Question.1)

Which features distinguish databases from Blockchain ledgers? Provide a comparative analysis of the two.

Answer)

Database	Blockchain
The database uses centralized storage of data.	Blockchain uses decentralized storage of data.
The database needs a Database admin or Database administrator to manage the stored data.	There is no administrator in Blockchain.
Modifying data requires permission from the database admin.	Modifying data does not require permission. Users have a copy of data; modifying the copies does not affect the master copy of the data as Blockchain is irresistible to modification of data.
Centralized databases keep information that is up-to-date at a particular moment	Blockchain keeps the present information as well as the past information that has been stored before.
Centralized databases are used as databases for a really long time and have a good performance record, but are slow for certain functionalities.	Blockchain is ideal for transaction platforms but slows down when used as database, especially with large data collections.

SN	Blockchain	Database
1	Blockchain is decentralized because there is no admin or in-charge.	The database is centralized because it has admins in charge.
2	Blockchain is permissionless because anyone can access it.	The database required permission because it can be accessed only by entities who have the right to access it.
3	Blockchains are slow.	Databases are fast.
4	It has a history of records and ownership of digital records.	It has no history of records and ownership of records.
5	Blockchain is fully confidential.	The database is not fully confidential.
6	Blockchain has only an Insert operation.	The database has Create, Read, Update, and Delete operations.
7	It is a fully robust technology.	It is not entirely robust technology.
8	Disintermediation is allowed with blockchain.	Disintermediation is not allowed with the database.
9	Anyone with the right proof of work can write on the blockchain.	Only entities entitled to read or write can do so.
10	Blockchain is not recursive. Here, we cannot go back to repeat a task on any record.	The database is recursive. Here, we can go back to repeat a task on a particular record.

s

Question.2)

Analyze, using a diagram, how a distributed ledger works, present its main characteristics, and explain how it differs from a “traditional” centralized ledger.

Answer)

Centralized ledgers

The double-entry accounting system we've discussed highlights an accounting system with a centralized ledger. Anything with a financial value is recorded in journals and posted to ledgers. These ledgers are just like the central repository of posted transactions, and they are the backbone of any organization.

However, centralized ledger systems have various drawbacks as well. For example, banks control the transactions that are posted into the bank's ledgers and they maintain total control over bank statements. In this case, they can penalize you at any given time and can transact money from your account at any given time. If such a centralized institute has malicious intent, then the consequences could be manifold; they could close down their business without prior notification, which prohibits any further transactions. These examples are used mostly by blockchain evangelists who lean more toward complete decentralization of trust authorities.

Let's look at a more viable challenge, pertaining to banks. Double-entry mandates the need for each bank to maintain its own ledger to reflect its perspective of truth, and as more banks are transacting with each other, they need to reconcile their version of the truth to derive a single version of the truth. Banks today spend time, money, and resources to ensure a consensus over a single truth.

Obviously, they have their ledger and hence their own system, which allows the financial industry to avoid any chance of a single point of control and a single point of failure. In addition, it becomes more interesting as a customer opens an account with a bank and puts his/her money with a level of trust in that banking institute. Now, the onus is on the banking institution to safeguard your money and information. On the other hand, the bank will invest a lot of time, money, resources, and effort into building and maintaining a system and then spend even more time, money, resources, and effort on integrating and checking with other banking institutes to ensure that their mastered system is in consensus with the other banking institutes' system to reach a common truth.

If you analyze this closely, you will see that each bank's ledger is actually replicating the functionality of the other banking institutions. Now, what if one of the banking institute's systems fails? Is this going to lead to a situation where reconciliation is not possible? Doesn't this sound more like a single point of failure? The answers lie in the distributed ledger discussed in the following section and throughout the book.

Distributed ledgers

Across the world, in the economical, legal, political, and institutional systems, the key elements are transactions, contracts, and documents. They dictate the relationship between countries, enterprises, organizations, communities, and individuals, and, most importantly, they are perceived to offer trust. Interestingly, these have not joined the digital transformation to a greater extent and for a greater cause. So, what is the solution? Distributed ledgers and DLT, along with blockchain, offer the solution to such critical challenges. In this section, we will explore more about distributed ledgers and DLTs.

In a distributed ledger, there is no central authority or a central administrator. It is an asset database that is shared over the network, where each party on the network has an identical copy of the ledger. These assets can be financial, legal, and electronic assets. Changes to the value of these assets are reflected throughout the network, and each copy of the ledger is appended.

