

SAWTOOTH CONSENSUS ENGINES

ADAM LUDVIK

PRIOR WORK

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

LIMITATIONS OF CURRENT STATE

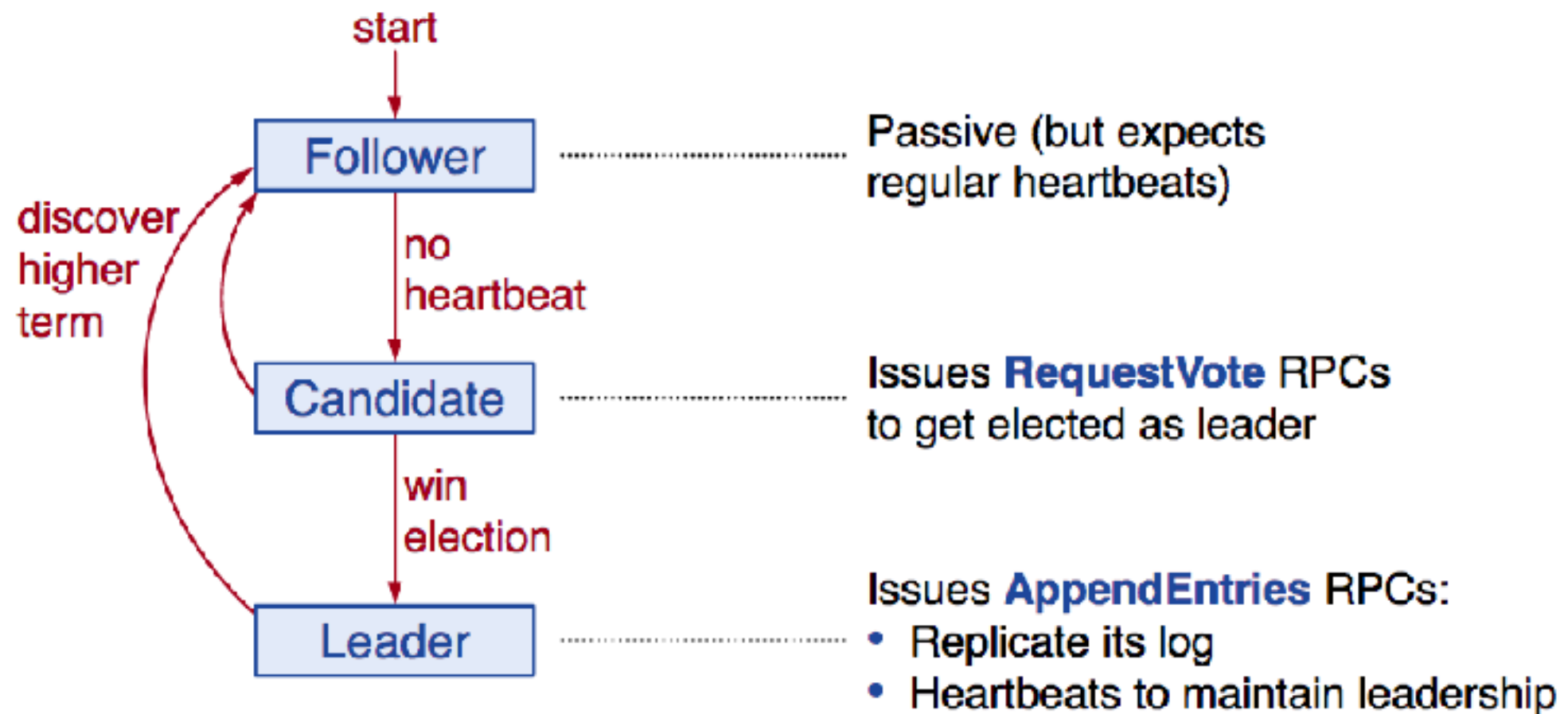
- ▶ “Greedy” block publishing (polled every 0.1 sec)
- ▶ Consensus is “reactive”, must wait for poll
 - ▶ Invalid PoET wait timers
 - ▶ Hard to guarantee liveness
- ▶ No mechanism for communicating with peers
- ▶ Consensus must be in the same language as the validator and run in the same process
- ▶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

