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 — used to create the actual signature hash

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 Assuming "harder" means "less convenient"
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 - Can't be completely anonymous because it is unlinkable
B. Pseudonymity - Each key generated is like a new username
C. Unlinkability - Public keys can be linked to a person/organization, especially when converting into fiat currency

14. Bitcoin supports smart contracts. (provide a brief explanation of your answer)

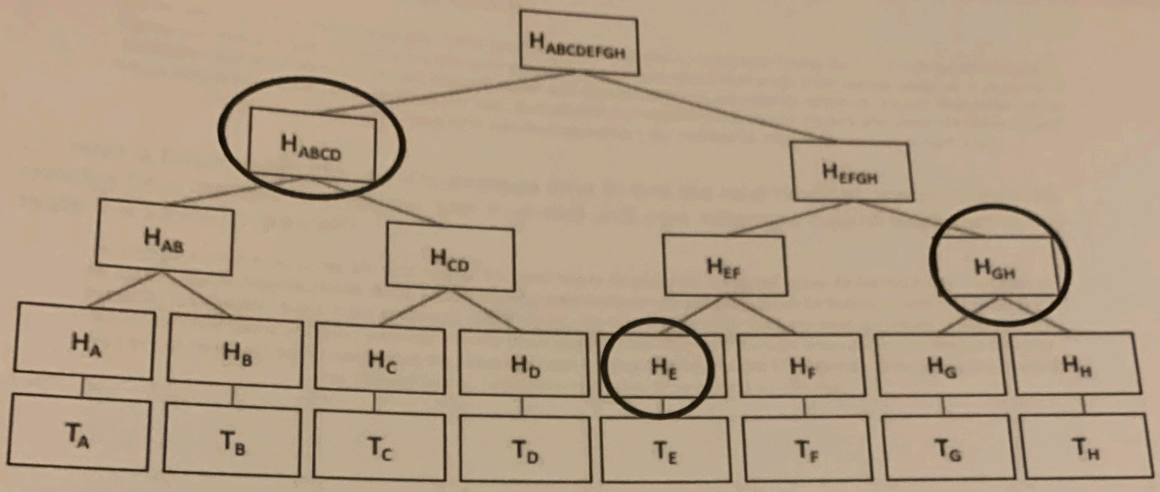
A. True While complex smart contracts are hard, smart contracts can be enforced by the blockchain, rather than by a legal representative or framework. One of the simplest examples is the example of micropayments, where both parties agree to refund all back to the user if there is dishonest dealings after a certain period of time.
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. UTXO is the unspent transaction output set.This set is used to make it easier for transaction inputs, since they no longer need to go through every block in the blockchain to make sure an input is valid, but can instead just traverse the set of all blockchain outputs. Outputs of transactions in a block are placed in an updated UTXO, and if that block gets broadcasted, the UTXO of the network is updated, and miners that want to build upon that block can validate transaction inputs that come from the new UTXO set. Miners use the UTXO set to quickly validate transaction inputs, that they are including in their block. Outputs from the UTXO set that are used are taken out of the UTXO set to prevent double spends.

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

In order for a miner to validate a transaction, he must first look at the inputs and outputs of the transaction. First, all the inputs must be located in the UTXO for him to verify that they have not already been spent. Then he needs to make sure that each signature on the input is valid. This is where the locking and unlocking scripts come in. Each output contains the locking script (scriptPubKey) which contains a condition required to spend the output (normally a signature). In order for an output to be used in a transaction input, along with the input, the owner of the input must provide an unlocking script (scriptSig) that contains the condition that the locking script requires. The miner can combine the locking script and the unlocking script and verify that the input is indeed valid, and that all required conditions are met. For more information on how exactly the miner uses the scripts to verify inputs, see the free response down below where I demonstrate it. With the inputs now valid, the miner then checks that the current input is not used somewhere else in his block, as each output in the UTXO can only be used once. He checks again to make sure that the output of the transaction is not negative, and also checks that, if necessary (as in it is a big transaction and so requires it) that the inputs are greater than the outputs, and he is rewarded for his work in including this transaction in his block. This is a tip for miners to give them an incentive to include transactions in their block.

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?

