



What you can do for Ethereum 2.0 a.k.a. sharding


Q2 2018

Ethereum Research

Hsiao-Wei Wang
([hwwhww/icebearhww](https://github.com/hwwhww/icebearhww))

Taipei Ethereum Meetup
June 12th, 2018

Updated: 2018/06/21

- ◇ [The latest research direction](#) is that the “**beacon chain**” that will produce random numbers with RANDAO-based scheme.
 - ◇ In the latest scheme, the **full Casper FFG** logic is in the beacon chain to support both beacon chain and shard chains staking.
 - ◇ In the latest scheme, there’s **no** a sharding manager contract in main chain to deal with block proposal and notarization logic. The finality of shards is determined by **cross-links**.
- 

What you can do for Ethereum 2.0 a.k.a. sharding



What you can do for Ethereum 2.0 a.k.a. sharding

What is sharding?



What you can do for Ethereum 2.0 a.k.a. sharding

What is sharding?

Where can you start to dig into sharding?



What you can do for Ethereum 2.0 a.k.a. sharding

What is sharding?

Where can you start to dig into sharding?

How can you contribute to Ethereum 2.0?



A decorative graphic on the left side of the slide, consisting of several overlapping teal-colored triangles and polygons that form a larger, irregular shape pointing downwards.

What is sharding?

Sharding

Layer 1

Scaling Solution

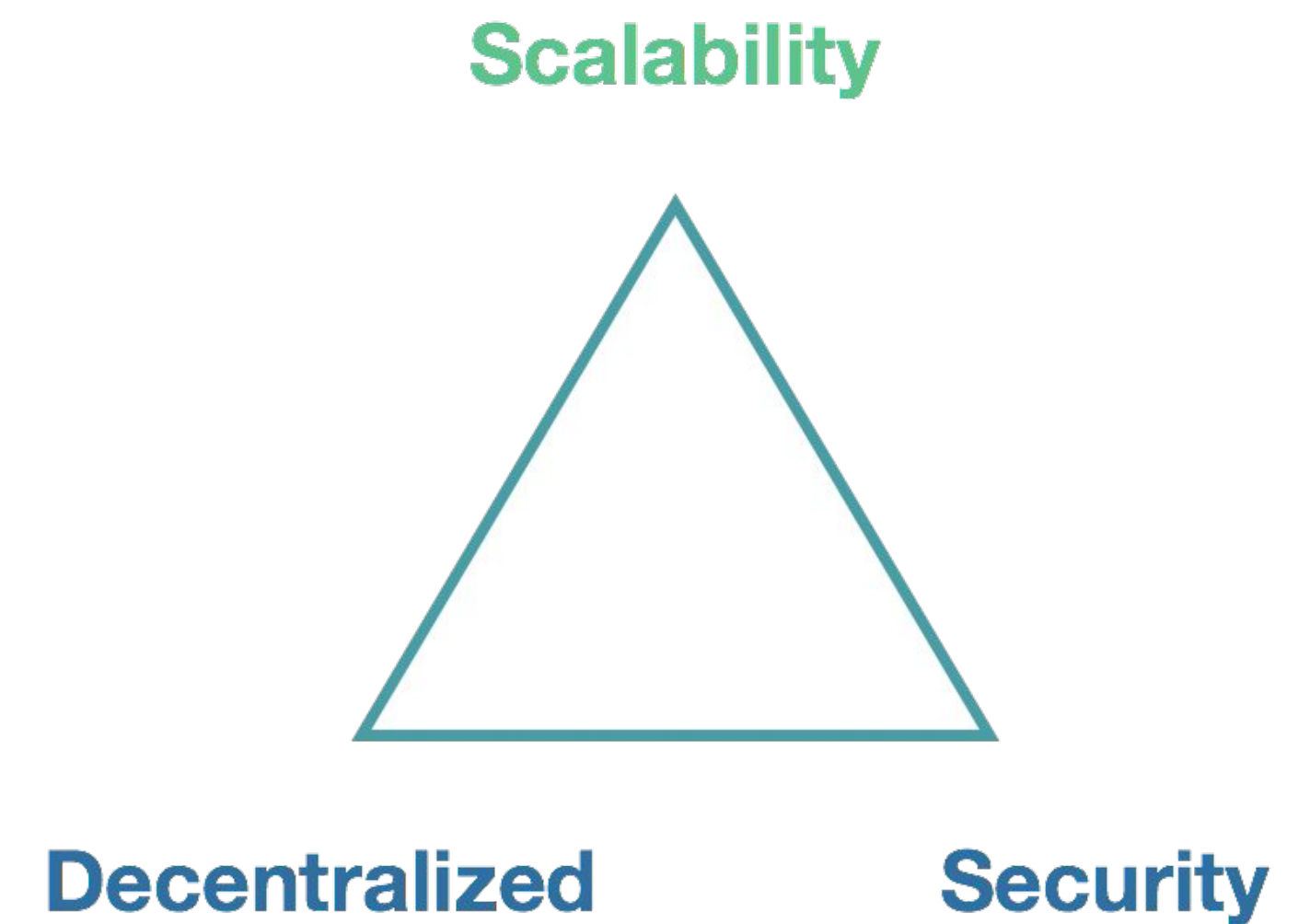


Sharding

Layer 1

Secure and Decentralized

Scaling Solution



Main Chain

The main Ethereum 1.0 blockchain



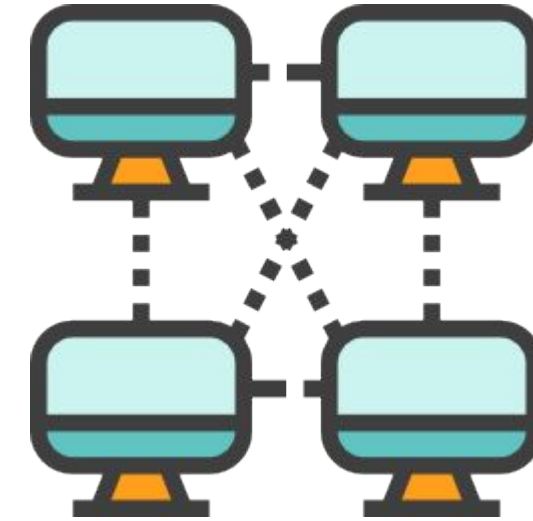
Shard Chains (Shards)

- ◇ Creating many new chains for [Ethereum 2.0](#)
- ◇ Each shard chain is a new [galaxy](#)



