Question 2: UTXO Management in Wallets

1. Identify a denial-of-service vector in this process, i.e., an adversarial attack strategy by dishonest and wealthy users that could result in failed withdrawals for legitimate users of Moonbase. Provide a fix for this DoS vector and argue informally that user withdrawals will never fail.

If malicious users coordinate and the blockchain is pseudo anonymous they can figure out Moonbase’s public key through high-volume transaction activity and record the received UTXO’s that Moonbase possesses. With the Moonbase’s UTXO data wealthy adversaries can game the randomness by targeting high-value UTXO’s for withdrawal and then re-depositing the money back into Moonbase in very small amounts such that the UTXO’s received are too small to fund transactions for legitimate users. One possible solution is to fix the maximum withdrawal amount for a user to be equal to the amount they deposited. This way Moonbase can enforce UTXO’s coming in and out of the platform to be in equilibrium. So, if the adversary splits 10 BTC into very small amounts they can only withdraw the small amounts at a time preventing a DoS attack. Another option that can lessen the chance of a DoS attack is if Moonbase enforces deposits to be in highly frequent denominations (Ex. $100, $1000, $10000) so that the most frequent UTXO’s exist in Moonbase’s database. This way adversaries cannot withdraw large UTXO’s and dilute it in the system through tiny UTXO deposits which would disable common users from withdrawing sufficient funds.

2. For each user withdrawal in the provided scheme, recall from class that two UTXOs need to be generated: one paying the target user, and one that is kept by Moonbase representing any leftover “change”. Provide a modification to the above strategy that will reduce the number of UTXOs Moonbase must maintain in its database.

Instead of funding withdrawals with a single random UTXO, Moonbase can employ a rule that every hundred withdrawal transactions, Moonbase can create a new transaction that “collects” the leftovers into a singular UTXO’s. The consolidation can then be used to fund future withdrawals. Moonbase just needs to create a UTXO that pays itself with the input references being the last few transactions. This is better than using a single random UTXO to fund withdrawals because if adversaries do a DoS attack described above the number of UTXO’s in the system will be very large and non-usable. Creating intermediate UTXO’s that collect deposits into one as well as withdrawal leftovers will reduce the total number of UTXOs Moonbase must maintain and protects Moonbase from DoS attacks.