Bitcoin relies on consensus from people. There are three types of consensus that bitcoin relies on: 1. Consensus about rules, 2. Consensus about history, 3. Consensus that coins are valid. Consensus about rules means that people agree on what makes a transaction and block valid, how nodes should behave, and the protocols that are need for bitcoin to operate. Consensus about history means that people agree on the blockchain, such as which transactions have occurred and who owns which coins. Lastly, consensus that coins are valuable is a general agreement that bitcoins do have value and are sought after.

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?

In order for a block to be mined the total hash of the block has to be less than the target value. As the hash rate increases in the system, blocks have had lower target values, making them increasingly difficult to solve by finding a hash of a block that is below the target value. About every two weeks (2016 blocks) the system evaluates itself and sees if it needs to lower or raise the target value based on how quickly blocks were mined before. This keeps the average time around 10 minutes because even though the hash rate has increased, the bitcoin protocol has made blocks harder to mine than at the beginning, keeping the average time to finding the next block to be around 10 minutes.

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

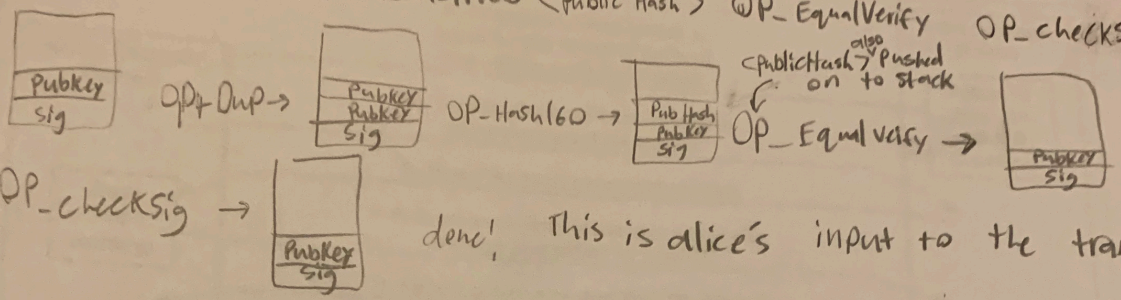
Proof-of-work is one of the consensus tools in bitcoin. Miners compete against each other to solve a hashing puzzle in order to get the blockchain reward. The odds that a miner is selected to broadcast the next block is linked with hashing power. Nodes are selected by their computing power by the network, because computing power most like will not be monopolized. Miners are given a target value, create a block out of valid transactions, and start hashing their created block over and over again, changing the nonce and trying to get a hash that is below the target value given. Nodes that have greater hashing power are more likely to find a random hash of a block that makes it valid. The miner then broadcasts their block to the other nodes on the peer to peer network, who then check to see if the block is valid, and can choose to accept or reject it. The miner who finds the block then recieves the mining reward of bitcoins.

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.

The "Bits" for block 600000 are 0x1715a35c, but the target is 0x00000000000000000015a35c0000000000000000000000000000000000000000. To find this target, you take the mantissa (15a35c) and multiply it by the base to the power of the exponent minus the bytes in the significant, which is 15a35c * 256^(0x17 -3). There are 32 bytes in the hex code, so the total number of bytes needs to add up to 32 as well.

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.

