Blockchain Assignment - 1

1) Which features distinguish databases from blockchain ledgers? Provide a comparative analysis of the two.

Ans Database:

Generally a database is a data structure which is used for storing information. It is an organised collection or storage of data which is able to store new data or access existing data. The data stored in a database can be organised using a database management system. The database administrator can modify the data stored in the database. A database is implemented using the client-server network architecture.

Database uses centralised storage of data.

Database needs a Database admin or Database administrator to manage the stored data.

Modifying data requires permission from database admin.

Centralised databases keep information that is up-to-date at a particular moment

Centralised databases are used as databases for a really long time and have a good performance record, but are slow for certain functionalities.

Blockchain:

A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Here, modification of data is not permissible by design. It allows decentralised control and eliminates the risks of modification of data by other parties with sufficient access to the system.

Blockchain uses decentralised storage of data.

There is no administrator in Blockchain.

Modifying data does not require permission. users have a copy of data and modifying the copies does not affect the master copy of the data as Blockchain is irresistible to modification of data.

Blockchain keeps the present information as well as the past information that has been stored before.

Blockchain is ideal for transaction platforms but it slows down when used as databases, especially with large collections of data.

2) Why is Blockchain a trusted approach?

Ans A Blockchain is, at its heart, a distributed ledger, that adds a new block of transactions every time miners/validators agree upon a given order of trades. The currency that powers the blockchain is called its native cryptocurrency.

Since Blockchain is decentralised at its core, there is no central authority that governs or controls the flow of currency or its value. The users are solely responsible for verifying transactions, and sustaining its steady circulation. This is done by reaching a consensus via various mechanisms including Proof of work, Proof of stake among others.

The data held by a Blockchain network is distributed as well, and not stored in a centralised server. Hence, Blockchain does not have a single point of failure, and the data is always secure, irrespective of one or more nodes being down.

Blockchain is an open-source technology, and hence it isn't held back with compatibility issues either. While it can efficiently be integrated with other applications, many decentralised applications are built on top of Blockchains as well.

However, the most important aspect of Blockchain is that it is arguably the most secure financial infrastructure that we have had thus far. It offers complete transparency and immaculate precision of transactions, since most trades on the platform are governed by trustless smart contracts, making it free from any human errors. These smart contracts are fed real-time data via Oracles, based on which they are executed without human interference.

3) Suggest which type of blockchain should be used for the security of donations in a charity organization. what benefits does the blockchain technology introduce in such a scenario? Explain your answer using an example.

Ans The type of blockchain that should be used for the security of donations in a charity organisation is Private Blockchains. It's because they typically use a "Proof-of-Authority" (PoA) consensus approach and are often used in internal, business secure environments to handle tasks such as access, authentication, and record keeping

The benefits that blockchain technology introduces in such a scenario are:

1. Automate administration: Smart contracts can automate common admin tasks, reducing strain on existing administrative staff and structures

2. Share data securely: Reduce data duplication and inaccuracies between organisations: use the same distributed ledger, secure and updated in real time

3. Trace individual donations: Blockchain creates a fully auditable chain of giving. Show donors exactly which person their money helped

4. Enable transnational donations: Show clearly where each individual donation came from and demonstrate tax and regulatory compliance

5. Establish verifiable identity: Blockchain can be a secure repository of verified identity, allowing those without documents to prove who they are

6. Accurately target aid: Ensure aid goes to the exact individuals who need it, checking their identities against the blockchain

7. Rapidly deliver emergency aid: Cooperate across agencies, geography and political borders to deliver emergency aid cohesively and rapidly

8. Donor anonymity: Anonymity correlates with larger donations; digital wallets can allow totally anonymous donations, eliminating 'donation shaming'

9. Goal-based fundraising: Imitate the success of GoFundMe and Kickstarter goal-oriented crowdfunding, attracting donations for specific goals

4) critically present and compare how smart contracts can be used in a lottery scenario.

Ans challenges faced by the Lottery Industry

1. Fairness: It is essential to ensure the integrity of the games to avoid the risks of manipulation or frauds. Lottery players doubt the fairness of lotteries and ask the following questions:

- Are the deal and ticket real or not?
- Is the random number generation (RNG) method secure and random?
- Are the prizes paid on time? Is the jackpot winner real?
- Is the money accumulated in one pool and used for social causes?

