National College of Ireland

National College of Ireland

MSCLOUD_JAN23B_I

Name: Rishabh Sinha
Email: x21171203@student.ncirl.ie

Blockchain Concepts and Technologies

Answer All Questions

Academic Honesty Declaration

I declare the following to be true for this submission:

- I have completed the task during the designated time window and declare it to be exclusively my own work.
- I have not received or attempted to receive assistance in preparing this response from any other person during the assessment window.
- I have not provided, or offered to provide, assistance to any other student by any means during the assessment window.
- **You are to submit your work using the same question sheet with the academic honesty declaration above unmodified.**
- **There are 4 pages in total in the question sheet, you are to submit the same sheet with your answers to the questions.**

The maximum number of pages allowed for your submission is 8.
This is including the question sheet.

Question 1: (20 Marks)

Highlight the potential web3 DApp implementations for the following business scenarios.

E.G: Provide a DApp solution for each of the 3 below scenarios respectively.

You are free to call upon your knowledge within the blockchain domain e.g., the use of Smart Contracts, DLTs and other similar technologies in the domain.

200 words max for each scenario.

1. Souvenir Shop
2. Recruitment Agency
3. Fine Arts Dealer

Ans 1: The potential web3 DApp solution for the following business scenarios are:

1. **Souvenir Shop:** A Decentralized marketplace and authentication platform powered by blockchain technology, smart contracts, and non-fungible tokens (NFTs). We can have a decentralized marketplace where local businesses can list their souvenirs for sale. "Smart contracts" would facilitate the transaction process by automatically executing the purchase agreement once the buyer and seller agree on the terms. These smart contracts will handle payment, escrow, and dispute resolution, ensuring secure and transparent transactions and we don't need intermediaries. We can utilize the concept of "NFT" As a solution for authenticity and provenance verification of the souvenir that are sold by having a unique "NFT" as a digital certificate of authenticity for the items that are listed. Hence, Buyers will be able to verify the ownership history of the item he is interested in and hence reducing the risk of purchasing fake or unauthorized items. We can also add feedback system where the feedback from the buyers will be recorded on the blockchain network and hence creating a transparent and immutable reputation record for sellers and will help buyer in taking informed decision and hence promoting trust within Souvenir Shop DApp. At last, we can also have a decentralized identity solution where users could control their personal information and authenticate themselves using blockchain-based identity protocols, reducing the reliance on centralized authentication systems.
2. We can have a decentralized platform using blockchain technology, smart contracts, and decentralized identity solution that can help this agency in hiring process while enhancing trust and efficiency. In this DApp Job seekers will be able to create their profile and upload their resume that will be linked to decentralized identities and hence the user will be able to have control over their personal information and will be able to securely share their personal information to with only potential employers. We can make use of "Smart Contract" for employment agreements, which can be created once the employer and candidate agree on the terms. Smart Contract will have the agreement details, salary, start date or any other related information and hence reducing contract disputes or fraud. We can have a reputation system integrated in our DApp which can provide transparent and verifiable records of the candidates' professional history and achievements with skill verification functionality added utilizing the concept of NFTs. Candidates can have NFTs representing their verified skills and certifications, which could be validated and trusted by employers and hence enhancing the credibility of candidates and will help employers taking informed decisions rather than only relying on candidates CV or interviews. We can also have a decentralized identity solution for privacy concerns, all the data can be stored in blockchain and hence reducing the risk of data breaches and unauthorized access.
3. **Fine Arts Dealer:** DApp for this business can serve as a decentralized marketplace for buy and selling creators' work. We can have a functionality for creators and collectors to create their profiles and put their art works for sale with all the information of the article to prove its authenticity. "Smart Contract" will ensure secure and transparent transaction process along with automating the payment, transfer of ownership, and royalty distribution mechanism. All the art works can be tied up with NFTs which will act as a digital token and will have all the information about art works ownership history and its authenticity that can be used for the verification by the collectors. These digital tokens can be traded between creators and collectors and thus ensuring transparent and immutable record of ownership. We can also have decentralized identity solution that allows creators and collectors to have full control of their personal information while verifying their identities maintaining trust and security within DApp. And at last, we can have fractional ownership of high-value artworks by issuing tokenized shares. Collectors will be able to own a fraction of an artwork and thus enabling liquidity in the Fine Arts market. Here, Smart Contract will manage the ownership rights and distribution of the shares or proceeds from potential sales or exhibitions.

