PrimeHash game for Plasma Prime

We need to use the mapping between integers and prime numbers for some cases in Plasma Prime:

- calculating H_{prime}

for Wesolowski proof

- calculating prime numbers for each coin

Also, it will be useful if we can use it without any precomputations in lazy mode.

I propose to use something like truebit protocol for deterministic mapping any uint256 number (excluding 0 and 1) to a prime number.

Let’s determine

Prime(I) := \max(n: 1 < n \leq I; n \in P)

.

We do not use any better computable subsets in the set of prime numbers, because it brings us additional work in the contract, as you can see below. Prime(I)

is not complicated to compute offchain for any 256bit I (not only PC but also cell phones are OK).

We can enumerate all plasma dust coins as Prime(I*offset)

and use not only 2^{40}

, but also 2^{50}

or more dust coins and do not need to store the data anywhere.

Also we can use PrimeHash(x) := Prime(keccak256(x))

for H_{prime}

calculation.

For onchain cases let’s use the game:

The game is simply generalizable for calculation with multiple prime numbers (it is enough to challenge one value to reject the calculation).