This is a set of notes from discussions with David Knott and Vi.

Users who successfully challenge an action on a Plasma contract should generally receive a bond for doing so. Current thinking on the actual magnitude of this bond has assumed that the bond should simply cover the gas cost of challenging. So, although challenges aren't supposed to be profitable, challenges are supposed to be free. If users are already required to monitor the Plasma chain and challenges are free, then users have no real incentive to disable automatic challenges in their client software.

Unfortunately, bond pricing isn't as simple as it seems. Whenever multiple challenges are submitted simultaneously, only one challenge can actually be successful. Each unsuccessful challenge still needs to pay at least the base transaction gas cost (21000 gas)

. Depending on network congestion, this base cost alone can range from anywhere from <$0.01 to >$0.50.

We can try to limit the number of challenges submitted at the same time by having clients strategically wait to see if other challenges are submitted, but this won't work in every case. We run into further issues if miners choose to front-run challenge transactions. A front-running miner would place their own challenges in front of other challenges in order to collect the bond

. Challenges by other users would always fail and always have to pay at least the base gas fee. It's unlikely that front-running will happen if the bond is sufficiently low and the cost of modifying client software is high, but it's something to consider.

If challenges are not free, then users may choose to only challenge if the exiting UTXO would directly impact the safety of their funds

. As a result of exit priority, the safety of a user's UTXO is only threatened when the total funds stolen is greater than the total sum of valid UTXOs with a lower priority than the user's UTXO. If the sum stolen is less than this amount, the user can be sure that their UTXO will be processed with enough funds in the contract.

In practice, these problems probably aren't as bad as they seem. The cost of submitting an invalid exit is pretty high for even a low bond on the order of a few USD. On the high end, a failed challenge submitted every Ethereum block (that's a lot of challenges) would only run on the order of ~$100k annually. Certain parties will probably have external incentives to challenge. With changes in Ethereum 2.0, it may be possible to block these double-challenges automatically in a way that doesn't charge gas for the second challenge.

So we're probably fine for now

. However, these are problems that don't currently have a convincing economic solution. We definitely need to consider these things going forward and come up with a stronger protocol that addresses these concerns without relying on extra-protocol assumptions.