ETHEREUM SHARDING

2018.02 郭世清

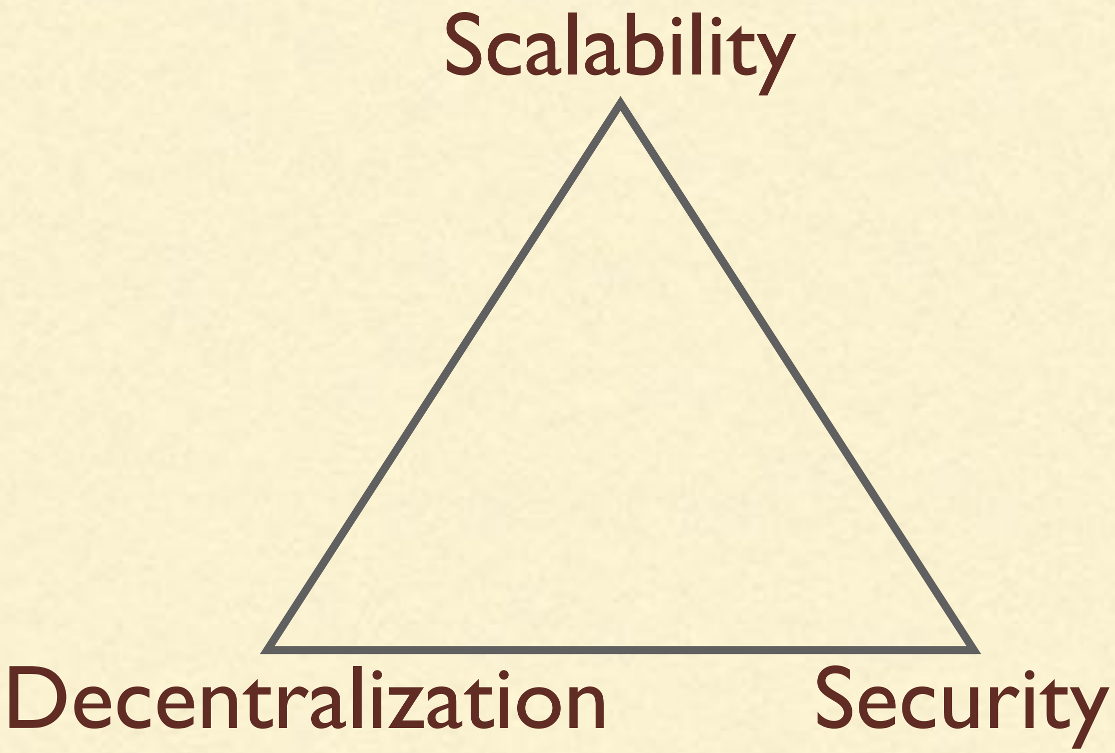
目录

- 挑战
- 基本设计
- 分叉选择
- 路线

- Ethereum的挑战

- 安全（共识、智能合约）
- 隐私
- 扩展性

- 扩展性挑战



- 链下

  Raiden、Plasma

- 链上

