Midterm

Question 1

a) In blockchain, blocks are cryptographically linked together. Explain how blocks are cryptographically linked. (4 marks)

b) "A major pain point for creatives in the music industry — such as songwriters, producers and musicians — is that they are the first to put in any of the work, and the last to ever see any profit. They have little to no information about how their royalty payments are calculated, and don't get access to valuable aggregate data about how and where people are listening to their music."

(Extracted and adapted from: https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again)

Using your own words, discuss **TWO (2)** ways where blockchain technology can help to distribute fairly the profit generated from the music to the stakeholders (songwriters, producers and musicians, etc) in the music industry. (6 marks)

c) Determine whether each of the following statements is true or false, and explain your answer:

(i) A public blockchain is more decentralised as compared to a private blockchain. (5 marks)

(ii) The adoption of Proof-of-Stake (PoS) consensus protocol can cause a blockchain network be more centralised as compared to the use of Proof-of-Work (PoW) consensus protocol. (5 marks)

(iii) Merkle Tree is a data structure used in blockchain to store transaction data. (5 marks)

[Total: 25 marks]

Glossary (**Crypto Glossary - Cryptopedia | Gemini**)

Light-Client Node

A light client, or light node, is software that connects to full nodes in a blockchain network. Unlike full nodes, light nodes do not keep a full copy of the blockchain, or communicate directly with the blockchain. Instead, light clients rely on full nodes as intermediaries. Light clients can be used to send some transactions and to verify the balances of accounts, but are significantly less functional than full nodes.

Question 1

(a) A new block added to the blockchain is linked to the previous block through the hashing mechanism. Each block contains the hashed data of the previous block, creating a chain of blocks that are cryptographylly linked together.

(b)

- The blockchain is a public ledger in which everyone has a chance to confirm transactions related to music and this will provide transparency and traceability.
- With the support of blockchain to the smart contract, payment and distribution can be operated automatically without control from the centralized authority.
- Blockchain technology is very easy for us to transfer the profit or loyalty to the stakeholders as the client can make payment easily to the stakeholders using the native cryptocurrency such as Ether.

(c)

(i) **True**. In public blockchain, everyone can join the network as it is a permissionless network and have a copy of the Blockchain ledger. Nobody controls the network and it allows anyone to have read and write access to it, thus it is decentralized. While for the private blockchain, it is more centralized as it is a permissioned blockchain and the ownership belongs to a single entity to control the network and that leads to reliance on third parties. It only allows invited users to read and approved participants to write data on it.

(ii) **False**. Proof-of-stake consensus protocol is able to reduce the financial barriers such as hardware requirements and electrical costs as required in Proof-Of-Work, hence, it is significantly more decentralized at the node level as the participants will only need to stake some amount of crypto (i.e Ether), an active internet connection, and a device such as a computer to join the blockchain and start to validate the block.

(iii) **False**. Merkle tree is blockchain technology and data structure that is constructed by hashing paired data (leaves) and continuing pairing and hashing until it remains a root hash. It summarizes all the transactions in a block and generates a digital fingerprint of the entire set of transactions so that it can be used to verify the consistency, integrity, validity of the data more efficiently (i.e the proof can be done easily and quickly)

19 December 2020

Question 1

"Blockchain is just another database system for storing data."

Comment on the statement above. (12m)

- From my point of view, I think this is a false statement.
- To illustrate, Blockchain is a **decentralized system** where it is managed using a peer-to-peer network as an open distributed ledger that does not require a central authority to control it. While the database is a centralized system, it is often managed by a centralized administrator.
- In blockchain, the **data** is **immutable** in which it cannot be modified after the block has been confirmed and propagated to the blockchain because of the hashing mechanism in which the block in the blockchain will be connected through the previous hashed block header to create a chain of blocks. In order to compromise the network, the attackers will need to have a computer that is more powerful than 51% of the network so that he can control which version of distributed ledger is valid. While for the database, it can be altered easily by issuing the SQL statement in which the authorized user can modify any data fields inside the database.
- In blockchain, it supports **data integrity** by using public key cryptography - digital signatures. For example, if a bad actor tries to change the message content, the modified message will generate a completely different digital signature, therefore it is pointless to do so. However, for databases, the bad actors alter data easily to spoof other users once they hacked into the database successfully.
- For some of the blockchain such as Ethereum, it **supports the execution of smart contracts** that provide the capability to embed business logic that opens up a wider blockchain technology application. While for the database, it does not support smart contracts and is only able to do the CRUD (create, read, update, delete) for the data fields inside a table.

