

BLOCKCHAIN AND CRYPTOCURRENCIES

Final Assessment



Name : Nishat Zereen

Id: w1842465

20th May 2022

Word COUNT: 2450

Table of Contents

[Answer to Question No 1(a) 1](#_Toc103905929)

[Answer to question no 1(b) 2](#_Toc103905930)

[Answer to question no 1(c) 2](#_Toc103905931)

[Answer to Question no 1(d) 4](#_Toc103905932)

[Answer to Question No 2(a) 5](#_Toc103905933)

[Answer to question no 2(b) 6](#_Toc103905934)

[Answer to question no 2(c) 7](#_Toc103905935)

[Answer to the ques no 2(d) 8](#_Toc103905936)

[References: 9](#_Toc103905937)

**Table of Figures**

[**Figure 1 Import the Bitcoin and private key** 1](#_Toc103905693)

[**Figure 2 Public key and Address** 2](#_Toc103905694)

[**Figure 3 multi-Signature** 2](#_Toc103905695)

# 

# Answer to Question No 1(a)

Bitcoin storage involves storing and managing Bitcoin secret keys. There are numerous methods for securely storing Bitcoin. Using a bitcoin wallet to keep funds would be regarded as a secure technique for a business to protect its funds. There are two ways the company can hold funds using the BITCOIN wallet. There are-

1. Hot Wallets and
2. Cold wallets.

Online wallets are sometimes known as hot wallets. The hot wallets operate on internet-connected computers, smartphones, and tablets. A hot wallet facilitates speedy access to and initiation transactions with the funds. However, since the wallet generates the private keys for the money on these internet-connected devices, this poses potential risks.

The cold wallet is the most secure way to store bitcoin. A bitcoin wallet cannot be compromised due to its lack of Internet connectivity. The cold wallet, also known as a "hardware wallet" and an "offline wallet," holds the user's address and private key and combines suitable computer software. A cold wallet is a wallet that is not connected to the internet, and this method has a lower risk of being compromised.

Now, one regulator shouldn't control it; to hold the key, the Bitcoin script allows people to expressly state that power over an address is divided among multiple keys. These keys can be stored separately and signatures created independently. The signed transaction will be created on some device, but an adversary can only block it from broadcasting to the network. No transaction can have valid multi-signatures without the other instruments.

**The solution to this problem –**

Multi-Signature is the remedy for the issue. The potential of a multi-signature has gained some popularity; it requires the support of multiple people (often three to five) for a transaction to occur. The inability of a single regulator or server to complete trades reduces the possibility of theft. People who can execute are selected, and when one of them must spend or send bitcoins, they seek assistance from others in the social gathering.

# Answer to question no 1(b)

The idea behind multi-signature is unscored by creating a secured wallet for the bitcoin owners. This is on the background that as a group has title to ownership of some amount of bitcoin, it should not be kept in a single partner's wallet. Therefore, with a multi-signature, all or some pairs of owners will be designated to sign before a transaction is validated. The bitcoin must be kept in a multi-signature address from where transactions regarding the funds would be initiated. The members can prove their identity through the public key generated from the private key.

# Answer to question no 1(c)

Python is used to generate private keys and multi-signature addresses for the multi-signature approach to transaction validation to prevent a single individual from holding bitcoins in their wallet. Detailed instructions are provided below.

Graphical user interface, text, application

Description automatically generated

**Figure 1 Import the Bitcoin and private key**

At first, the person needs to install bitcoin, and after that, he needs to import the bitcoin library, which will be able to create and run command lines to generate wallet addresses and keys. Then the person needs to make his private key, and he is not supposed to share his private key with anyone else. Therefore, this key must be kept secret as one risks losing their bitcoin to anyone who gets access to it. Here this report shows the private key for understanding, but this key will not be used for other purposes.

Graphical user interface, text, application, email

Description automatically generated

**Figure 2 Public key and Address**

After that, he can generate his public key by using his private key. The public key enables the verification of digital signatures, which serves as evidence of the private key's ownership, and the next step is to generate the BITCOIN address.

Graphical user interface, text, application, email

Description automatically generated

**Figure 3 multi-Signature**

The syntax creates random keys as the private keys, which are alphanumeric. The private keys will be the only means by which bitcoin transactions can be validated, that is, spent by the partners. There are three private keys for multiple people, and the next step is generating public keys.

Next, the multi-signature syntax shown above creates a multi-signature address which builds trust between partners who jointly own bitcoins and makes it more secure by not allowing one party to transfer coins without the other parties unilaterally. Therefore, the business partners (Alice, Bob, and Coo) must have a multi-signature address for storing their funds.

