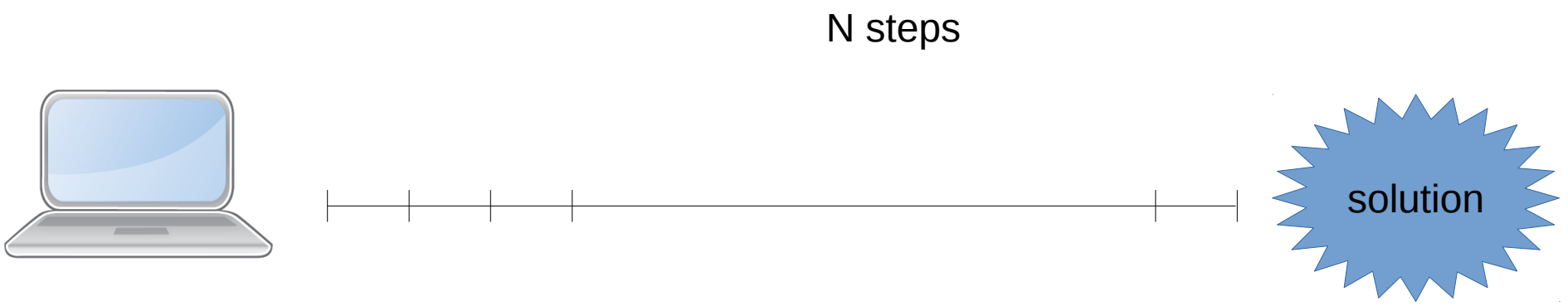
Test 8 - alternative mining puzzles

Puzzle Requirements [ID: 498029]

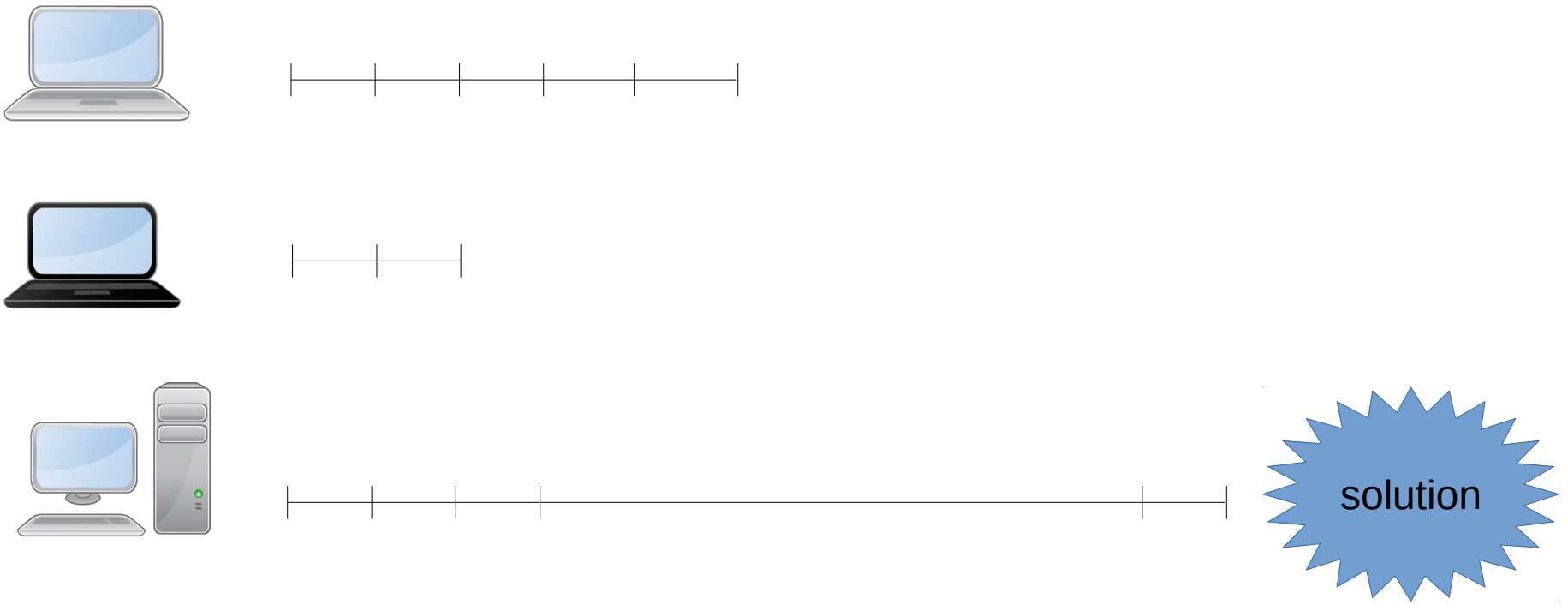
Consider a mining puzzle that requires miners to compute n consecutive hashes that are greater than a given hash in order to win the next reward. Explain whether this puzzle satisfies the essential puzzle requirements!

