Below is a copy of this brief document and an image.

ABSTRACT.

We sketch a mechanism which randomly assigns each staker to their next shard by using their Verifiable Random Function (VRF). We sketch proofs for unpredictability, liveness, and biasability. Many details and optimizations are omitted in favor or conciseness and simplicity.

Definition

(Sketch.) VRF-based random next-shard mechanism

.

- A staker's VRF output determines their next shard, time at that shard, etc. When a staker must move to their next shard, they compute their VRF on an input x

based on the previous n

VRF outputs from stakers who just moved. (Say x

is the xor of the previous n

VRF outputs.)

- A new staker deposits a stake (say 32 Eth) and a public key which corresponds to their VRF. New stakers must wait n

VRF outputs from when they deposit before computing their first VRF output. For security, this first VRF output is not used as input to other staker's VRFs.

Theorem.

Assume that there is an honest majority of stakers. Then a VRF-based random next-shard mechanism gives unpredictability and liveness, but not unbiasability.

Proof. (Sketch.)

- Unpredictability is achieved by having n

large enough that there is a high probability that at least one in every n

consecutive VRF evaluations is by an honest member.

- Liveness is achieved by participation of the honest majority.

- Unbiasability is not

achieved because a staker can choose to withhold their VRF output.

Remarks.

- Bias from withholding a VRF output is local

– withholding only helps one (or few) stakers under the attacker's control. This withholding can cost their stake, so it is not worth it unless they are close to attacking a specific shard and lucky enough to be sent to that shard.

- Unbiasability may be achieved(!) with a VDF (verifiable delay function) producing the input to each VRF.

- The honest majority assumption can be relaxed to a lower percent.

- There may be an unequal number of stakers in each shard. But if the VRFs provide uniform randomness, and there are many stakers, then there is high probability that the shards have a nearly equal number of stakers.

- A beacon chain can be used to record each VRF output, along with any new staker's stake.

- VRFs are already used by Algorand and Ouroboros blockchains, but they don't have shards (yet) and have different VRF inputs and different output meaning. This mechanism is novel because inputs and outputs are local

to each staker.

[

drawing

1875×628 99.6 KB

](https://ethresear.ch/uploads/default/original/2X/9/96c95d25fd32207d5f7d5cb594826a4c79e39036.png)