CONSENSUS ALGORITHMS ARE STATE MACHINES

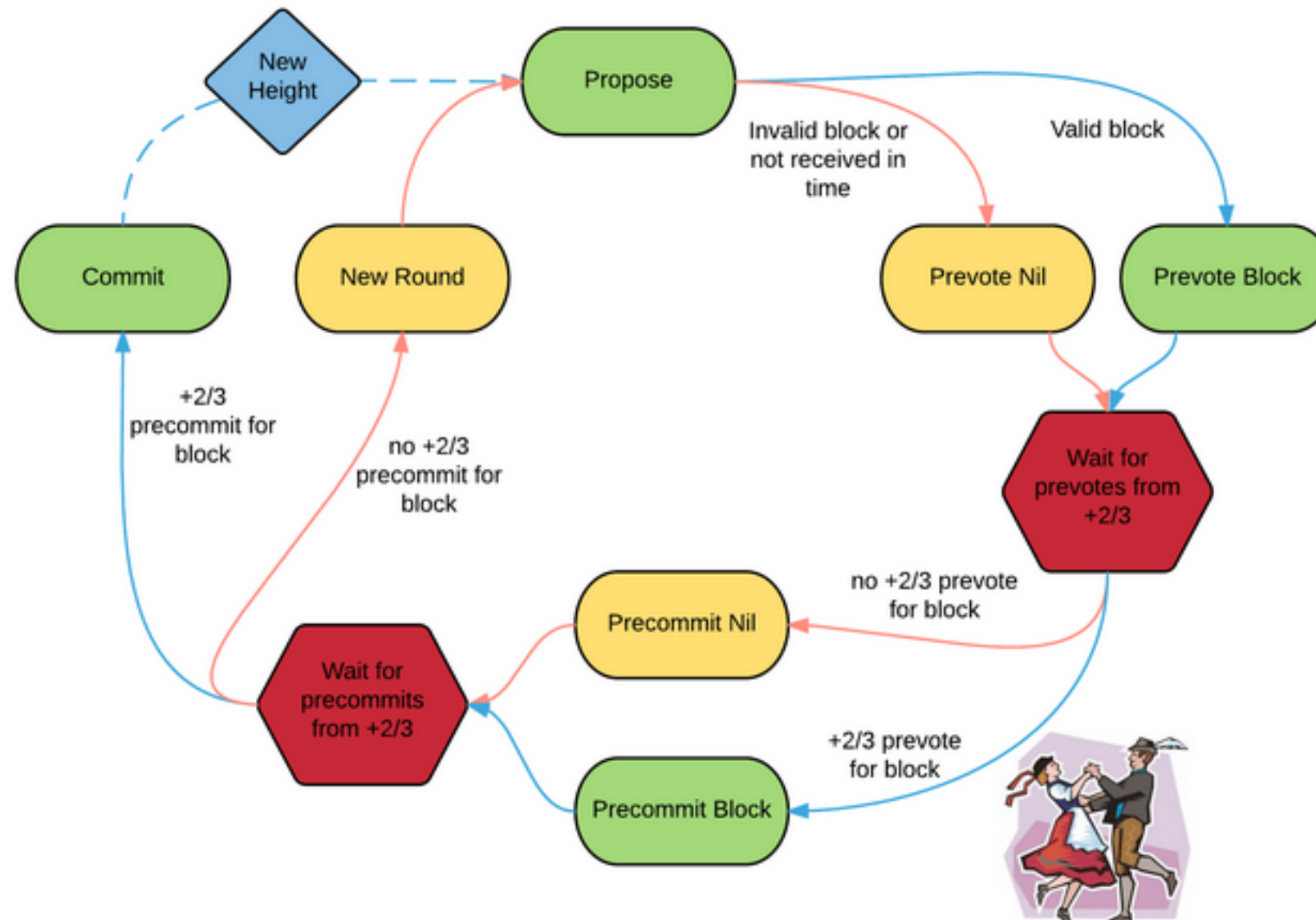
- ▶ Transitions:
 - ▶ Peer messages
 - ▶ New block
 - ▶ Internal Interrupt

