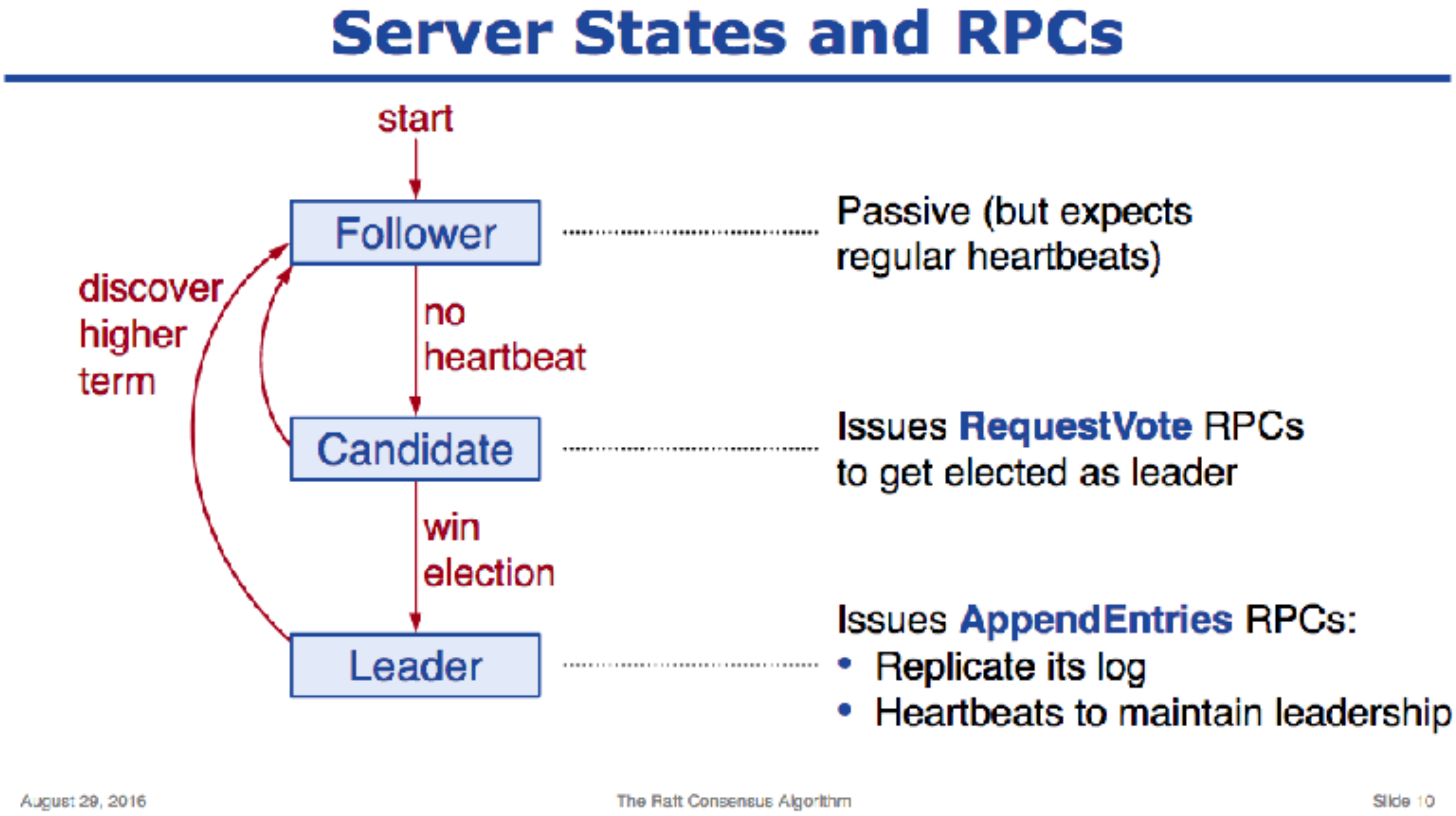
LIMITATIONS OF CURRENT STATE

- “Greedy” block publishing (polled every 0.1 sec)
- Consensus is “reactive”, must wait for poll
    - Invalid PoET wait timers
    - Hard to guarantee liveness
- No mechanism for communicating with peers
- Consensus must be in the same language as the validator and run in the same process
- Tightly coupled with Sawtooth Validator internal structure

