Verifiable Delay Function: Application

Kaixuan Wang

Shanghai Jiao Tong University

December 9, 2020

Randomness Beacons

content...

Randomness Beacon's Applications

content...

Consensus from any Proof of Resource

Proof of resource

Proof of resource: proves miner owns X% of total resources
Break into X proofs of 1% of resources

1. Proofs $\pi_1, \pi_2, ..., \pi_X$ have distinct values
2. Each π_i gives one independent random trial:

$$R_i = HASH(\pi_i) \in [0, N]$$

3. Miner finds $R = Min(R_1, R_2, ..., R_n)$
4. Miner then evaluates a **VDF** with a time delay proportional to R on unpredictable challenge derived from π and previous block

Consensus from any Proof of Resource

Proof of resource

Miner with X% of resource should in expectation mine X% of blocks in any chain window(chain quality)

1. Miner wins block if it samples the lowest delay parameter
2. Probability that miner who makes X% of all random samples obtains the minimum (delay parameter) of all random samples is X%

Proof of replication

content...

Computational timestamping

content...