Homework2

Part 1 (Selfish mining and mining pools)

Read the following materials about selfish mining attacks and block withholding attacks among mining pools:

1. Selfish mining paper: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf
2. Mining Pool System Study (Read Chapter 6): https://arxiv.org/pdf/1112.4980.pdf
3. How to destroy Bitcoin (Optional): https://www.bitcoin.org.hk/media/2017/05/How_to_Destroy_Bitcoin.pdf

You may also want to search the web for additional materials. Then answer the following questions.

Why withholding a mined block can enable the attacker to gain more rewards? Note that the attacker still expects to generate the same number of blocks.

In the selfish mining strategy, if the attacker always loses the propagation battle, how much computation power does he need for the attack to be profitable? Why?

Consider the fact that most miners now join mining pools to mine cryptocurrencies, what's the economic consequence of the selfish mining vulnerability?

Search the web to survey the mining pool distributions of top cryptocurrencies: BTC, ETH, LTC, XMR, and ZEC. How many of them are vulnerable to selfish mining attacks?

Describe the rationale of the block withholding attack. Why this can be a strategy for a large mining pool to attack small mining pools.

In reality, selfish mining does not happen very often but the block withholding attack happens a lot. What's the reasons behind this?

Any other questions you want to discuss in the class?

Part 2 (Ethereum)

Read the Ethereum white paper (https://github.com/ethereum/wiki/wiki/White-Paper). Answer the following questions:

Ethereum uses account model to store the blockchain state. One claims that the account model can reduce the average size of simple transfer transactions comparing to the UTXO model. Do you think this is true or not? Explain why.

One claims that comparing to the account model in Ethereum, the UTXO model can provide anonymous transactions if the user creates a new address for every transaction. Do you think this is true or not? Explain why.

Why Ethereum introduces a GAS limit for the block? What if we remove the GAS limit and put back the traditional block limit of 1MB like Bitcoin?

Ethereum sets up a different GAS amount for different EVM operations. Why?