RAFT STATE MACHINE

Server States and RPCs

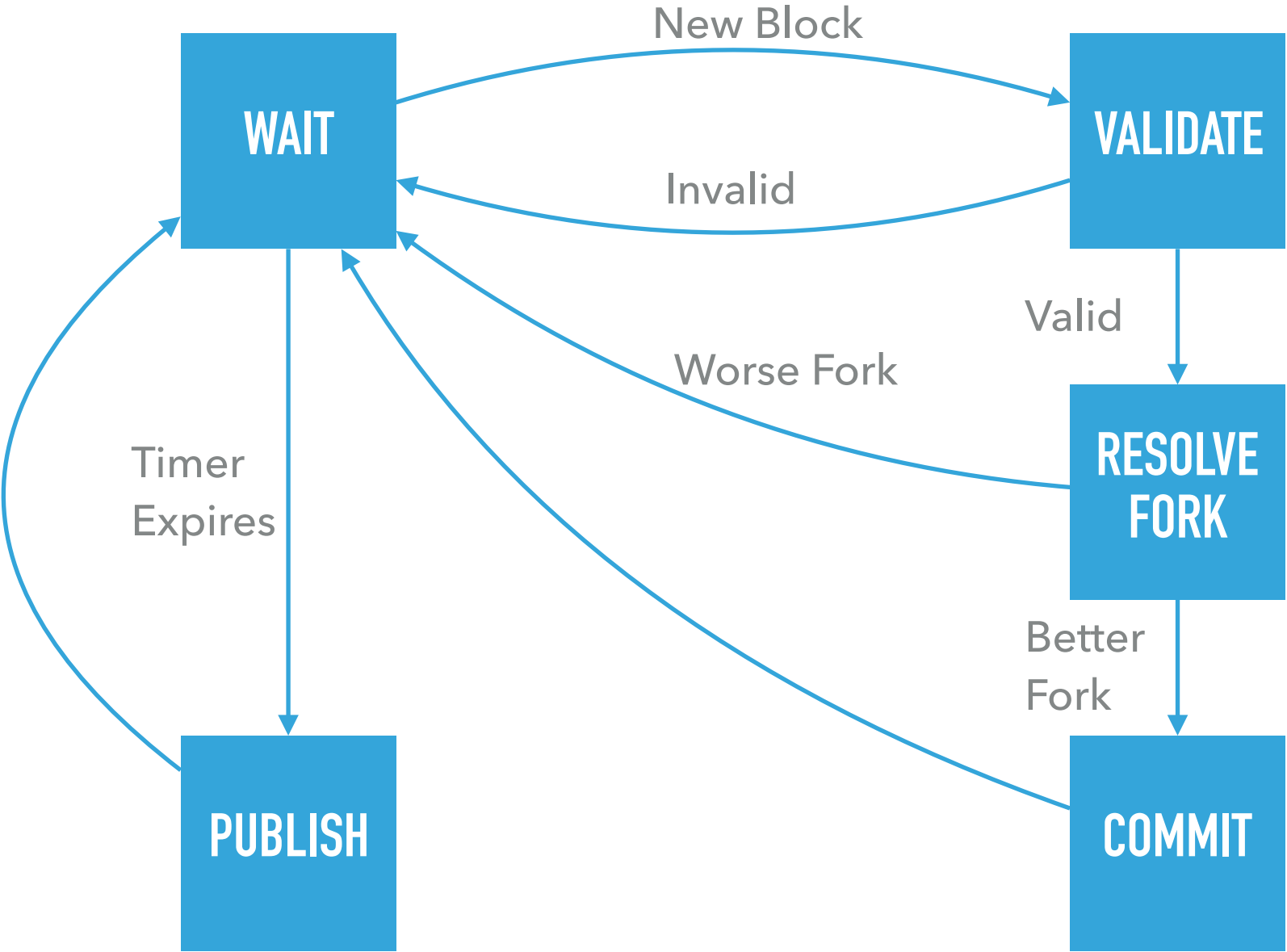


TENDERMINT STATE MACHINE



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

POET STATE MACHINE



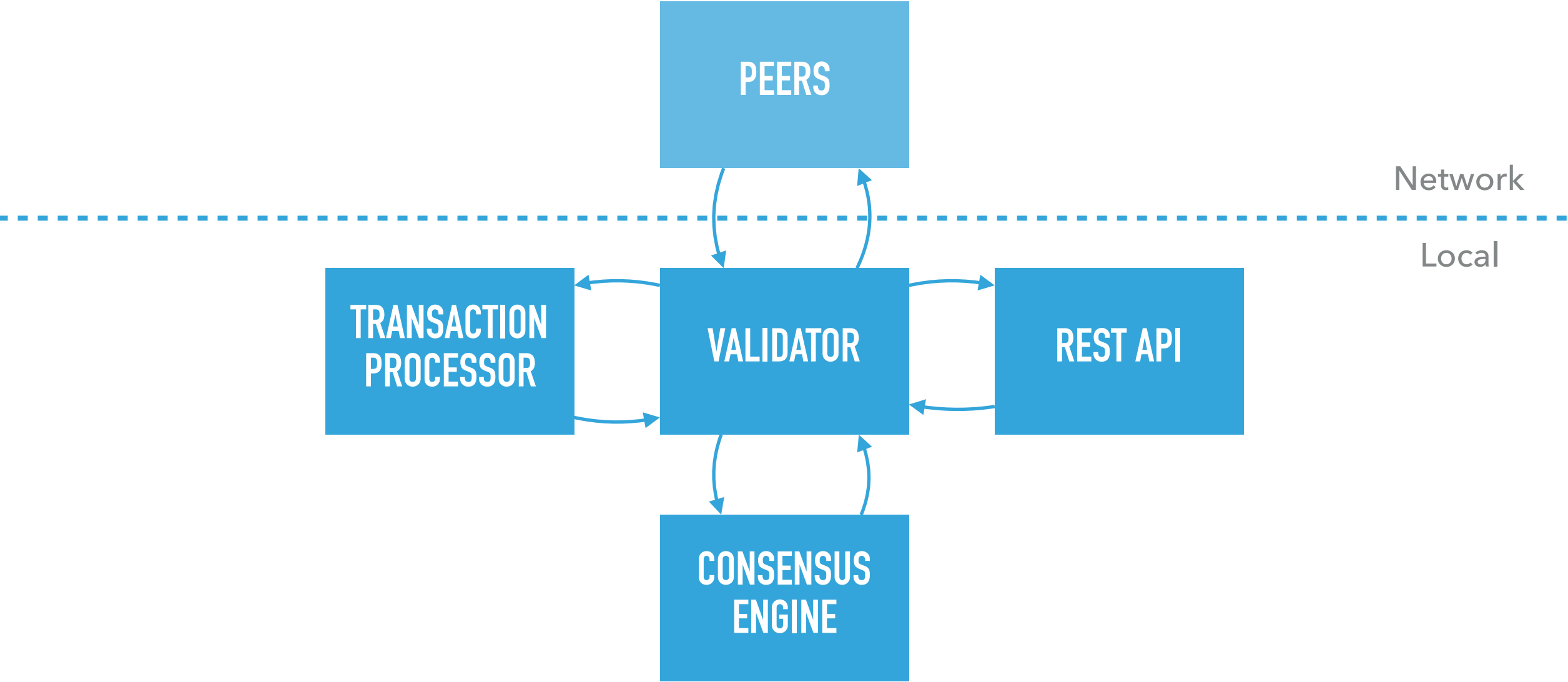
SAWTOOTH VALIDATOR SHOULD FACILITATE CONSENSUS

- ▶ 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

- ▶ In best position to make decisions
- ▶ Limit expensive full-validation of blocks
 - ▶ Fork resolution *before* block validation
- ▶ Decide when to commit
- ▶ Decide when to publish
 - ▶ Whenever sensible, not whenever possible

