Name – AYUSH BADGUJAR

ASSIGNMENT 1 (SUBMISSION 22st DECEMBER)

1. List out 5 different use cases of blockchain technology. Mention at least one use case relevant to IITK Campus Community.

Ans. A) Fee payment can be done using blockchain technology. Many people can’t tranfer this much large amount of money in one go and they have to use net banking, upi or other ways, not all can pay using credit card. Sometimes it takes time for banks to process this much huge payment.

B) Foreign money exchange can be made easier using blockchain tech, spending money in another country, with the bonus of having no foreign transaction fees.

C) Health centre data management can be made more secure using blockchain technology.

D) Campus election for different roles like Gensec etc can be made more secure and ensure no tampering of votes takes place. This can be extended for India’s election process also.

E)

1. List out 5 different blockchain networks in use. Write down what their speciality/specific use case is. What consensus mechanism do they use?

Ans. A) Bitcoin – Also known as BTC, first cryptocurreny . Provides a decentralized store of value and medium of exchange. It is an assecible and versatile currency , it can be used to perchase goods and services from the growing list of places that accept it. Governments can’t control Bitcoin like they can with centralized fiat currentcy such as the US dollars. Consensus mech is proof of work that is miners have to solve hard maths problems to validate transactions and to create new blocks.

B) Solana - SOL, it is fast and has low transaction costs, it is designed for dApp(decentralized applications – software that runs on a decentralized network, not controlled by a single authority, hence collectively controlled by their users) that required high throughput (amount of service or product that a company can produce and delicer to a client within a specified period of time) such a Defi platforms , nfts and gaming  
Consensus mechanism is PoH and PoS, it combines PoH timestamping mechanism that orders transacrions and with PoS , where validators are chosen to create blocks. PoH enables very fast transactions processing.

C) Ethereum – ETH, is a decentralized blockchain with smart contract fuctionality (a comp prog or a transaction prot that is intented to auto execute, control or document events and actions according to the terms of a contract or an agreement). ETH allows anyone to deploy permanent immutable dApps onto it, with which users can interact. On 15 sept 2022, ETH transitioned its consensus mech from PoW to PoS. Here some validators are selected to create blocks and validate transactions based on the amount of ETH they hold and are willing to stake.

D) Algorand – Algorand is an energy-efficient, quantum-secure, single-layer blockchain with instant finality, consistently high throughput, and low fees. It has 4 types Lofty (fractional homeownership by tokenizing real estate), Folks finance (innovation and powerful integration), Labtrace (authenticate and verify medical data and combating AL manipulation and ensuring research integrity in medical and academic fields) and Wholechain (enables companies to collect verifiable data at every step of the supply chain and ensures that data is immuabke thru the use of Algorand blockchain tech). Consensus used in this is PPoS(Pure proof of stake ) – selection of validators is random, proportional to amt of ALGO tokens they stake, providing high security and decentralization while maintaining fast transaction finality.

E) Cosmos – ATOM , cosmos is a decen network that facilitates interoperability(achieved thru IBC inter blockchain communication, transfer of data and token btw indep blockchains wo needing a central intermediary ) between multiple blockchains allowing them to communicate and share data, also often referred as internet of blockchains. It has modular architecture cosmos SDK (framwork to build BC that are customizable and optimized for specific use cases), modular approach makes it easuer for developers to build spicialised BC tailored to their needs wo reinventing the wheel. Consensus mech – tendermint BFT byzantine faut tolerance where validators reach agreement on the state of the blockchain in a decentralized manner, ensuring high availability and security.

1. Write a program in any programming language that simulates the cryptographic problem solved in PoW. (Find the smallest nonce (a whole number) such that SHA-256 hash of the new string is less than the threshold.)   
   Input by user: String  
   Output: Nonce, Time taken to find the nonce

You can assume a threshold like 0x000FF…..F (that is the first 3 hexadecimal digits should be 0 for the nonce to be accepted). Also assume that the nonce has to be appended at the end of the given string.

Code with output –

import hashlib

import time

user\_input = input("Enter the string =")

nonce = 0

start = time.time()

while True:

h = hashlib.new('sha256')

with\_nonce = user\_input + str(nonce)

h.update(with\_nonce.encode())

hashed\_result = h.hexdigest()

if hashed\_result[:3] == "000":

break

else:

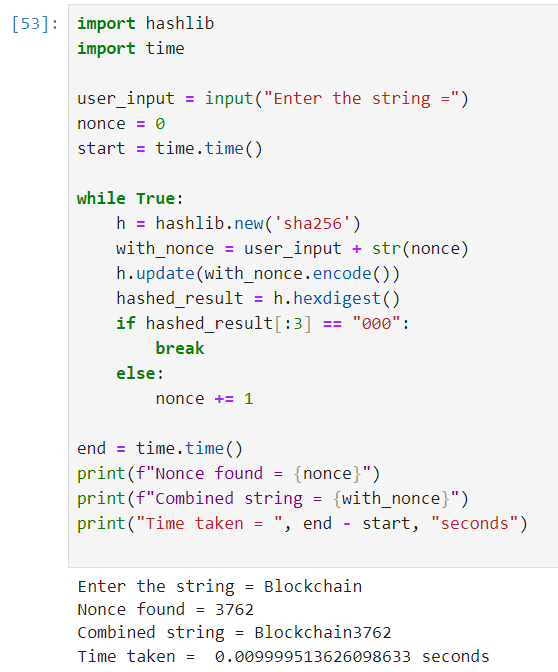
nonce += 1

end = time.time()

print(f"Nonce found = {nonce}")

print(f"Combined string = {with\_nonce}")

print("Time taken = ", end - start, "seconds")