A giant retail company would like to explore the feasibility of using Blockchain technology to manage its supply chain. In the current supply chain management process used by the company, many processes are done using paper-based documents and not being updated in real time. In this proposed new supply chain management system, **data transparency is required** as other participants need to know what step or sequence the transported item reaches to be prepared for their part. **Transaction history and data immutability are desired**, which enables the company to trace back the origin of the transported commodity and auditing the condition of the item.

You, as a Blockchain solution consultant, evaluate the suitability of applying Blockchain to manage the supply chain. (13m)

Things need to be considered for applying Blockchain : **Transparency**, **Traceability**, **Get rid of third party, Immutability**

- In order to evaluate the suitability of applying Blockchain to manage the supply chain, we have to first look at whether the supply chain requires a database or not - Yes, it needs a database to store the data such as transaction, order, flow of products (shipment).
- Next, it requires shared write access across different parties such as farmers, production factories, retailers, etc. They are all trusted parties but decentralized among all participants.
- Next, the supply chain does not need a trusted party to act as a trusted gatekeeper as the execution of smart contracts will help to record the ledger entries, automation of penalty fee and release payment automatically if certain conditions are met.
- Based on these requirements, we know that it is suitable to apply Blockchain to manage the supply chain. Next, we have to decide the type of blockchain that can be applied in the supply chain.
- A supply chain will need to have control functionality as the company will only grant the permission to invited participants to have the read and write access to this blockchain.
- Afterward, the transaction has to be private in which the transaction can only be accessed by the approved participants. Data transparency is provided by blockchain as the transaction can be viewed by approved participants on the network in which all the data is indelible and auditable.
- Data immutability has been provided by the blockchain by using the previous hashed block header and storing it into the current block to ensure immutability.
- In conclusion, a private blockchain with only invited and approved participants to have read and write access and controlled by a single entity should be applied to the supply chain.

Question 2 (What is Immutable Ledger in Blockchain and Its Benefits)

a. Immutability is one of the important characteristics of a Blockchain ledger

   i. **Explain the reason why a Blockchain ledger is immutable (6m)**

      - The key element that makes a blockchain become immutable is because the block has been **cryptographically hashed** using hash algorithms.
      - Hash function is deterministic and a one way function which cannot be reversed-engineered. It is nearly impossible to obtain the same hash value from two different sets of input data. Thus, hash value is a unique value that identifies one block in Blockchain.
      - The current block will include the 256 bits hash of the previous block header. This creates a chain of blocks that are cryptographylly linked together. Any alteration in the block data can lead to inconsistency and break the blockchain which makes it invalid.
      - If the attackers want to compromise the network, the attackers will need to have a computer more powerful than 51% of the network to launch 51% attacks so that they can effectively control which version of the distributed ledger is valid.

ii. Identify and discuss ONE (1) possible threat to immutability of Blockchain (6m)

- The possible threat to immutability of Blockchain is **51% attack**. This implies that the attacker(s) have a computer more powerful than 51% of the network.
- Blockchain is a decentralized network where nobody owns it. However, the miners can join together to gain a higher network hash rate compared to other mining pools (individual participants or groups of users), then it can break the immutability of the blockchain by creating a majority of hashing power.
- This allows the attackers to control which version of distributed ledger is valid and rewrite the transaction that is supposed to be "immutable" as well as modify the transaction in future or in the past.
- It also allows them to do double spending that can inflate the money supply which erodes the currency value to secure their own profit.

Discuss what a Merkle Tree is and identify THREE (3) impacts to the transaction verification process if Merkle Tree is not used in Blockchain. (13m)

- Merkle tree is a blockchain technology that is constructed by hashing paired data (leaves), then continuing pairing and hashing the result until it remains a root hash. It is used to find out whether two different nodes have the same data. Merkle tree summarizes all the transactions by producing a digital fingerprint of the entire set of transactions.
- Without the Merkle tree, it is hard to prove the validity and content of data. To illustrate, if we directly hash all the transactions in one time, it will be very difficult to verify a specific transaction as the verification will require a large amount of information to be transmitted across the network.
- Without a merkle tree, every node has to store a complete copy of every transaction on the blockchain network. It will then require a large memory or disk space and causes the proofs to become slow and difficult to compute.
- In order to prove the integrity of data, the full node which is used for validation will require a lot of computing power to compare the digital ledger which is energy-intensive as it needs to download the full copy of the transaction from another peer node.

Question 3

Identify and discuss the mechanism used in Ethereum that protects the sender from higher-than expected transaction costs due to execution of the code in a way different from what was intended (For example, a bug that causes an infinite loop).