  Sharding

- 其他

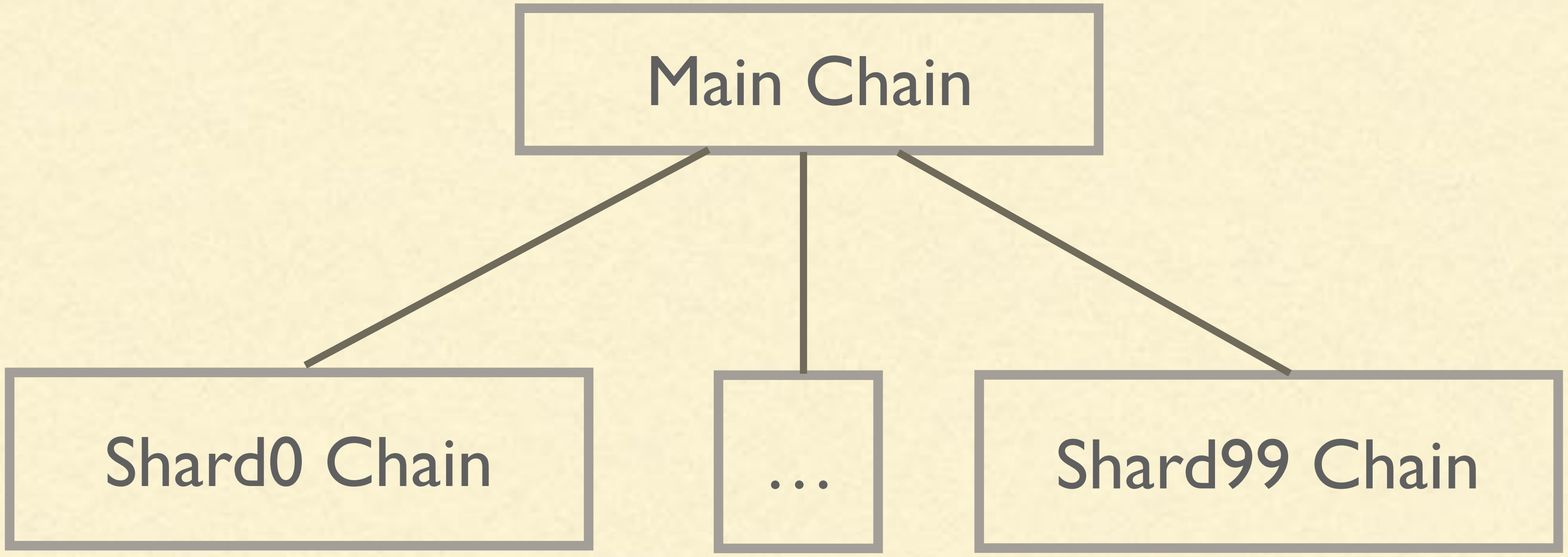
  大区块、超级节点、多链

- 术语

- State
- Transcation
- Receipt
- History
- Merkle Tree
- State Root
- State Transition Function
- Light Client