1. Find out what is UTXO. Explain it in few words.

Ans. The Unspent Transaction Output (UTXO) model is a key concept in blockchain technology, used by cryptocurrencies like Bitcoin to manage transactions. A UTXO represents a piece of cryptocurrency that has been recieved but not yet spent, & it becomes the input for new transactions. This system ensures transperancy and prevents double-spending, as each UTXO can only be used once. When a transaction is made, the UTXO is consumed, and new outputs are created for the recipient and any change returned to the sender.

Unlike account based models, the UTXO model tracks unspent outputs instead of account balances, offering greater scurity and immutability. However, it can be more complex for users to understand and requires more storage as the blockchain grows. Cryptos like Cardano extend this model with eUTXO, adding support for smart contracts. Despite its challenges, the UTXO model is crucial for ensuring the relibility and traceability of blockchain networks. Its role in preventing fraud and maintaining ledger accuracy makes it a cornerstone of decentralized finance.

1. Why is a blockchain said to be immutable?

Ans. There are 3 main reasons for blockchain to be immutable. Consensus mech (PoW, PoS etc) , cryptography (hashing with sha256 , sha512 etc) and decentralization (No authority controlling the processes). Once a blockchain records data, it cannot alter or delete it wo leaving a permanent and transparent record of the change. This provides high transparency and accountability hence making it a powerful tool for auditing and regulatory compliance. To change or tamper any data in the blockchain one has to do a 51% attack which take a huge amount of power which is not feasible. This is because if any one block is changed one has to change all subquent blocks to mimic it to other copies of blocks that other people have which is nearly impossible.

1. When a fraudulent block is added to a blockchain with PoW consensus mechanism by a criminal who does not have the ability to perform 51% attack, how is the fork resolved?

Ans. In a blockchain with PoW if someone tries to add a fake block but doesn’t have enough power (less than 51% of the network), the system automatically fixes it. When the fake block is shared, other computers (nodes) in the network check it. If the block has mistakes or fake data, most honest nodes reject it. However, if some nodes accept it, a fork happens—two versions of the blockchain are created: one with the fake block and one without it.Honest miners continue to work on the valid chain, ignoring the one with the fake block. Since the attacker doesn’t have enough power to keep their chain growing faster than the valid one, the real chain quickly becomes the longest.

In poW, the network always trusts the longest chain because it has the most work done. The fake chain is abandoned, and any valid transactions from it go back into the system to be processed later. This system ensures that fake blocks can’t last long, keeping the blockchain safe and secure. Attackers need more than 51% of the network’s power to succeed, which is very hard to achieve.

1. What is ‘Nothing-at-stake’ problem in PoS? How is this avoided?

Ans. In the event of a fork, whether the fork is accidental or malicious attempt to rewrite history and reverse a transaction, the optimal strategy for any miner would be to mine on every chain, so that the miner gets their reward no matter which fork wins. Thus, assuming a large number of economically interested miners, an attacker may be able to send a transaction in exchange for some digital good (usually another cryptocurrency) and receive the good and then start a fork of the blockchain from one block behind the transaction and send the money to themselves instead, and even with 1% of the total stake the attacker's fork would win because everyone else is mining on both.

The "nothing at stake" problem in blockchain systems can be avoided by introducing punishments for validators who misbehave:

Punishing validators - validators can be punished for validating on both chains at the same  
 time, or for validating on the wrong chain.   
 Punishing block creators - Block creators can be punished if it can be proven that they are  
 creating blocks on another network.   
 Using a slashing mechanism - in blockchains with sequential block production, a punishment  
 mechanism called slashing can be used to protect against the nothing-at-stake problem.   
 Using a protocol that combines BFT and Nakamoto consensus - A protocol that combines  
 BFT and Nakamoto consensus can be used to defend against the nothing-at-stake  
 problem. This protocol can decouple a BFT-like block production system from a Nakamoto  
 like finalization system

1. Explain why 51% attack is less probable with PoS than with PoW.

Ans. 51% attack means when someone gains most of the control of the networks concensus power. With this one can manipulate BC, double spend coins or prevent new transactions from being confirmed. Likelihood of a 51% attacks depends mainly on the consensus mech used that is PoS or PoW. It is generally considered PoS is less probable to attack wrt PoW for the following reasons –