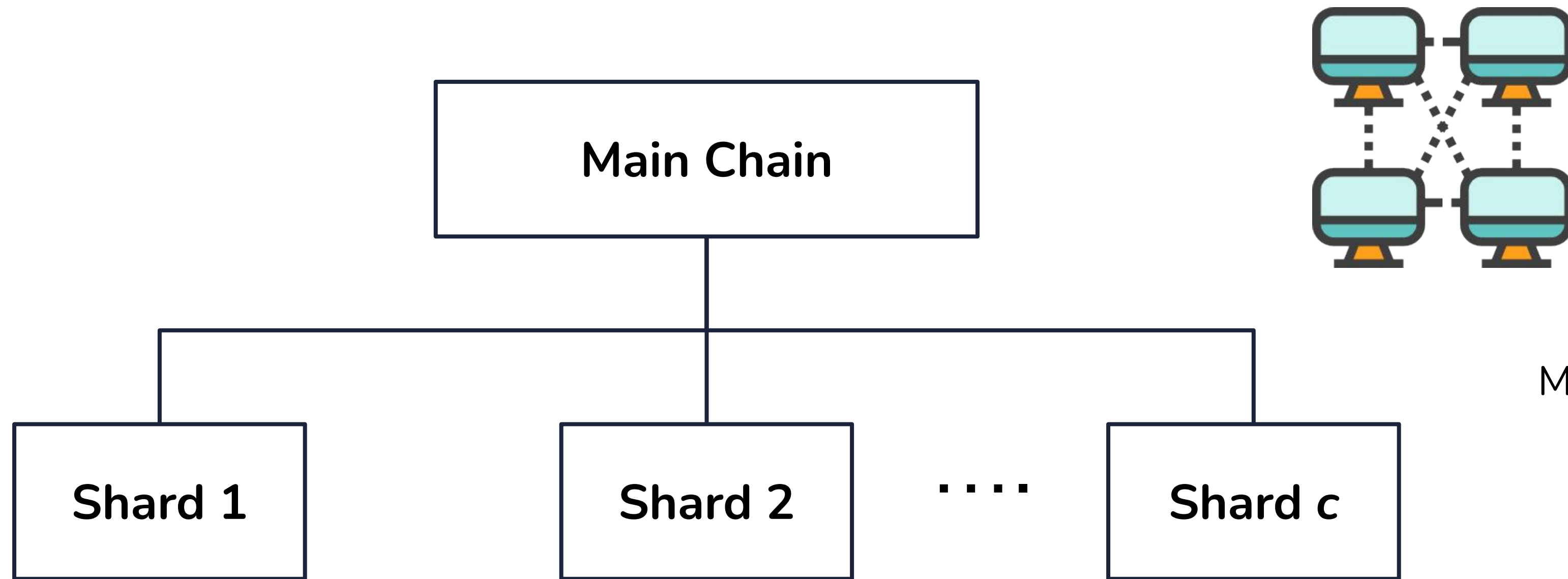
Quadratic Sharding

Main Chain



Computation: each computer can process c transactions, the main chain can process c transactions.

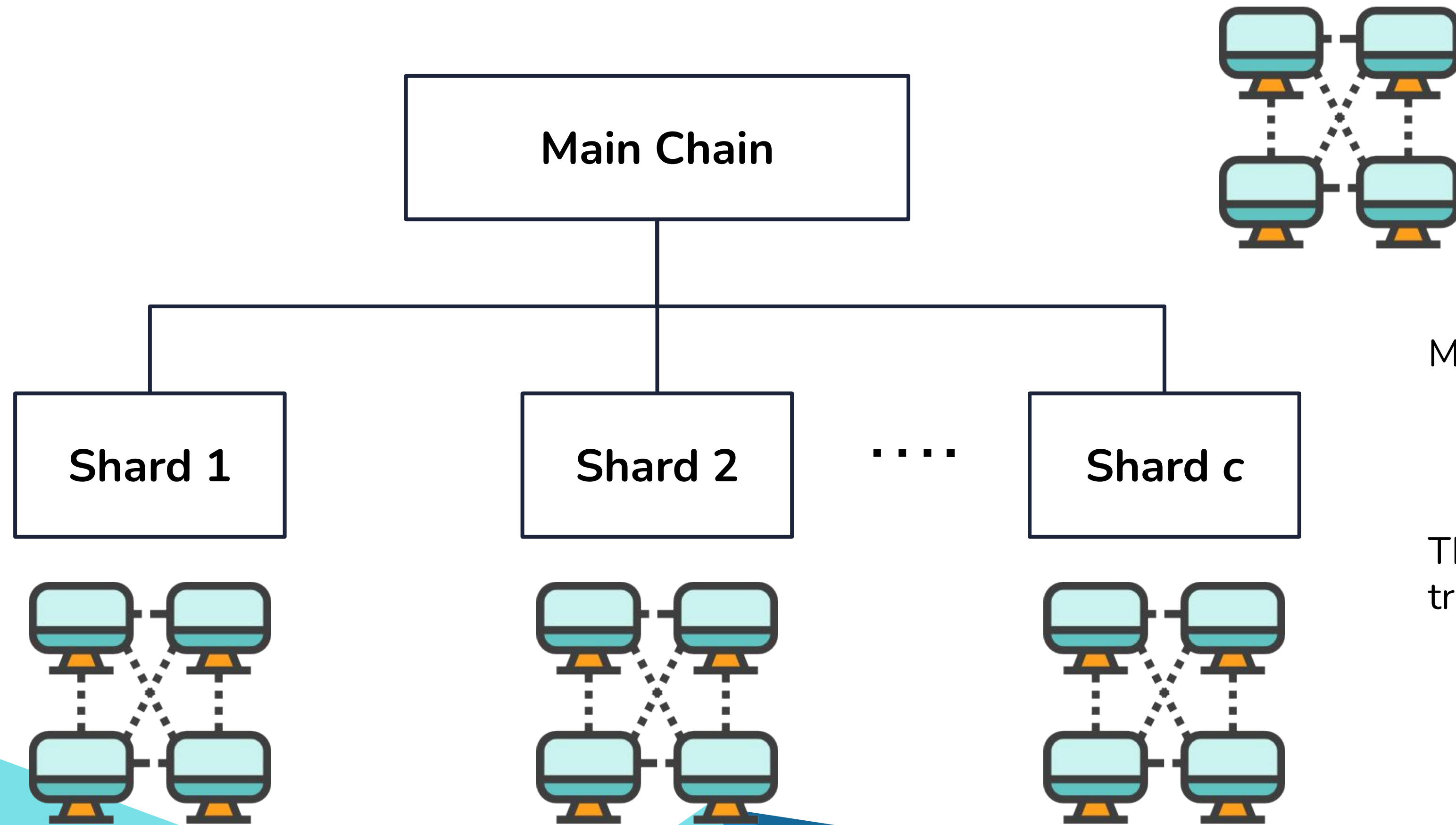
Quadratic Sharding



Computation: each computer can process c transactions, the main chain can process c transactions.

Main chain nodes can watch c shards

Quadratic Sharding



Computation: each computer can process c transactions, the main chain can process c transactions.

Main chain nodes can watch c shards

The whole system can process c^2 transactions

Goal: Tightly Coupled Sharding Chain

- ◊ Some proofs of the shard chains will be written into main chain block.
- ◊ A main chain block is **invalid** if the shard chain blocks proofs (links) that included are **invalid**.





