NAME: _____

CS 401R Blockchain Technologies

Winter 2020
Mid-Term Exam

Open Book. No Time Limit.

Multiple choice section: you may write explanatory notes on your test if a question is ambiguous.

Written answer questions: Answer each question as completely as possible. Partial credit may be given. Write legibly and explain your thoughts and arguments clearly. Remember, the easier it is to read your answer, the easier it is to give you credit. If a question seems ambiguous, make reasonable assumptions, state your assumptions, and then answer the question accordingly. Be sure to answer all parts of the questions. If you need more room to answer a question, you may write on the back of any page. I encourage you to make your answers clear and concise. Extra credit may be given for especially well-written exams.

Use these examples as background when answering questions about scripts

Bitcoin Script Samples:

OP_DUP OP_HASH160 <PubkeyHash> OP_EQUALVERIFY OP_CHECKSIG

<Sig> <PubKey>

OP_HASH160 <Hash160(redeemScript)> OP_EQUAL

<OP_0> <sig> [sig] [sig...] <redeemScript>

redeem script: <OP_2> <A pubkey> <B pubkey> <C pubkey> <OP_3> OP_CHECKMULTISIG

Part 1 Multiple Choice

1. In the Bitcoin network, when all the miners are working to determine the next block in the blockchain, which of the following are exactly the same (identical) for all miners? Assume no forking is in progress. (select all that apply)

A. The target value in the block header
B. The Merkle root in the block header
C. The previous hash in the block header
D. The coinbase transaction contents
E. The hash of the current block

2. Which of the following are required for *creating* a digital signature? (select all that apply)

A. The public key
B. The private key
C. Both the public and private key
D. No keys are required
E. Message to be signed
F. Hashing algorithm

3. Which of the following types of modifications of a blockchain data structure can be detected by someone who holds a hash pointer to the most recent block in the chain? (select all that apply)

A. Deletion of a block
B. Re-ordering of blocks
C. Inserting a new genesis block
D. Removing a transaction from a block

4. In a typical transaction (not the coinbase transaction)

A. There is one signature that covers all the inputs
B. Each signature signs a single output
C. Each output contains a signature
D. Each input contains a signature

5. Bitcoin Micropayments use the following (select all that apply)

A. Proof of burn
B. Tor
C. Pay-to-script hash
D. Time-locked transactions
E. Multisignature transactions

6. Which of the following require a soft fork? (select all that apply)

A. Decreasing the maximum permitted size of blocks
B. Increasing the maximum permitted size of blocks
C. Disabling the OP_SHA1 instruction
D. Require that each transaction sort the outputs in order

7. Blocks contain a tree of transactions instead of a flat list because (select all that apply)

A. It is more efficient proving that a transaction is included in a block
B. It results in smaller blocks
C. It is easier to insert or remove transactions while the block is being assembled
D. It is easier to search for a given transaction

8. Which of the following statements are true about cold wallet storage? (select all that apply)
A. Cold storage stores keys in a device without network access
B. Cold storage can store any number of bitcoins
C. Cold storage is harder to use
D. Hot storage needs to contact the cold storage in order to transfer bitcoins to it

9. Which of the following observations usually suggests that addresses A and B may be controlled by the same user/entity?
A. There is a transaction with A and B as output addresses
B. There is a transaction with A and B an input addresses
C. There is a transaction with A and B as input addresses

10. A block in the blockchain was found at time t. What is the probability that the next block was found at or before time t + 10 minutes? Assume that the total hash power of the network stays constant.
A. More than 50%
B. Less than 50%
C. Exactly 50%

11. If two conflicting transactions A -> B and A -> C are both broadcast almost simultaneously from different nodes, what determines which one will eventually end up in the block chain?
A. Both transactions will end up in the blockchain in time
B. The miner who finds the next block will likely resolve the tie by including one of the transactions in the block
C. The transaction that was broadcast first will win
D. The transaction that reaches the majority of the nodes first will win

12. How is the Bitcoin difficulty defined?
A. 51% or more
B. current_target / maximum_target
C. maximum_target / current_target
D. The time it takes to find the next block