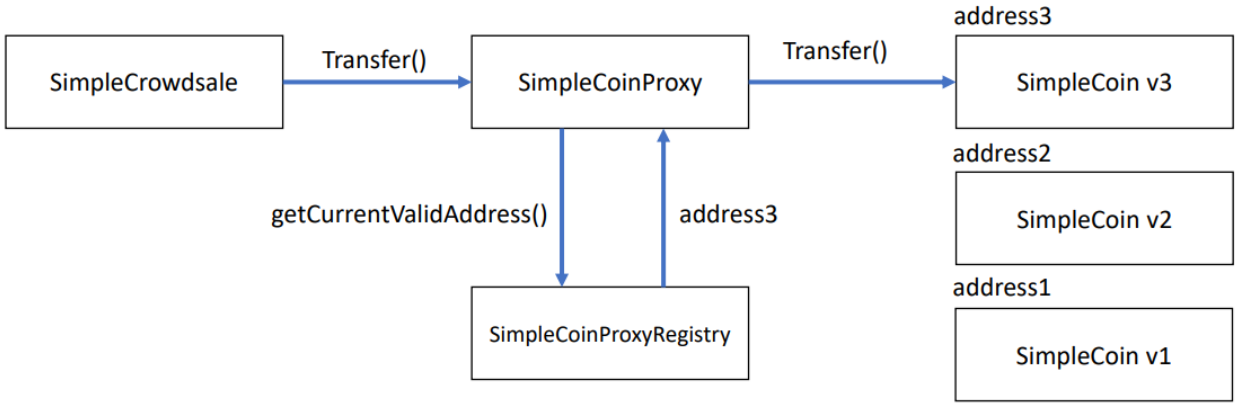
- Sender can set a limit of maximum amount of gas that a transaction should consume
- If the gas available ends before the completion of transaction, the EVM will throw a gas exception and the transaction will roll back.
- However, even if EVM throws an exception, the miner still charges the gas in Ether and they collect the related transaction fee as usual.

Explain what a Function Modifier is and identify the importance of using Function Modifiers in smart contract writing.

- A function modifier is a compile-time source code roll-up. It can change the behavior of the function.
- It is specified at the entry of the function and executed before the execution of the function begin
- It normally checks the condition using require function. If the condition fails, the transaction that call the message can be reverted using revert function
- No recording on the Blockchain as all the transactions will be rejected and all its state will be reverted
- Rules, laws, policies and governances are coded as modifier
- It is important as it avoids unnecessary execution of function and waste of gas. Furthermore, it is able to control who/what can execute to the function, at what time the function needs to be executed and what pre-condition needs to be met before accessing the function.

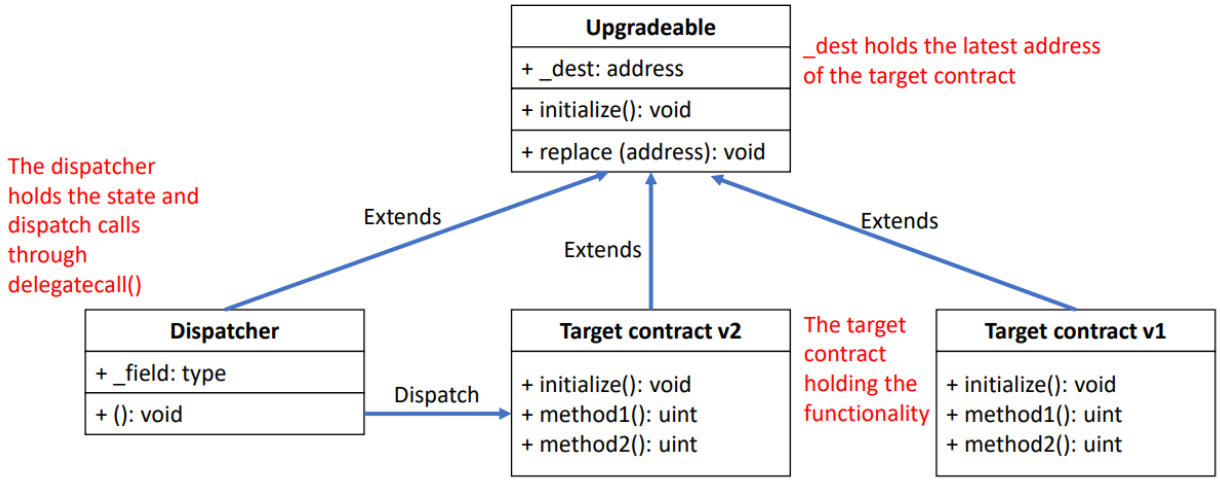
Once you have deployed a contract, it cannot be changed even if you have discovered a bug or security vulnerability after the deployment. You may at most freeze it or destroy it. Examine TWO (2) approaches that can provide contract upgradeability.