Question 2: (10 Marks)

Explain the purpose of the below code segment: Provide reference and citations of key documentation where appropriate.

```
let account;
 const connectMm = async () => {
   if(window.ethereum !== "undefined") {
    const accounts = await ethereum.request({method: "eth_requestAccounts"});
    account = accounts[0];
    document.getElementById("userArea").innerHTML = `User Account:${account}`;
 }
```

Ans 2: The above code is using "*Ethereum.request"* method from "*web3.js*" library to request access to the users Ethereum account on their **M**eta**m**ask wallet.[1][2] Variable "*account*" is used to store the Users Ethereum account address. An asynchronous function "*connectMm*" checks if "*window.ethereum*" object is not undefined and checks if users have Metamask extension installed on their browser. "*await*" keyword waits for the response to retrieve accounts before assigning account address to the "*account*" variable and update the content of an HTML element with the id "*userArea*". *"innerHTML"* property is used to display the users Ethereum account address. This code snippet enables web3 DApp to connect with Metamask wallet [3] and retrieve users Ethereum account address for authentication or further use in the main program.

Question 3: (5 Marks)

The Term sustainability has cropped up in recent times relating to Blockchain Technologies and crypto currencies. Provide some of your own brief insights regarding sustainability within the Blockchain Domain. Provide 3 Talking points and briefly expand.

Ans 3: As blockchain technology develops, sustainability is something that is being discussed more and more. Below are my three talking points related to sustainability in blockchain technologies and crypto currencies:

1. **Energy Consumption:** The energy consumption of blockchain technology is a significant issue, especially in the context of digital currencies like Bitcoin. In a proof-of-work (PoW) consensus method, mining and validating transactions needs a large amount of computational power and energy. Blockchain networks can therefore have a sizable carbon footprint, especially those with a lot of users, article referenced in [4]. It's important to keep in mind that not all blockchains employ proof-of-work (PoW), and alternative consensus mechanisms like proof-of-stake (PoS) are becoming more and more popular because they consume less energy.
2. **Scalability and Efficiency:** The scalability and efficiency of blockchain networks are other facets of sustainability in blockchain technologies. In order to support more transactions and users without sacrificing efficiency, scalability issues must be resolved as blockchain technology use advances. Many approaches, including sharding and layer-2 protocols (like the Lightning Network), aim to increase the sustainability of blockchains by boosting their scalability and lowering their resource demands. [5]
3. **Environmental Impact:** Sustainability in the blockchain technologies goes beyond energy use to account for a wider range of environmental effects. Electronic waste can be produced during the manufacturing and disposal of mining-related gear, such as specialized ASICs (Application-Specific Integrated Circuits), an article is published by BBC News and C&en[6][7]. Also, the reliance on specific consensus procedures can cause the concentration of mining power in areas with inexpensive energy, thereby escalating environmental imbalances. To increase the overall sustainability of blockchain technology, efforts are being focused on promoting ethical mining techniques, supporting the use of renewable energy sources, and investigating environmentally friendly consensus procedures.

Question 4: (10 Marks)

What is Proof of Stake? Detail your response including references to randomness, its role in decentralized consensus, power consumption and Delegated Proof of Stake.

Ans 4: Blockchain networks use Proof of Stake (PoS) as a consensus mechanism to establish decentralized consensus. Block validators in Proof of Stake (PoS) are chosen based on their ownership or "stake" in the network [15] , as opposed

to Proof of Work (PoW), which requires miners to solve difficult math problems. Based on the number of tokens they possess and are ready to "lock up" as collateral[8], validators are selected to add new blocks and validate transactions. To maintain fairness in the selection process, randomness is essential in PoS. Validators are chosen depending on their stake using a variety of methods, including Randomized Block Selection and Coin Age Selection. Randomness fosters a more decentralized network where no single entity has authority over the consensus procedure because it prohibits any individual or organization from accumulating an excessive amount of power[8]. PoS's lower power usage is one benefit over PoW. PoW uses a lot of energy because miners compete to solve puzzles that need a lot of computing. PoS eliminates the need for mining that consumes a lot of energy because validators are chosen according to their stake. As a result, PoS is more eco-friendly and energy-efficient, which allays worries about the carbon footprint of blockchain networks[8]. A delegation technique is used in Delegated Proof of Stake (DPoS), a PoS variant. Participants who hold tokens in DPoS have the option of assigning their voting rights to vetted people and entities that are referred to as "delegates" or "witnesses." Those with tokens who have delegated their stake are accountable for block production and validation through delegates. Delegates are often chosen through voting, in which token holders support the delegates they believe will best serve their interests. By decreasing the number of validators actively taking part in the consensus process, DPoS improves scalability and efficiency. Token holders can take part in consensus through delegation without specialized knowledge or a lot of processing power. Conversely, delegates can concentrate on protecting the network and upholding consensus. With the use of this delegation model, blockchain networks can process more transactions per second, confirm blocks more quickly, and use resources more effectively.[8][9][10]

Question 5 (20 marks)
Define the four fundamental concepts, which you believe made the creation of the bitcoin blockchain possible in 2009, and how these concepts interact and combine to enable blockchain as a disruptive technology. You must also critically appraise why you have selected these as the most fundamental concepts.

