Nicole Su, ts885

1. A dishonest group of users (group of coordinating adversaries) could:

1. Create numerous small deposits to Moonbase, generating many small UTXOs
2. Monitor the blockchain to observe Moonbase's UTXO set
3. Time their attack when legitimate users are trying to make large withdrawals
4. Flood Moonbase with a high volume of small withdrawal requests

Since Moonbase selects UTXOs randomly, it might select small UTXOs that are insufficient for large legitimate withdrawals. If most of Moonbase's funds become fragmented into many small UTXOs, large withdrawals could fail due to the inability to find a single UTXO large enough to cover them. In this case, transactions are too large, making them expensive or even invalid due to Bitcoin’s block size limit.

Possible fixs:

1. Periodically merge small UTXOs into larger ones to keep the UTXO set manageable.
2. Replace the random selection of UTXOs to select UTXOs intelligently, preferring fewer, larger inputs instead of many small ones. (for example: maintain a reserve of larger UTXOs specifically for handling large withdrawals)
3. Set minimum deposit sizes to prevent cheap UTXO spam.

2. Moonbase can adopt batched withdrawals which is process multiple withdrawals in a single transaction when possible. They can combine several pending withdrawals into one transaction with multiple outputs. This reduces the number of transactions and therefore the number of change UTXOs.