Since the traditional lotteries fail to answer the above questions, lotteries lack fairness in the system. Therefore, it is essential to bring fairness to the lottery systems.

2. Availability: Due to the smaller size of the domestic market, users from different countries cannot get involved in the biggest lotteries in the world. They are restricted from participating in smaller local lotteries. Also, the lottery participants have no control over how much money should be collected from ticket sales, and lottery winnings are taxed in some countries. 3. Distribution of funds: Lotteries serve as funding for charity and other social projects. But in many cases where countries have high levels of corruption, players can question the fair distribution

of funds. Since there is no way to get information about the distribution of funds, it could be the biggest challenge for the players to build trust in the specific lottery association. Because the blockchain is a distributed ledger technology with a secure write-forward authentication system, it can add data without the risk of a single point of failure. Every node involved in the blockchain network has a copy of the ledger. users can update the information into the ledger without the involvement of a third party. It gives individuals more power and flexibility. Therefore, the blockchain can be well implemented in the lottery or gambling industry.

How smart contracts can be used in a lottery scenario?
Step 1: Players sign up to the lottery platform Lottery players need to sign up to the platform to participate in the lottery and become its member. They sign up to the blockchain lottery system with the following information • Name • wallet Address • Email Id • Phone Number After the successful sign-up, players can get alerts and notifications related to ticket openings on a regular basis.
Step 2: Admin announces the ticket openings and deploys the smart contracts Admin announces the ticket openings on the platform and the notification is sent to the users. They also deploy smart contracts, which contain predefined rules for the lottery game to bring fairness and transparency to the ecosystem. Smart contracts ensure what

information should be shared with which stakeholder in the system, providing privacy and disclosure of data. Since the players can buy the tickets with cryptocurrencies, their identities remain anonymous. The transactions stored on a public blockchain allows traceability and makes it easier to resolve disputes/scandals related to lotteries.
Step3 : A Random number is generated and recorded on the blockchain since the random number generator is based on the blockchain, the algorithm relies on recent random blockchain transactions. It pulls a specified amount and order of numbers to generate each winning number sequence. Because nobody is aware of the next transaction in the blockchain, the lottery platform adds an extra layer of randomness to the selection process. Once the random number is generated and matched to the player's ticket number, they are awarded and money is automatically sent to their respective wallets. The funds to be distributed to players are defined in the smart contracts. Therefore, the decided commissions and funds are paid out to every player on the platform. Moreover, the smart contract code is available publically on the platform; players can check the rules defined in the contracts to confirm if the funds are distributed in a fair way or not. Step 4: Players can trace back the history of records of transactions since the transactions are recorded on the blockchain, players can trace back the history to know who had won the jackpot and if the commissions and wins are paid out as defined in the smart contracts.

5) use an online service to illustrate how consensus is built in a distributed system with no central authority

Ans In any centralised system, like a database holding key information about driving licences in a country, a central administrator has the authority to maintain and update the database. The task of making any updates–like adding/deleting/updating names of people who qualified for certain licences–is performed by a central authority who remains the sole in-charge of maintaining genuine records. Public blockchains that operate as decentralised, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the blockchain, and on the block mining activities. In such a dynamically changing status of the blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all-important task is performed by the consensus mechanism, which is a set of rules that decides on the legitimacy of contributions made by the various participants (i.e., nodes or transactors) of the blockchain. There are different

kinds of consensus mechanism algorithms, each of which works on different principles: The proof of work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanism of bitcoin needs high energy consumption and a longer processing time. The proof of stake (PoS) is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it. However, this comes with the drawback that it incentivizes cryptocoin hoarding instead of spending. While PoW and PoS are by far the most prevalent in the blockchain space, there are other consensus algorithms like Proof of Capacity (PoC) which allow sharing of memory space of the contributing nodes on the blockchain network. The more memory or hard disk space a node has, the more rights it is granted for maintaining the public ledger. Proof of Activity (PoA), used on the Decred blockchain, is a hybrid that makes use of aspects of both PoW and PoS. Proof of Burn (PoB) is another that requires transactors to send small amounts of cryptocurrency to inaccessible wallet addresses, in effect

"burning" them out of existence. Another, called Proof of History (PoH), developed by the Solana Project and similar to Proof of Elapsed Time (PoET), encodes the passage of time itself cryptographically to achieve consensus without expending many resources.