## Challenge 1: Understanding how new blocks are added to the ledger and how the proof of work prevents malicious nodes from taking over the MONS network

Possible Questions:

* Process of making a payment
* Resistance against hacking

Requirements of question:

* How new blocks are added
* POW
* Preventing malicious nodes from taking over the MONS network

How it Works

* Transaction from Alice to Bob added to transaction pool
* Nodes on network responsible for validating transactions and grouping them into blocks known as miners
* POW must be completed to add block to blockchain
* POW involves miners finding a nonce (number only used once)
  + Hash (e.g. SHA-256) with specific difficulty level
    - Non-invertible
    - Deterministic
    - Collision resistant
  + Difficulty level (e.g. Hash starting with five 0s)
    - The higher the difficulty level, the more 0s required
    - Harder to find a hash which fulfills criteria
* Miner then submits block with nonce to the network
* Assuming 0 network latency, if nodes contributing a total of more than 50% of network computational power agrees that the nonce is valid, reach distributed consensus, block added to blockchain
* Miner given block reward

How this prevents malicious nodes from taking over network

* Because >50% of network’s computing power has to accept the block, malicious blocks are not accepted into the blockchain by non-malicious miners
* Fraudulent blocks cannot be added to the public blockchain

51% Attacks as the only means to take over a network

* Malicious nodes can take over a network by using a 51% attack
* A single mining pool (group of miners) owns more than 50% of the network’s computational power
* Subverts POW as the probability of the mining pool finding the nonce is significantly higher than the rest of the network
* This enables the mining pool to conduct a takeover attack, leading to a double spent problem

Process of Double Spending

* In the case of multiple blockchains, the blockchain with the longest POW chain (more blocks) is deemed as the most “legitimate” chain
* The malicious miner can validate blocks on a private blockchain without broadcasting the solutions to the public blockchain
* Malicious miner spends cryptocurrency using public blockchain on real world commodities but does not add this transaction to his private blockchain
* Malicious miner uses the higher computational power to catch up with the public blockchain, adding as many blocks as possible to the private blockchain
* Once the private blockchain has more blocks that the public blockchain, the blockchain is broadcasted
* Since this malicious blockchain has the longest POW chain (most blocks), other nodes on the network accept the entirely new blockchain

Conclusion and Synthesis

* The POW process with the distributed consensus prevents malicious nodes from taking over the network
* One of the key vulnerabilities being 51% attack
* Since MONS is to be used by the entire city, it is exceedingly difficult and costly to own more than 50% of the computational power of miners
* Additionally, having more than 50% simply increases the probability of finding more nonces, but does not guarantee that the malicious miner will always find a nonce faster
* A significantly long block time, such as 10 minutes compared to 20 seconds, can be used to further reduce the probability of the malicious miners taking over the network
* Citizens should not be concerned with malicious nodes taking over the MONS network

## Challenge 2: Understanding how the MONS architecture is scalable and can remain efficient as the number of users increases

Possible Questions:

* Features that enable the Blockchain to scale
* Issues that arise with more users

Increase confirmation time of blocks

Increase of cost for transactions

Block complexity increase leads to increased hardware requirements an therefore energy issues

Blockchain size increase expands the requirements on each node

Effect of increasing number of nodes on creating and verifying blocks

Potential scalability steps

Increase number of transactions per block

Increase block size

More efficient hashing algorithms

Reducing block creation time

Improve speed of consensus

Off-chaining and sub chains

## Challenge 3: Understanding the use of cryptographic techniques in the MONS project

Possible Questions:

* Purpose of digital signatures/how it works
* Importance of hashing that enable the blockchain to function

Without a central authority in the blockchain, cryptographic techniques are required to ensure that transactions made in the blockchain is secure.

Hashing one of the cryptographic techniques used in the MONS project. A hash is a function that converts input data to an output of a fixed length. A cryptographic hash, such as the SHA-256, has the properties of …..

