Design from conversation with vi, David Knott, Ben Jones, and Eva Beylin. Thanks to Eva Beylin & Kelsie Nabben for review/edits.

TL;DR

We can enable fast withdrawals without Plasma contracts by taking advantage of root chain smart contracts. Withdrawals can then be handled as tokenized debt, and we can build a marketplace from there.

Background

Fast withdrawals are a construction in Plasma that effectively boil down to an atomic swap between the Plasma chain and the root chain. They're useful because Plasma withdrawals are slow (2 weeks, in our implementation), and people usually want their money quite quickly. The Plasma paper discusses one such construction that relies on outputs being locked to contracts:

Funds are locked to a contract on a particular output in the Plasma chain. This occurs in a manner similar to a normal transfer, in that both parties broadcast a transaction, and then later commit that they have seen the transaction in a Plasma block. The terms of this contract is that if a contract is broadcast on the root blockchain and has been finalized, then the payment will go through in the Plasma chain.

However, we currently don't support funds locked to contracts in Plasma. This post describes a simple fast withdrawal mechanism that ensures the liquidity provider will be paid after the full withdrawal time without the need of Plasma contracts. Like the original fast withdrawal design, this design relies on Plasma data availability.

Pay-to-Smart-Contract

We take advantage of the fact that Ethereum smart contracts cannot produce signatures, and therefore cannot spend funds on the Plasma chain. However, Ethereum contracts can

initiate an exit by calling the Plasma contract. This makes it possible for a user to send child chain funds to the address of an Ethereum contract, where these funds can no longer be spent but can be withdrawn.

In the case that a user doesn't want to wait for the Plasma exit, we can enable fast withdrawals by deploying a special contract to Ethereum - let's call this a "liquidity contract". Any user may force the contract to trigger a slow Plasma exit of any utxo where the user is the sender. This action creates an ERC721 token for the user that represents the right to receive the value of the exit once it processes. The user can then quickly and simply receive value of their utxo (minus a fee in the form of a discount) by transferring or selling this token to any other user.

For clarity, here's a quick user flow:

1. Alice has 10 ETH on the child chain and wishes to quickly withdraw to the Plasma chain instead of waiting two weeks.
2. Bob is okay waiting two weeks for the exit to process, so he's willing to front Alice the money now in exchange for a discount.
3. Alice and Bob will use an Ethereum liquidity contract.
4. Alice sends her 10 (child chain) ETH to the address of the liquidity contract. This a Plasma transaction, not an Ethereum transaction.
5. Alice sees that her transaction to the contract has been included in the Plasma chain. The contract now owns a utxo received from Alice.
6. Alice calls a function in the smart contract that triggers an exit from this utxo. The contract credits Alice with a token representing the future funds from this exit.
7. Bob is willing to pay 9 ETH for a 10 ETH token that will "mature" (to take some bond terminology) in two weeks.
8. Bob has data availability, checks the Plasma chain, and sees that Alice's exit is not invalid. Bob tells Alice that he's willing to purchase her exit token.
9. Alice sells her 10 ETH token to Bob for 9 ETH. Alice receives 9 ETH now, and Bob will receive 10 ETH once the exit processes. Bob has "earned" 1 ETH (in the form of a discount) for providing a liquidity service to Alice.

Markets

To ensure that Alice is able to receive funds from the Plasma chain quickly, there must be a marketplace for her tokens. It's possible to create any number of schemes that give users the best possible price. For example, each user could hold a short auction for their token or could arrange a sale out-of-band.

It’s also possible to reintroduce the concept of rating agencies to create more liquid markets. These agencies would attest to the validity of the exit. Liquidity providers could then give a market price for each token (based on value & time to process). This means that users can quickly sell their tokens and receive their funds without having to spend time finding a liquidity provider or waiting for an auction to complete.

Furthermore, it’s probably also possible to sell parts of a token, but gas costs make this more infeasible for low-value tokens.

An auction seems like the simplest mechanism in the short-term.

Notes

As always, feedback and comments are more than welcome. Please feel free to challenge any part of this, there very well may be issues.