CSE 40622 Cryptography
Writing Assignment 10 (Lecture 23-26)

Name: Walker Bagley (wbagley)

1. (Page 10-11, 15pts) Full nodes do not need to check whether a transaction already exists in the blockchain or not. Why is that not necessary in the Bitcoin protocol? In other words, why would duplicate transactions (*e.g.,* "send 10 BTC from UTXO-1 to addr-A") not be included in the Bitcoin's blockchain?

   Answer:

   If a transaction already exists in the blockchain, then the input UTXO will have been spent already and thus is not available. So, when the nodes go to validate a new block with a duplicate transaction, they will fail as there is no UTXO source for the duplicate transaction.

2. (Page 17, 15pts) Assume that the SHA-256's digest is equally likely to be any integer from 0 to $2^{256}-1$. Use this as well as the consensus mechanism of the Bitcoin to argue that miners are well-motivated to monitor the growth of blockchain so that they can discard the hash calculation with $Hash_t$ and use the newly added hash $Hash_{t+1}$ for their hash calculation. Assume that the miners' only objective is to get the block rewards.

   * Miners can choose to keep doing their hash calculation and add the block at the same height as the recently added one. Why would they want to discard their current work and switch to the recently added block?

   Answer:

   If the miners' only objective is to get block rewards, then they should monitor the growth of the blockchain and move to calculating the next hash if a block is added. This is because once a hash is calculated and a block is added to the blockchain, the addition is broadcast to all other nodes, which will form a consensus on the updated blockchain. So, if the miner were to continue working on calculating the hash for a block that has already been added, it will become orphaned since the blockchain already reflects the addition of that block. Further, because the hashes are evenly distributed from 0 to $2^{256}-1$, there is no "progress" to be lost by moving on to calculate the next hash or advantage in staying on the current hash.

3. (Page 19, 15 pts) Taeho claims that Satoshi's expectation is likely to be false because of the following reasons.

   - The target θ is already too low nowadays, and it takes too much electricity and time for finding a block.
   - Because of the cost, miners are not motivated to perform mining if the transaction fees are not large enough.
   - Users can hardly pay too much as the transaction fees, so eventually the Bitcoin network will die without miners willing to mine blocks.

   Argue against Taeho's claim and explain why his claim is not necessarily true.

   - Hint: What happens if fewer miners participate in mining...?

   Answer:

   Realistically, with the high cost associated with mining blocks, there will be a decrease in the number of miners willing to compete, which would reduce the number of orphaned blocks and time "wasted" by miners looking for nonces for a block that another miner is able to find first. Ideally, the time spent mining blocks that don't end up generating profit by being added to the blockchain would be reduced to 0, but nonetheless would decrease. Then, there will still be incentive for the remaining miners to continue, thus extending the life of the Bitcoin network. Further, with less mining competition,

there will be more incentive for miners to include multiple transactions in their blocks, which would help them earn more in transaction fees as well as the block rewards, which are decreasing, meaning transaction fees become more important with each block that is mined.

4. (Out of no where, 20 pts) Explain why the following behaviors will not give attackers free bitcoin.

   4.1. Write an arbitrarily large change amount back to attackers' address in the "change" output so that attackers generate free bitcoin for themselves.

   Answer:

   The source UTXO for the transaction does not necessarily have enough Bitcoin to pay for an arbitrarily large transaction fee. The sum of transaction outputs must not exceed the sum of inputs, so this is impossible.

   4.2. Instead of the current block reward, miners write 50 BTC as the block reward in the CoinBase transaction so that they get 50 BTC as block rewards regardless of the halving schedule.

   Answer:

   No honest nodes will accept/validate this block since the CoinBase transaction must match the halving schedule, so it will not get published to the blockchain, therefore nullifying its value.

   4.3. Broadcast the block even if $Hash_t$ is larger than the target θ_t in order to earn the block reward.

   Answer:

   Honest nodes that have adjusted the target θ_t will use that target to validate incoming blocks and thus will reject the block with a hash exceeding the threshold.

   4.4. Hard-code the value 0 to $Hash_t$ so that $Hash_t < \theta_t$ will be always true. **Answer:**

   If $Hash_t = 0$ it does not represent the data contained within the block and thus is not a correctly computed hash. So when nodes try to validate this block, the hash will be incorrect and the block will be rejected.

5. (Page 20-21, 15pts) What makes it impossible for the miners to cheat by stealing the block rewards when s/he discovers the valid block header (*i.e.,* the right nonce leading to $Hash_t < \theta_t$)? Why can't s/he just broadcast the block and receive the block reward on his/her own? Assume that the pool leader has some way to verify whether pool members correctly calculate the hash by using the block given by the pool leader.

   Answer:

   The miners are only given $H(b_t)$ and $Hash_{t-1}$, so they have enough information to calculate the hash of the block if they find the right nonce. However, only the pool leader has the actual information/transactions contained by the block and therefore the miners cannot broadcast the block on their own since it must contain the information leading to the correct hash.