***GASLIMIT is the actual amount of gas spent at the completion of the Block creation.***

False

***The Ethereum Accounts can send transactions for ether transfer or they can send transactions to invoke a smart contract code***

True

***Ethereum full node hosts the software needed for transaction initiation, validation, mining, block creation, and smart contract execution.***

True

***Miner nodes receive, verify, gather and execute transactions.***

True

***A Smart Contract is a piece of code deployed in the Blockchain node. Execution of a smart contract is initiated by a message embedded in a transaction.***

True

***In Bitcoin, the standard practice for a merchant is to wait for n confirmations of the paying transaction before providing the product. While the network is finding these confirming blocks, the attacker is building his own branch which contradicts it. When attempting a double-spend, the attacker finds himself in the following situation. The network currently knows a branch crediting the merchant, which has n blocks on top of the one in which the fork started. The attacker has a branch with only m additional blocks, and both are trying to extend their respective branches. Assume them honest network and the attacker has a proportion of p and q of the total network hash power, respectively.***

### Section 1

***Let denote the probability that the attacker will be able to catch up when he is currently z blocks behind. Find out the closed form for with respect to p, q and z. Detailed analysis is needed. (Hint: satisfies the recurrence relation .)***

**Answer**: According to the hint, satisfies the recurrence relation , reform the equation in terms of :

Where the should be 1 in this case since the attacker has the same block as the chain (p=q):

### Section 2

***Compared with the Bitcoin white paper, we model m more accurately as a negative binomial variable. m is the number of successes (blocks found by the attacker) before n failures (blocks found by the honest network), with a probability q of success. Show that the probability for a given value m is*** .

**Answer**: Since that the equation of the probability of an event with time successes and times of failures can be written as:

In the trail, the last trail must be failure so the last successes is coming before the last failure, so there should be total trails. Hence, it can be written as:

***Suppose a mining pool wants to blacklist transactions from address X. In other words, they want to freeze the money held by that address, making it unspendable.***

### Section 1

***The mining pool announces that they will refuse to work on a chain containing a transaction originating from address X. Explain why this strategy can guarantee that the blacklisted transactions will never be published if the mining pool has the majority of the hash power.***

**Answer**: If a transaction from address X is included from the miner, then the pool will fork since the pool has the most of the hash power, which will create a longer chain in order to invalidates the chains contains the transaction from the address X. Hence, the miner will be informed that this block will be invalidated.

### Section 2

***The mining pool announces that they will attempt to fork if they see a block that has a transaction from address X, but they will give up after the transaction from address X has k confirmations. The success of this attack depends entirely on the motivation of other miners to join the attacker. If a miner includes a transaction from address X in his block, he will receive block reward plus transaction fee from address X. Otherwise, the miner only receives block reward. Suppose the attacker controls q = 20% of the network hash power. Let k = 2 and block reward be 12.5 BTC ≈$48, 550. What is the minimum transaction fee address X has to pay in order to avoid being blacklisted? (Hint: first find out the probability that the attacker successfully prunes the block containing a transaction from address X.)***

**Answer**: The probability that the attacker successfully build the block is . Hence, in order to avoid attacking, the payment amount should be:

Where the total amount should be greater than the block reward, hence:

***Describe all events that cause each transition in the state transition diagram in Lecture 3, Slide 35***

| Begin | End | Probability | Event |
| --- | --- | --- | --- |
| 0’ | 0 |  | Honest miner mines a block on the main branch |
| 0’ | 0 |  | Honest miner mines a block on the selfish miner’s block |
| 0’ | 0 |  | Selfish miner mines a block on the private branch |
| 0 | 0 |  | Honest miner mines a block |
| 1 | 0’ |  | Honest miner mines a block on the main branch, selfish miner publishes the private branch containing one block |
| 2 | 0 |  | Honest miner mines a block on the main branch, selfish miner publishes the private branch containing two blocks |
| n | n+1 |  | Selfish miner mines a block on the private branch |
| n | n-1 |  | Honest miner mines a block on the main branch |

***At which transitions in the state transition diagram in Lecture 3, Slide 35, the honest miners would earn the block reward, and how many?***

| Begin | End | Probability | Reward |
| --- | --- | --- | --- |
| 0’ | 0 |  | 2 |
| 0’ | 0 |  | 1 |
| 0 | 0 |  | 1 |