This post describes a potential attack on certain implementations of plasma cash. Thanks to@gakonst for review.

Suppose for concreteness we have the following exit procedure.

1. Anyone can exit their coin by providing the last two transactions in the coin's ownership history (ie. the coin they are exiting C

and its parent P(C))

. This sets a deadline T

at some number of blocks into the future (say T = block.number + 80600

) and initializes a counter h = 0

representing the number of unaswered challenges.

1. Challenges can be made before T

; a type (i) and type (ii) challenge cancels the exit; a type (iii) challenge is written to storage and h

is incremented. [1]

1. At any time, h

can be decremented by providing a response to a type (iii) challenge (which is then deleted)

1. An exit with h = 0

can be finalized when block.number

    T

.

Then the following attack is possible:

1. Alice signs a transaction to Bob and provides the signature to the operator.

[

A

4608×3456 3.3 MB

](https://ethresear.ch/uploads/default/original/2X/e/ed15e8407fc1f8fee3e33217a0eca420b39a74db.jpeg)

1. The operator includes a double-spend from E, some spends of that, includes the spend to B among them, and withholds all the blocks

[

B

4608×3456 3.57 MB

](https://ethresear.ch/uploads/default/original/2X/5/575554081d21371c04fceac212319cba6c019e5c.jpeg)

1. Eve exits coin C
2. The only challenge possible is a type 3 challenge with coin A
3. Eve waits until the block height is greater than T to reveal B, cancelling the challenge
4. It is too late to start a new exit with B

Note that similar attacks are possible against many variants of the exit game round structure; if we require that h

be set to 0 before T

then B

can be revealed at block height T-1

. The general attack is to reveal B

“as late as possible”. An equivalent statement is that the exit game requires 5 inclusion proofs in the worst case (and not 4 as a naive analysis might conclude), or 4 rounds (instead of 3), and that the round structure must support this.

Two ways to support this include explicitly extending the exit game resolution deadline, or allowing “limbo” transactions in cancellations.

Footnotes

[1] see https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/ for definitions of type 1, type 2 and type 3 challenges