Michael Scholl
ID: 619801206

Project 3 Stellar

For this project we needed to implement a Coin Flip game using the Stellar network. To go about this project I first had to research everything I was hoping to know about the Stellar system and how to interact with it. I followed the guide in order to understand how to send and receive lumens over the test network. I assumed for this project I was going to need to use a server and therefore used the same Corba server from my previous project that had some errors I guess as I was coding it on a mac with Eclipse. With the Corba server I would host all the information for interaction but did not want to share any of the bankers or users KeyPairs over the network. A banker would log into the server and say that he was banker while a user would log in as a user only knowing the bankers account ID. The server would host the game and when a bet was placed the secret code would be sent to the server and the secret code would also be hashed into the memo of the Stellar network payment. The server would then send the secret code to the banker while the banker checked to see if the secret code matched the hash code given over the memo. This would be confirmed or not confirmed depending on whether or not the values matched.

I felt that the idea I had above was a fair way of implementing the system and that the ability to cheat was low due to the server only seeing the number. The banker would be the only one receiving both hash values and numbers. So as long as the banker is playing fair and sends the winnings out cheating should not occur. The issue was I found no way of reading the memos correctly so hashing had to occur over the server and to the banker. Resulting in my network being hackable assuming you could get to the server. This strategy could be changed by hashing the secret code on server side but would most likely leave the same issues.