- **Proxy techniques** - The client does not directly interact with the instance of the library, instead it communicates with the proxy. Which is, proxy returns the valid address of the instance from a registry contract and forwards the call to the valid address.



SimpleCoin upgradeable through a SimpleCoinProxy contract.

- **Inheriting from the abstract upgradable contract**



Question 4

Discuss the fundamental differences between a fungible token and a non-fungible token. Give ONE (1) appropriate example for each type of the token.

Fungible token

- Has same value and identical to another of the same type (not unique)
- Divisible into smaller amounts
- Interchangeable with another of the same type
- Example: Cryptocurrency (Ether, Bitcoin)

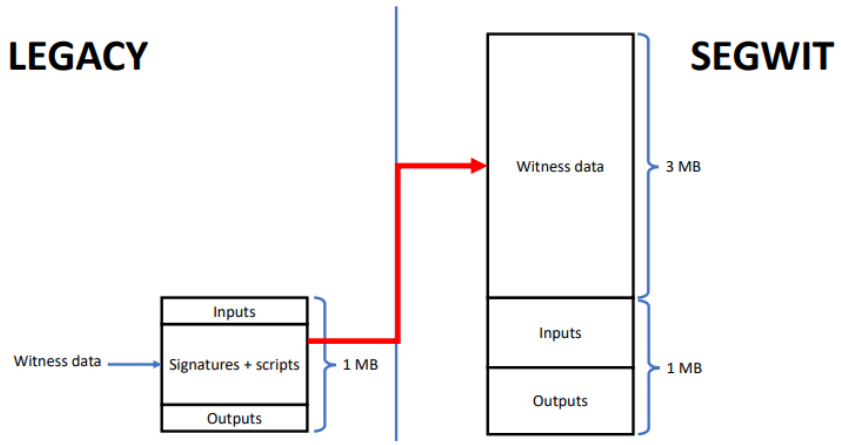
Non-fungible token

- A special type of cryptocurrency token that represents something unique
- Not mutually interchangeable
- Can represent certificate of any kinds and tokenization of all types of assets
- Example: Collectibles (CryptoKitties), Asset rights

Scalability issue has been one of the known issues of Blockchain. For example, Bitcoin can only process 3 to 7 transactions per second, and Ethereum can process around 20 transactions per second. Suggest TWO (2) possible approaches that can solve the scalability issue.

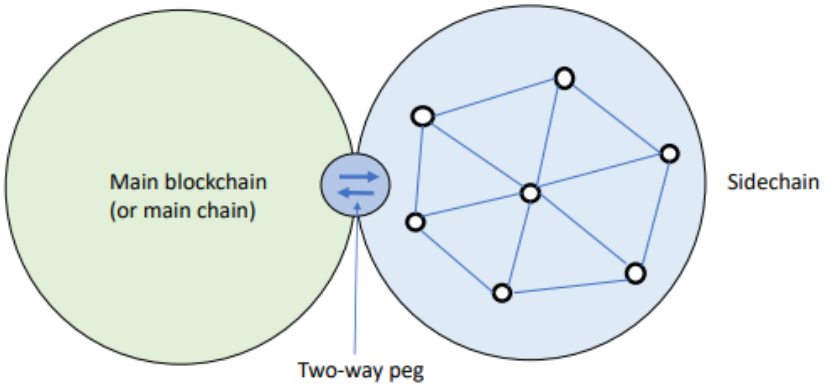
Layer 1 Scaling Solution: Segregate Witness (SegWit)

- Some data in the witness portion of a Bitcoin transaction will be moved to another part of transaction
- These data will excluded from block size calculation, effectively reduce the overall space needed for a transaction in a block
- This allows more transactions to be stored in a block, thus effectively increasing the transaction throughput.