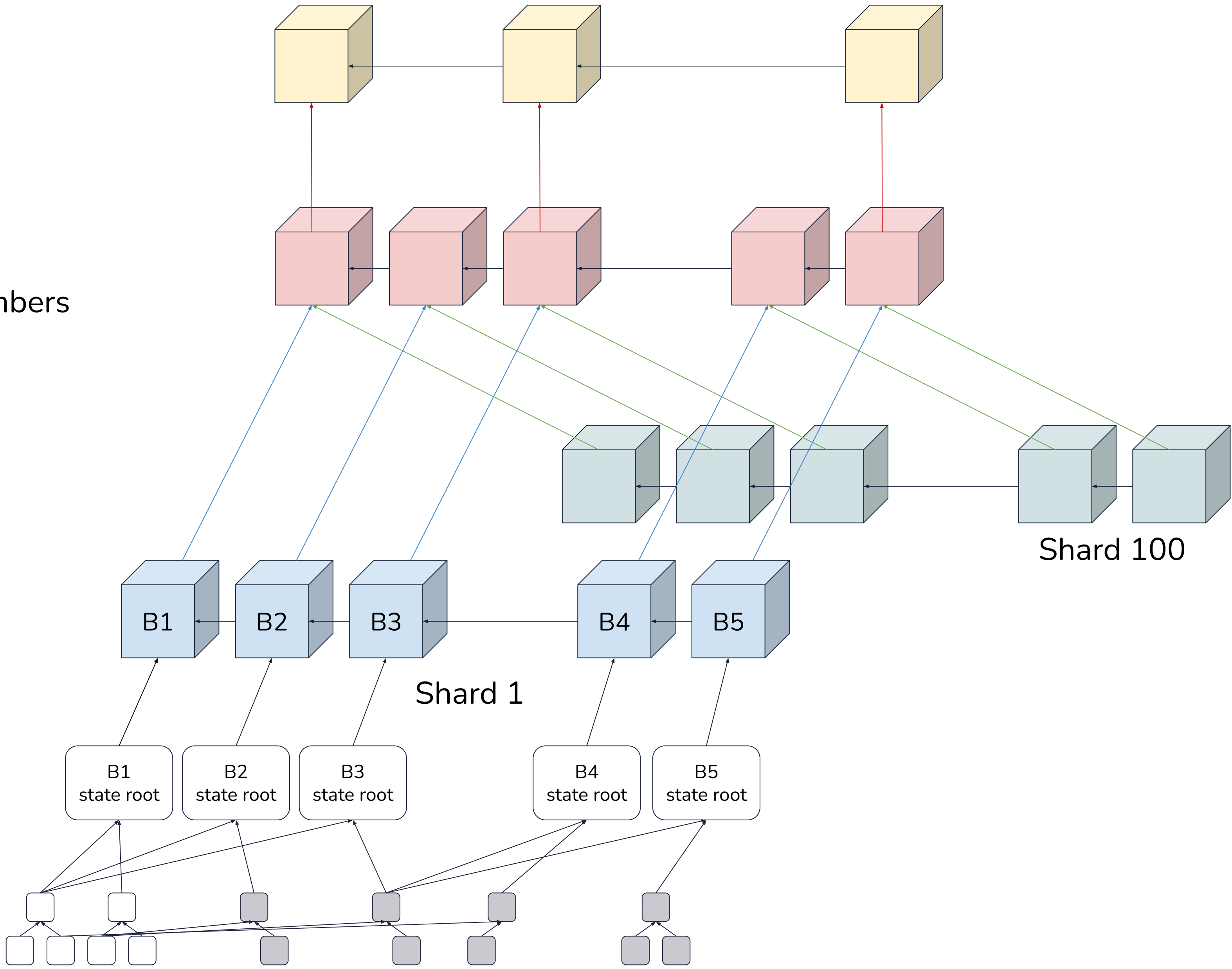
Recent R&D Concept

Main Chain
provides staking

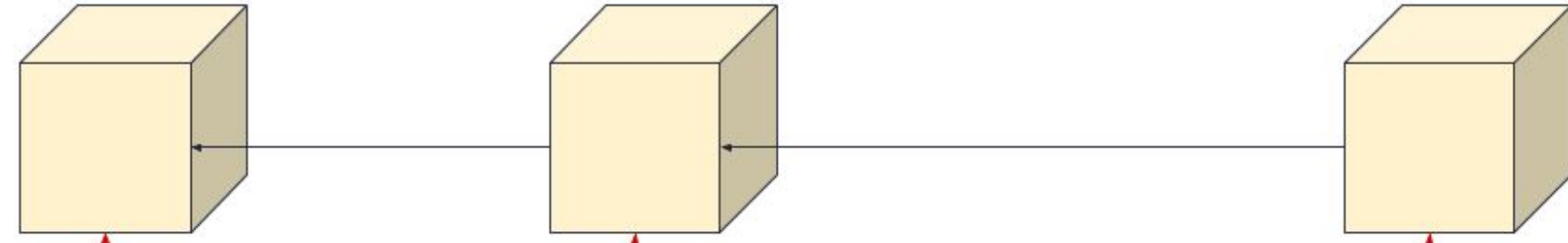
Beacon Chain
provides random numbers

Shard Chain
provides data

VM
provides state
execution result



Main Chain
provides staking

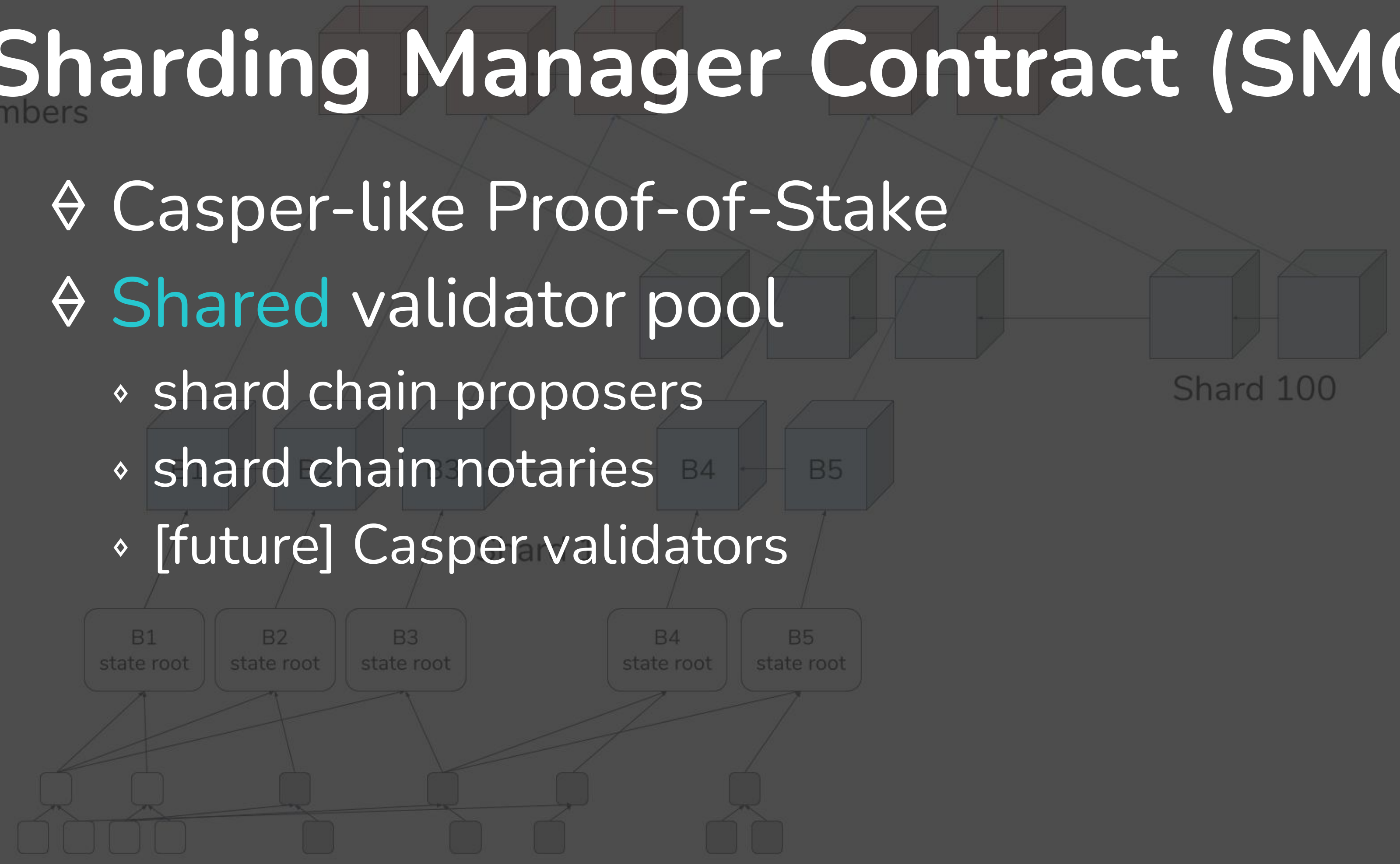


Staking – Sharding Manager Contract (SMC)

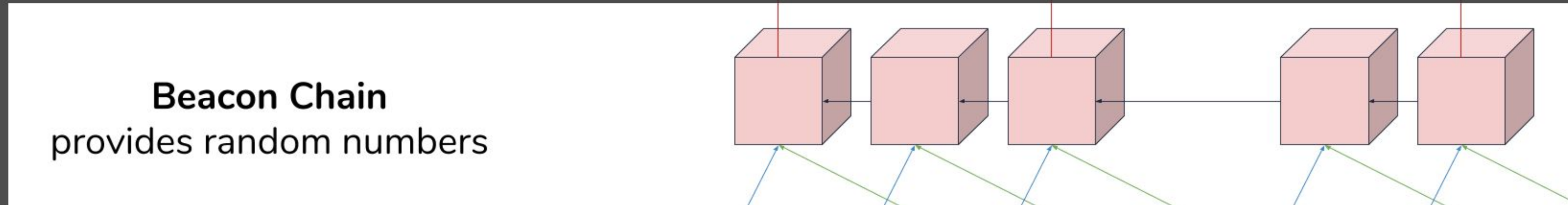