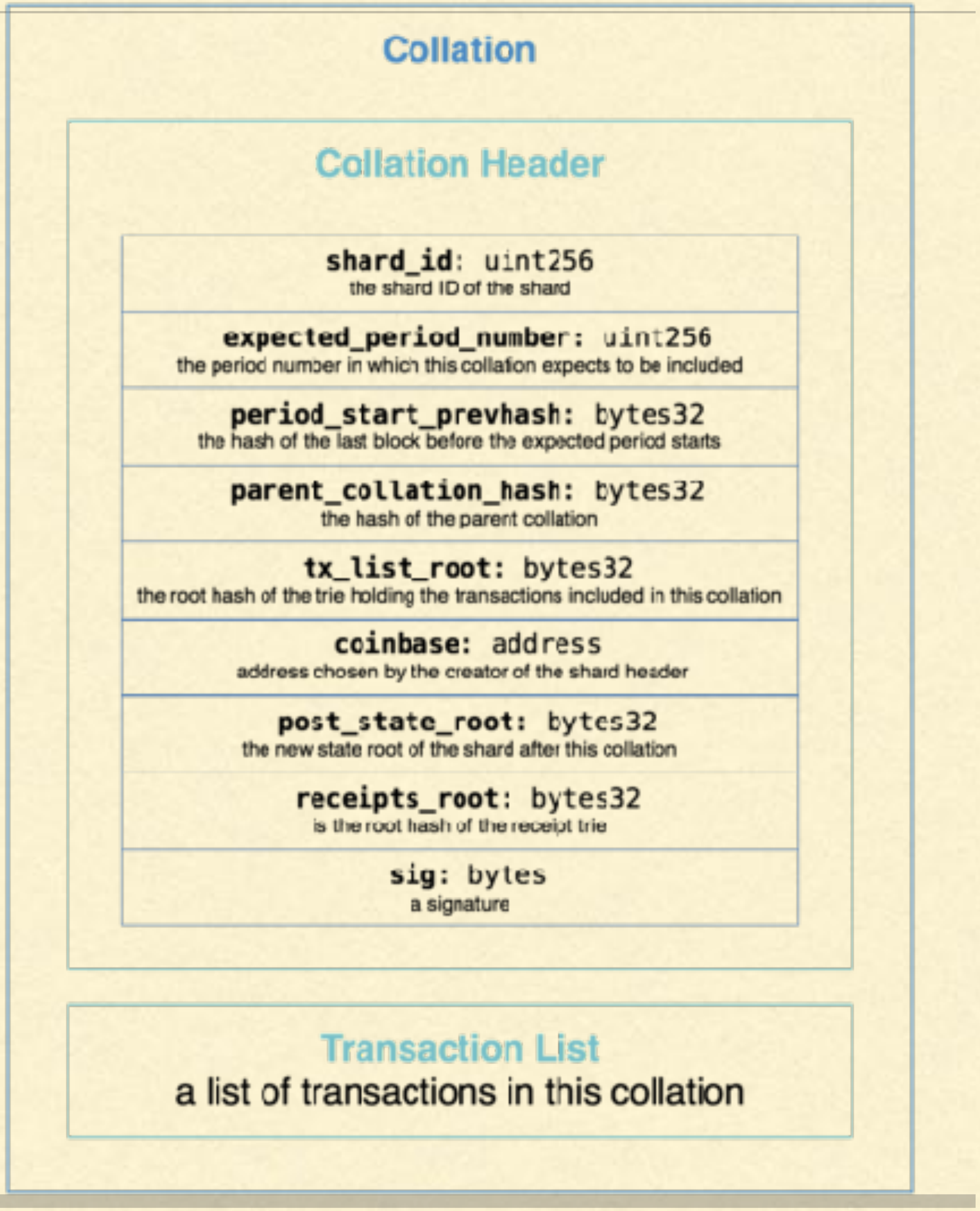
- 基本设计

- 状态分片
- 二次分片
- POS
- Validator Manager Contract



- 基本概念

Main Chain	Shard Chain
Block	Collation
BlockHeader	CollationHeader
Miner	Callator



Collation

Collation Header

shard_id: uint256
the shard ID of the shard

expected_period_number: uint256
the period number in which this collation expects to be included

period_start_prevhash: bytes32
the hash of the last block before the expected period starts

parent_collation_hash: bytes32
the hash of the parent collation

tx_list_root: bytes32
the root hash of the trie holding the transactions included in this collation

coinbase: address
address chosen by the creator of the shard header

post_state_root: bytes32
the new state root of the shard after this collation

receipts_root: bytes32
is the root hash of the receipt trie

sig: bytes
a signature

Transaction List
a list of transactions in this collation

- 基本概念

Super-full node	处理所有的交易，并维护状态
Top-level node	处理所有的Block，不处理分片的Collation
Single-shard node	Top-level node，同时处理某个Shard的交易与维护状态
Light node	验证BlockHeader，读取特定Shard的状态