# Answer to Question no 1(d)

**Centralised network:**

In a centralised network, there is a central network owner. The owner of the central network serves as a single point of contact for sharing information. When there is a single central owner, a centralised network becomes a single point of failure, its most significant flaw. There are higher privacy risks, and the networks take longer for some people living far away. In addition, because the owner stores only a single copy of the resource, repeated access to it causes an access difficulty over time. However, the advantages of a centralised network are that it is simple and can be developed quickly, and the maintenance cost is affordable.

**Decentralised network:**

Numerous central owners have a copy of the decentralized network's resources. A centralised network avoids the most significant risk posed by a single point of failure. If there are several owners, information can still be retrieved if one of the central nodes fails. It gives better performances and allows for a more diverse and flexible system. Additionally, having several owners slows down the speed of information access. It also can have security and privacy risks to users and provide inconsistent performance. A decentralised network requires higher maintenance costs.

**Distributed network:**

The distributed network is the decentralised network taken to the extreme. It avoids centralisation completely. The main idea for the distributed network lies in the concept that everyone gets access, and everyone gets equal access. As a result, the distributed network is fault-tolerant, transparent, and highly secure. However, it is challenging to deploy, and the maintenance cost is very high.

# Answer to Question No 2(a)

**Proof of Work (PoW) –**

There is a demand for decentralised exchange approval using blockchains like Ethereum. Historically, Ethereum, like other cryptographic currencies, depended on a consensus process known as proof of work (PoW).

Markus Jakobsson and Ari Juels coined "Proof-of-work" BITCOIN dominates. It allows secure digital transactions without a third party. A prover shows a verifier that they spent a certain amount of computational time (Jakobsson and Juels, 1999).

Bitcoin obtains proof of work using hash puzzles. For example, for creating a block, the node proposing the partnership is required to find a number (nonce) such that when you concatenate the nonce, the previous hash, and the list of transactions that make up the block, the resulting hash output should be a number that falls within a target space that is relatively small in comparison to the output space of the hash function.

Proof of work can be used to validate all past and present transactions. Mining is the process of solving a puzzle that results in a monetary incentive for the individual who solves it. Miners compete to be the first to answer a complex mathematical problem that will produce this new block, assuring that they will receive rewards.

**Proof of Stake (PoS) –**

'Proof of Stake' is a consensus process that chooses who validates the next block based on how many coins you possess, rather than miners solving cryptographic riddles using computer power as they do with traditional 'Proof-of-Work.'

Proof of stake (PoS) is different because transaction validators stake crypto instead of miners. First, validators are chosen based on how much and how long they've held cryptocurrency. Other validators can then certify a block. When enough attestations are received, a block can be added. "Forging" or "minting" a block proposal pays validators.

Finally, Proof of Stake is distinguished from Proof of Work because no new coins are generated or mined. Since all coins are created initially, mining businesses should only be reimbursed through transaction fees or fees. In addition, PoS is significantly more energy-efficient than PoW because it decouples the consensus procedure from energy-intensive computer computation. It also means that securing the blockchain requires fewer computational resources.

# Answer to question no 2(b)

**DeFi –**

Decentralized finance (DeFi) is a developing financial system based on secure distributed ledgers comparable to those used by cryptocurrencies. The system eliminates banks' and institutions' authority over money, financial products, and services. There are several benefits of swapping in DeFi.

Key benefits of swapping in Defi:

1. The Defi applications are not required to involve mediators or other parties. But, first, only a smart device, can be a mobile or a tablet, etc., is required.
2. DeFi doesn't require permission. Anyone with a crypto wallet and internet can use DeFi. Users can trade and exchange assets without bank transfers or costs. (Other crypto-specific expenses, like gas, may apply.)
3. Transactions are executed in real-time; as soon as a transaction is finalised, the underlying blockchain is updated, and interest rates are modified several times every minute.
4. Transparency is another benefit. Every Ethereum blockchain transaction is broadcast to the network and validated by other users. Any user can witness network activities with this level of transaction data availability.

**Performance comparisons between Defi and traditional financing –**

The argument between decentralised and traditional finance is raging. There are some significant differences between the two.

