I have been looking into the Plasma MVP with a specific interest in the fraud proofs of this initial system. It appears to me that the following is occurring (if I am wrong please let me know and I will update the topic):

1. User makes deposit on mainnet. This somehow triggers a UTXO being generated on the plasma chain (the mechanics of this are unclear to me from the code)
2. User starts a withdrawal on the mainnet of a specific plasma UTXO belonging to him. For the MVP itlooks like this must be the initial UTXO generated from the deposit in step 1.
3. If the user has spent this TXO (in a plasma block which has been checkpointed), someone can provide that signed plasma transaction as a challenge and block the withdrawal.

A few questions arise:

1. Am I interpreting this UTXO fraud proof correctly? i.e. a user may only withdraw based on the original UTXO and anyone may prove that a malicious deposit with a signed transaction spending that UTXO?
2. How would a user withdraw a split UTXO? i.e. if I deposit 5 ETH into a plasma chain and spend 2, how could I withdraw the remaining 3? Would I include a new UTXO and similarly allow anyone to prove that I had spent that particular UTXO?
3. How does this fraud proof extend to an account-based deposit/withdrawal? i.e. is there an example of a reasonably compact fraud proof for an EVM plasma chain?