Validator Manager Contract

- deposit(address validationCodeAddr, address returnAddr) returns uint256

  validationCodeAddr满足purity-verified

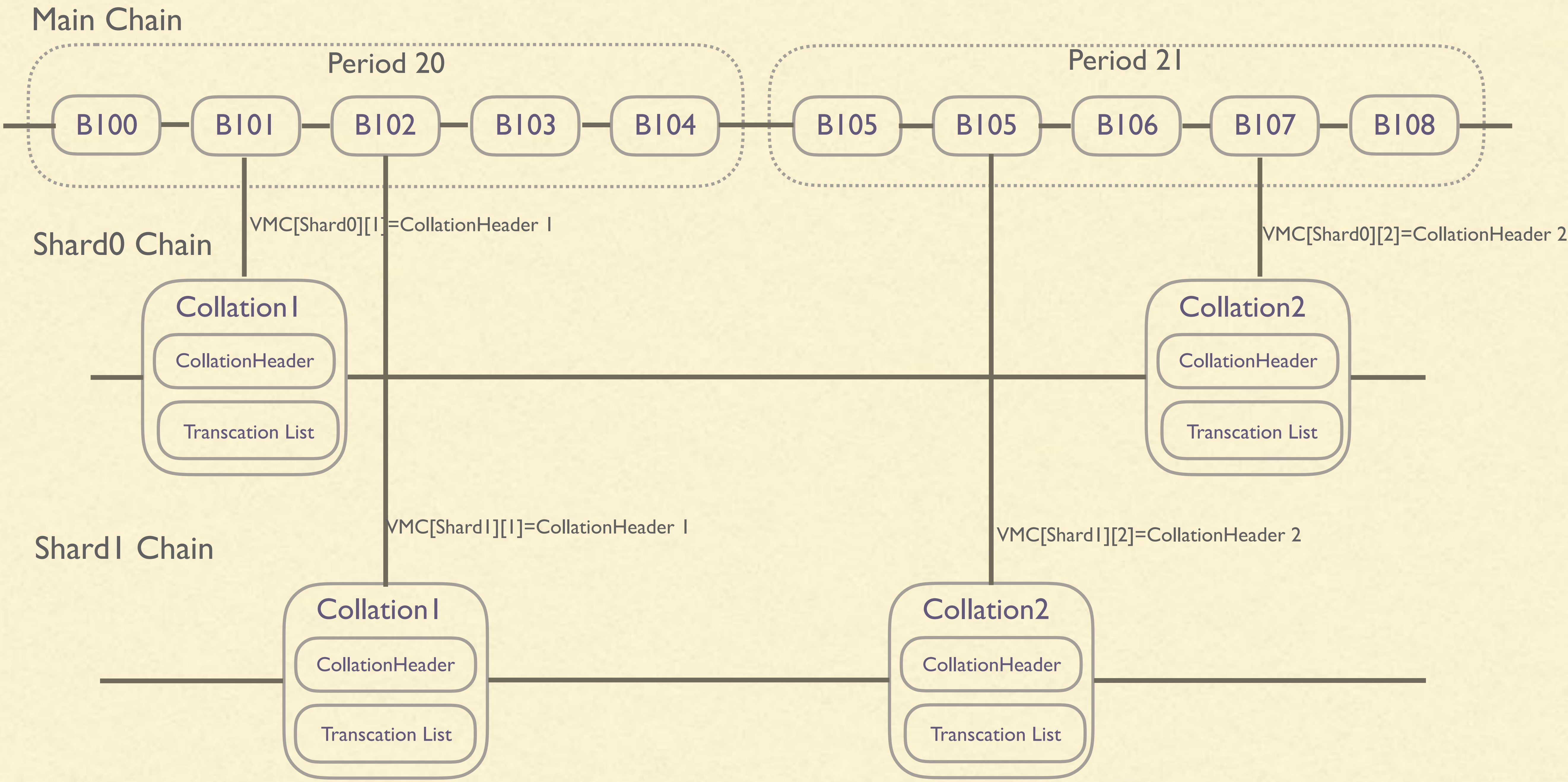
- withdraw(uint256 validatorIndex, bytes sig) returns bool
- getEligibleProposer(uint256 shardId, uint256 period) returns address