Ans 5: Decentralization, consensus, cryptography, and immutability are the four key ideas that made it feasible to create the Bitcoin blockchain in 2009. These ideas interact with one another and work together to make blockchain a disruptive technology with the potential to completely alter several sectors. Let's examine each idea in detail to comprehend its importance:

1. **Decentralization:** A fundamental tenet of blockchain technology, decentralization refers to the removal of a central authority or middleman in charge of the network. With Bitcoin, there has been no longer a need for a government or central bank to oversee transactions. Instead, a network of computers known as nodes hosts the blockchain, guaranteeing that no single entity has total authority over or can manipulate the system. By strengthening the network's resistance to censorship and individual points of failure, decentralization fosters openness, security, and resilience. By providing people ownership over their own assets and data, it empowers people and promotes a more transparent and inclusive financial ecosystem.

2. **Consensus Mechanism**: This system allows network members to agree on the legitimacy of transactions and the sequence in which they are added to the blockchain networks. The consensus algorithm used by Bitcoin is called Proof of Work (PoW), and it relies on miners competing to complete computationally challenging math puzzles that confirm transactions & add blocks to the network. Not depending on a centralized authority, this approach makes sure that all participants come to a consensus regarding the status of the blockchain. PoW guarantees integrity and security within a decentralized network by rewarding miners.

3. **Cryptography**: Blockchain technology relies heavily on cryptography, which offers secure and impermeable transactions. Data is encrypted and verified using cryptographic techniques to ensure its secrecy, integrity, and validity. Cryptographic methods like public-private key pairs and digital signatures are employed in the Bitcoin blockchain to safeguard transactions and confirm ownership. The confidentiality of their transactions is ensured by cryptography, which enables participants to provide proof of ownership without disclosing their private keys. Additionally, it permits private communication while guarding against fraud and unwanted access.

4. **Immutability:** Once information is stored on a blockchain, it cannot be changed or modified. Every block within the blockchain has a cryptographic hash which is based on the data it contains and the hash of the block before it. It

becomes computationally impossible to update historical records as a result of the chain of blocks that are created. Any alteration to one block will invalidate all future blocks. By providing a transparent and secure ledger of transactions, immutability maintains the authenticity and legitimacy of the blockchain. It is appropriate for applications like supply chain management, and some apps we discussed earlier in answer 1 like digital identity, Souvenir shops, Recruitment agencies, Fine Art dealers, and intellectual property rights because it also supports provenance verification.

These four ideas are seen as essential to the development of the Bitcoin blockchain as a result of their combined ways in which they address the most pressing problems with trust, security, and transparency. Decentralization makes ensuring that no one organization has complete authority, fostering trust and lowering the possibility of manipulation. By enabling agreement on the blockchain's current state, the consensus process ensures its integrity and security. Secure transactions are made possible by cryptography, which also guards against illegal access. The accuracy and tamper-resistance of recorded data are ensured by immutability. Together, these ideas lay the groundwork for blockchain technology and enable its potential for disruption in a range of industries. Blockchain applications in finance, for instance, enable cross-border transactions that are quicker, cheaper, and more transparent while minimizing the need for middlemen. Blockchain addresses challenges of counterfeiting and ensures ethical sourcing by providing end-to-end visibility and traceability in supply chain management. Additionally, blockchain has effects on decentralized finance, voting procedures, healthcare, and intellectual property.

Question 6 (20 marks)

Critically explain and detail a transaction lifecycle process, you are free to choose either Bitcoin or Ethereum transaction lifecycle. Within your response ensure to detail each key function and process within the lifecycle, an illustration or diagram can be used to support your response.

Ans 6: For Ethereum, the transaction's lifecycle process entails several crucial operations and procedures that guarantee the trustworthy and safe execution of transactions. Each stage is described in depth below:

1. **Transaction Initiation**: The transaction is started by an externally owned account (EOA), which is normally run by a person. An action, like as transferring ETH between accounts, initiates the transaction. The transaction contains necessary details including the sender's and recipient's addresses, the transaction's value, the gas limit, and optional data.