Layer 1 Scaling Solution: SideChain

- SideChain carries additional information about the network transaction off the main blockchain to offload some on chain data.
- Side chain is an independent Blockchain that linked to the main layer of Blockchain
- Side chain rely on own security mechanism and does not depend on the security of the main chain
- A federated side chain uses multiple trusted sets of parties to sign block and hold funds in multisignature addresses.
- Use the concepts of 2-way pegs that enable users to move funds/digital assets from one chain to another chain in a more decentralized manner
- Side chain can be used as a way to test the new features that may not be ready for use on parent Blockchain



19 December 2020 [B]
Question 1

a. Public Blockchain and Private Blockchain are two types of Blockchain.
   i. Compare and contrast Public Blockchain with Private Blockchain (8m)
      - Public blockchain is a permissionless blockchain in which everyone can join and leave the network at any time whereas the private blockchain is a permission blockchain in which only selected participants can access it.
      - In public blockchain, everyone has the same right to read, write or participate within the blockchain. While for a private blockchain, only the invited users can read the data and approved participants can write the data to the private blockchain.
      - Public blockchain is a decentralized system in which nobody controls the network while for the private blockchain, it is more centralized because the ownership belongs to one single entity to control the network which relies on third-parties to transact.
      - In public blockchain, the participant does not know each other and the transaction speed is slow because it takes time to reach a consensus on the network while for private blockchain, the participant is known and the transaction speed is fast since the accessibility is limited to invited participants, the consensus can be reached much more quickly.

   ii. Is it more appropriate to use a Public Blockchain or a Private Blockchain in a business/enterprise environment? Justify your answer. (7m)
      - In my opinion, I think private blockchain is more suitable to be applied in business/enterprise environments compared to public blockchain.
      - This is because the private blockchain can improve the performance in which it can handle a huge amount of transaction data in a short period of time (process the transaction in fast speed).
      - Moreover, In private blockchain, the business/enterprise can gain more control over data and more privacy with well-defined permission control compared to the public blockchain that allows anyone to join and have read/write access to it.
      - For instance, the business/enterprise can configure the rules such as who can participate in the consensus process, who can read and write to the blockchain and how the blockchain nodes are allocated on the network.
      - By doing this, it can still retain transparency and traceability of data while only allowing the invited participants to access the information and approved participants to write the data on it.
      - One of the popular private blockchain used by businesses/enterprises is Hyperledger Fabric which can handle 3500 transactions per second compared to the Blockchain that can only handle 3 to 7 transactions per second.

b. Differentiate between Proof-of-Work (PoW) consensus protocol and Proof-of-Stake (PoS) consensus protocol. (10m)

Pow	PoS
In order to add the block into blockchain, the miner has to compete to solve the difficult mathematical puzzle by finding a nonce to be plugged into the hashing algorithm in order to fit certain constraints by using their computer processing power.	There is no competition in Pos, an algorithm will be used to determine the winner based on the user's stake.
In Pow, the computing power determine the probability of mining the block successfully	In PoS, the amount of user's stake determine the probability of validating the new block
In Pow, the first miner to solve the mathematical puzzle will receives a reward	In PoS, the validators who propose a valid block would not receive block reward but they will receive the transaction fee
In Pow, in order to add a malicious block into blockchain, the bad actors will require more than 51% of computer processing power.	In PoS, in order to add a malicious block into blockchain, the bad actors will need to hold more than 51% of all cryptocurrency on the network
The algorithm of Pow requires massive amount of electricity which consume a lot of energy (energy-intensive)	The algorithm of PoS is more energy-efficient and the amount of electricity to validate the new block is substantially low

Question 2 [not sure in the syllabus or not]

a. Ethereum uses a modified version of Merkle Tree called Merkle Patricia Trie

i. **Discuss THREE (3) things that can be efficiently checked by a client in a verifiable way using Merkle Patricia Tries. (6m)**

- Whether the transaction is included in the block
- What are the output of the transaction
- Whether the account exists
- What are the balance of the account

ii. **Explain why the binary Merkle Tree is not suitable to be used and a Merkle Patricia Trie must be used in Ethereum. (6m)**

- In Ethereum blockchain, the state of variables normally present in a key-value map and it will keep updating over the time. For example, the account balance and nonce of accounts will change oftenly, new accounts will also frequently be inserted as well as the keys in storage are frequently inserted and deleted. Hence, Ethereum needs to keep track of these states.

- Unlike transactions in Bitcoin, it will never update once the block has been confirmed and propagated onto the blockchain, which is the technology used by Bitcoin, merkle tree would not update the transaction.
- Therefore, in Ethereum, we need a data structure that enables us to keep track of the changes and is able to compute the new tree root in a short period of time after an insert, update, delete operation without recomputing the entire tree and the merkle patricia tries is able to achieve it.

b. Discuss the **importance of an incentive model in a Blockchain network**. Identify the differences between the incentive model of Bitcoin and Ethereum. (13m)
   - Incentive model is a critical part of the overall economic design of an effective Blockchain network. The incentive mechanism has been introduced to encourage the miner node to mine the new block into the blockchain. By publish the block successfully into the blockchain, the miner can receive the block reward and transaction fees
   - Incentive model of Bitcoin - Pow
   - Incentive model of Ethereum - PoS

Question 3

a. Differentiate the two types of nodes in Ethereum (8m)

- **Miner Node**
  - The miner processes the latest transaction and consolidates them into the blockchain. In return, they will receive a transaction fee and mining reward in Ether if they manage to create and propagate the block onto the network successfully.
  - The miner will propagate the blocks they've consolidated onto the blockchain to other peers of the network.
  - The miner nodes have performance requirements which need a high hash rate as they need to do a lot of hashing in order to find a nonce that fits its constraint to solve the puzzle to create a block successfully.

