Problem 1. Suppose two groups independently implement the Bitcoin protocol. Some miners run implementation A and other miners run implementation B. At some point an attacker finds a vulnerability in implementation A that causes miners running that implementation to accept transactions that double spend a UTXO. Implementation B treats such transactions as invalid.

a. Suppose 80% of the mining power runs the buggy implementation and 20% runs the non-buggy one. What will happen to the blockchain once a block containing a double-spending transaction is submitted to the network?

b. What will happen to the blockchain in the reverse situation where 20% of the mining power runs the buggy implementation and 80% runs the non-buggy one?

Problem 2. In this exercise we look at two estimates for the amount of energy consumed by the Bitcoin network. Assume in your answer that the current exchange rate is 1BTC = US$6000 and that there are no transaction fees (only the block reward of 12.5BTC per block). Recall that energy is measured in killoWatt-hours (kWH). You may assume that one bitcoin block is generated every 10 minutes exactly.

a. Estimate the network's hourly energy consumption assuming the entire block reward is spent on electricity for mining. Use US$0.05/kWH as the price of energy and express your answer in kWH.

b. Next, estimate the network's hourly energy consumption assuming all mining is done on an Antminer S9 Hydro that has a hash rate of 18 terra-hash/sec and consumes 1.7 kW of power (running the device for an hour consumes 1.7 kWH of energy). Assume the current difficulty of generating a bitcoin block is $D = 2^{75}$.

c. Explain why there is such a large gap between the two estimates.

Problem 3. Recall that a selfish miner temporarily refrains from publishing mined blocks in an effort to get several blocks ahead of other miners, thereby causing other miners to waste effort mining orphan blocks. When a selfish miner is only one block S ahead of the public chain, if another miner mines and publishes a block O at the same height as S, the selfish miner immediately publishes S. Let γ be the probability that, when this happens, an honest miner will try to mine the next block on S instead of on O. What is a backwards-compatible change in honest miners' behavior that would result in $\gamma \approx 0.5$?

Problem 4. Mining pool sabotage. Recall that in section we discussed now mining pools enable individual miners to lower the variance of their earnings, while keeping the same expected returns. Participants repeatedly submit shares (blocks that are valid at a lower difficulty) to prove how

much work they are doing. Whenever the pool finds a block, the coinbase from that block is split among the participants in proportion to the number of shares each submitted. One risk of this is sabotage, in which a participant submits shares, but withholds full solutions if they are found (no coinbase is awarded for these withheld solutions).

a. Consider a participant with mining power $\beta \in [0, 1]$ (as a fraction of global mining power) in a pool with total mining power $\alpha \in [0, 1]$ (as a fraction of global mining power), where $\beta < \alpha$. What is the expected fraction of the overall mining rewards (the rewards collectively earned by the entire network) that this individual will earn if he or she mine honestly? Assume rewards are distributed proportionally to the number of shares submitted by each participant.
Hint: there is no need for complicated expectation calculations throughout this entire question.

b. What is the expected fraction of the overall mining rewards (the rewards collectively earned by the entire network) that this individual will earn if it devotes all of its power to sabotage?
Hint: Because β power is no longer used to find blocks, the total network mining power is now only $(1 - \beta)$ times its full power. Therefore, P's useful mining power, as a fraction of the entire network, is now $(\alpha - \beta)/(1 - \beta)$.

c. Now consider two pools, P_1 and P_2 with mining power α_1 and α_2, respectively. What will P_2's expected share of the total earnings be if it dedicates $\beta < \alpha_2$ power towards sabotaging P_1? Note that when P_2 finds a block, it gets the entire coinbase. When P_1 finds a block, P_2 receives a fraction of the coinbase proportional to the number of shares P_2 generated while mining for P_1.
Hint: P_1's total mining power is now $\alpha_1 + \beta$, but only α_1 is used for finding a new block.

d. Provide concrete values for $\alpha_1, \alpha_2, \beta \in [0, 1]$ in which this attack is profitable for P_2 over honest behavior.

Problem 6. Bob posts the following wallet contract to Ethereum to manage his personal finances:

```
contract BobWallet {
    function pay(address dest, uint amount) {
       if (tx.origin == HardcodedBobAddress) dest.send(amount);
} }
```

Suppose Mallory can trick Bob into calling a method on a contract she controls. Explain how Mallory can transfer all of Bobs money to her own account.