

CSEC 519
Blockchain and Cryptocurrency Technologies
Homework 3

Deadline 25 May 2023 09:40
NO LATE SUBMISSIONS !!!!!

Investigate the Bitcoin block n using blockchain.com (or any similar webpage or a local copy of the Bitcoin blockchain) where n is your 6-digit METU ID number (NOT your full 7-digit ID):

1. (20 Points) **Hash Puzzle Solution:** What is the hash of the block header? How many zero **bits** does it start with?
2. (20 Points) **Coinbase Transaction:** Investigate the coinbase transaction. What are the block and fee rewards? Is there anything the miner included in the coinbase transaction to work as a nonce to solve the mining puzzle (anything other than transferring the mining fees to an address)?
3. (20 Points) **Wallets:** How many transactions are in that block? Count every **different** incoming and outgoing addresses. What are the percentages of regular wallets (that start with "1"), P2SH addresses (that start with "3"), and BECH32 addresses (that start with "bc1")? Can you explain the huge difference between these three numbers?
4. (20 Points) **Vanity Addresses:** List the vanity addresses in that block (if there are any)?
5. (10 Points) **Hidden Messages:** List the hidden messages included in transactions (if there are any)?
6. (10 Points) **Hidden Messages 2:** Find at least one hidden message in the block 666666 of Bitcoin Cash (BCH), not the Bitcoin (BTC).

NOTE: You are expected to submit your homework as a single PDF file.