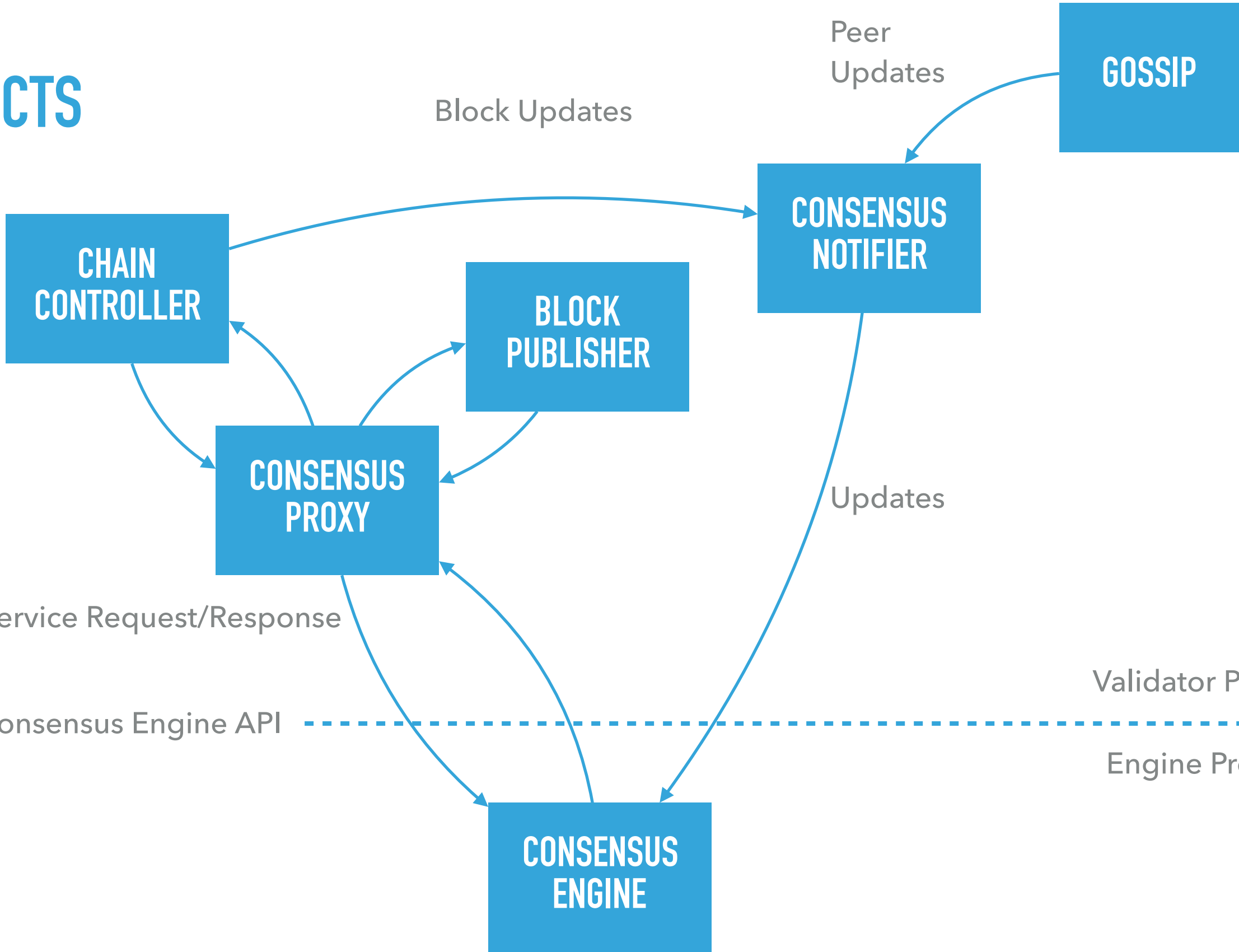
NETWORK / IPC



CONSENSUS ENGINE API

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

OBJECTS



CONSENSUS ENGINE SDKS

- ▶ Language specific abstractions
 - ▶ Rust
 - ▶ Python
- ▶ Encapsulates message encoding and handling

