**PlasmaCT Block Format**

|  |  |  |
| --- | --- | --- |
| Position | Description |  |
| 0 | BlockHash | bytes32(…below…) |
| 1 | BlockNumber | uint |
| 2 | NewOutputsMerkleRoot | bytes32 : merkel\_tree(utxo\_set) |
| 3 | TotalTxHash | bytes32 : keccak256(I[], O[], kernels[], bp[], offset) |
| 4 | NewKernelsHash | bytes32 : keccak256(new\_kernels[]) |
| 5 | S\_new | point : schnorr\_recover(new\_kernels[]) |

Normal Exit (A)

1. A wants to exit
2. A submits a Merkle proof that is a valid output for a published block

Challenge Exit (B)

1. B challenges A’s exit in the following ways:
   1. B submits TotalTx corresponding to a later BlockHash, which does not include in its outputs
      1. How to validate? (tons of gas…)

Challenge Block (B)

1. B challenges C’s block in the following ways:
   1. Challenge bulletproof in TotalTx
   2. Challenge

**PlasmaCT Transaction Types**

Basic Send:

Arbitrary Inputs, one output. No bulletproofs required.

Sender:

1. Sends

Receiver:

1. Picks random blinding factor
2. Calculates
3. Calculates
4. Publishes transaction

Change Send

Arbitrary inputs, arbitrary outputs. Bulletproofs required for each output.