ESE 403 Fall 2018
Projects
Due 5PM Monday, November 26

Blockchain: Bitcoin and cryptocurrencies are potentially the future of payment systems. Blockchain technology is based on a consensus game to determine who adds the next block of transactions to the chain and, thus, win the transaction fees. In this project you will be considering Nash equilibria for this consensus game to find how many resources to devote to mining operations.
Initial Reference: Tullock (1980)

Detailed Description:
Bitcoin and blockchain truly began with Nakamoto's white paper [1]. The foundation of this decentralized ledger is the mining operations. In short, miners collect transactions together into "blocks" to add to the ledger. The manner in which the block is added is decided by a consensus game. A hard cryptographic problem is presented to all miners, the first to solve the problem wins the transaction fees on the block plus a fixed fee. Key to this game is that the more resources are applied, the harder it is to win, making it a Tullock contest [2]. In this setting, if miner i has x_i resources devoted to mining operations its expected payout is (a fixed multiplier of) $x_i/\sum_j x_j$. In determining the resources to consider investing in mining operations, the miner needs to purchase computational resources (fixed costs) and pay for energy bills (variable costs). Given fees from winning the mining operation c and energy costs for miner i given by e_i, miner i is thus seeking to maximize:

$$\max \left(\frac{c}{\sum_j x_j} - e_i\right)x_i \quad \text{s.t.} \quad x_i \leq y_i, \quad x_i \geq 0$$

where y_i are the computational resources of miner i. Over time, each miner must decide, also, how many resources to devote to investing in computational resources y_i. This will depend on the costs of computers and the expected long term returns of investing.

For this project you should consider the game theoretic problem with fixed computational resources. You should follow this up by formulating and considering a setting with each miner also determining their long term investments in computational resources. Sensitivity to returns c and costs for energy e_i and computational resources should also be considered.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. White paper.

[2] Gordon Tullock. Efficient rent seeking. In *Toward a Theory of Rent Seeking Society*, pages 97–112. Texas A&M University Press, 1980.