- **Full Node**
  - The full nodes will be responsible for verifying the validity of blocks they have received from other nodes, then they will keep propagating them to the rest of the network. The transaction and block that do not comply with the Ethereum policy will be discarded.
  - For example, when a sender initiates the transaction in Ether, the full node will verify whether the sender has enough balance and whether the sender really is the one who initiates the transaction. If the person has insufficient ether, the full node will make this transaction as invalid and drop it.

- Full nodes do not have performance requirements as they do not need to solve the complex mathematical puzzle.

b. Explain why the execution of a transaction in Ethereum is charged in units of gas from the security perspective (7m)

- In short, gas fees help keep the Ethereum network secure. This is because by requiring a fee for every computation executed on Ethereum network, it can prevent the attackers from spamming the network by launching a Ddos attack as the cost of attacking the network is high.
- Next, the Etherum is able to protect the sender from higher-than-expected transaction costs due to the code executed differently from what was intended such as hostile infinite loops, the transaction in Ethereum will need to set a gas limit to how many computational steps of code execution it can use.
- The standard of an ETH transfer requires 21,000 units of gas, if the user put a gas limit of 50,000 for a simple ETH transfer, then the EVM would consume 21,000 and return the remaining 29,000 back to the user.

  Reference: Gas and fees | ethereum.org.

Differentiate a utility token from a security token

What is the difference between Utility Tokens and Security Tokens? — Bitpanda Academy

Utility token	Security token
It is used by companies to raise interest in their products, and for application and value creation in services provided in blockchain ecosystems.	A security token represents a share in the company issuing the token. Investors who buy such tokens hope to turn a profit from investing.
Serves as a specific utility such as gain access to a service, application or resource	Investment contract is representing the legal ownership or physical asset which have been verified within the Blockchain
Token value does not relate the current state of the valuation of a company	Token value correlates directly to the valuation of the company issuing the token
High scam potential because of insufficient regulation	Low scam potential because of well-defined regulations
Currently little consensus on the regulation of cryptographic token of any kinds	Investors and company have to be in compliance with the Howey test

20 DEC 2021

Public Blockchain and Private Blockchain are two types of Blockchain.

Discuss TWO (2) advantages of Private Blockchain over Public Blockchain by using your own words (8m)

- The performance of the private Blockchain is better than public Blockchain as less nodes are participants in the ledger. Since access to the private blockchain is limited to selected participants, it is faster and can process a higher number of transactions per second as the consensus can be reached quickly compared to public Blockchain.
- In a private Blockchain, the entity can gain more control over data and more privacy with well-defined permission control compared to the public blockchain that allows anyone to join and have read/write access to it. For instance, it can configure the rules such as who can participate in the consensus process and who can read and write to the blockchain thus providing more data privacy while preserving transparency.

"In terms of the degree of decentralization, Private Blockchain is more decentralized." Do you agree? Justify your answer. (7m)

- No, I'm totally not agree with this statement
- In private blockchain, single entities will control the network. Thus, it leads to reliance on third-party which is more centralized compared to public Blockchain. In another word, the ownership belongs to one entity.
- Private blockchain is a permissioned network in which it is not open to anyone but only allows selected participants to join the network. Hence, the participants are known in the private blockchain.
- Only invited users can read the data and approved participants write data on the private blockchain.
- All these factors show that private blockchain is more centralized instead of decentralized.

There are a wide range of applications for Blockchain technology. Identify ONE (1) application that is suitable to make use of blockchain technology. Discuss THREE (3) reasons why Blockchain technology is suitable to be used in your identified application.

Application

Supply chain management system

Reason(s)

Blockchain allows organizations to **track all types of transactions (i.e history) more securely and transparently**. For instance, organizations can trace the flow of products (i.e origin, processing, distribution and transportation) easily through Blockchain. This transaction will be recorded securely, creating immutable documentation from manufacturer to sales which increases accountability and transparency as well mitigating the illegal activity.

