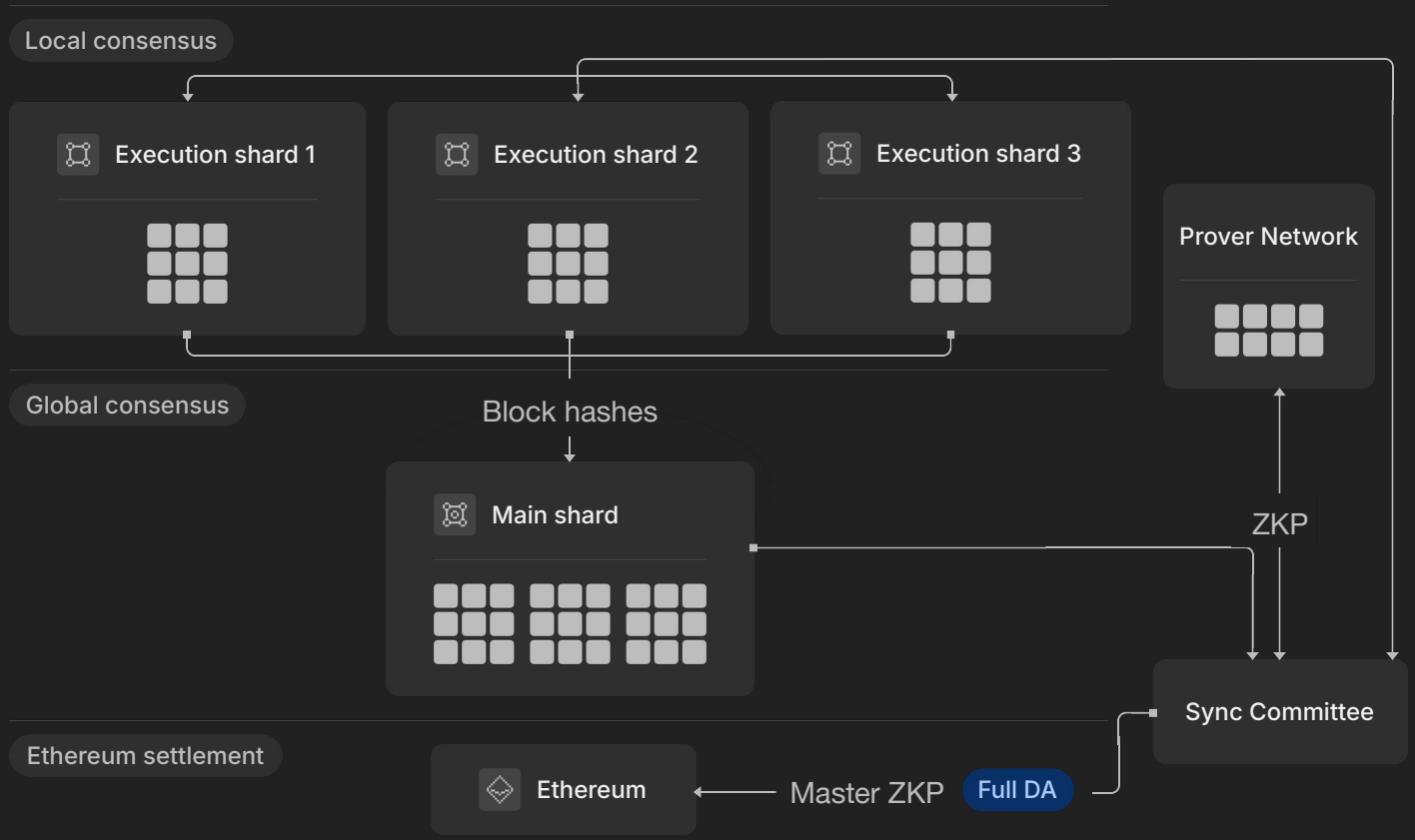
=nil; Foundation

Understanding zkSharding Through a Multi-Chain Lens

Ilia Shirobokov

zkSharding

Sharded zkRollup for parallel dApps execution



Blockchain Sharding

Blockchain sharding is a mechanism that partitions computational power and state to allow parallel execution of transactions within a blockchain architecture.