- ◊ Casper-like Proof-of-Stake
- ◊ **Shared** validator pool
 - ◊ shard chain proposers
 - ◊ shard chain notaries
 - ◊ [future] Casper validators

Shard Chain
provides data

VM
provides state
execution result



Random Number Generation



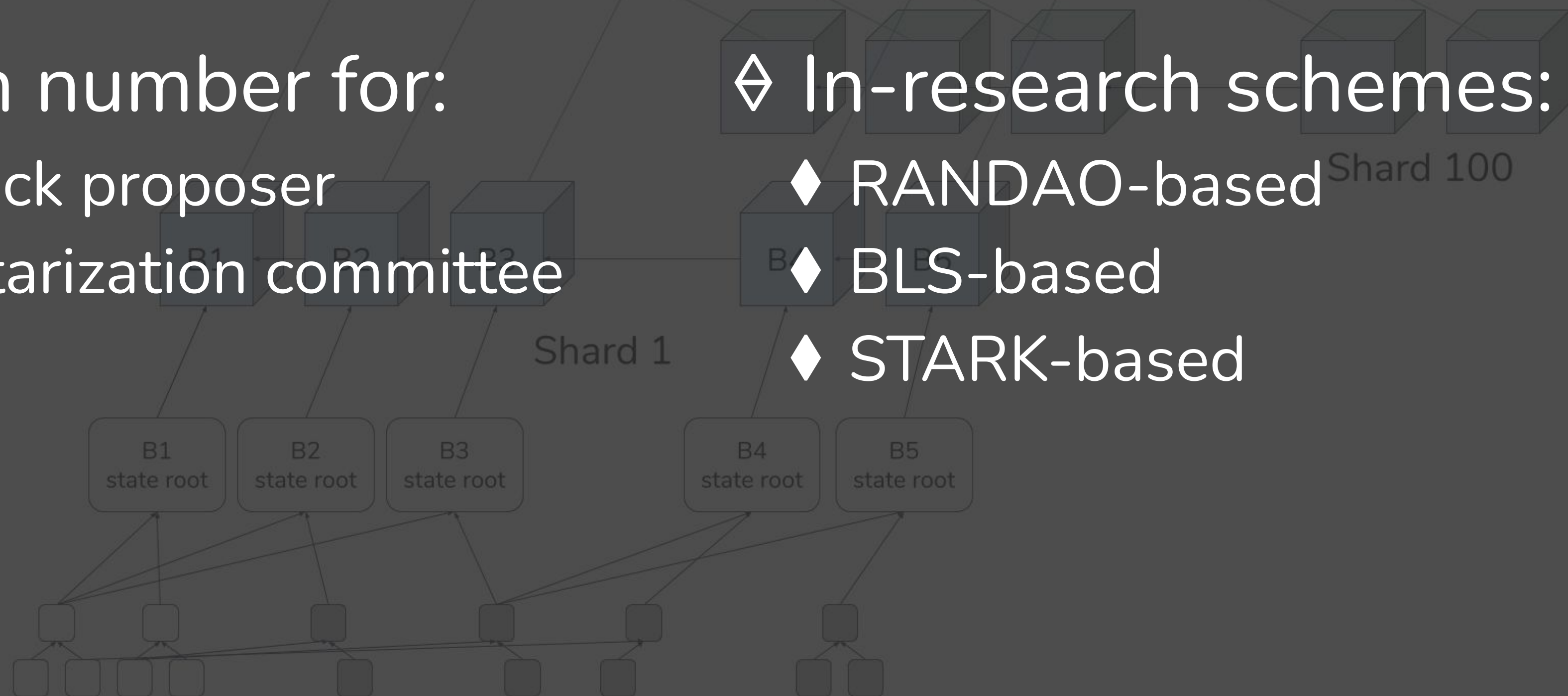
◊ Use random number for:

- ◊ Selecting block proposer
- ◊ Selecting notarization committee

◊ In-research schemes:

- ◊ RANDAO-based
- ◊ BLS-based
- ◊ STARK-based

VM provides state execution result



Data Layer

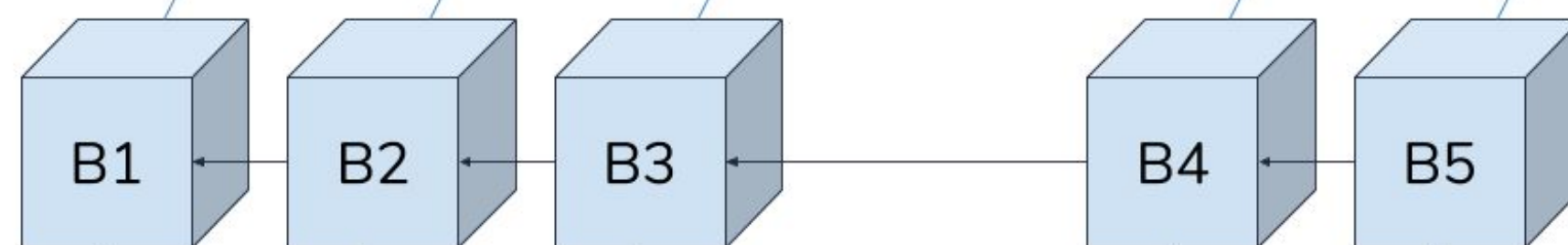
◊ Only data-consensus

◆ Block bodies are just **blobs**, no state root in the header

◆ Data availability

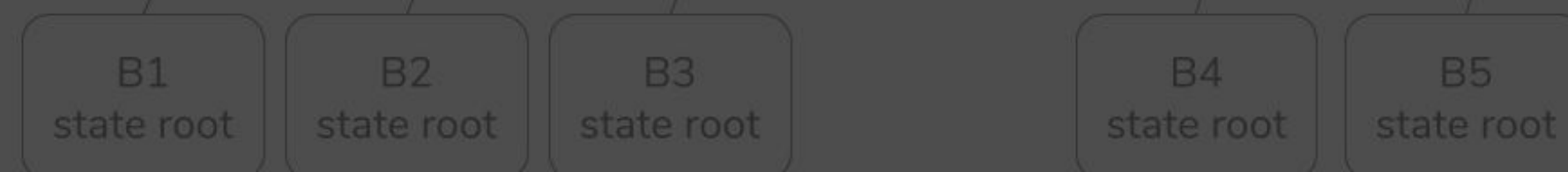
Beacon Chain
provides random numbers

Shard Chain
provides data

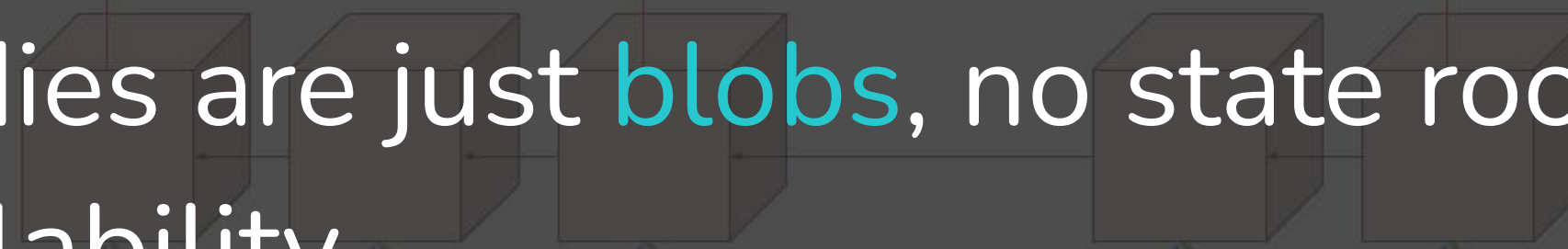
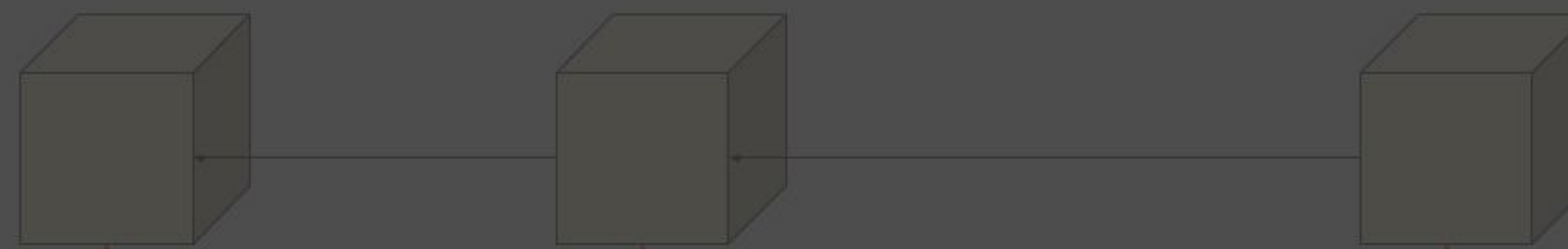


Shard 1

VM
provides state
execution result



Shard 100



State Layer

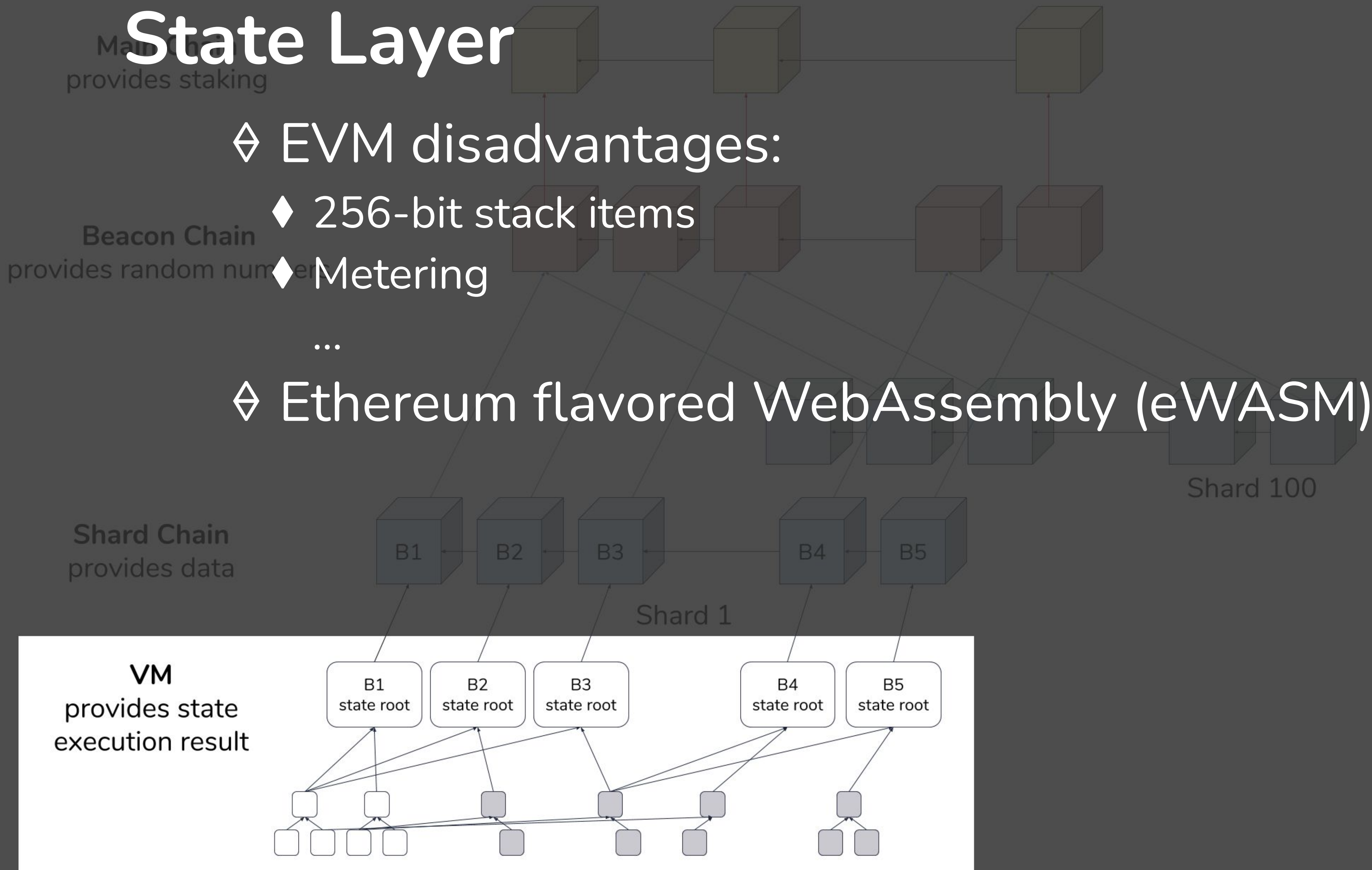
◊ EVM disadvantages:

◆ 256-bit stack items

◆ Metering

...

◊ Ethereum flavored WebAssembly (eWASM)





**Where can you
start to dig into?**

Sharding Protocol	P2P	Efficient Scheme	State Execution	Engineering	Security
Random Number Generation	libp2p Transport Layer	Digital Signature Scheme	eWASM	Backend System and API Design	Formal Verification
Block Proposal	Sharding Network Topology	Efficient Accumulator	Account Abstraction	Testnet DevOps	System Audit
Notary Committee Selection		Data Encoding n' Decoding	Account Restriction	UX for Devs	
Data Availability			Stateless Client		
Casper Integration			Cross-shard Transaction		

Sharding Protocol

P2P

Efficient Scheme

State Execution

Engineering

Security

Random Number Generation

libp2p
Transp
Layer

Vitalik Buterin: [Sharding FAQ](#)

Block Proposal

Shard
Netw
Topol

Ethereum Research Discourse

 <https://ethresear.ch/> 

Vitalik's favorite forum, next only to reddit.com/r/Buttcoin.

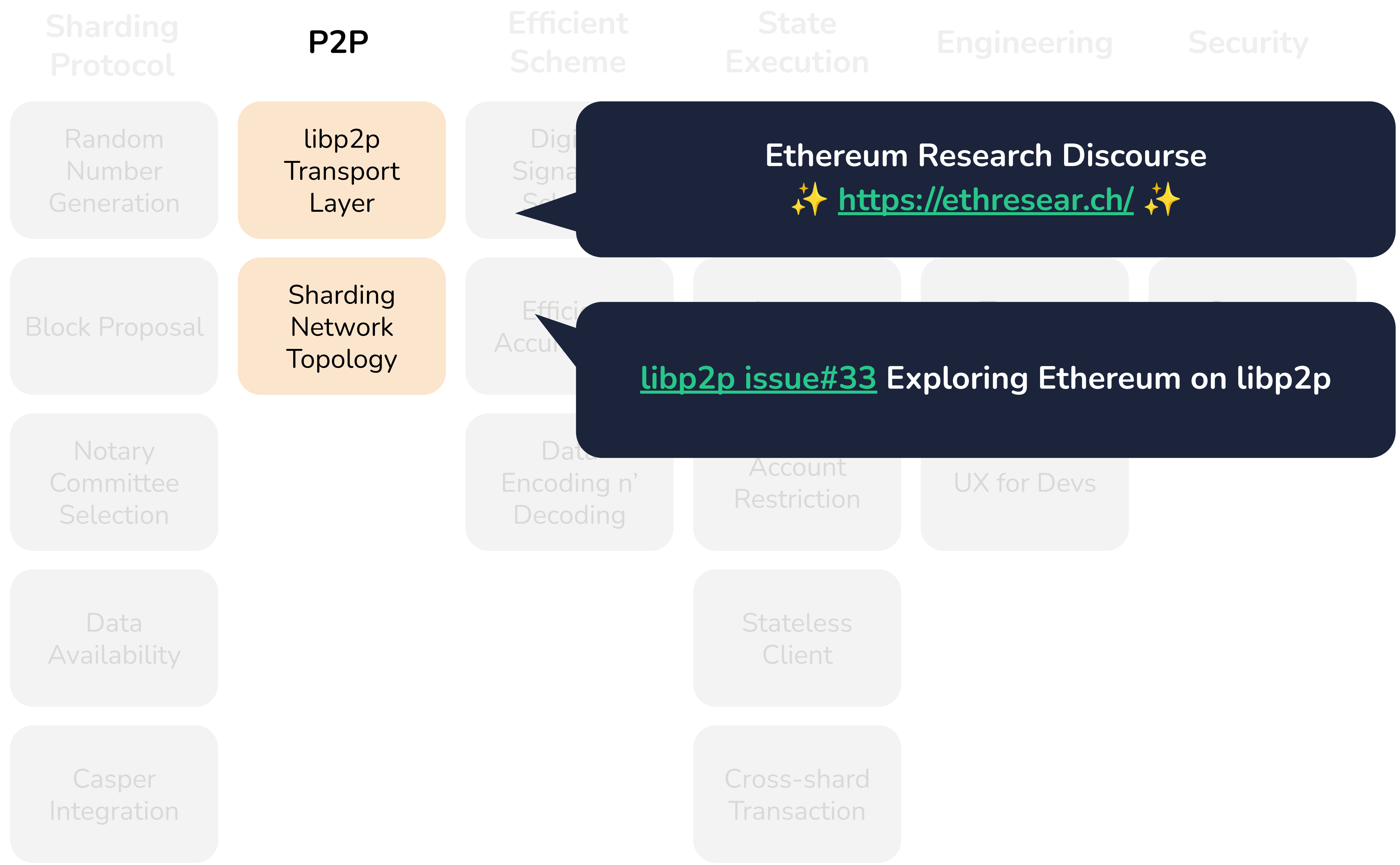
Notary Committee Selection

Data Availability

Vitalik Buterin: [A note on data availability and erasure coding](#)

Casper Integration

Read Casper first! [EIP 1011](#)



