Cryptofinance

by Cyril Grunspan

December 10, 2025

1 Statistics

1.1

Choose a hash function, generate a list of hashes, and check statistically whether the distribution is uniform.

1.2

Choose a hash function and create proof-of-work problems suited to your computer. Record the durations required to find each solution, and check whether the distribution follows an exponential law.

2 Mining strategies

2.1

Simulate strategy 1+2 and numerically evaluate its performance. Compare the results with the theoretical formulas.

2.2

Same question with selfish mining. Plot the graph highlighting the parameters (q, γ), where q denotes the miner's hashing power and γ its connectivity, for which the strategy is more profitable than the honest one.

2.3

Consider the optimal selfish mining. Choose a connectivity parameter and hashing power q. Determine, as a function of (a, h), the optimal decision the miner should make, where a is the number of blocks mined by the attacker on their fork and h is the number of blocks mined by the honest miners.

3 Bitcoin Thresholds

3.1 Determine the hashing power threshold above which an otherwise honest miner would find it advantageous to mine on an orphan block they produced, despite being one block behind the official blockchain.

3.2

In the case where a rational miner has no connectivity ($\gamma = 0$), determine the threshold in terms of hashing power beyond which this miner has no incentive to reveal a block they have just discovered on top of a block from the official blockchain.

4 Bonus

4.1

Study the possibility of conducting repeated double-spending attacks. Define a framework for such attacks (for example, if the miner's delay relative to the official blockchain exceeds a fixed value A, they abandon the attack and resume mining on the latest block of the official blockchain), and evaluate the performance of the attack as a function of the double-spent amount. Conclusions?

4.2

Implement the article *Commitment Attacks on Ethereum's Reward Mechanism.* https://arxiv.org/abs/2407.19479