It splits the original system into shards, where each shard is responsible for processing only a portion of the transactions.

Blockchain Sharding Classification

Chain Creation

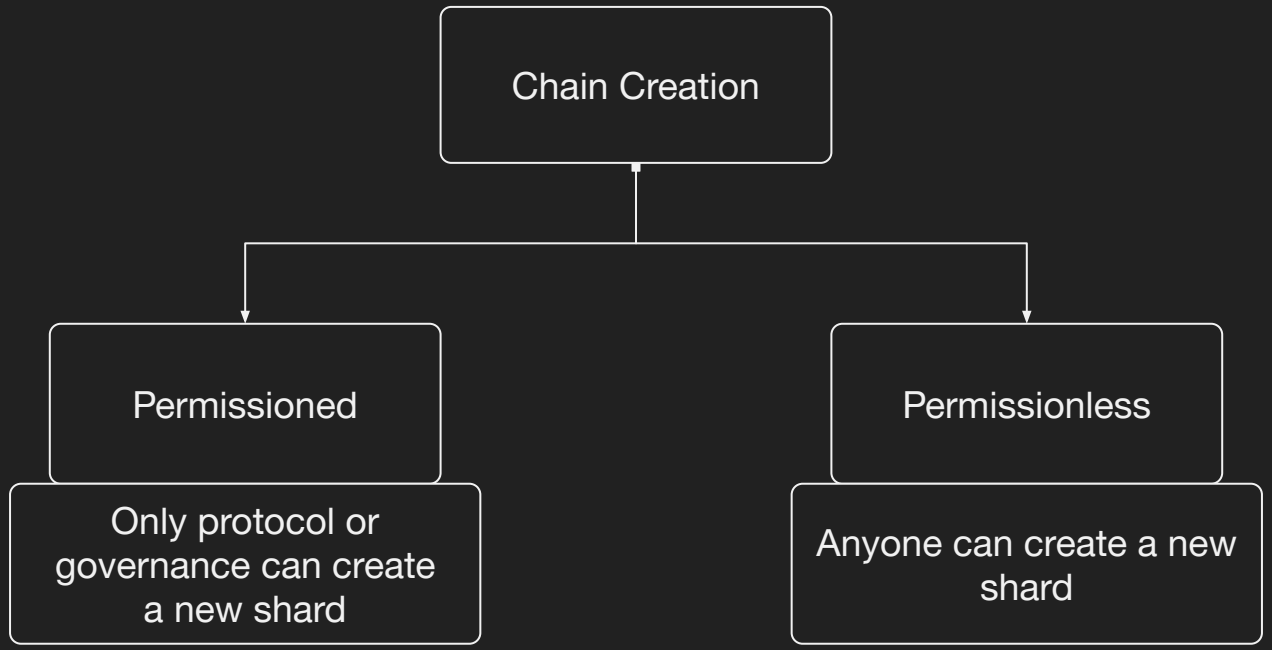
Inter-chain Structure

Cross-shard Messaging

Fee Model

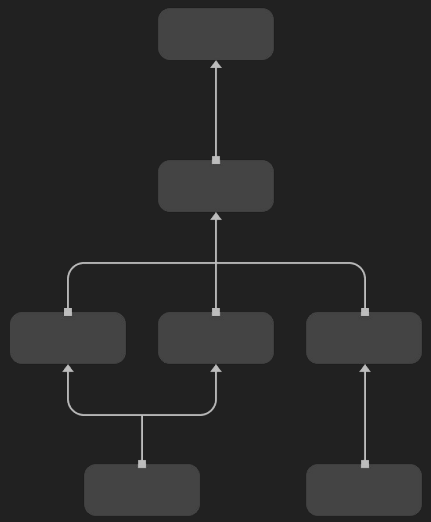
Shard Creation

Is the user able to create a new shard?