2. **Signing a transaction:** To establish the transaction object's legitimacy and prevent fraud, it must be signed using the sender's private key. The signing procedure is managed by an Ethereum client like “Geth”, which creates a signature using the sender's private key. The signature guarantees the transaction's cryptographical security and that it came from the sender.

3. **Submission of a transaction:** The transaction is sent to the Ethereum network for processing after being signed. The transaction is added to a transaction pool with other pending transactions after being broadcast to the entire network.

4. **Execution and Transaction Verification:** Transactions from the pool are chosen by validators, commonly referred to as miners, and added to blocks. The Ethereum Virtual Machine (EVM) executes the chosen transactions, which modifies the network's state. The gas limit establishes the maximum amount of compute the transaction is permitted to use during execution. To reimburse validators for their computational labor, gas fees are paid by the sender.

5. **Block finalization and justification:** A block containing the transaction must go through a justification and finalization process before it can be added to the blockchain. Reaching a predetermined level of network consensus on the block's legitimacy is necessary for block justification. Finalization firmly establishes a block's position in the blockchain, making it very expensive and difficult to change. High levels of assurance that the transaction is completed and immutable are provided via finalized blocks.

During the transaction lifecycle, the following crucial variables are involved:

1. **Gas Fees:** Transactions must pay gas prices to reimburse validators for their computation costs. Gas prices and network congestion, among other variables, affect gas expenses.

2. **Nonce**: The transaction contains a nonce, which is a counter that increases progressively and shows the transaction number from the sender's account. Replay attacks are avoided, and the right sequencing of transactions is guaranteed.

3. **Cryptographic Hashing:** Cryptographic hashes, which give each transaction a distinct identifier and allow provenance verification, are used to identify and monitor transactions.

4. **Interactions using Smart Contracts:** Ethereum facilitates interactions with deployed smart contracts in addition to standard transactions. In these interactions, the smart contract address is specified, and data is provided in accordance with the contract's Application Binary Interface (ABI).

Following this transaction lifecycle procedure ensures that transactions are executed securely and decentralized, providing immutability, trust, and transparency inside the blockchain network.

Question 7 (5 marks)
Detail why you are expected to wait for a certain number of confirmations after receiving a cryptocurrency transaction?

Ans 7: A critical security step that helps ensure the integrity and finality of the transaction is to wait a specific number of confirmations after receiving a cryptocurrency transaction. The main justifications for needing to wait for confirmations are as follows:

1. **Consensus and Block Finalization:** Cryptocurrencies, like Bitcoin and Ethereum, rely on a decentralized consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate and confirm transactions. Confirmations refer to the number of blocks that have been added to the blockchain after the block containing the transaction. Each new block represents additional computational work and consensus, making the transaction more secure. Waiting for confirmations allows the network to reach a consensus on the validity and order of transactions, ensuring that the transaction is not part of a temporary or orphaned branch of the blockchain.
2. **Double Spending Protection**: A hostile actor could try to spend the same cryptocurrency twice in a double-spending attack. You reduce the danger of accepting a transaction that might later be revoked or substituted by another by waiting for confirmations. The likelihood of a successful double spend declines noticeably as confirmations rise. A higher level of trust that the transaction is permanent and has been approved by the network can be attained by waiting for repeated confirmation.

3. **Forks and Chain Reorganizations**: The blockchain may occasionally experience forks or reorganizations as a result of network upgrades, modifications to the consensus rules, or momentary forks brought on by network delay. During these occasions, previously verified transactions may be revoked or swapped out for new blockchain branches. Chain forks and reorganizations could potentially have an adverse effect, therefore waiting for confirmations can assist. A transaction is less likely to be impacted by such events the more confirmations it has.

4. **Network Security and Attack Mitigation:** Additionally, waiting for confirmations can assist defend against network attacks, such as 51 percent attacks. Most of the the network's computational power (hash rate) is taken over by the attacker during a 51% attack, giving them the ability to possibly tamper with transactional data. You provide the network enough time to detect and reject any transactions that were created fraudulently or maliciously by waiting for confirmations.

Depending on the cryptocurrency and its underlying consensus mechanism, a transaction may need more confirmations before being deemed secure. In order to achieve a high level of security for Bitcoin, it is generally advised to wait for at least six confirmations, which takes around an hour. The suggested number of confirmations for various cryptocurrencies may vary depending on elements like block duration, network size, and consensus method. It's crucial to remember that

while waiting for confirmations improves transaction security, it does not offer 100% assurance. A transaction with many confirmations can occasionally still be undone or invalidated, but the likelihood decreases dramatically with each subsequent confirmation.

Question 8 (10 marks)
Critically assess how the use of Hashing Algorithms contribute to the functionality of the blockchain network, citing key contributions and implementations within the network.

