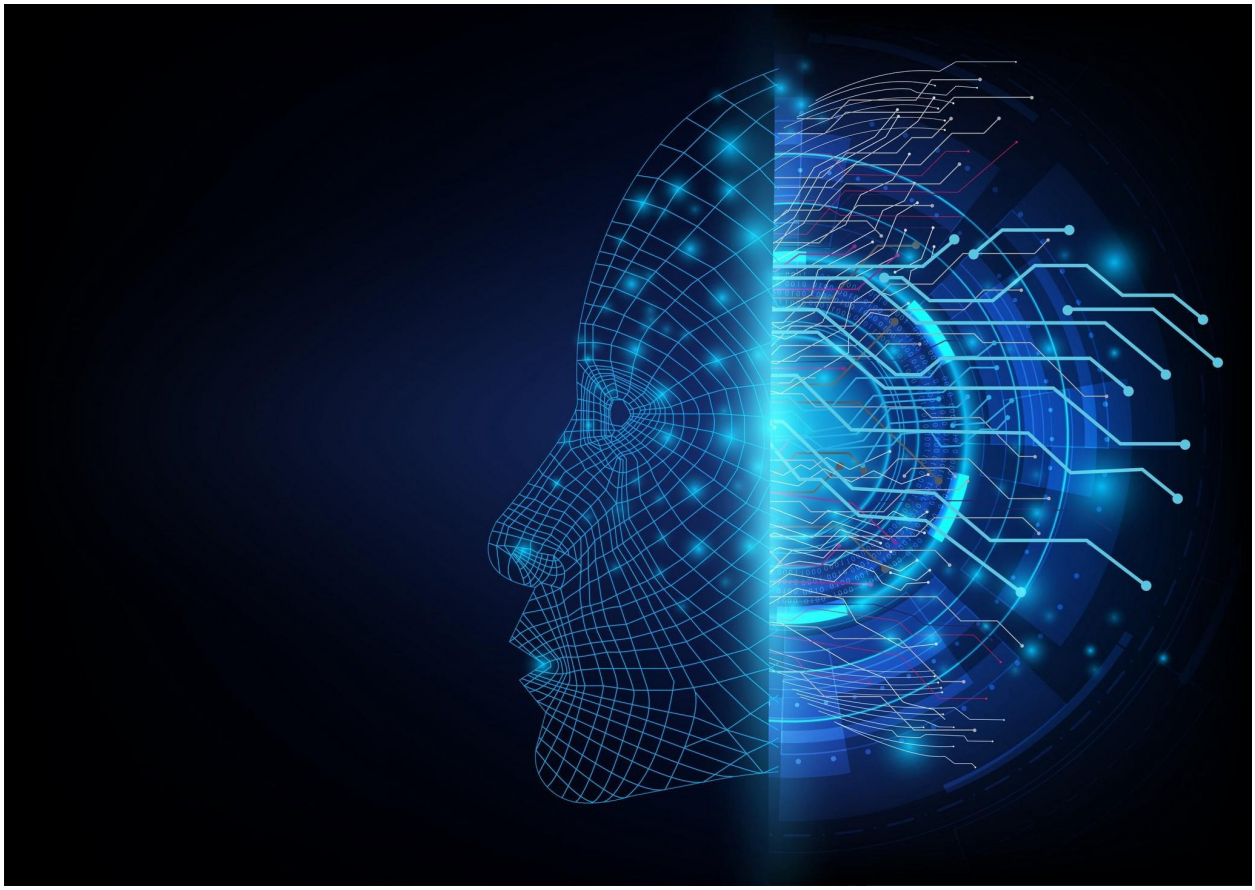
Question 1

Candidate Number: 59069

Blockchain Computing - CS3BC20



1. (a) Suppose that it is intended to use Blockchain technology to support the authenticity and traceability checking of goods in the following supply chains:

(i) Authenticated Pure Virgin Olive Oil
(ii) Infection traceable Organic Eggs

For each of the above two supply chains specify the Block data structure in terms of variables that would need to be represented.
(4 marks)

i)

Header:		Type:	Description
	PreviousHash	String	Stored hash of previous block
	CurrentHash	String	Stored hash of current block
	Index	Integer	Place in the blockchain
	TimeStamp	DateTime	Time block was created
	CurrentLocation	String	Current location of Oil
	Authentication	String / Boolean	Authenticity rating
	Origin	String	Original location
If (PoW)	Nonce	integer	Used for proof of work mining
	Difficulty	Int / double	Used for proof of work mining
Body:			
	Transactionlist	List of transactions	List of transactions -> transfers

ii)

Header:		Type:	Description
	PreviousHash	String	Stored hash of previous block
	CurrentHash	String	Stored hash of current block
	Index	Integer	Place in the blockchain
	TimeStamp	DateTime	Time block was created
	EggType	String (could be INT)	Type of Egg
	Infection	String / Boolean	Either True/False infected, or details about the infection e.g. what it's infected with
	Origin	String	Original location
If (PoW)	Nonce	integer	Used for proof of work mining
	Difficulty	Int / double	Used for proof of work mining
Body:			
	Transactionlist	List of transactions	List of transactions -> transfers

(b) In addition to authenticity, there is a requirement to keep an auditable record of refrigeration in-transit end-to-end as well as the expiry-date (e.g. as for the Pfizer BioNtech Vaccine, or fast perishable food such shellfish), therefore you are required to:

(i) define the block data structure that best supports these additional requirements for the distribution chain of such goods, and
(ii) suggest a blockchain solution stack to enforce a delivery for the vaccine or shellfish with a specified cold temperature maintained throughout transit.