Ethereum Research Discourse

🌟 <https://ethresear.ch/> 🌟

[libp2p issue#33](#) Exploring Ethereum on libp2p

Sharding Protocol

P2P

Efficient Scheme

State Execution

Engineering

Security

Ethereum Research Discourse

🌟 <https://ethresear.ch/> 🌟

Digital Signature Scheme

eWASM

Backend System and API Design

Formal Verification

Block Proposal

Sharding Network Topology

Efficient Accumulator

Sparse Merkle Trees (SMTs)

RLP Replacement

Data Encoding n' Decoding

Account Restriction

UX for Devs

Data Availability

Stateless Client

Casper Integration

Cross-shard Transaction

Sharding Protocol

P2P

Efficient Scheme

State Execution

Engineering

Security

GH: [ewasm/design](#) and [gitter](#)

eWASM

Backend System and API Design

Formal Verification

Block Proposal

Sharding Network Topology

Efficient Accumulator

Account Abstraction

Nicholas Lin ([twedusuck](#)): [Account Abstraction in Sharding](#)

Jannik Luhn: [Account List](#)

Account Restriction

UX for Devs

Data Availability

Stateless Client

Vitalik Buterin: [Stateless Client Concept](#)

Vitalik Buterin: [Sharding FAQ](#)

Cross-shard Transaction

Sharding Protocol

P2P

Efficient Scheme

State Execution

Engineering

Security

Trinity Ethereum Client is Trinity

Backend System and API Design

Formal Verification

Testnet DevOps

System Audit

UX for Devs

ethereum / py-evm

Unwatch 82 Star 496 Fork 213

Code Issues 103 Pull requests 9 Projects 3 Insights

Filters is:issue is:open label:Sharding Labels Milestones New issue

Clear current search query, filters, and sorts

<input type="checkbox"/>	<input type="checkbox"/>	18 Open	<input checked="" type="checkbox"/>	37 Closed	Author	Labels	Projects	Milestones	Assignee	Sort
<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMC integration with py-EVM	Sharding							4
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Super minimal pseudo-sharding test-test-network	Sharding							2
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Minimal sharding protocol	Sharding	Work in progress						3
<input type="checkbox"/>	<input checked="" type="checkbox"/>	SMC (VMC) get_validators_max_index	Sharding							5
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Minimal testnet for sharding	Sharding							17
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Paygas refund issue	Sharding	Sharding - state layer						9

Sharding
Protocol

P2P

Efficient
Scheme

State
Execution

Engineering

Security

Yoichi Hirai: [Formal Verification of Ethereum Contracts](#)

Formal
Verification

Dr. Christian Reitwiessner: [Formal Verification of Smart Contracts \(IC3-Ethereum Crypto Boot Camp\)](#)

System
Audit

Notary
Committee
Selection

Data
Encoding n'
Decoding

Account
Restriction

UX for Devs

Data
Availability

Stateless
Client

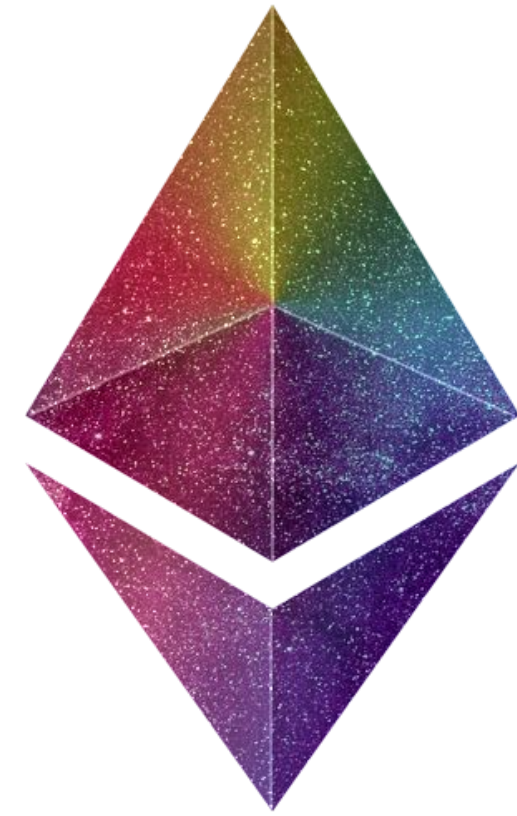
Casper
Integration

Cross-shard
Transaction



**How can you
contribute to
Ethereum 2.0?**

Join ShardCoin ICO!



ethereum
shard coin

re-ico pre-sale: August 7th

Join ShardCoin ICO!

**NO NO NO NO NO
NO NO
THAT'S A SCAM!!!**

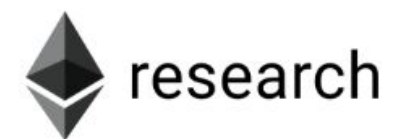
ethereum

shard coin

re-ico pre-sale: August 7th

Ethereum Research Discourse

<https://ethresear.ch/>



Discussion about sharding. See also:

Sharding ▾

Latest

Top

+ New Topic



Topic	Users	Replies	Views	Activity
Blob serialisation		26	1.3k	1d
Registrations, shard count and shuffling		6	322	3d
A proposal for structuring committees, cross-links, etc		0	362	5d
Leaderless k-of-n random beacon		3	427	6d

Sharding Manager Contract

ethereum / sharding Unwatch 111 ★ Star 378 Fork 73

[Code](#) [Issues 8](#) [Pull requests 0](#) [Projects 1](#) [Insights](#) [Settings](#)

Sharding manager contract, and related software and tests [Edit](#)

[ethereum](#) [python](#) [sharding](#) [vyper](#) [Manage topics](#)

[417 commits](#) [3 branches](#) [4 releases](#) [10 contributors](#)

Branch: [master](#) [New pull request](#) [Create new file](#) [Upload files](#) [Find file](#) [Clone or download](#)

[hwwhww](#) Merge pull request #110 from hwwhww/makefile [...](#) Latest commit 8082e35 5 hours ago

.github	Create ISSUE_TEMPLATE.md	2 months ago
docs	Fix Markdown Syntax	24 days ago
sharding	Merge pull request #104 from NIC619/fix_from_block_and_enforce_PEP3102	2 days ago
tests	Merge pull request #104 from NIC619/fix_from_block_and_enforce_PEP3102	2 days ago
tools	Add remaining type hints in sharding package	11 days ago
.bumpversion.cfg	Bump version: 0.0.2-alpha.1 → 0.0.2-alpha.2	a day ago
.gitignore	Use newer pyethereum with flag	7 months ago

Python Implementation - Trinity

ethereum / py-evm

Unwatch 82 Star 496 Fork 213

Code Issues 103 Pull requests 9 Projects 3 Insights

Filters is:issue is:open label:Sharding Labels Milestones New issue

Clear current search query, filters, and sorts


<input type="checkbox"/>	18 Open ✓ 37 Closed	Author	Labels	Projects	Milestones	Assignee	Sort
<input type="checkbox"/>	SMC integration with py-EVM Sharding #799 opened 11 days ago by jannikluhn		Sharding				4
<input type="checkbox"/>	Super minimal pseudo-sharding test-test-network Sharding #571 opened on 18 Apr by jannikluhn		Sharding				2
<input type="checkbox"/>	Minimal sharding protocol Sharding Work in progress #539 opened on 10 Apr by hwwhww		Sharding				3
<input type="checkbox"/>	SMC (VMC) get_validators_max_index Sharding #456 opened on 12 Mar by hwwhww		Sharding				5
<input type="checkbox"/>	Minimal testnet for sharding Sharding #419 opened on 28 Feb by pipermerriam		Sharding				17
<input type="checkbox"/>	Paygas refund issue Sharding Sharding - state layer #413 opened on 27 Feb by jannikluhn		Sharding				9

