# Abstract

**Abstract.** Cryptocurrency is a decentralized digital currency that can be sent from user to user on a peer-to-peer network. The public ledger used to record these transactions is called the *Blockchain*. The Blockchain is run by groups or pools of participants called *miners*. The collaboration of miners and their rewards are proportional to the resources they dedicate to mining a *block* on the Blockchain. However, there are strategies miners can use which results in profitability not being proportional to the resources dedicated.

The aim of this project is to demonstrate strategies that don’t follow the common protocol, for miners to maximise their own profits larger than the share of resources they contribute to the pool. This is known as *“Selfish Mining”*. Selfish Mining, if profitable, is considered to be a threat to Bitcoin and other Blockchain based cryptocurrencies, as it undermines the principle of decentralization as honest miners could join the ever-growing selfish *pool* of miners. I created a program in Python that emulates a well discussed Selfish Mining Attack, discussed in “Majority is not Enough: Bitcoin Mining is Vulnerable” by Ittay Eyal and Emin Gün Sirer [1]. This program demonstrates that Selfish Mining is profitable with less than half of the computational power available to the pool. From this model, I have created an alternate strategy, in order to demonstrate how profitability varies from strategy to strategy.