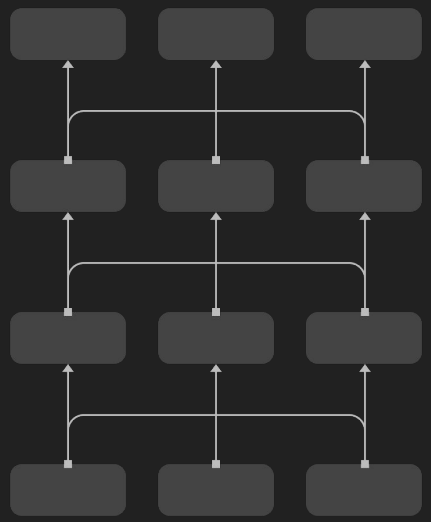


Inter-Chain Structure

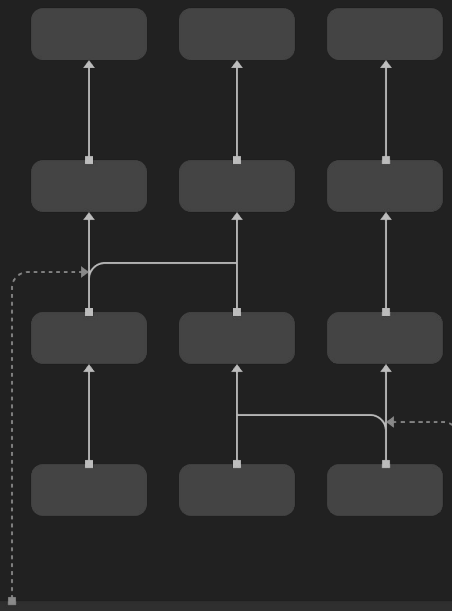
DAG with a single source



DAG with enforced updates

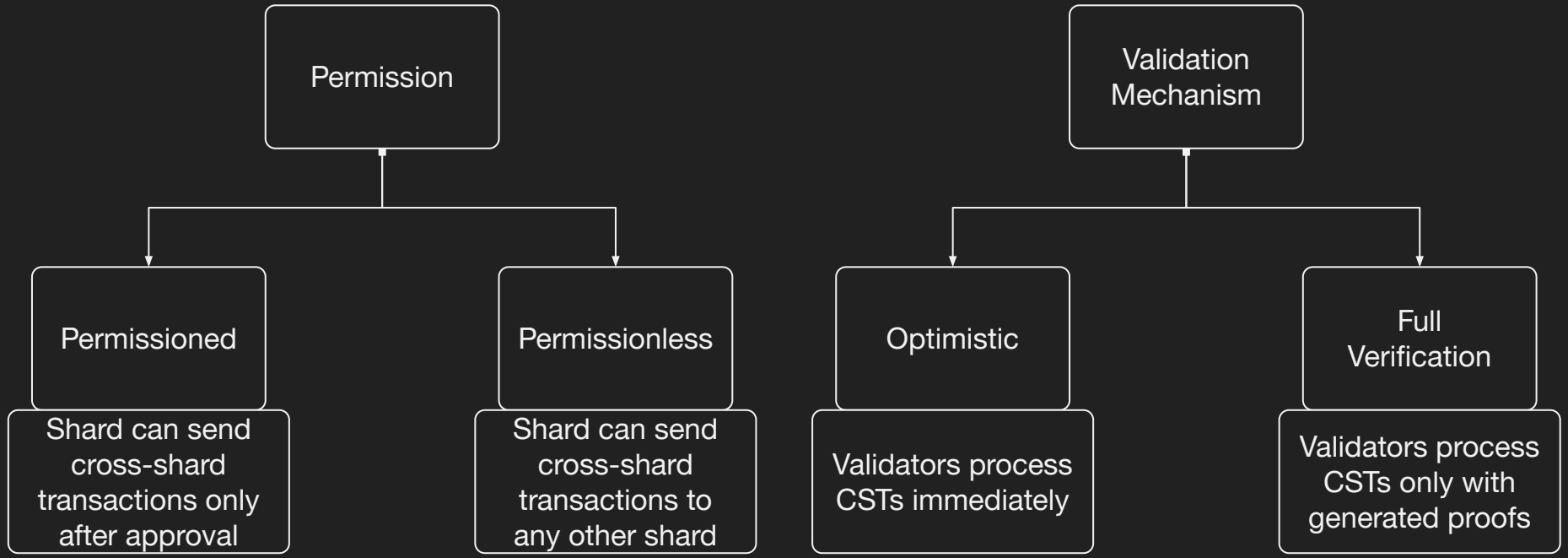


DAG without enforced updates

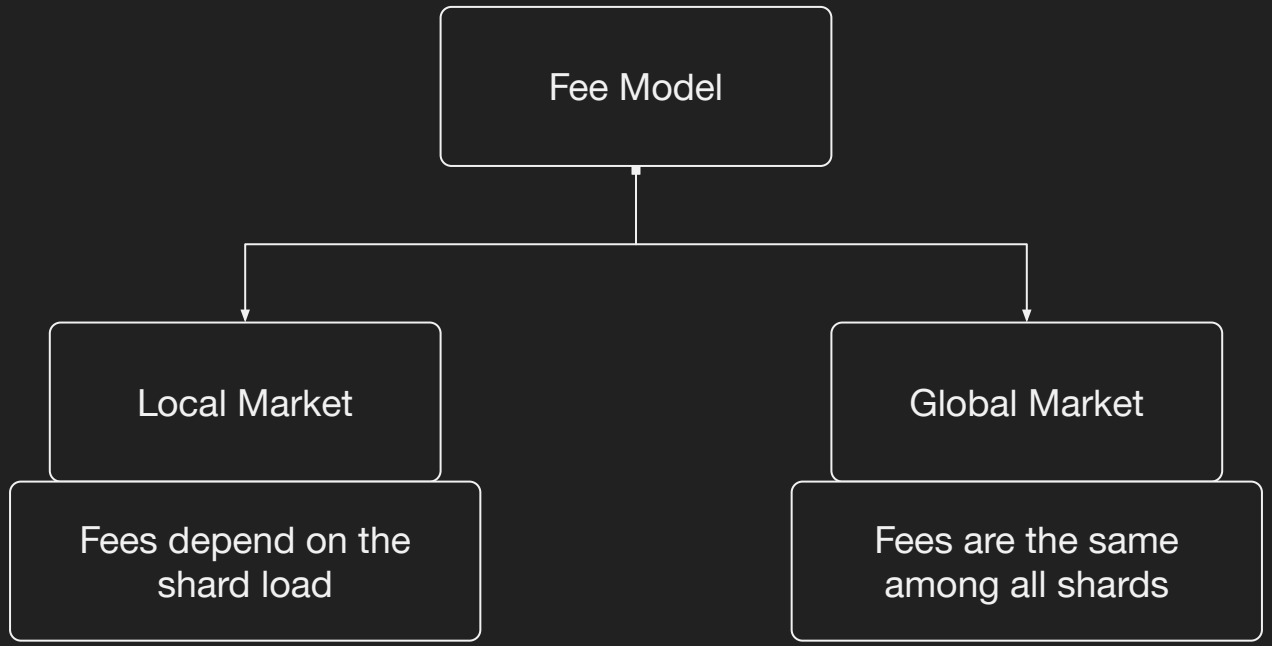


Cross-shard transaction is sent here

Cross-Shard Messaging

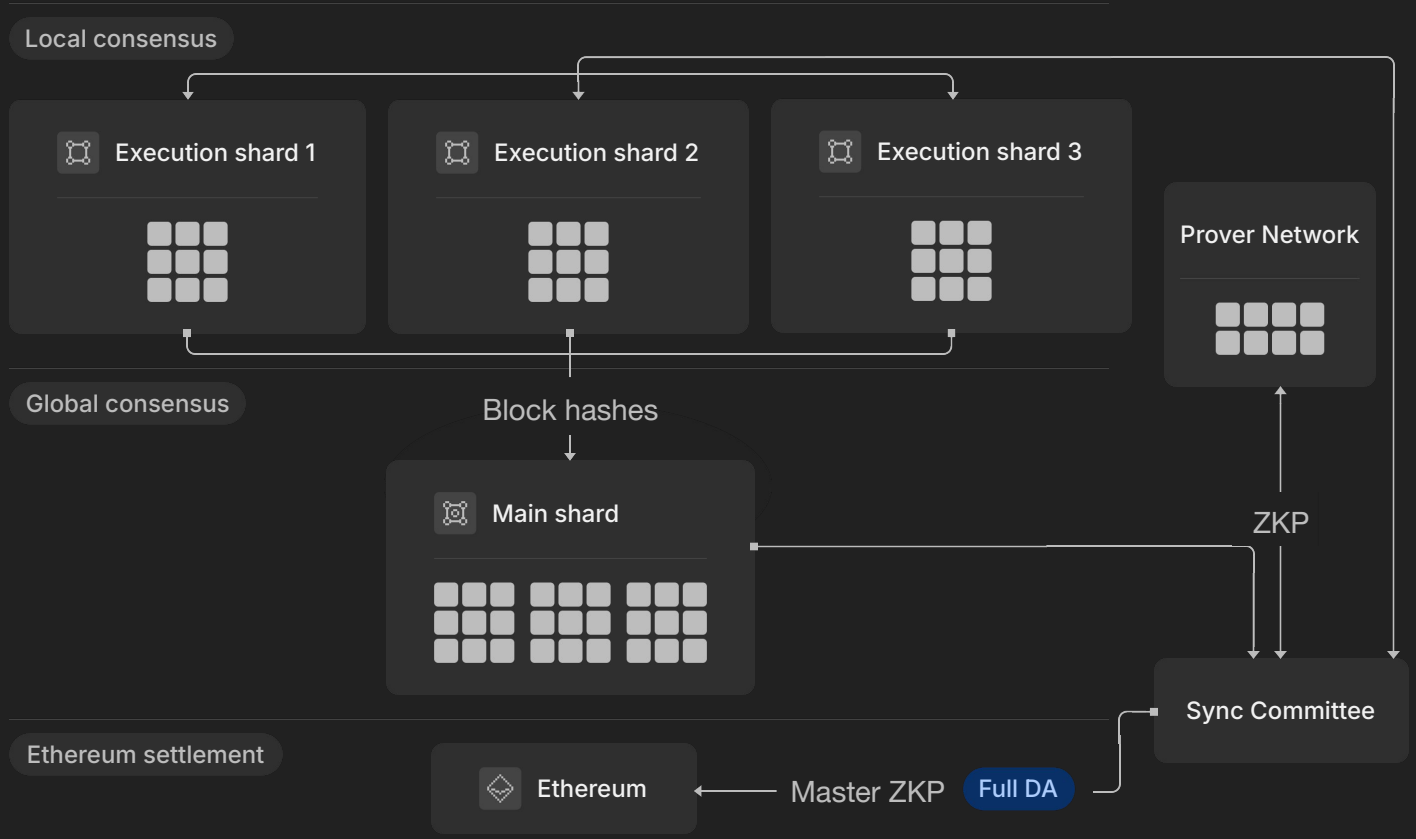


Fee Model


Fee Model
Local Market
Fees depend on the shard load
Global Market
Fees are the same among all shards

Framework Application To zkSharding

zkSharding Architecture



zkSharding: Chain Creation

From the chain creation perspective, zkSharding operates as a permissioned-by-protocol system: new shards are only created when existing execution shards become overloaded. Each new shard starts from an empty genesis block with no prior user data.

Permissioned
Chain Creation

zkSharding: Inter-Chain Structure

DAG with Enforced Updates structure, where execution shards and the main shard are connected through **ShardDAG** rules:

- Each block links to the previous block in its chain
- Each block references a previous block in the main shard
- Each block links to a set of blocks from other shards

Permissioned Chain Creation	DAG with Enforced Upgrades

zkSharding: Cross-Shard Messaging

- Non-atomic: Transactions on the destination shard may be reverted, and smart contracts must handle these errors.
- Optimistic: Validators in the destination shard process transactions without waiting for zk-proof generation.
- Permissionless: Any shard can send transactions to other shards without additional setup, ensuring free-flowing cross-shard communication.

Permissioned Chain Creation	DAG with Enforced Upgrades
Optimistic, permissionless	

zkSharding: Fee Model

Local fee market model. While a shared base fee applies to all transactions, additional fees are determined via a first-bid model.

