I think I came up with an easy way to scale Ethereum. This kind of thing is usually wrong, so let me try here. For sharing security among shards, I think merged blocks are enough.

Data Structure

Changes to Block Header and Transaction

I start from the Byzantium version of Ethereum. I add a 256-bit value shardID

to the blockheader. I also add a 256-bit shardID

to the transaction.

A valid block can only contain transactions of the same shardID

as shown in the block header.

An unsealed block

is very similar to a block, but without nonce and mix hash components in the block header.

Merged Block

A merged block between two shards contain

- a mix hash
- a nonce
- an unsealed block of shard ID A
- an unsealed block of shard ID B

A merged block is valid if

- the unsealed block A

is valid

- the unsealed block B

is valid,

- The nonce and the two unsealed headers yield the mix hash, and a number smaller enough to pass both shard's current difficulty, and
- it's ancestors don't contain any fork of any shard

The blockhash of a merged block is the same for both shards. A block's parentHash can point to a merged block. That's why blockheader needs a shardID.

After a merged block, the difficulty of shards A

and B

are still independent.

Fork choice rule

(a) heaviest path (doesn't work)

First, we choose the heaviest path. A path can go along the parentHash of any shards. Its weight is the sum of difficulties. We choose the tip of the heaviest path. Its ancestors don't contain any fork of any shard, so a chain is automatically chosen for each shard.

But, then, mining on a non-heaviest-path is quite unsecured.

(b) heaviest tip

Instead of choosing a best path, we can choose the heaviest tip (considering all ancestors of the (merged) block). Then, the

ancestors of the tip do not contain forks on any shards, and we get a sequential history on all shards.

Q & A

- Is a merged block atomically contained in both shards or neither?
- Yes.
- Yes.
- why would miners merge-mine?
- because they can get rewards on both shards.
- because they can get rewards on both shards.