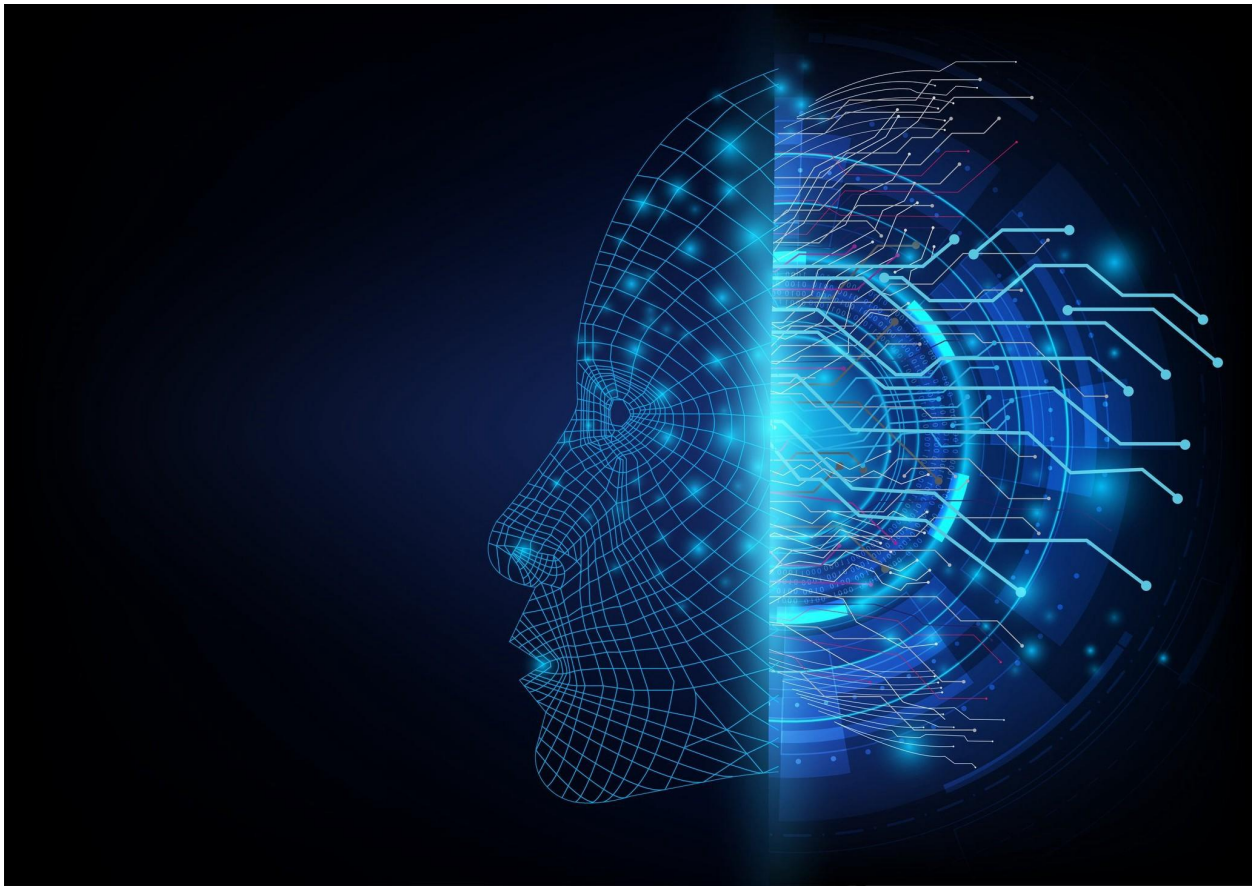
Question 3

# Candidate Number: 59069

## Blockchain Computing - CS3BC20



3. (a) A malicious node wishes to introduce an invalid node into the Blockchain network. With reference to the Byzantine Fault Tolerance capability of the blockchain, explain how this attempt is doomed to fail.

(3 marks)

Byzantine fault tolerance aims to defend a system against component failure which prevents others from reaching an agreement when required for a correct operation.