Application SDK

Consensus SDK

Transaction Processor

Driver

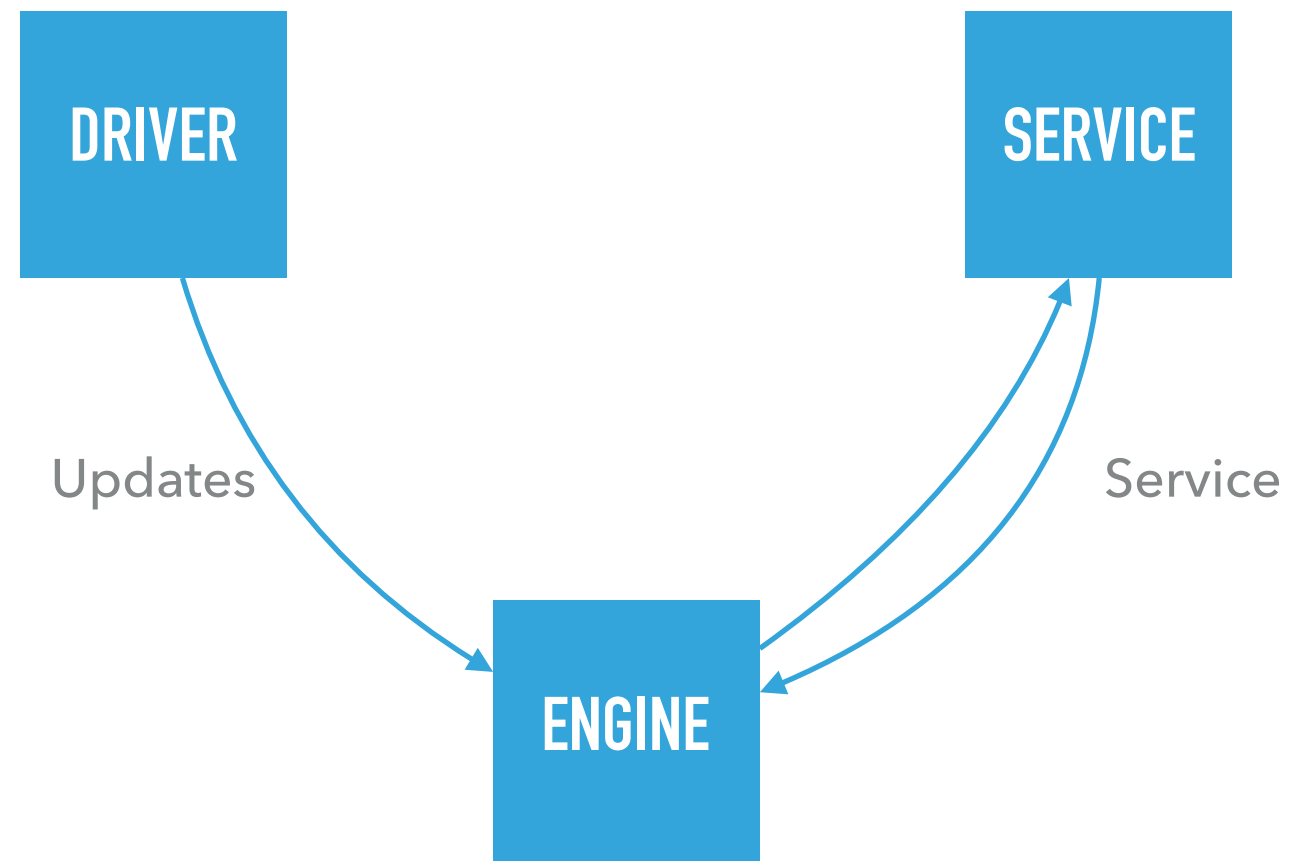
Transaction Handler

Engine

Execution
Context

Service

CONSENSUS SDK



CONSENSUS SERVICES PROVIDED

▶ P2P Messaging

- ▶ SendTo
- ▶ Broadcast

▶ Block Creation

- ▶ InitializeBlock
- ▶ FinalizeBlock
- ▶ CancelBlock

▶ Block Directives

- ▶ CheckBlock
- ▶ CommitBlock
- ▶ IgnoreBlock
- ▶ FailBlock

▶ Queries

- ▶ BlocksGet
- ▶ SettingsGet
- ▶ StateGet

CONSENSUS NOTIFICATIONS PROVIDED

▶ **Peer Updates**

- ▶ Connected
- ▶ Disconnected
- ▶ New Message

▶ **Block Updates**

- ▶ New Block
- ▶ Block Valid
- ▶ Block Invalid
- ▶ Block Committed

RUST SDK WALKTHROUGH