  BlockHash伪随机种子，与保证金成比例

- addHeader(bytes header) returns bool

  链上验证

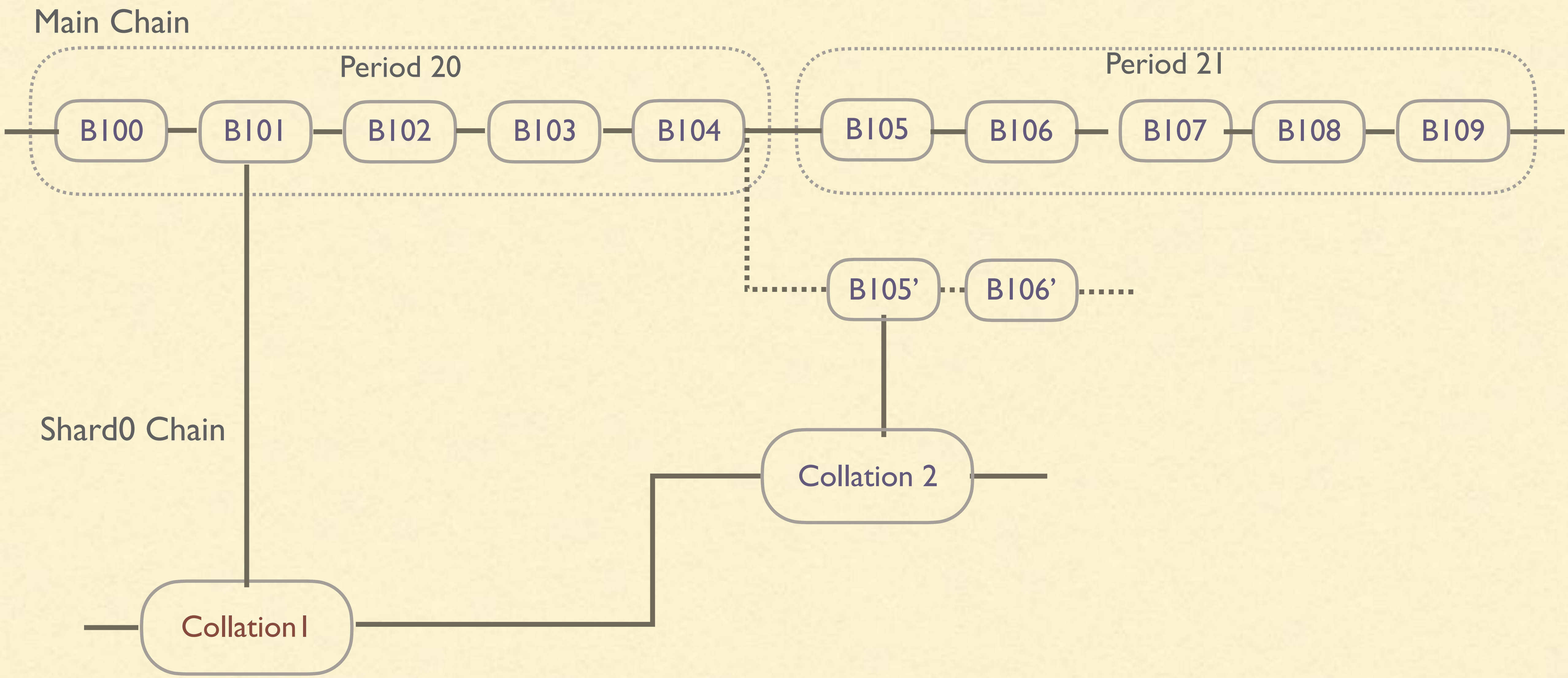
- 二次分片


Main Chain
Period 20
Period 21
B100
B101
B102
B103
B104
B105
B105
B106
B107
B108
Shard0 Chain
VMC[Shard0][1]=CollationHeader 1
VMC[Shard0][2]=CollationHeader 2
Collation1
CollationHeader
Transcation List
Collation2
CollationHeader
Transcation List
Shard1 Chain
VMC[Shard1][1]=CollationHeader 1
VMC[Shard1][2]=CollationHeader 2
Collation1
CollationHeader
Transcation List
Collation2
CollationHeader
Transcation List

