Homework 5 - Bitcoin

Foundations of Blockchain Technology and cryptocurrencies

Fall 2019

Sharif Blockchain Lab
Sharif University of Technology
Department of Electrical Engineering

Deadline: Sunday 1398/9/17 At the beginning of the class

(The Homeworks will be collected at the beginning of the class. 3 minutes after the start of the class the homeworks will not be accepted).

Do you really think you know Bitcoin and Ethereum?

In this question, we aim to resolve the many unanswered questions you may have about Bitcoin and Ethereum. Answer 25 of the questions thoroughly. Try to choose those that you do not know the answer beforehand. Don't hesitate to search.

1. What information exists in a block header? Find the block which the number is equal to the 5 rightmost digits of your Student ID and show the existing data on that block.
2. Calculate the throughput of the Bitcoin network (Transaction per second) according to the current maximum size of the Bitcoin block size and minimum transaction size?
3. Assume you want to send your friend some Bitcoin. What information do you need from your friend in order to send him Bitcoin.
4. What is the negative consequence of decreasing block time from ten minutes to 10 seconds?
5. Who determines the networks difficulty? Is it possible to difficulty be different for miners?
6. Is it possible that sometimes people see different versions of blockchain in Bitcoin network?
7. Can two double spend transactions exist in the same chain, even for a moment? What about two forked chains? How does Bitcoin handle this problem?
8. The nonce field size in Bitcoin is 32 bits. 232 states may not be enough to solve the Proof of Work puzzle. How can miners extend the probing space?
9. What is the motivations for running full nodes?
10. Someone states that an address can be generated offline. Is his claim valid?
11. If you loose your private key, can you access your account in some other way?
12. Assume you have lost your Bitcoin address. How can you recover your address?
13. What is the goal of having checksum in Bitcoin addresses?

14. Can you obtain someones public key by having his/her address?

15. After you issue a transaction, what do you do in order to propagate the transaction to the network?

16. When creating a transaction, do you determine the receiver of the fee?

17. When and how does the miner receive his reward?

18. When a miner mines a block, does he instantly and definitly receive his rewards? Is it possible to mine a block and not get a reward? Explain.

19. Is it possible for a transaction to never be mined? Can you spend that money again? Will it count as double spending?

20. Whats the difference between hard fork and soft fork? Give an example for each of them in the Bitcoin network.

21. How does a node find other nodes to connect to in the network?

22. Why would a miner put your transaction in a block? How can you incentivize the miners to include your transaction in their block faster?

23. Ultimately when the reward for building block becomes zero, what is miners motivation for building them?

24. Is it right to assume that always a miner with most processing power wins? Why?

25. Explain SPV algorithm. Considering the current network information, how many expected bits of information does a node need in order to prove a transaction exists in the network using SPV?

26. What is the difference between an UTXO base network and an account base?

27. Assuming that the total hash power of the network stays constant, what is the probability that a block will be found in the next 10 minutes?

28. What is the incentive for people to join mining pools?

29. How can someone that is part of a mining pool, prove that he is putting effort in mining?

30. What is the difference between mempool and mining pool.

31. Alice has paid her rent to Bob in advance, using a Bitcoin transaction with nLocktime of 1 month. How can Bob make sure that she doesnt spend the same UTXO sooner?

32. Explain the flooding algorithm in the Bitcoin network.

33. How can a SPV node prevent others from mapping its addresses to its IP?

34. A miner may have more transactions in its pool than what can be included in a block. How does it choose the transactions to build the block?

35. Is it possible for a miner to work on empty blocks (only including the coinbase transaction)? 2

36. Is it possible for 2 miners working on exactly identical blocks? Why?
37. What is the purpose of reward halving in Bitcoin? When is the next halving?
38. What is the difference between Bitcoin Cash and Bitcoin Gold?
39. A user doesnt like Bitcoin Cash, but he had 10 Bitcoins before the fork. How many Bitcoin and Bitcoin Cash does he have after the fork?
40. What are Uncle Blocks in Ethereum blockchain? What is the implication of having them in system?
41. Which script language is Turing-complete, bitcoin or ethereum?How it solves infinite loop?
42. A block header in ethereum blockchain contains which roots? explain about them briefly.
43. A ethereum account contains which fields? explain about them briefly.

The Gamblers Ruin Problem

In the Bitcoin paper[1], the security is modeled with the Gamblers Ruin problem in section 11. Explain this problem and its solution. Also explain the relation between this problem and Bitcoin. Argue whether this model is a complete security model for Bitcoin or not.

Bitcoin script

Alice is on a backpacking trip and is worried about her devices con- taining private keys getting stolen. She wants to store her bitcoins in such a way that they can be redeemed via knowledge of a password. Accordingly, she stores them in the following **ScriptPubKey** address:

```
OP_SHA256
<0xeb271cbcc2340d0b0e6212903e29f22e578ff69b>
OP_EQUAL
```

a Write a ScriptSig script that will successfully redeem this transaction given the password.
Hint: it should only be one line long.

b Suppose Alice chooses an eight character password. Explain why her bitcoins can be stolen soon after her UTXOs are posted to the blockchain. You may assume that computing SHA256 of all eight character passwords can be done in reasonable time.

c Suppose Alice chooses a strong 20 character passphrase. Is the ScriptPubKey above a secure way to protect her bitcoins? Why or why not?
Hint: reason through what happens when she tries to redeem her bitcoins.

[1] https://bitcoin.org/bitcoin.pdf