Puzzle Requirements [ID: 498029]



Puzzle Requirements [ID: 498029]

- No



Alternative Mining Puzzle [ID: 498025]

Alternative Mining Puzzle [ID: 498025]

What are the reasons to look for alternative mining puzzles?

You have to decide on every statement: [right] or [wrong]

right	wrong	
○	○	Bitcoin miners do not get enough benefits as the mining reward drops over time
○	○	Bitcoin mining consumes a huge amount of electricity
○	○	Bitcoin mining puzzle requires to adapt too often (roughly two weeks)
○	○	Optimized custom hardware is more efficient at bitcoin mining than stock hardware

Alternative Mining Puzzle [ID: 498025]

right	wrong	
○	◉	Bitcoin miners do not get enough benefits as the mining reward drops over time
◉	○	Bitcoin mining consumes a huge amount of electricity
○	◉	Bitcoin mining puzzle requires to adapt too often (roughly two weeks)
◉	○	Optimized custom hardware is more efficient at bitcoin mining than stock hardware

ASIC Resistant Puzzles [ID: 498026]

Which of the following statements about ASIC resistant puzzles are correct?

You have to decide on every statement: [right] or [wrong]

right	wrong	
○	○	ASIC mining has higher performance than normal hardware mining
○	○	Memory-hard puzzles are detrimental for ASIC-mining because they require a huge amount of memory to solve the puzzles, but not CPU
○	○	Script puzzles require a large amount of memory because they need to calculate a complicated hash function
○	○	The performance of memory is more stable than for CPU

ASIC Resistant Puzzles [ID: 498026]

right	wrong	
◉	○	ASIC mining has higher performance than normal hardware mining
◉	○	Memory-hard puzzles are detrimental for ASIC-mining because they require a huge amount of memory to solve the puzzles, but not CPU
○	◉	Script puzzles require a large amount of memory because they need to calculate a complicated hash function
◉	○	The performance of memory is more stable than for CPU

Proof of Stake [ID: 498028]

Which of the following statements about Proof of Stake are correct?

You have to decide on every statement: [right] or [wrong]

right	wrong	
○	○	The probability of winning a mining right is roughly proportional to the size of stake
○	○	All miners have the same chance to create the next block because they are randomly chosen
○	○	Miners make more benefits (money) with Proof of Stake than with Proof of Work
○	○	Specialized ASICs have no advantage over stock hardware at mining

Proof of Stake [ID: 498028]

right	wrong	
◉	○	The probability of winning a mining right is roughly proportional to the size of stake
○	◉	All miners have the same chance to create the next block because they are randomly chosen
○	◉	Miners make more benefits (money) with Proof of Stake than with Proof of Work
◉	○	Specialized ASICs have no advantage over stock hardware at mining

Tezos Baking/Endorsing [ID: 498030]

Which of the following statements about baking/endorsing are correct?