Ans 8: The blockchain network's ability to function depends on the employment of hashing algorithms, which make several important contributions and implementations that improve the security, integrity, and effectiveness of the network. Let's evaluate the importance of hashing algorithms in the context of blockchain:

1. **Data Integrity**: To generate a distinct digital fingerprint of data, hashing techniques like SHA-256 (Secure Hash Algorithm 256-bit) are utilized. Applying the procedure to the data yields a fixed-length string of characters that serves as this fingerprint, or hash. Each block in the blockchain network contains a hash of the header from the preceding block, essentially chaining the blocks together. This establishes a tamper-evident framework wherein every modification to a block's data or the sequence of blocks will change the corresponding hash, rendering it computationally impossible to alter the blockchain's history covertly. The integrity and immutability of the data stored on the blockchain are guaranteed by hashing algorithms.
2. **Consensus on Proof of Work (PoW):** A key element of the PoW consensus mechanism employed in blockchain networks like Bitcoin is hashing algorithms. In proof-of-work (PoW), miners compete to discover a nonce (a random integer) that, when paired with the block's data, yields a hash that satisfies specified predefined conditions (such as a predetermined number of leading zeros). A miner must put in a lot of computing effort to locate the nonce, and if they do, the block is accepted and added to the blockchain. Miners must solve the underlying mathematical challenge provided by hashing algorithms to maintain the network's security and decentralized consensus.
3. **Security of Transactions and Addresses:** Blockchain networks use hashing algorithms to create cryptographic addresses and check the accuracy of transactions. Hash functions are used in public-key cryptography to create shorter, fixed-length addresses from longer public keys. For instance, the SHA-256 hashing algorithm is used by Bitcoin to transform a public key into a Bitcoin address. Hashing methods are also employed in transaction verification to generate a unique identifier (transaction hash) for each transaction. For ensuring the legitimacy and integrity of transactions within the blockchain network, this hash is used as a reference.
4. **Merkle Trees**: Hashing techniques make it possible to use Merkle trees, a data structure that effectively checks the accuracy of big data sets. Merkle trees construct a hierarchical structure by combining various hashes into a single hash using hash functions. Merkle trees are used in blockchain networks to represent a block's transactions. The block's header contains the root hash of the Merkle tree, which offers a succinct summary of the block's contents. Participants can quickly validate the inclusion of transactions without having to analyze the entire block by verifying the root hash. Blockchain networks are more scalable and effective when using merge trees.
5. **Digital Signatures**: In blockchain networks, digital signature techniques include hashing algorithms as a key component. The integrity and validity of messages or transactions are guaranteed by digital signatures. In these techniques, the material that must be signed is first hashed, and the hash is then encrypted using the sender's private key. The associated public key can be used to validate the generated digital signature. Hash functions are essential in this process because they give the data a fixed-length representation, which speeds up the signing and verification procedures.

Bibliography

[1] Đ. Hoàng, "How To Connect Web3 With MetaMask?," ethereum.stackexchange.com, 15 January 2020. [Online]. Available: https://ethereum.stackexchange.com/questions/67145/how-to-connect-web3-with-metamask.

[2] F. Vogelsteller, R. Ghods, V. Maia, M. Garreau and E. Marks, "Ethereum Provider JavaScript API," eips.ethereum.org, 30 June 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1193.

[3] Metamask, "Connecting to MetaMask-Etherium provider API," Metamask, [Online]. Available: https://docs.metamask.io/wallet/reference/provider-api/#connecting-to-metamask.

[4] J. Sedlmeir, H. Buhl, G. Fridgen and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," springer.com, 9 May 2020. [Online]. Available: https://rdcu.be/dcxg3.

[5] S. Singh, "Understanding The Blockchain Layered Architecture To Solve The Scalability Challenges," binance, 29 September 2022. [Online]. Available: https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solutions.

[6] BBC News, "Bitcoin mining producing tonnes of waste," BBC News, 20 September 2021. [Online]. Available: https://www.bbc.com/news/technology-58572385.

[7] M. Peplow, "Bitcoin poses major electronic-waste problem," cen, [Online]. Available: https://cen.acs.org/environment/sustainability/Bitcoin-poses-major-electronic-waste/97/i11.

[8] D. T. H. D. N. N. C. T. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," IEEE Access, 26 June 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2925010.

[9] seb1220, "CONSENSUS MECHANISMS," ethereum.org, 13 January 2023. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/.

[10] D. Larimer, "Delegated proof-of-stake consensus.," EOS.IO Technical White Paper v2, 2018. [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#delegated-proof-of-stake-consensus.