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.

A DoS can be a malicious user that creates very large amounts of small transactions to exhaust available UTXOs. Moonbase can set an amount limit per UTXO to reduce the risk of this DoS. For the compensating method, Moonbase should also adjust the amount limit per UTXO dynamically, assuming this method is strictly enforced, the UTXO set and transaction processing time is monitored properly, there will always be enough UTXOs so that user withdrawals will never fail.

2. For each user withdrawal in the provided scheme, recall from class that two UTXOs actually 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.

Moonbase can group multiple UTXOs that are large enough to fund the withdrawal and use smaller UTXOs to make up leftovers. This way Moonbase can reduce the amount of UTXOs they need to maintain in the database.