With the support of Blockchain to **smart contract**, payment upon delivery of products and penalty fees can be operated automatically without the need of 3rd parties, which can reduce the risks of fraud and make the supply chain more decentralized and efficient.

Blockchain **provides trust to the stakeholders**. This is because the data on the Blockchain is decentralized and immutable, therefore, they can trust the data they see on the Blockchain by ensuring no one alters the data. Unlike a traditional supply chain, data storage structure typically requires all stakeholders to keep their own records, and therefore disputes arise when those records do not match up.

It also **facilitates integration of financial and logistics services**, enabling greater data collaboration between stakeholders. Integrated payment solutions reduce the time between ordering and payment processing, ensuring timely movement of products.

Question 2
Immutability is one of the important characteristics of a Blockchain ledger.

Explain the reason why a Blockchain ledger is suitable to be used for transaction auditing by using your own words.

Blockchain is an immutable, open distributed ledger that can record transactions among multiple parties in a verifiable and permanent way. Blockchain can be used as a source of verification for reported Blockchain (traceability). For instance, instead of asking clients to send bank statements to third parties, an organization can easily verify the transactions on Blockchain Explorer, a public Blockchain ledger as all the transactions can be viewed by anyone on the network (transparency).

Illustrate how 51% attacks can post a threat to immutability of Blockchain.
51% attacks happen when a user or a group of users have the network mining power more than 50% on the network. If this occurs, the attackers can control which version of distributed ledger is valid and rewrite the transaction that is supposed to be “immutable” as well as modify the transaction in future or in the past. It also allows them to do double spending that can inflate the money supply which erodes the currency value to secure their own profit.

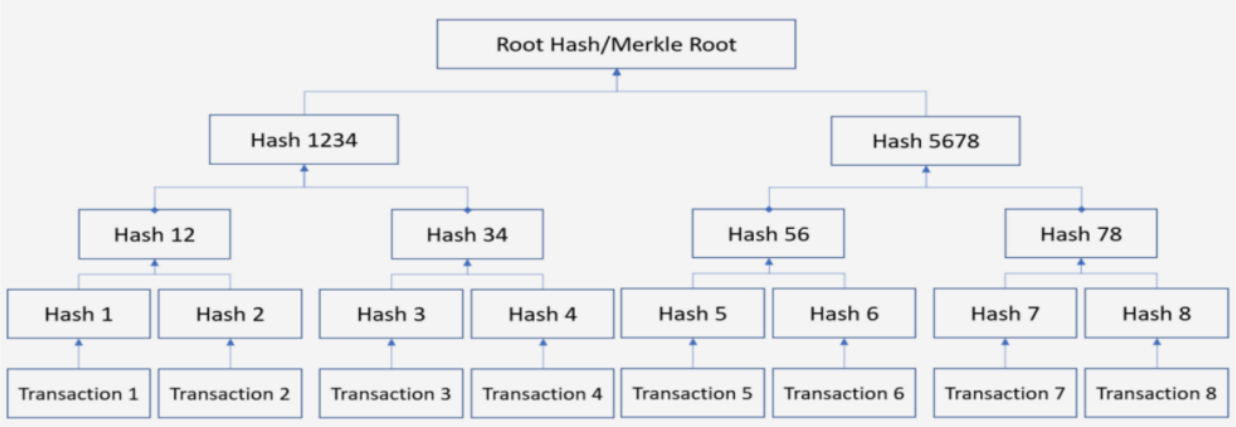
Simplified Payment Verification (SPV) verifies transactions without running a full node

Discuss THREE (3) benefits of using Merkle Trees by SPV clients in verifying the existence of a transaction in a block.

- It allows users to verify a specific transaction without downloading the whole blockchain.This allows you to send and receive transactions using a light-client node
- It significantly reduces the memory needed to verify that data has maintained its integrity and hasn’t been altered.

- It requires less data to be broadcast across the blockchain network to verify data and transactions. This improves the efficiency of a blockchain.

Figure 1 shows a Merkle Tree for a block in a Blockchain ledger. Identify the information needed by a SPV client to verify that transaction 3 has been processed and included in a block.



In order to verify whether the transaction 3 is included in a block, the information needed by a SPV client will be Hash 12, Hash 4 and Hash 5678 downloaded from the full node. Afterward, These 3 information will be combined with Hash 3 and come out a merkle root hash. Then, it can be compared with the merkle root that downloaded from another full node to verify whether transaction 3 has been included in the block.

