Blockchain consensus abstractions

Peter Czaban
peter@parity.io
Replicated state machine

- Replicas
- State
- State transition rules
- Instructions
- Primary
Sealing
Chain without consensus

- Transaction submission
- Transaction broadcast
- Block building
- Block broadcast
- Block verification
Transaction submission
Transaction broadcast
Block building
Block broadcast
Block verification
Parity implementation

- Standard Ethereum RPC interface
- 2000 tx/s
- Low footprint
- Robust networking
- Chain specification in json format
Consensus Engine abstraction

- Header seal generation
- Header seal verification
- Chain scoring rule

Additional:

- Block sealing trigger
- Proposal stashing
- Message broadcast and handling
- Additional transaction verification
- Additional state handling at open or close
Common features

- Generated header is accepted by all
- It is eventually possible to generate a header
- There is an eventual ordering over valid chains
- Views are changed on every block
Chain scoring

- PoW: difficulty
- Height chain scoring: height
- Popular chain scoring: $\text{const} \times \text{height} + \text{length(signers)}$
Current Engine implementations

- Ethash
- Null Engine
- Instant Seal
- Basic Authority
- Authority Round
- Tendermint
- Abab
Null Engine
Instant Seal
Instant Seal
Validator engines

- Basic Authority
- Authority Round
- Tendermint
- Abab
Validator set abstraction

- Membership check
- Draw based on nonce
- Total count

Optional:

- Report malicious behaviour
- Report benign misbehaviour
Validator set

- Immutable
- Part of state

contract ValidatorSet {

    function getValidators() returns (address[]) {}

    function reportMalicious(address validator) {}

    function reportBenign(address validator) {}

}
Stateful validator set

- Majority support
- Proof of Stake
Validator reporting

- Engine decides when
- Slashing, kicking, call to action
- Rejecting blocks without report
Basic Authority
Authority Round and Ethash
Authority Round partition

View = 1
Authority Round partition

View = 2
Authority Round partition

View = 3
Authority Round partition

View = 4
Authority Round partition

View = 4
Authority Round partition

View = 5
Authority Round partition

View = 5
Tendermint

Propose -> Prevote -> Precommit -> Commit
Failure with chain scoring

View = v
Failure with chain scoring

\[
\text{View} = v + 1
\]
Failure with chain scoring
Abab

- Maintains safety
- Improves speed / bandwidth
- Inspired by Zyzzyva and Aardvark
Abab

1. Primary issues a proposal
2. Replica responds with a vote
3. After $\frac{2}{3}$ of votes are gathered the block is committed
Abab

1. Primary issues a proposal
2. Replica did not receive a valid proposal within timeout
3. Replica issues a view change message
4. Next primary receives $\frac{1}{3}$ view changes
5. Next primary issues a proposal with new view signatures
Future directions

- Validator set contract implementations
- Various chain scoring + consensus implementations
- Threshold signatures
- Other state machines
- Extending the interface
Implement your own

- Messaging and seal format
- Internal state machine
- Chain scoring
- Validator set modification rules