7CCSMDLC TUTORIAL QUESTIONS and SOLUTIONS

TOPIC 3: MINING

TUTORIALS WEEK 4

Q1. What is measured by Bitcoin Days Destroyed (aka Coindays destroyed)? What were the coindays destroyed on Bitcoin Blocks 630,000 and 668,005?

Bitcoin days destroyed in a block is a measure of transaction volume on the Bitcoin Blockchain. It is obtained by calculating, for each input to each transaction in a block, the number of bitcoin in that input to the transaction multiplied by the number of days since those bitcoin in that input were last spent. This gives the number of coindays destroyed for that input, and these coindays destroyed values are then aggregated over all inputs to all transactions to the particular block.

Block 630,000:	6,836.56 coindays destroyed
Block 668,005:	21,392.41 coindays destroyed

Source: blockchair.com/bitcoin/block/630000

Q2. Does Ethereum use the UTXO model used by Bitcoin? Why or why not? What are the advantages and disadvantages of UTXO-based systems versus account-based systems?

No. Ethereum does not use an UTXO system, but uses an account-based system.

Ethereum's original purpose was to provide a platform for the operation of smart contracts, and smart contracts work better with an account-based system than with an UTXO system. (The reason for this is because account-based systems enable multiple-ownership of transaction outputs.)

The main advantages of an UTXO system are:

- UTXO allows for Simple Payment Verification, where a client verifying payment does not need to download the entire Bitcoin blockchain.
- This allows for multiple verification processes checking on different transactions can do so in parallel since they are checking on different inputs, which allows for greater scalability.
- UTXO systems allow users to generate different system addresses for the outputs for each transaction, which supports privacy of transactions.

The main disadvantages of UTXO are:

- Apps built on top of the Bitcoin blockchain are limited in the amount of blockchain state they can impact. This feature may be considered by some to be a security advantage, since it reduces the potential impact of programs running over the blockchain.
- Each output is owned by one user (the user having the private key for that Bitcoin address), whereas use of smart contracts may often require outputs to be owned by multiple users.

The advantages and disadvantages for account-based systems are the reverse of these, with the addition of:

- Most people find it easier to understand account-based systems, since bank accounts and most other financial accounts (eg, electricity accounts) operate this way.

Q3. What is a "Goldfinger" attack on Bitcoin? Is there a plausible situation where such an attack makes economic sense for the attackers? What would the attackers need?

A Goldfinger attack is named after the character Mr Auric Goldfinger in the 1964 James Bond movie, *Goldfinger*. In the movie, Mr Goldfinger seeks to contaminate with radiation the US Government's reserves of gold, thereby reducing the world supply of gold. He believes this will lead to an increase in the price of gold, thereby making his own holdings of gold more valuable.

Based on this, a Goldfinger attack on Bitcoin is a malicious 51% attack seeking to undermine the economic value of Bitcoin. Within the Bitcoin system, there would seem to be no rational economic motivations for such an attack. However, from outside the system, motivations could be:

- For reasons of national security or law enforcement, since many criminal web-sites use Bitcoin for payment, a government or state entity might seek to bring the system down.
- A non-state actor, such as a social movement, could seek to undermine the system to achieve some social goal – for example, environmental groups opposed to the high power usage caused by the PoW protocol may seek to reduce or eliminate that usage by reducing public confidence in the Bitcoin blockchain.
- For wider economic reasons. For example, the attackers might reason that a successful attack would lead to many people selling their Bitcoin holdings, and so prices could fall. If the attackers had taken so-called "short" positions (i.e., positions on a derivatives or futures exchange betting that the Bitcoin price will fall) before the attack, then they would stand to make a profit from a fall in the price.

These are all plausible reasons from outside the Bitcoin system that could motivate a malicious attacker or attackers. The attacker or attackers would need more than 50% hashing power (which is usally referred to as "51% hashing power").