1. Resourse requirements – PoW requires one to have control over 50% of the total mining power which is very expensive due to high cost of hardware and electricity and infrastructure. poS requires controlling over 50% of the staked coins, whose whole aamount is usually far lesser than the cost required in PoW. The financial investment required to control such a large portion of the stake is often far greater than the energy and hardware costs in PoW.
2. Security of stakes in PoS vs. mining in PoW - In PoS, validators are paid as a job to act honestly because if they are found to act maliciously, they risk losing their staked assets (the "slashing" mechanism - Slashing typically occurs when a validator is found to be double-signing or being inactive during their assigned duties, causing potential harm to the network's integrity. The amount slashed can vary based on the severity of the offense and the specific rules set by the blockchain protocol.). This provides a strong deterrent against trying to gain control over 50% of the network. In PoW, miners who control more than 50% of the computational power can attack the network without directly risking their mining resources in the same way. While they may lose some rewards due to disrupted mining, they aren't immediately punished in terms of lost capital as in PoS systems.
3. Costs of Attack and Motivation - In PoW, while the cost of performing a 51% attack can be high in terms of hardware and electricity, it is a more straightforward process. The attacker simply needs to gather enough computational power, and there is no direct economic penalty to their actions other than the loss of potential future rewards. In PoS, a 51% attack is much harder to pull off, and the attacker faces significant risks. If they manage to control 50% of the staked assets and engage in malicious behavior (e.g., double-spending), they risk losing their entire stake through slashing. This makes the economic cost of the attack much higher compared to PoW.
4. What are digital signatures in the context of blockchains?

Ans. A digital signature is a mathematical scheme that is used to verify the integrity and authenticity of digital messages and documents. It may be considered as a digital version of the handwritten signature or stamped seal. The digital signatures use asymmetric cryptography i.e. also known as public key cryptography which uses public (can be shared with anyone ) and private keys (kept to be secret) to encrypt and decrypt data. This code acts as proof that the message hasn’t been tampered with along its way from sender to receiver. A digital signature is intended to solve the problem of tampering and impersonation and tampering thus it gives a recipient reason to believe - the message is sent by the claimed sender i.e. Authentication, the sender cannot deny having sent the message i.e. Non-repudiation, the message was not altered in the transit i.e. Integrity. A document is signed to show that is approved by the user or created by the user. The signature is proof to the recipient that this document is coming from the correct source. The signature on the document simply means the document is authentic. To verify digital signatures the recipient applies a verification technique to a combination of the message and the signature to verify authenticity. So here a copy of the signature is not stored anywhere. There is One to One relationship between message and signature. Every message has its own signature.

1. What is the Oracle Problem? How is it solved?

Ans. The oracle problem highlights a key challenge in blockchain technology: ensuring trusted oracles , external data providers feeding real-world information into smart contracts—deliver accurate and reliable data. If oracles are hacked or manipulated, it can disrupt smart contracts, causing errors and vulnerabilities. This issue is a major hurdle for blockchain adoption, where accurate data is critical.

Chainlink addresses this through decentralized oracle networks (DONs), which use advanced security measures to prevent data manipulation or failure. Being open-source, Chainlink’s code is accessible for the blockchain community to review and improve, ensuring reliability and security.

To enhance functionality, Chainlink uses external adaptors, allowing oracles to securely connect to external systems and APIs, even password-protected ones. This enables smart contracts to access data from diverse sources, expanding their usability. It’s decentralized setup prevents a single point of failure, ensuring data availability and resilience.

A key feature is data siging, where each oracle node cryptographically signs the data it provides. This allows users to trace data back to its source and evaluate oracle performance, fostering transparency. Service agreements between smart contracts and oracle providers include terms, penalties, and rewards, incentivizing accurate and timely data delivery.

Reputation systems track oracle performance, helping users choose reliable providers based on success history. Nodes can also undergo certifcation services, ensuring they meet high security and trust standards, such as KYC compliance or location requirements.

It further supports advanced cryptography and hardware, enabling features like zero-knowledge proofs and trusted execution environments. These enhance privacy, security, and allow for off-chain computations, making Chainlink a robust solution to the oracle problem.

Bottom of Form

1. What are Zero-knowledge proofs? How are they used in the context of blockchains?

Ans. A Zero-Knowledge Proof (ZKP) is a cryptographic technique that allows one party to prove to another that they know a fact without revealing the actual information. It ensures the verifier only learns the truth of the statement, not the underlying data. There are two types: interactive, requiring multiple rounds of communication, and non-interactive (NIZKPs), which provide a single proof that can be verified without interaction. In blockchain, ZKPs solve key issues like privacy, scalability, and security. They enable private transactions, such as those on Zcash, where transaction details remain hidden but the transaction's validity is still verifiable. zk-Rollups, a Layer 2 solution, use ZKPs to batch transactions off-chain, improving scalability by reducing data storage on the main chain. ZKPs also allow for secure identity verification, where users prove their credentials without revealing sensitive data, and can be used for proof of solvency, allowing exchanges to prove they hold enough assets to cover customer deposits.

The main benefits of ZKPs in blockchain are privacy, efficiency, and security, but challenges like computational complexity and the need for a trusted setup in some cases exist.