Hashes are used in several aspects of the blockchain. It enables the blockchain to be immutable. Something about Merkle trees, something about reduction of storage size something about nonce.

It is also used in the encryption algorithms used in the blockchain.

Asymmetric encryption in the form of digital signatures is one of the cryptographic techniques used in the MONS project. In the context of the blockchain, it is used to ensure that a transaction is intended to be made by the sender. This means that for a transaction,

A send 10 coins to B

the digital signature ensures that this transaction is made by A and not forged by anyone else. This prevents others, such as B (the receiver), from making a false transaction and sending coins to themselves, stealing money from others.

A digital signature works via an asymmetric encryption algorithm, usually the Elliptic Curve Digital Signature Algorithm (ECDSA). When a sender wants to make a transaction, they first craft the transaction data which includes the amount and the receiver. This data is hashed to produce a unique string representing the transaction data. The sender then uses their private key, which is only known by them, to “sign” the transaction hash using the digital signature algorithm. The output from the algorithm is the Digital Signature. Both the original unencrypted transaction data and the digital signature is then broadcasted to the rest of the network.

For other nodes to verify that it is a valid transaction, they first generate the hash of the transaction data received. They also then use the public key of the sender on the digital signature received to produce a hash value. This hash value is compared to the hash of the transaction data. If they match, it means that it is a valid transaction. It they don’t, that means the transaction may have been forged.

In conclusion, hashing and digital signatures are an integral part of the blockchain. It is what provides the security capabilities the blockchain and enables it to function practically with high resistance to malicious attacks.

## Challenge 4: Explaining to Santa Monica citizens how their MONS balance is calculated from transaction data securely stored in a publicly accessible blockchain ledger

Possible Questions:

* Purpose of transparency of the blockchain
* How to add a new user to the blockchain

## Challenge 5: Investigating how the distributed nature of a blockchain cryptocurrency and the confirmation process may have disadvantages for the citizens of Santa Monica

Possible Questions:

* Disadvantages of a blockchain
* Security limitations

Problems with confirmation process:

* Takes time
* During the confirmation process, it is unreasonable for merchants to ask the customers to remain at the shop premises
* If the users leave with the products purchased before the confirmation process is complete, it is possible for them to double spend the coin
* They can make an invalid transaction, giving the merchant a false believe that they have made payment when they do not have enough currency in the first place for the payment to be processed. By the time the merchant realises this, it may already be too late.

In the event of simultaneous completion of the proof-of-work by 2 or more miners, there would then be multiple chains at that point in time. The transaction may only exist in one of the blocks and not the other. To solve the problem of having multiple chains, nodes in the blockchain would choose the longest chain as the valid one. Hence, all the network has to do is to wait for more blocks to be added to the chain and accept the longest one since it is unlikely over multiple consecutive blocks that 2 or more miners solve the proof-of-work at the same time.

The blockchain confirmation process for a transaction is essentially the number of blocks has to be added to the transaction block for it to be considered with high certainty that it is the longest chain. Since blocks could take time to be created, the confirmation process also takes a significant amount of time. It is unreasonable for shops to keep their customers at the shop for the duration of the confirmation process.

Lack of a central authority can present a few problems.

Easier for criminal financial activity since it is hard to link a wallet address to an organisation thereby providing anonymity for these illegal businesses.

No central authority to prevent or dispute fraudulent transactions. Large financial transactions that seem suspicious are flagged out by bank employees which would confirm with the sender the details of the transaction. This is not possible in a distributed network since no single entity has control over the network. Furthermore, the immutability of the network also means that historical transactions cannot be reversed or changed.

Solutions:

Off chaining

* Basically instead of sending coins from 1 wallet address to another, just give the whole wallet
* No transaction cost and it’s instant
* Not very feasible as 1 wallet is required per transaction
* Off-chaining can also be done by relying on a third-party which guarantees the value of the transaction like paypal. But this is sort of bypasses the whole distributed idea thing