The original limbo exit described at https://ethresear.ch/t/reliable-exits-of-withheld-in-flight-transactions-limbo-exits/ solves the problem that a malicious operator could force a user in certain circumstances to go through 2 exit games to withdraw his coin. However, an analogous problem appears in this situation

[

ehGYRhz.jpg

5312×2988 478 KB

](https://ethresear.ch/uploads/default/original/2X/8/84691fe0f2f322878e8775b1f8a92d74acc4caaf.jpg)

in which a transaction spending C comitting to inclusion in B is sent, but B is withheld. We would like to cancel the fraudulent exit. Currently C must be submitted to try to challenge the exit, and if the challenge is cancelled, the cancellation reveals that C was spent in B. In that case, the revealed child of C can be submitted to actually cancel the fraudulent exit.

We can use the same technique as limbo exits to avoid the need for two challenges. We start by viewing a limbo exit as an explicit claim that the rightful owner (ie the result of the CFCR defined by the non-limbo-exit-CFCR) is contained in a set of two directly lineal coins. We can use a similar claim in the exit game.

Here is the full game spelled out, modifying the exit game from https://ethresear.ch/t/plasma-cash-with-smaller-exit-procedure-and-a-general-approach-to-safety-proofs ; there are two possible exits. For clarity “providing a proof of a transaction” means providing a merkle proof from the transaction root of a comitted plasma block, while “providing a transaction” just means providing a digitally signed message.

Type 1 Exit

1. Anyone can exit their coin by providing a proof of a transaction in their coin’s history, say C
2. An exit can be challenged in three ways: i) by providing a proof of a transaction spending C

, or ii) by providing a transaction C^*

in the coin’s history before C

, or iii) providing a proof of a transaction C^*

in the coin’s history before C

and a transaction T

spending C^*

included in a block before C

1. A type (i) challenge cancels the exit immediately. a type (ii) challenge can be cancelled by providing the direct child of C^*

. a type (iii) challenge can be cancelled by providing the direct child of C^*

which is not the output of T

, or by providing a committed transaction spending the output of T

.

Type 2 Exit

1. Anyone can exit their coin by providing a proof of a transaction in their coin’s history, say C

, and a transaction T'

spending C

. A successful exit sends ether to the output of T'

.

1. An exit can be challenged in four ways: i) by providing a proof of a transaction different from T'

spending C

, or ii) by providing a transaction C^*

in the coin’s history before C, or iii) providing a proof of a transaction C^*

in the coin’s history before C

and a transaction T

spending C^*

committing to a block before C

, or iv) providing a committed transaction spending the output of T'

.

1. Same as (3) in type 1 exits; additionally, type (iv) challenge cancels the exit immediately.