The shared base fee covers:

- L1 Proof Verification
- Main Shard Maintenance

Permissioned Chain Creation	DAG with Enforced Upgrades
Optimistic, permissionless	Local Fee Market Model

Framework in Action

Onchain game with NFT sales

- Fast communication between users
- Load peaks during sales

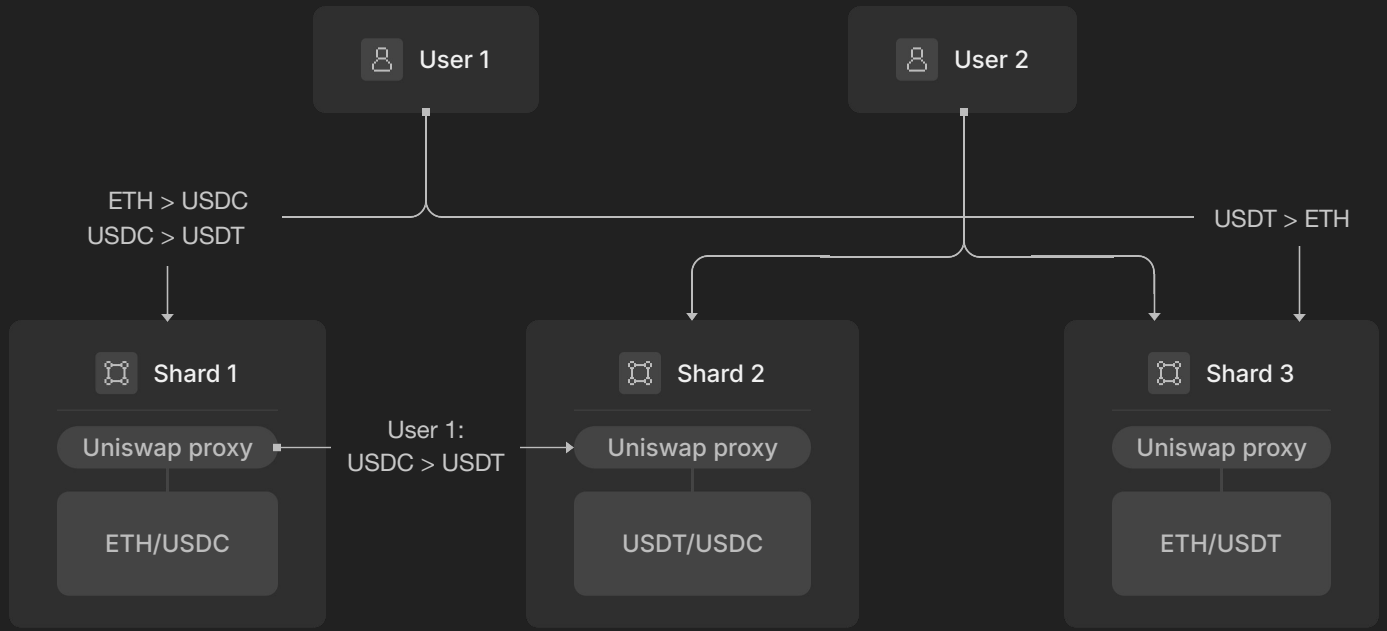
Optimistic, permissionless

Permissioned Chain Creation

Global Fee Market Model

Properties Combinations

Permissioned Chain Creation + Optimistic, permissionless = Application Scaling



Properties Combinations

DAG with Enforced Upgrades + Local Fee Market Model = Market-Driven Load Balancing

DAG with Enforced Upgrades + Optimistic, permissionless + ZKPs = Trustless Parallel Computations

=nil; Foundation

Play the =nil; Devcon game on Telegram

Earn as many points as you can to win

Top 20 players will get:

- Tangem hardware wallet card pairs
- =nil; water bottles & merchandise
- Meet & greet with =nil; team

How to earn:

Complete quests
100-10,000

Complete quizzes
50-200+

Battle other players
Win & get all player treasures

Find Nilmons around the city
To unlock quests and use new Nilmons in battles

Upgrade your Nilmons
Use treasures to power up them and increase chances to win battles

=nil;

@NilDevConGameBot

learn more about =nil; – visit nil.foundation

Thank you!

X: @ilia_shirobokov
TG: @SK0M0R0KH

https://nil.foundation/