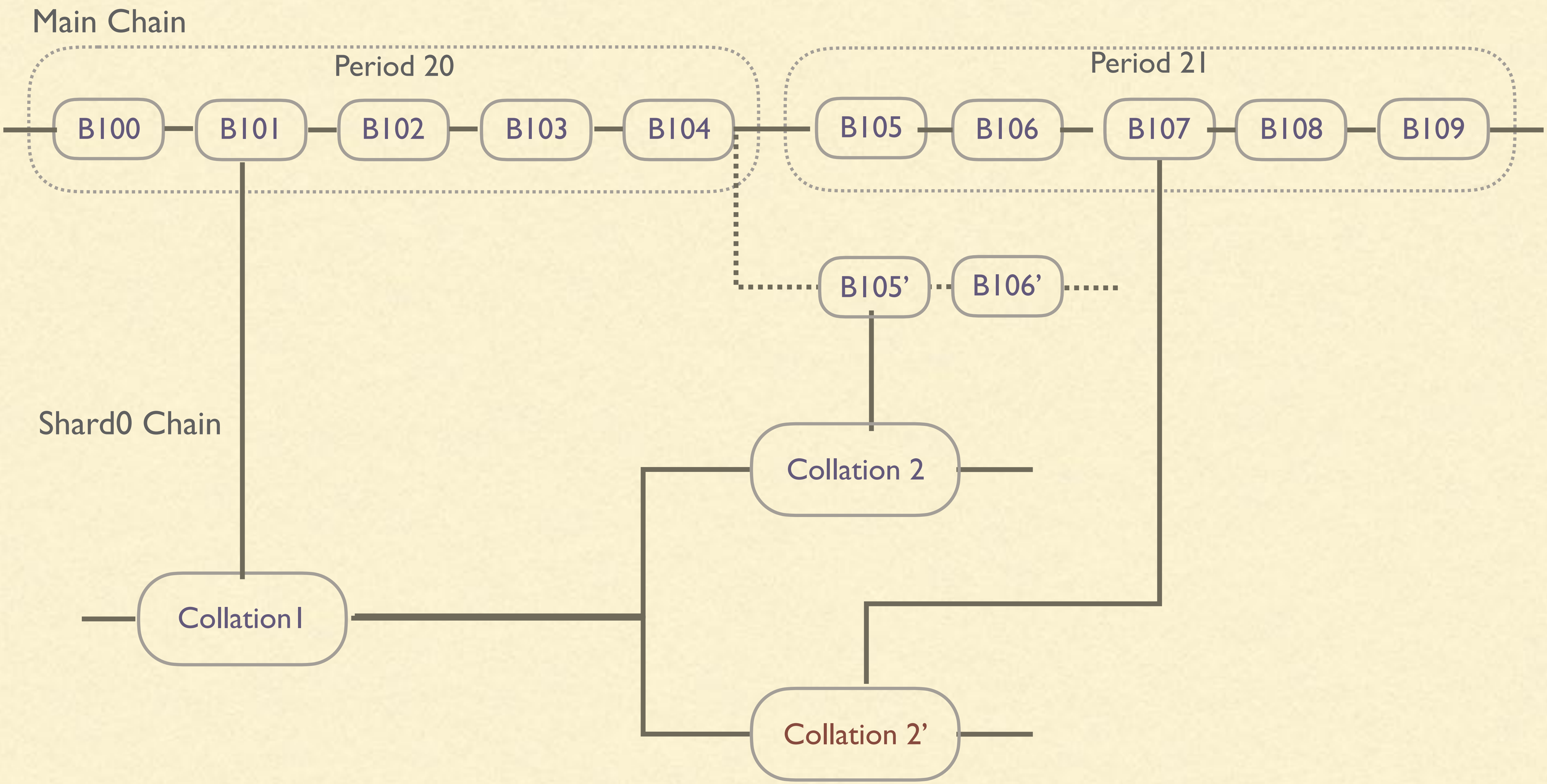
分叉选择

- Main Chain：最长有效链
- Shard Chain：最长有效Main Chain中的最长有效分片链

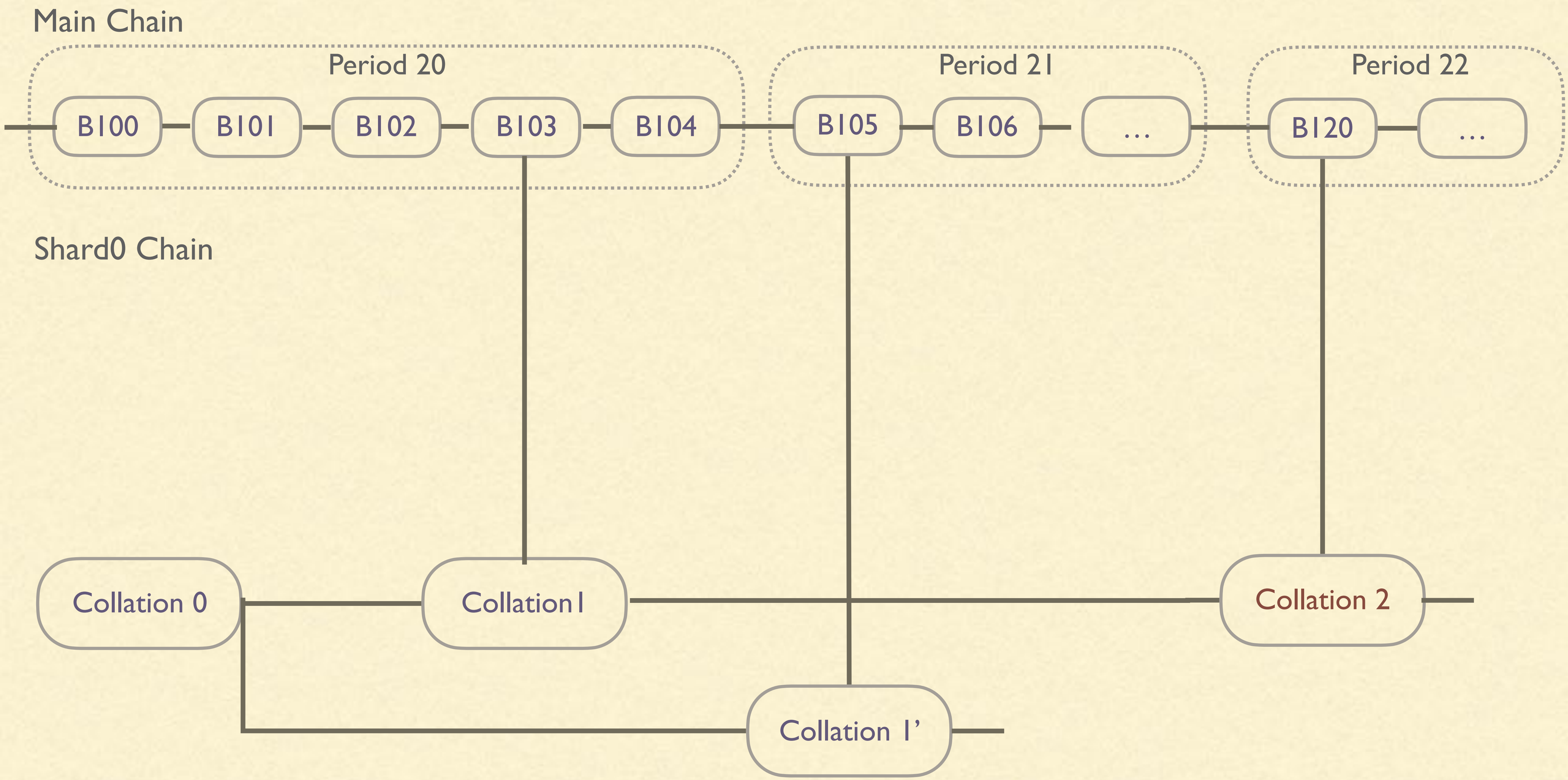
- 分叉选择


Main Chain
Period 20
Period 21
B100
B101
B102
B103
B104
B105
B106
B107
B108
B109
B105’
B106’
Shard0 Chain
Collation 2
Collation1

- 分叉选择


Main Chain
Period 20
Period 21
B100
B101
B102
B103
B104
B105
B106
B107
B108
B109
B105’
B106’
Shard0 Chain
Collation1
Collation 2
Collation 2’

- 分叉选择


Main Chain
Period 20
Period 21
Period 22
B100
B101
B102
B103
B104
B105
B106
…
B120
…
Shard0 Chain
Collation 0
Collation1
Collation 2
Collation 1'

- 挑战

- 跨Shard通信
- Shard接管攻击
- 欺诈检测
- 超二次分片
- 透明分片

跨Shard通信

- Main Chain中继
- 跨Shard信道，Main Chain见证

- 路线

- Phase 1:二次分片
- Phase 2:双向楔定
- Phase 3:协议优化（Collation Header）
- Phase 4:协议紧耦合

参考资源

- https://github.com/ethereum/wiki/wiki/Sharding-FAQ
- https://github.com/ethereum/sharding/blob/develop/docs/doc.md
- https://github.com/ethereum/sharding/tree/develop/sharding
- https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649
- http://ethfans.org/posts/vitalik-buterin-lays-roadmap-ethereum-visa-levels-quadratic-sharding
- http://ethfans.org/posts/Ethereum-Sharding-Concept-20171203-Shenzhen
- https://docs.zilliqa.com/whitepaper.pdf
- https://www.rchain.coop/