CONSENSUS ALGORITHMS ARE STATE MACHINES

- Transitions:
  - Peer messages
  - New block
  - Internal Interrupt

RAFT STATE MACHINE



Server States and RPCs

Passive (but expects regular heartbeats)

Issues **RequestVote** RPCs to get elected as leader

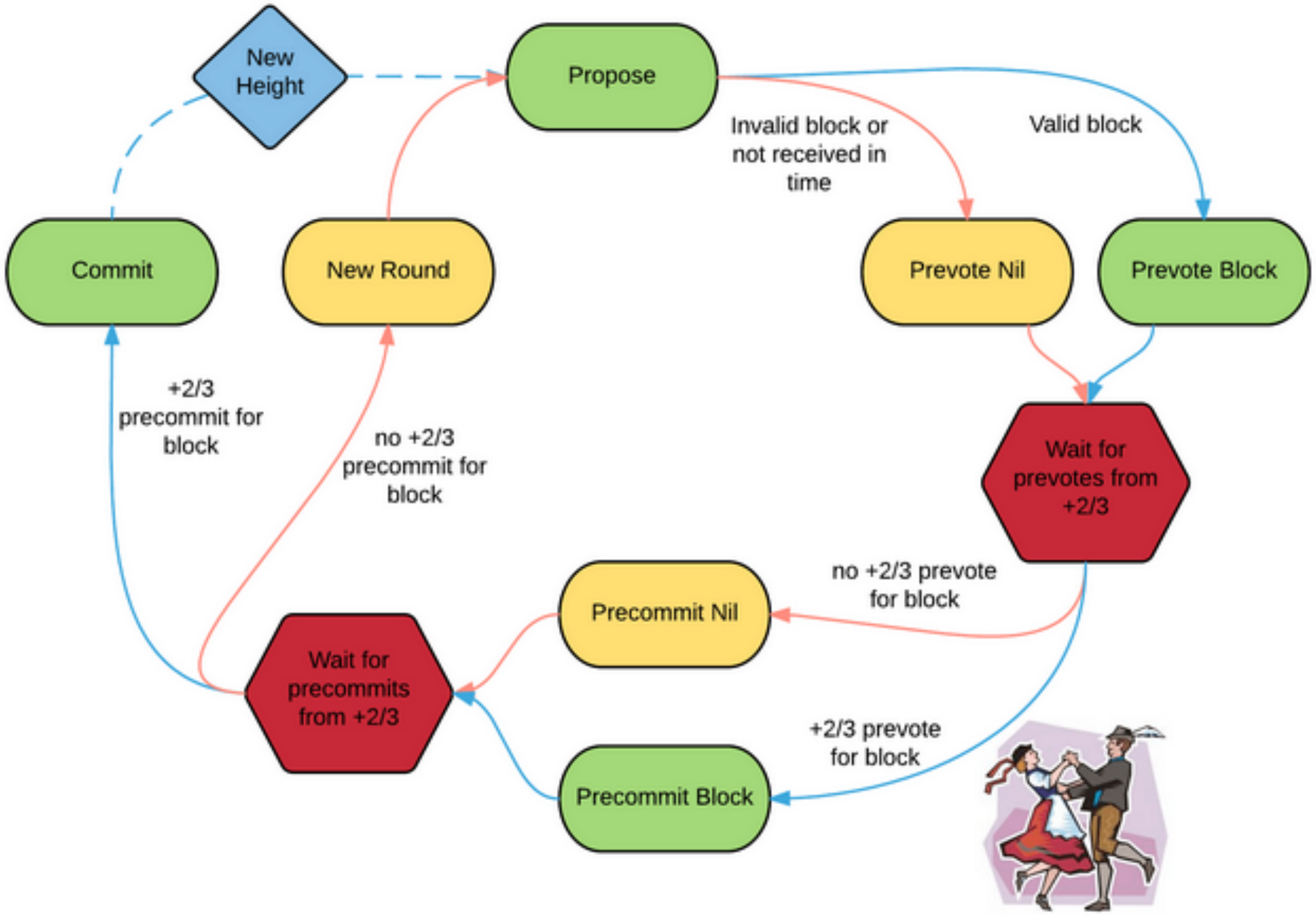
Issues **AppendEntries** RPCs:

