Special thanks to Karl Floersch and David Knott for helping to come up with this.

We can make exiting from Plasma cheaper in the normal case by simplifying the contents of an exit transaction; instead of actually including a Merkle proof, a transaction would simply contain a list of (block number, coin index) pairs. There would be an extra type of challenge mechanism where anyone could challenge to require you to actually provide a Merkle branch in order to complete a withdrawal.

In the normal case, this reduces the cost of a single exit to ~log(t) + log© bytes (eg. assuming one Plasma block per minute running for one year, and 1 million coins, 39 bits ~= 5 bytes); with a full Merkle proof it would have cost 640 bytes. Many exits can be batched together into a transaction with one signature.

In Plasma Cash, the extra challenge mechanism could simply exist in parallel with other challenge mechanisms; the only practical consequence is that anyone can attempt to make an invalid exit, and not just previous owners of a coin. In Minimal Viable Plasma, the only type of challenge is to provide a child UTXO proving the given TXO was spent; this could be done regardless of whether the actual TXO is provided or just an index.