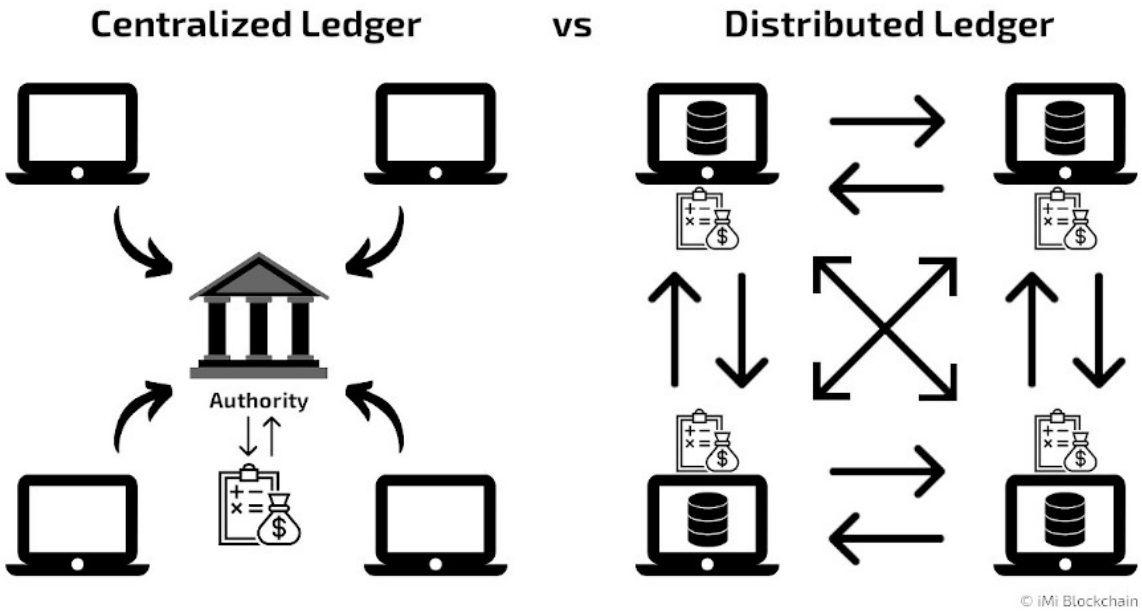
Many organizations, governments, and institutes use a central database of the ledger, which we discussed in the Centralized ledgers section. A centralized ledger needs a central authority to be trusted by transacting parties; however, in a distributed ledger, the need for a third party is omitted, which is one of the gravitational forces behind the attraction to DLT. Here, I have quietly used the term DLT because a distributed ledger can be pronounced as a shared ledger or a DLT, and they are one and the same.

What's disruptive about a DLT is that the ledger database is distributed, spread on all of the nodes or computing devices across the network, and each node has an identical copy of the ledger, where nodes update themselves independently. All of the participating nodes reach an agreement to establish a single truth (true copy) for the ledger through a process called consensus. Once a consensus is reached, the distributed ledger is updated automatically and the latest truth (true agreed copy) of the ledger is appended on each node separately. While reading this paragraph, you might think about the reconciliation process of banks to establish trust and an agreement on the ledger. With DLT, trust (reconciliation) and consensus (agreement) happen seamlessly and automatically.

We just found out that there is no central authority in the previous story to maintain the distributed ledger. DLT empowers systems to reduce the dependencies on various central authorities such as banks, lawyers, governments, regulatory offices, and third-party authorities. Distributed ledgers omit the need for a central authority to validate, authenticate, and process transactions. Transitions on DLT are timestamped and have a cryptographic unique identity, where all records in question are available for the participants to view, and this ensures that the verifiable and auditable history of the transaction is

stored immutably.

In the decentralized distributed ledger, the transaction is replicated to the distributed ledger, which means all the participating nodes' copies of the ledger are appended; however, there is no central single database. It is the network that is decentralized. Such a system needs a decentralized consensus as there is no single point of contract, authority, or party. Hence, to ensure trustlessness, the consensus is a must. In a traditional database system, a single party acts on behalf of the transacting clients to modify the state of the system. However, in a distributed ledger, any party can record, and the protocols and algorithms govern the posting of transactions on the network's ledger.