Question 3
Differentiate a miner node from a full node in Ethereum [8m]

- A miner node processes the latest transaction and consolidates them onto the Blockchain in exchange for the transaction fee and minting rewards if they manage to execute the consensus mechanism successfully.
- They propagates the block they consolidate to the other peers on the Blockchain
- They have performance requirements as they need to have sufficient and efficient computing power to solve the puzzle in order to add the block onto the blockchain.

Identify THREE (3) advantages of using smart contracts in creating rules, procedures or policies for decentralized applications. [9m]
???

Smart contracts usually require control over who or what can execute a function, at what time a function needs to be executed and what are the preconditions to be met before getting access to the function. Discuss a feature in Solidity language that can be used to validate input values to a function before the execution of the function and identify the advantage of this feature. [8m]
Function modifier. It can be used to modify the behavior of the function. To illustrate, it can be used to check the condition using the “require” function. It is specified at the function entry

and executed before the execution of the function begins. If the condition is false, the transaction that calls the message can be reverted using the revert function. No recording on the Blockchain since the transaction will be rejected and all its state will be reverted. Hence, it avoids unnecessary function execution and waste of gas.

Question 4
Tokenization is one of the use cases of Blockchain technology.
Compare and contrast a utility token with a security token.
Utility token

- Utility in the context of token means that the blockchain based token must have some use outside of the financial speculation
- Utility token is used to access to the resource, application and files
- Example: Filecoin which is a token to grant user access to space on a decentralized cloud storage platform

Security token

- A security token derive their value from an external, tradable asset such as real-estate and stock
- A security token is an investment contract as specified in SEC
- Designed to provide a promise a return
- Invest contracts are regulated devices used around the world for fundraising
- Token that is proposed in many ICOs could be considered a security token. Thus, they are regulated in the jurisdiction of issuance.

The fractionalisation and tokenization of real estate is a hot topic. If a token is used to allow fractional ownership of a real-estate, shall the token be considered as a utility token or a security token? Justify your answer. [5m]

- The token shall be considered as a security token.
- A security token derives its value from an external, tradable asset such as real-estate.
- A security token represents a share in the company issuing the token. Investors who buy such tokens hope to turn a profit from investing

Discuss THREE (3) challenges that need to be addressed by Blockchain technology [15m]
Scalability

- The performance of Blockchain infrastructure should not degrade with an increasing number of transactions. Blockchain should increase scalability with given current limitation of Blockchain
- Bitcoin can process 3 to 7 transactions in one seconds whereas Ethereum can process around 20 transactions per second. They are not like VISA which can process 1500 transactions per second. This is no enough for cryptocurrency network to truly take off on a massive scale
- One of the factors that affect scalability on Blockchain includes block size. The increasing number of transactions in blockchain networks leads to a time-intensive

process for executing transactions. For example, a Bitcoin block size was restricted to 1MB and the growing number of transactions in the network has led to increasing block size rapidly thereby affecting scalability.

Privacy

- The blockchain is publicly available and every transaction can be traced back to the first genesis block. Bitcoin is said to be pseudonymous which means that it has data points that are not directly associated with a specific individual but where multiple appearances of a person can be linked together
- The blockchain data is open to everyone for viewing including attackers that want to exploit information for financial gain. This is a big concern for blockchain. Thus, privacy will become one of the biggest growth areas for blockchain technology in coming years
- The content on Blockchain should be visible or selectively disclosed to the participants that are involved in the transaction. The developers and stakeholders are realizing the need to not transmit all data about the transaction.

Interoperability

- Interoperability is considered an important precursor to Blockchain mass adoption
- As more organizations begin to adopt Blockchain, there is a tendency for them to develop their own system with varying characteristics such as governance rules, consensus protocol and etc
- However, these separate Blockchain do not work together and there are currently no standards for them to communicate with each other. The lack of interoperability can make mass adoption become an impossible task.
- Hence, the goal of interoperability is to enable smooth information sharing, faster execution of smart contracts and be more user-friendly between different Blockchain.

Question from Lecture Notes (Chapter 2 Part II)

Can hash functions and public-key cryptography alone provide a secure and trusted blockchain network?

No, these 2 elements will be needed to form the foundation of the Blockchain.

Hash functions have a major role in linking the blocks to one another and also in maintaining the integrity of the data stored inside each block. Any alteration in the block data can lead to inconsistency and break the blockchain, making it invalid. This feature makes the data reliable and secure on the blockchain. Any changes in the block data will lead to difference in hash value and make the blockchain invalid, making it immutable.

Digital signatures provide integrity to the process as they are easily verifiable and cannot be corrupted. They also hold the quality of non-repudiation, making them similar to the signatures in the real world. It ensures that the blockchain is valid and the data is verified and correct.