Alice's script: OP_DUP OP_HASH160 <Public Hash> OP_EqualVerify OP_checkSig

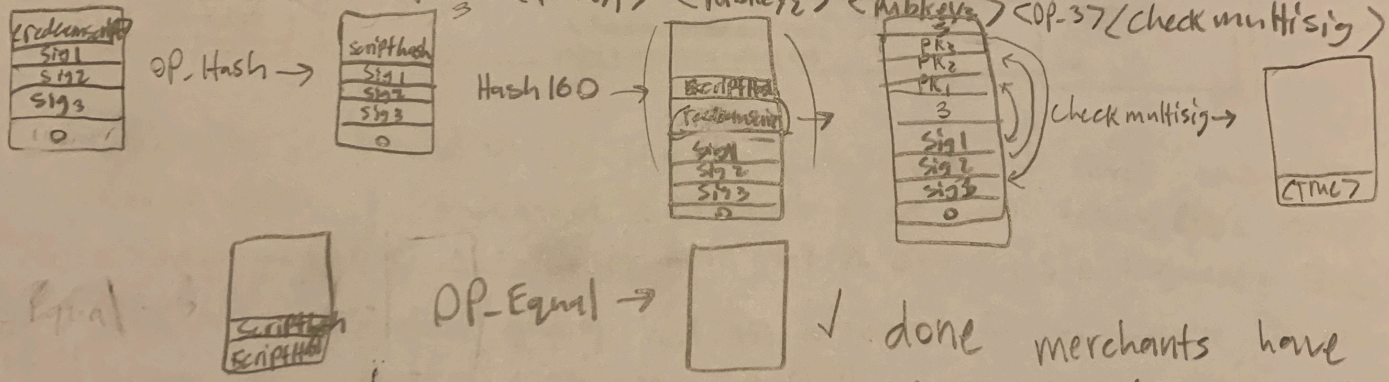


OP_checkSig →

done! This is alice's input to the transaction

Merchants to spend: OP_Hash160 <Hash160(redeemscript)> OP_Equal

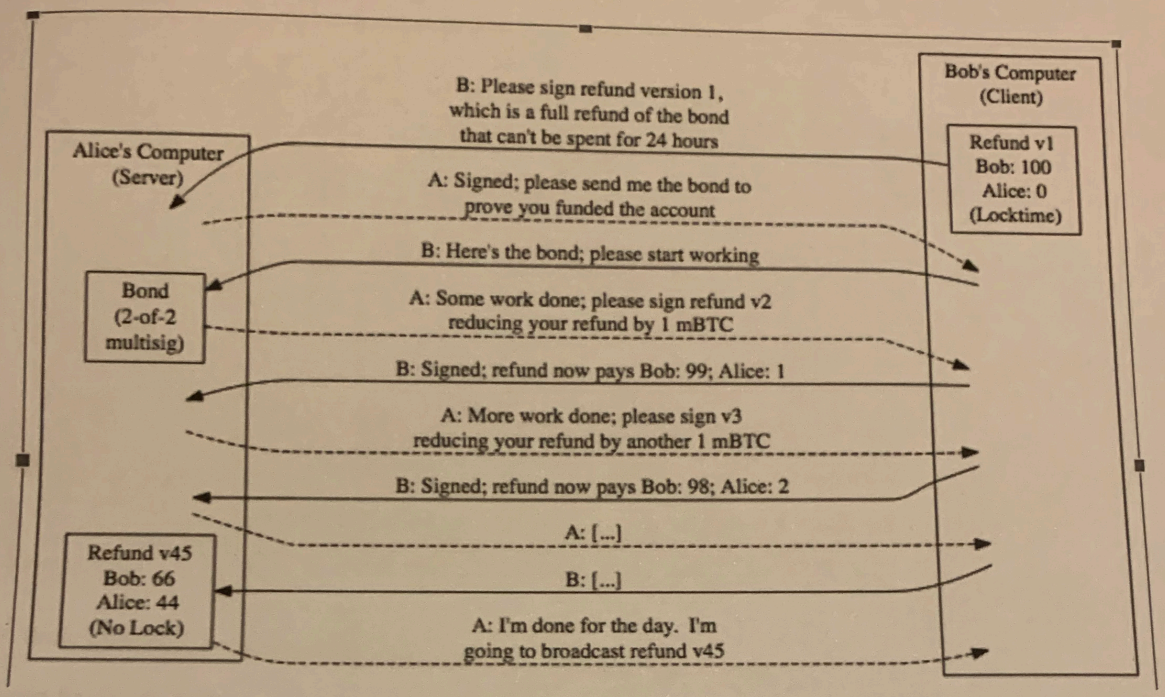
redeem script = <OP_2> <Pubkey1> <Pubkey2> <Pubkey3> <OP_3> <checkmultisig>



OP_Equal →

✓ done merchants have approved and can spend the money

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.



Only v45 is placed on the blockchain, as this is the final transaction. Refund version 1 is recorded to prevent Alice from taking Bob's money without working. As Alice gets work done, she requests Bob to sign a transaction giving her an amount for her work. Bob can review the work and sign the pay. This goes on until Alia finishes working. She must then Broadcast to the block chain v45, or else after 24hr, Bob will get all his money back.