Bounty



photo credit: [Gitcoin Medium](#)

Other On-going Implementations

- ◇ Status.im - [Nimbus](#) (Nim)
 - ◇ ConsenSys - [PegaSys](#) (Java)
 - ◇ Prysmatic Labs - [geth-sharding](#) (Golang)
 - ◇ Drops of Diamond - [Diamond Drops](#) (Rust)
 - ◇ Cross-client gitter channel: [ethereum/sharding](#)
- 

Grants



ethereum
foundation
grants

◇ Scalability

◇ Usability

◇ Security

◇ Hackternship

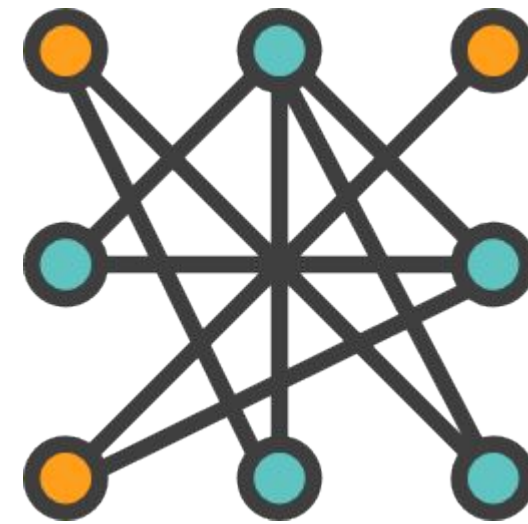
◆ 10-week \$10K externship for your spare-time working on
Ethereum!

◇ [Other Grants for Ethereum related work](#)

We are looking for ...



Blockchain Researchers



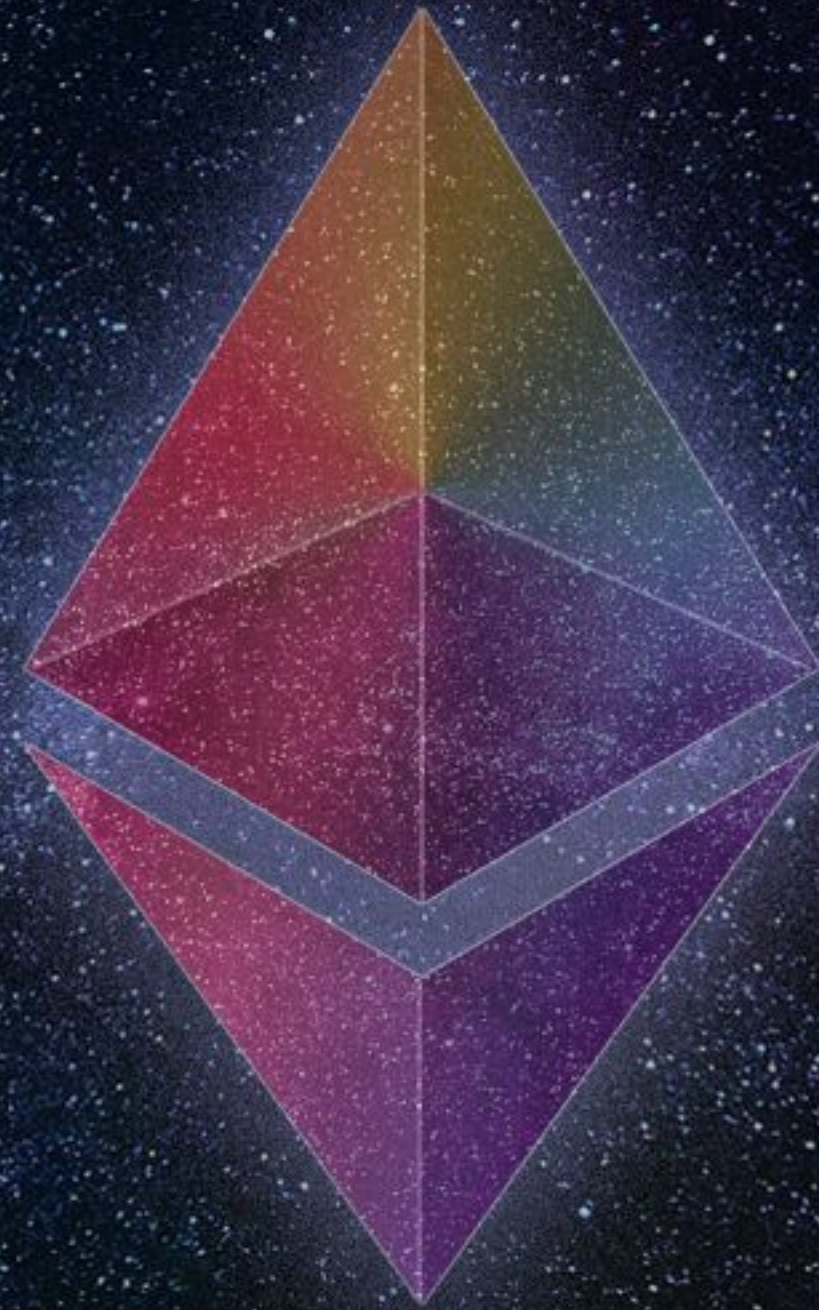
P2P Masters



Experienced Python Engineers

Email jobs+sharding@ethereum.org with subject line: "sharding"

Thank you!



CREDITS

Special thanks to all people who made and share these awesome resources for free:

- ☐ Presentation template designed by [Slidesmash](#)
- ☐ Photographs by [unsplash.com](#) and [pexels.com](#)
- ☐ Vector Icons by [Matthew Skiles](#)
- ☐ Icons made by Becris from [www.flaticon.com](#) is licensed by CC 3.0 BY
- ☐ [The bear picture](#)

Presentation Design

This presentation uses the following typographies and colors:

Free Fonts used:

<https://www.fontsquirrel.com/fonts/nunito>

Colors used



Sharding Protocol	P2P	Efficient Scheme	State Execution	Engineering	Security
Random Number Generation	libp2p Transport Layer	Digital Signature Scheme	eWASM	Backend System and API Design	Formal Verification
Block Proposal	Sharding Network Topology	Efficient Accumulator	Account Abstraction	Testnet DevOps	System Audit
Notary Committee Selection		Data Encoding n' Decoding	Account Restriction	UX for Devs	
Data Availability			Stateless Client		
Casper Integration			Cross-shard Transaction		

Main Chain
provides staking

Beacon Chain
provides random numbers

Shard Chain
provides data

VM
provides state
execution result