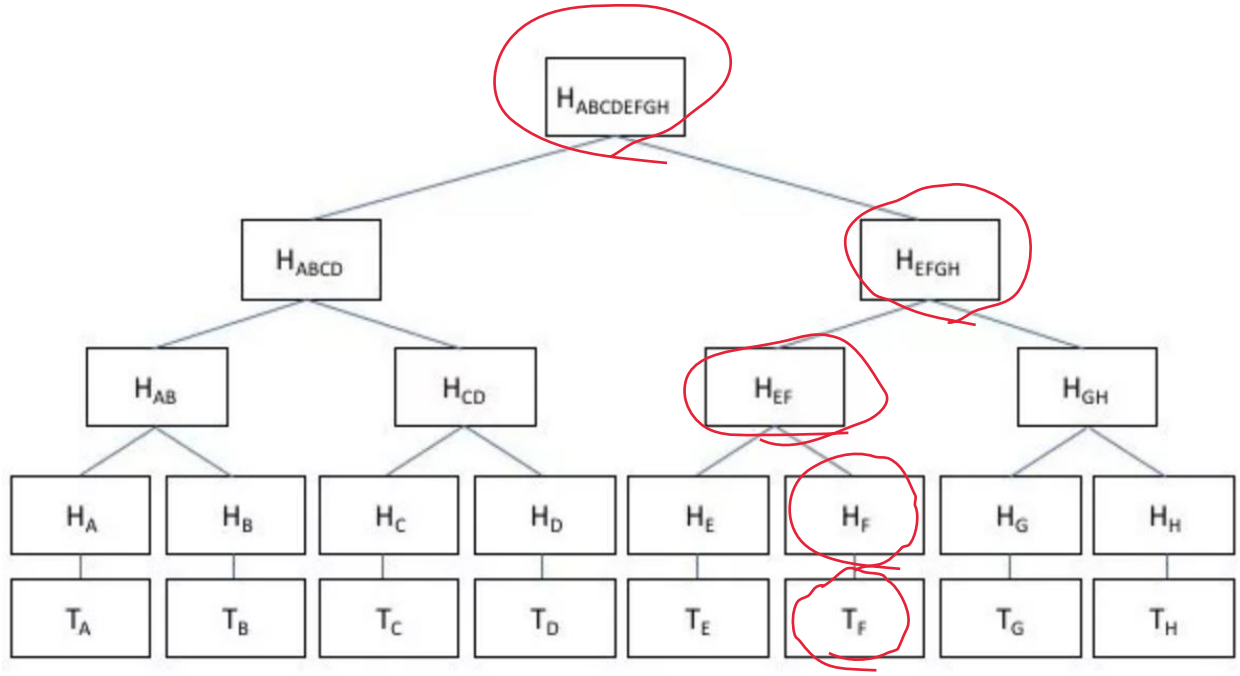
13. Which of the following does Bitcoin support? (select all that apply) For each one, write a short sentence explaining why or why not. Limit to one sentence each.
A. Anonymity
B. Pseudonymity
C. Unlinkability

14. Bitcoin supports smart contracts. (provide a brief explanation of your answer)
A. True
B. False

15. Which of the following is true about transaction fees? (select all the apply)
A. The transaction fee is equal to the sum of the inputs minus the sum of the outputs
B. The transaction fee is equal to the sum of the outputs minus the sum of the inputs
C. The transaction fee is paid to the miner that proposes the block

Part 2 Written Answer

16. Suppose a verifier has only the root of a Merkle tree. Show the proof of inclusion that would be sent to the verifier for transaction F in the following Merkle tree by **circling each node** in the tree that will be included in the proof.



17. What is the UTXO in Bitcoin? Your answer should include **why** it is used, **how** it works, and **who** uses it.

18. Describe how a miner validates a transaction, including the role of the locking and unlocking scripts. Be as specific as you can.

19. What do we mean when we say that Bitcoin is a decentralized system.

Bitcoin is not controlled by a single entity (business, government, country, etc.) and so it is decentralized. It is a peer to peer network, it is open to anyone, and relies on all the other contributers to function. There is no central authority that governs it, therefore it is "decentralized".

20. What does consensus mean in Bitcoin?

21. How is Bitcoin able to keep the average time to find the next block at approximately 10 minutes from the time that Bitcoin was invented until now when the overall hash rate of the system is so much greater?

22. Explain Bitcoin's proof of work? Your answer should explain in detail what a miner does.

23. What is the target value in block 600,000 for Bitcoin? Use a blockchain explorer like btc.com. List the shorthand notation included in the block header. Also include the full hex representation (including all leading zeros) and describe how you derived it.

24. Suppose Alice purchases an item from a merchant for 2 BTC. The merchant has a policy that three managers must approve every transaction. Describe how this transaction occurs between Alice and the merchant using Bitcoin. Explain all of the scripts that are involved for Alice to make the payment and for the merchant to spend the money. Explain how the transactions are validated by showing the contents of the stack at each step of the validation.

25. Suppose Bob wants to rent a service from Alice by paying for the service as he goes. The following diagram explains how micropayments work in Bitcoin. Give a detailed description of micropayments that explains the following diagram. Describe the scripts that are involved, and explain which ones are placed in the blockchain and when.