(4 marks)

b)i)

Header:		Type:	Description
	PreviousHash	String	Stored hash of previous block
	CurrentHash	String	Stored hash of current block
	Index	Integer	Place in the blockchain
	TimeStamp	DateTime	Time block was created
	startTemp	Single	Temperature at start of journey
	EndTemp	Single	Temperature at end of journey
	CurrLocation	String	Current Location
	Origin	String	Original location
If (PoW)	Nonce	integer	Used for proof of work mining
	Difficulty	Int / double	Used for proof of work mining
Body:			
	Transactionlist	List of transactions	List of transactions -> transfers

ii) The use of a Ethereum style technology stack complete with smart contracts would suit this implementation.

Relations	Smart Contract Application Layer
Assets	Record of Transactions Blockchain Layer
Governance	Consensus Rules Blockchain Layer
Network	P2P Network Blockchain Layer
Infrastructure -(Possibly superfluous)	TCP/IP Internet Layer

(c) State and justify the type of Blockchain to be used for each supply chain for cases (a) (i) and (ii) above.

(1 mark)

In both situations it seems that a private blockchain would be appropriate, as it is likely these services are provided by private businesses and therefore only necessary to be governed by this body, the higher level of security,privacy and performance is favoured as the data does not need to be publicly accessible, and only requires visibility for the participating parties. In a situation where more than one body is interacting with the process, it is possible to opt for a private-permissioned blockchain, however private seems most appropriate. If it is required that the data is visible to all, a public blockchain may be used.

(d) Justify why Proof-of-Work and Proof-of-Stake Consensus methods should not be expected to be vulnerable to the same type of attacks and describe one type of security threat that the Proof-of-Stake could be exposed to.

(5 marks)

Proof-of-work(PoW) and proof-of-stake(PoS) are two different consensus algorithms. PoW operates by using advanced cryptographic & mathematical equations that are too complex for a human to solve & thus must be solved using a computer. These equations are always unique, meaning a solved equation can be recognised as authentic.

Proof-of-stake opts to validate by making sure that validators have a quantity of tokens for the blockchain already, this results in a requirement for any potential attackers to gain a large proportion of tokens on the blockchain in order to mount an attack; an effective deterrent.

Due to the nature of these algorithms, a malicious actor wouldn't approach them in the same ways, for example, a "51% attack" where a malicious body is able to obtain more than 50% of the mining power, is a legitimate attack on a PoW mechanised blockchain, as it would allow the malicious body to make changes to an individual block, allowing them to alter it for personal gain.

In a PoS mechanised blockchain, this would be an ineffective attack as it would require the malicious actor to acquire 51% of the total currency in circulation, which could only be achieved initially through legitimate methods, this would likely cost the actor significantly more than they could gain.

One vulnerability offered by the PoS system over the PoW system is due to the fact that ultimately the richest node in the network must be trusted in order to not cheat the system. While nodes gain no benefit from fooling the system due to the devaluation of their currency if the blockchain's integrity is damaged, this does open new security

threats such as the possibility of the “bribe attack”, which operates by an actor performing a spending transaction and then secretly creates an alternative “forked” chain, which will later be substituted in place of the real chain, reversing the original transaction. In a PoW network this is likely to cost approximately 50 times more than on a PoS system.

(e) Briefly describe each of 4 distinct routes to a double-spend attack that could be mounted on a blockchain.

(6 marks)

Sybil attack - A sybil attack works by having an attacker flood the network with a large number of nodes with pseudonymous identities and try to influence the network, appearing like unrelated individuals, but operated by a single operator.

Objective to target number of nodes on the network as a whole opposed to single user, generate fork in ledger allowing attacker to double spend amongst other attacks.

Selfish mining - Most blockchains consider the longest chain to be the true latest version of the ledger, this means that a selfish miner can try to keep building blocks in stealth mode on top of the existing chain and when they build a lead of greater than 2 blocks over current chain, they can publish the private fork which will be accepted as longest fork, by performing transactions on public network prior to publishing private fork, they can reverse transactions ultimately allowing a double spend.

TimeJack - Timejack attack works by taking advantage of the necessity for some nodes to depend on internal timings derived from the median time reported from peer nodes. By adding multiple malicious actors into the network, essentially “Eclipsing” the target node, which will then decline blocks from the actual network as the timestamp would not match. This allows double spending as transactions performed by the targeted node can not be submitted to the actual network.

Finney - Finney attack works on the provisor that it is possible to mine a block with one of your own transactions in, and keep it in stealth mode. If a merchant accepts the unconfirmed transaction then you can transfer the earlier transacted currency, after this the earlier mined block previously kept in stealth mode can be published before the new transaction is confirmed on the network.

A variant of this is called a “Race Attack”.