You have to decide on every statement: [right] or [wrong]

right	wrong	
○	○	The more rolls you own, the higher priority you get on the priority list
○	○	An endorser can have more than one slot for endorsing a block
○	○	Bakers/endorsers will lose their money at any time later if they double baked or endorsed
○	○	Assuming that there are 100 rolls for baking, one roll is 10,000 XTZ. If you have 39000 XTZ, the probability of being given the rights to create the next block is 39%

Tezos Baking/Endorsing [ID: 498030]

right	wrong	
○	◉	The more rolls you own, the higher priority you get on the priority list
◉	○	An endorser can have more than one slot for endorsing a block
○	◉	Bakers/endorsers will lose their money at any time later if they double baked or endorsed
○	◉	Assuming that there are 100 rolls for baking, one roll is 10,000 XTZ. If you have 39000 XTZ, the probability of being given the rights to create the next block is 39%

Block Reward in Tezos Proof of Stake [ID: 498027]

- What is the maximum block reward that a baker can receive?

Baking reward

$$\text{Reward} = \text{block reward} + \text{all fees paid by transactions}$$
$$\text{Block reward} = e \cdot \text{BAKING\_REWARD\_PER\_ENDORSEMENT}[p']$$

- BAKING_REWARD_PER_ENDORSEMENT $= [1.250, 0.1875]$
- e is the number of endorsements the block contains
- p' depends on p

Block Reward in Tezos Proof of Stake [ID: 498027]

Block reward = e · BAKING REWARD PER ENDORSEMENT[p’]

- e is the number of endorsements the block contains
- BAKING REWARD PER ENDORSEMENT = [1.250, 0.1875]

Block reward_max = 32 * BAKING REWARD PER ENDORSEMENT[0] = 32 * 1.250 = 40

Tezos Baking/Endorsing Deposit [ID: 498031]

- Assuming that BLOCKS PER CYCLE = 2016, how long does it take for a baker/endorser to receive the deposit money back after baking/endorsing?

Tezos Baking/Endorsing Deposit [ID: 498031]

- Blocks are group into cycles of BLOCKS PER CYCLE = 2016 blocks.
- TIME BETWEEN BLOCKS = one minute
- 1 cycle = 2016 minutes (1 day 9 hours 36 minutes)
- PRESERVED CYCLES = 5 cycles = 2016 * 5 = 10.080 minutes = 168 hours (7 days)

Security deposit: frozen for PRESERVED CYCLES = 5 cycles = 7 days

Tezos Security Deposits [ID: 498032]

- Assuming that the total amount of staked tokens is 720,000,000 XTZ and BLOCKS_PER_CYCLE = 2048 how many percent of this amount is stored in security deposits?

Tezos Security Deposits [ID: 498032]

BLOCKS_PER_CYCLE = 2048 * 5 = 10240

Tezos Security Deposits [ID: 498032]

((BLOCK_SECURITY_DEPOSIT + ENDORSEMENT_SECURITY_DEPOSIT * ENDORSERS_PER_BLOCK) * (PRESERVED_CYCLES + 1) * BLOCKS_PER_CYCLE)

= (512 + 64*32) * (5 + 1) * 2048

= 31457280

% = 31457280/720000000 = 4,37

Algorand: Pure Proof of Stake [ID: 498024]

Which of the following statements about Algorand: Pure Proof of Stake are correct?

You have to decide on every statement: [right] or [wrong]

right	wrong	
○	○	There is absolutely no double spending because the owners of 100 tokens randomly agree on (sign) the proposed block
○	○	There is no need for deposits
○	○	The winners for creating the next block are selected and stored in the last block
○	○	A user can not cheat on winning a ticket

Algorand: Pure Proof of Stake [ID: 498024]

right	wrong	
○	◉	There is absolutely no double spending because the owners of 100 tokens randomly agree on (sign) the proposed block
◉	○	There is no need for deposits
○	◉	The winners for creating the next block are selected and stored in the last block
◉	○	A user can not cheat on winning a ticket