Blockchain Technology Fall, 2023
Tutorial 6, Week 12 (Nov 28)
Due Date: Dec 22

Questions(100 points):
Suppose Alice has a UTXO/coin $(PK_A, 115)$ on bitcoin blockchain, Bob has a UTXO/coin $(PK_B, 120)$, and Carl has a UTXO/coin $(PK_C, 12)$. Suppose someone has known the binding between the public keys and the real identities, say PK_A and Alice,PK_B and Bob, and PK_C and Carl. Please describe how the users can use the coin-mix service to enhance their privacy.
Hints: you need to describe the procedure in details, include the information between the users and the server, as well as the transactions generated in this procedure.