1. Public blockchains control all decentralised financial transactions. However, conventional finance and public government oversee all operations, including regulations and licenced financial organisations.
2. Because it is more open and transparent than traditional finance, decentralised finance continues to gain traction. Moreover, because there are no hurdles to entry, anyone with programming abilities can contribute to developing financial services and tools on top of public blockchains.
3. In contrast, the traditional financial system is unlikely to welcome the rising trend due to high entry barriers. Moreover, obtaining relevant licenses and authorisation from regulators has hampered innovation in conventional economic systems.
4. Defi's development as an alternative to the standard monetary system is still in its infancy, although various applications make its use advantageous for individuals. For example, Defi might give many people access to banking in locations where conventional money has failed.
5. In contrast to the traditional banking industry, which is governed by various rules that can make it difficult for individuals to do cross-border business, Defi permits transactions to be conducted without worrying about national security breaches.

# Answer to question no 2(c)

**ICO –**

Initial Coin Offerings (ICOs) include the production of digital tokens by young micro-SMEs and their distribution to investors in exchange for fiat cash or, in most cases, significant cryptocurrencies (Bitcoin or Ether).

Pros of ICO –

1. In ICO, the companies can go for ICO at their early stage and get investors worldwide. In contrast, IPO takes time and potential VC.
2. SMEs can go for ICOs; project base, plan base companies can have their ICOs without any financial track record. However, only stable businesses with all their financial and operational records can apply for IPO.
3. ICO is open to all the investors, and thus the company can get an international recognization. On the other hand, IPO is sometimes restricted to institutional investors.
4. ICO can be traded 24/7. It has no time limitations, but the IPO is traded in a fixed session.

Cons of ICO –

1. The regulatory framework of ICO is very unclear, whereas IPO has all the regulated offerings, i.e., extensive requirements around registration, marketing of offering disclosure, etc.
2. In ICO, the volatility is extreme, and the valuation is very challenging, whereas IPO manages its trading and the valuation depends on the financial condition.
3. In the secondary market, the volatility of ICO is extreme, and they have high counterparty risks. At the same time, IPO has marginal requirements for counterparty risk and market rules for trading.
4. ICO holders get the dual function of tokens, voting, and other rights. In addition, however, IPO holders get governance rights, ownership, and dividends.

# Answer to the ques no 2(d)

To build the NFT, at first, two folders were made; one was the 'IMAGES' folder, and another was the 'JSON' file. After that, all the images were kept in the image file and uploaded to the 'Pinata' home of NFT media platform. After that, some python codes were run to create the 'JSON' files, and the CID for the images file was used from the Pinata platform. After that, the 'JSON' files were taken to the 'JSON' folder and uploaded to the Pinata platform.

After that, on the REMIX website, a contract was made using an ‘NFT.sol’ file, and there the Name, the Symbol, and INITBASEURI were set for the contract. In addition, the CID for the 'JSON' file was given in the INITBASURI like this - 'ipfs://CID Address/.' After that, a collection was visible on the open sea page.

The address for the 'open-sea' is - <https://testnets.opensea.io/collection/est-apartments-nft-collection>

The Contract Address - 0x3A471ec127bBd5C8C856cE80B3Cb4f276249De6F

EST is an Architecture Company concentrated on interior designs for houses and apartments. Their goal is to redecorate your home and make them look professional and organised. On this platform, they upload 3D interior designs. A person/customer can choose to have this design in their home from this platform. If a person holds the NFT, they will get priorities and discounts while decorating their own home by them.

These NFTs are the designs that the company is offering to its customers. Also, this company is registered with a decentralised platform; from there, one can buy and sell the NFTs and make some profit.

The first NFT is a view of a sitting room, including a couch and a floor mat on the wooden floor and excellent wall paint to make the room look gorgeous. The properties are the background, floor, couch, and window.

The second NFT is a corner view of a sitting room, including a couch, a chair, a tea table, and a shelf. The properties of the NFT are the background, the floor, floor mat, view, and furnished or not.

The third NFT is another way of decorating the sitting room, with a view of a kitchen of a one-bedroom flat. This one contains a lot of items of furniture and a cozy couch. The properties of the NFT are background, floor, window, and couch.

# References:

Medium. 2022. *Decentralized Finance vs. Traditional Finance: What You Need To Know*. [online] Available at: <https://medium.com/stably-blog/decentralized-finance-vs-traditional-finance-what-you-need-to-know-3b57aed7a0c2> [Accessed 19 May 2022].

Jakobsson, M. and Juels, A. (1999). Proofs of Work and Bread Pudding Protocols(Extended Abstract). *Secure Information Networks*, 258–272. Available from https://doi.org/10.1007/978-0-387-35568-9\_18.