- Replicate its log
- Heartbeats to maintain leadership

August 29, 2016 The Raft Consensus Algorithm Slide 10

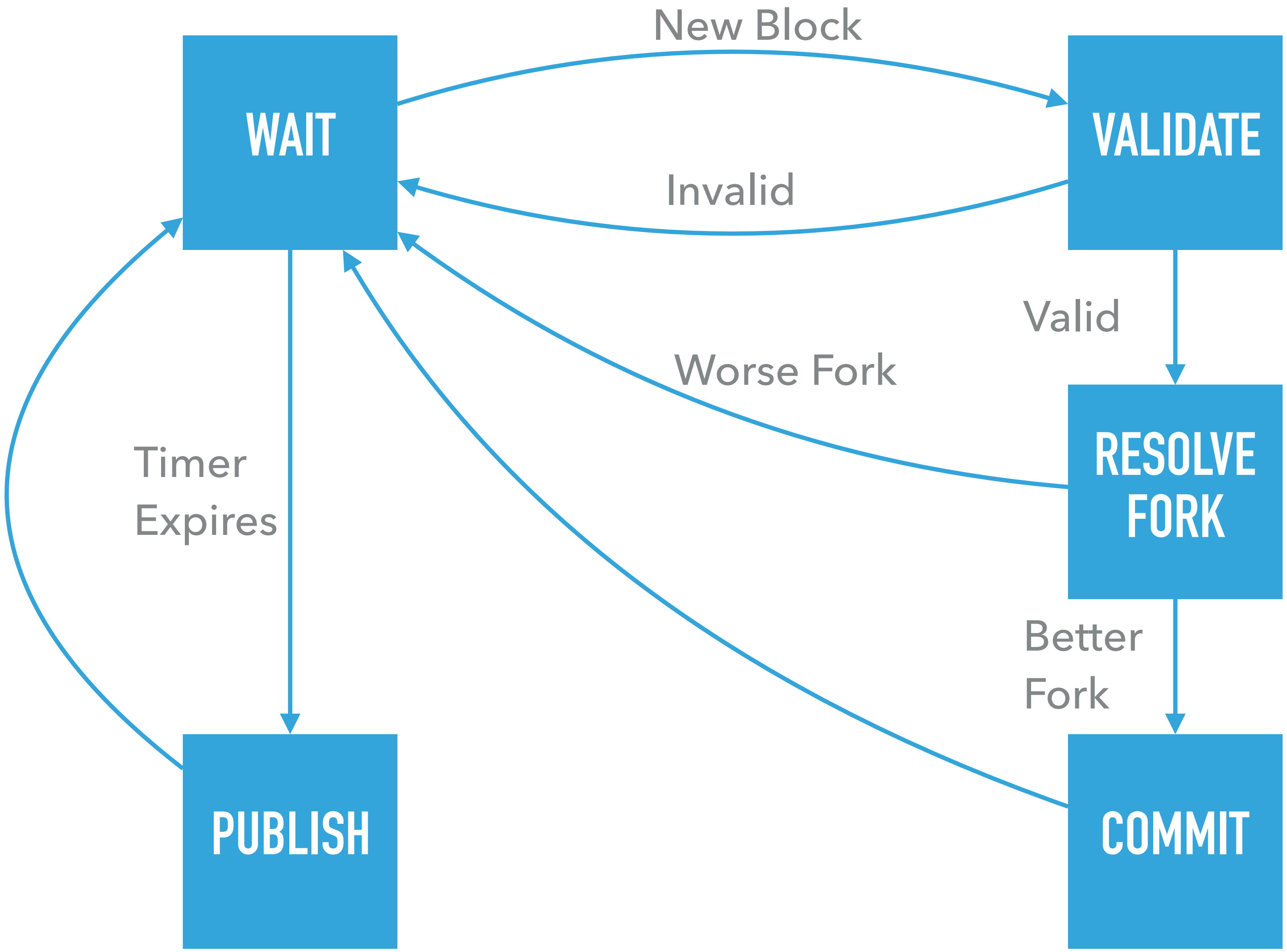
https://raft.github.io/slides/uiuc2016.pdf

