Simulation of Distributed Cryptocurrency System

Luke Beatty, Matt Zahar

Our goal is to implement a cryptocurrency system that is able to broadcast transactions, broadcast new blocks, and have the functionality to mine for new blocks. We will implement a blockchain system that holds previous transaction blocks and gives users the ability to push and pull necessary data to and from the blockchain through a handful of functions. Users will be able to send and receive cryptocurrency by creating new transactions and signing it with their own secret key. These transactions are then verified by checking the signatures, ensuring balances are non-negative, and checking for double spending. All users will have access to the same puzzle and will have the ability to push their solutions to the blockchain, which in turn will verify the solution and broadcast the new block if the solution is correct. We will create mock transactions and mining solutions in order to test the above functionality.