Short S[NT]ARK exclusion proofs for Plasma

Reading STARK-based accumulators proposed by @vbuterin, I summarize that current prooving schema looks so:

1. Arbitrary slices
2. Aligned slices
3. STARK-based accumulator
4. STARK-based exclusion proof for history reduction

Let's consider some reduction of these stages up to:

1. Arbitrary slices
2. S[NT]ARK-based exclusion proof for history reduction

We do not need to do anything with aligned slices (\div \log N

complexity) and do not need to do anything with inclusion/exclusion proof for the aligned slices (also \div \log N

complexity).

As it turned out, zk-SNARKs are useful to make batch exclusion Merkle proof for Plasma Cashflow.

The state of Plasma Cashflow is looking something like this:

[

View with better resolution.

](https://raw.githubusercontent.com/snjax/drawio/master/plasma%20cashflow%20state.svg?sanitize=true)The space of plasma at the picture equals to [0, 1000000)

. So, each block contains this interval inside the root node. There are transactions included in the block and voids inside the leaves.

It is enough to prove the existence of a NULL node at the current slice for any chunk of blocks to prove exclusion of the slice.

We do not need to prove tx validity, signatures or something like this. Here is the example circuit written on pseudocode, it is a very simple construction with Merkle prooves inside only:

gadget ExclusionProof(slice, blockSum:public, nullIntervals[N], sumMerkleProof[N] :private) for i:= 1..N: root[i]:=SumMerkleProof(nullInterval[i], NULL, sumMerkleProof[i]) nullInterval[i].x1 <= slice.x1 slice.x2 <= nullInterval[i].x2 blockSum == hashsum(root)

Below I represent computations for 10k tps plasma with one block per 5 minutes publishing:

There are about 3000000

tx per block. The Merkle tree depth is 22

. If we use 160bit cryptography, there are about 30k constraints per block. If we use 10M constraint SNARK, it can prove 300 blocks with 300 bytes proof size.

Raw Merkle proof of 300 blocks weights 300 kilobytes. So, we got x1000 disk space reduction to store the history.

There are 100k 5minute blocks per year, so the history of the coin without reduction weights about 100 Mb and history of the coin with reduction weights 100 kb.

The S[NT]ARKs do not need to be checked onchain. That means that STARKs and recursive SNARKs may be used. One thing we need to implement onchain: plasma state and challenges using S[NT]ARK-friendly hash functions. We can do it not expensive through truebit or SNARKs+truebit.

Related links

@barryWhiteHat Roll_up / roll_back snark side chain ~17000 tps

@vbuterin A sketch for a STARK-based accumulator

[Plasma call #16

](https://www.youtube.com/watch?v=0ApUUoWYt8U)

Plasma cashflow spec

@vbuterin, RSA Accumulators for Plasma Cash history reduction

Alessandro Chiesa, Lynn Chua, Matthew Weidner On cycles of pairing-friendly elliptic curves

Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza Scalable Zero Knowledge via Cycles of Elliptic Curves