TENDERMINT STATE MACHINE


New Height
Propose
Invalid block or not received in time
Valid block
Commit
New Round
Prevote Nil
Prevote Block
+2/3 precommit for block
no +2/3 precommit for block
Wait for prevotes from +2/3
no +2/3 prevote for block
Precommit Nil
Wait for precommits from +2/3
+2/3 prevote for block
Precommit Block

https://tendermint.readthedocs.io/en/master/introduction.html#consensus-overview

POET STATE MACHINE

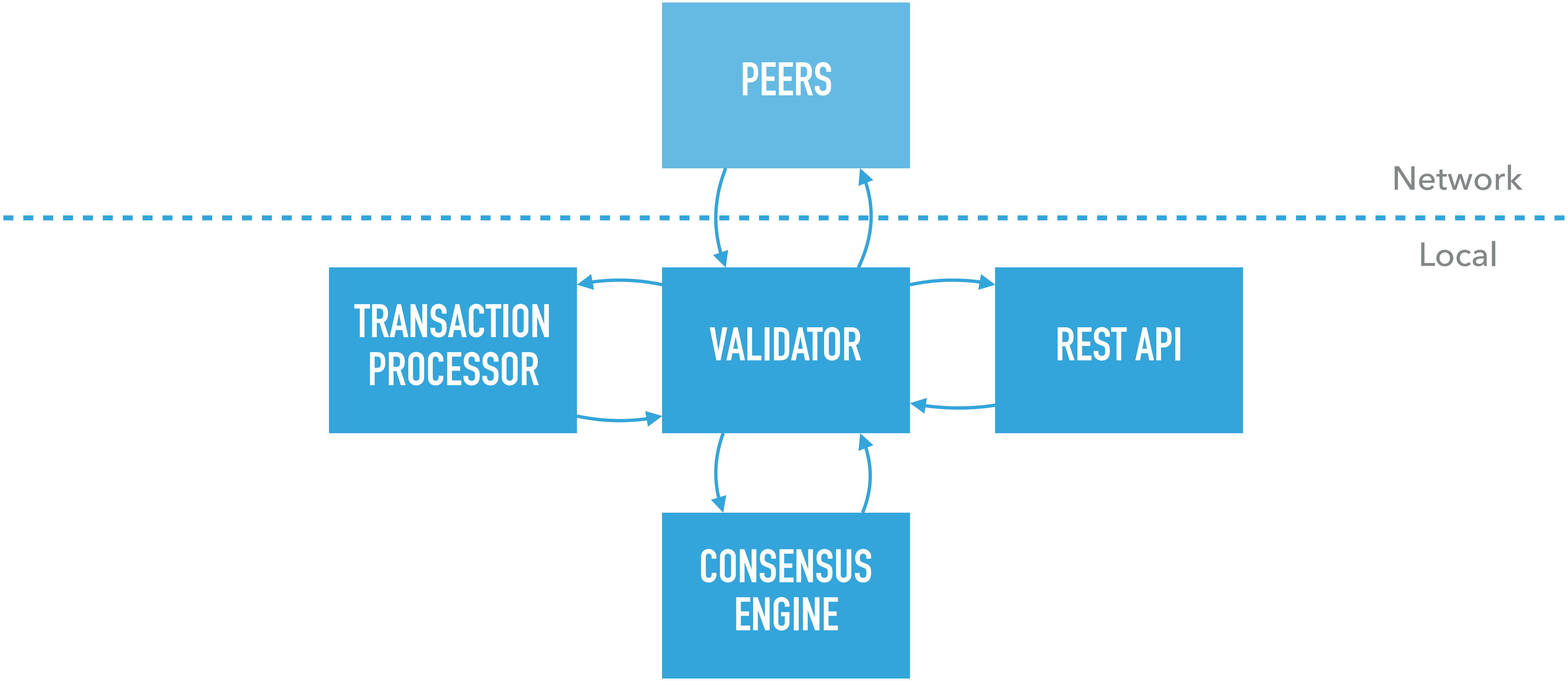


SAWTOOTH VALIDATOR SHOULD FACILITATE CONSENSUS

- Provide **updates** that are relevant to consensus
- Provide **services** that are required by consensus
  - P2P networking
  - Batch validation
  - Signature verification
  - Fork management

CONSENSUS SHOULD DRIVE

- Most correct component to be making decisions
- Choose when to do expensive full validation of blocks
  - Fork resolution *before* block validation
- Choose when and which blocks to commit
- Choose when to publish blocks
  - Whenever sensible instead of whenever possible


PEERS
Network
Local
TRANSACTION PROCESSOR
VALIDATOR
REST API
CONSENSUS ENGINE

CONSENSUS ENGINE API

- Language agnostic protobuf messages:
  - Data Structures
  - Update messages (Notify/Ack)
  - Service messages (Request/Response)

CONSENSUS ENGINE SDKS

- Language specific abstractions
  - Rust
  - Python
- Encapsulates message encoding and passing

RUST SDK WALKTHROUGH