This means that if a sufficient number of components in the system continue to function as intended, the overall system can remain active. Therefore by attempting to introduce a singular invalid node into the blockchain, this attempt is doomed to fail, as it can be ignored or voided. For an attack like this to be successful, the attacker would need to introduce enough invalid nodes to surpass the byzantine fault tolerance level.

As long as there are sufficient uncorrupted nodes, the invalid nodes become irrelevant.

(b) A malicious actor has managed to steal a large sum of cryptocurrency from the users' wallets by hacking an exchange. The affected Blockchain community has agreed that a rollback should occur so that funds can be returned to their original owners. Explain what happens when a rollback occurs on a blockchain.

(3 marks)

Rollback often occurs when a block chain has been compromised. A rollback is an action taken in which the blockchain is "rolled-back" or reverted to a previous state. This is achieved by having a backup or "Fork" of the blockchain, prior to the attack. The chain is then reverted back to the state before the compromised block was added to the chain, this means all transactions after the compromised block will be removed and the legitimate transactions will need to be restated.

(c) State what ethical and social concerns are associated with rolling back a Blockchain and what the wider implications of the adoption of a rollback might be.

(4 marks)

The majority of ethical and social concerns associated with the rolling back of a blockchain come from those legitimate transactions and blocks will be lost. This could result in a loss of money for some innocent parties which could be catastrophic. Furthermore, the mined blocks would need to be re-mined resulting in a huge issue due to the power consumption required. One of the largest factors is that blockchains are solely focussed around creating a trusted environment and a rollback would directly damage the trust in the system from the users.

(d) What alternative mitigation measures may be open to this community in order to avoid a rollback but at the same time ensure that the perpetrators could not benefit from the proceeds of their crime?

(4 marks)

The most likely alternative method of mitigation measures that could avoid the need for a rollback would be a “Chain reorganisation”. This is the process of deactivating the compromised chain by means of creating a new longest (and therefore accepted) chain. Due to the fact that the longest chain is deemed the most correct, the legitimate users of the blockchain can work together and agree to work on the same version of the blockchain in order to increase the rate at which blocks are added to the chain, when the number of blocks surpasses the fork with the compromised block in, this will become the new accepted chain, and then the nodes can return to working on their own chains.

This operates in a similar methodology to how a selfish miner Attack would operate, with virtuous purposes instead of malicious intent.

Once the compromised chain is rejected, all those transactions in that chain will be void, if nodes opt to not work together to create a new longer chain, this would be counterproductive for those nodes, because as long as enough nodes work together the new chain will become the accepted meaning any nodes still working on the old chain will have to repeat their transactions.

(e) Discuss two major type of threats that could expose the blockchain to the risk of insecure re-centralisations; suggest a possible regulatory measure that may help reduce at least one such source of threat to the blockchain and the cryptocurrencies sector.

(6 marks)

***This question is very badly worded and ambiguous in what it is asking***

Two major threats that could expose blockchain to risk of insecure recentralisation, are the option of using a cryptocurrency exchange to trade cryptocurrencies, introducing a required level of trust for the exchange, or the option of trading directly with another user, requiring a level of trust for this other user. This bypasses the need for using a bank as an intermediary, but also introduces a huge amount of risk including the possibility of exchanges being hacked and currency stolen.

Miners and nodes can group together to form “mining pools” in which they work together opposed to competing against each other, splitting the rewards amongst the participating nodes.

This ideology increases the risk of 51% attacks.

A command chain can be implemented in a centralised blockchain in order to counteract some of these flaws and reintroduce a minor level of trust. And improving the confidence required to make it work.

3 major issues with centralised blockchains are that they violate the trust as the centralisation sets the stage and almost encourages potential corruption. It also means an overlooking body has control over the entire system. Furthermore it creates a single point of failure, as it is centralised at one point. Centralised blockchains also reduce innovation as decentralisation allows the idea and power of creativity to be placed in the hands of the public.

A decentralised blockchain is almost always more desirable.