Question.3)

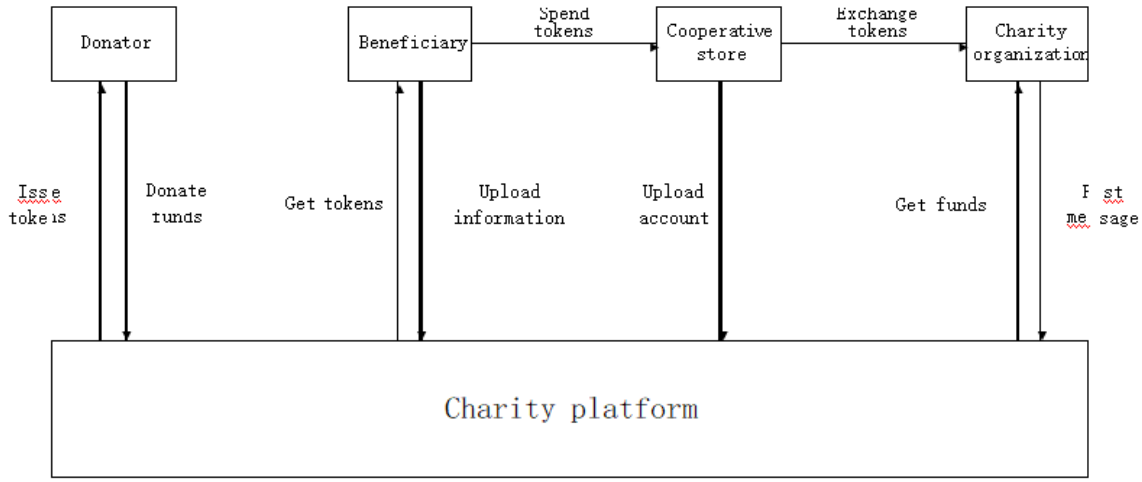
Suggest which type of blockchain should be used for the security of donations in a charity organization. What benefits does the blockchain technology introduce in such a scenario? Explain your answer using an example

Answer)

Charity System Mode

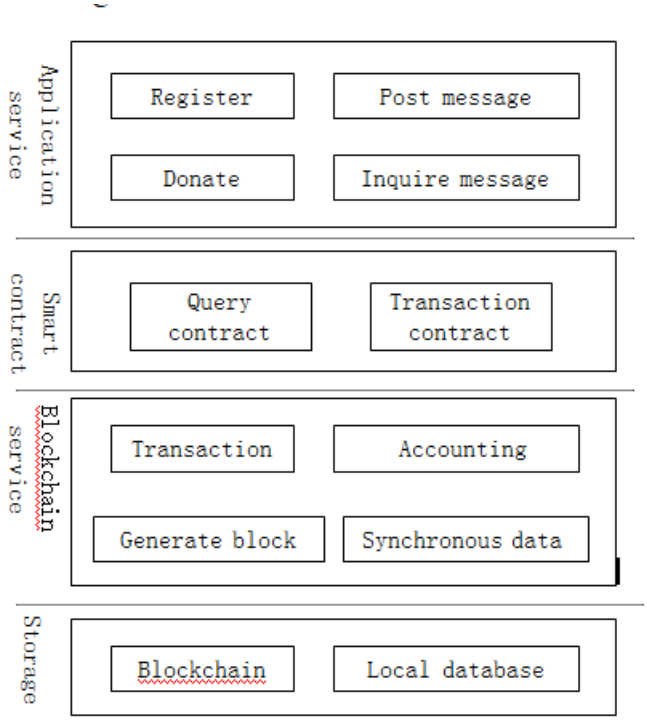
The charity system mode proposed is shown in Figure. There are four roles: donors, beneficiaries, charity organizations, and cooperative stores. The charity organizations get the information or seek help and create charity projects through the platform. Donors learn about charity projects on the platform, then donate to beneficiaries or charity organizations. Beneficiaries upload their information to the platform for help, and they can get and spend tokens in cooperative stores. The transactions that occurred in the stores will be uploaded to the charity platform. The cooperative stores

supply services or goods to the beneficiaries to obtain tokens. The tokens can be exchanged for real money by charity organizations. The flow of funds has been fully recorded on the blockchain, which allows transactions to be tracked and funds prevented from being abused.



Proposed Platform Architecture

We divide the platform into four layers, as shown in Figure 3. The application service layer encapsulates a variety of applications, including account registration, post charity information, donating funds, and inquiry messages, providing users with the functions of the platform directly. The smart contract layer includes various scripts and smart contracts. It encapsulates query methods, transactions process, and other details. The blockchain service layer implements the functions of distributed accounting of the charity platform, including package block, getting consensus on the transaction, broadcast block, and synchronizing data to a local database. The storage layer is used to store data, including blockchain storage and local storage.



operation of the charity platform, as follows:

1. Donor

After successful login, the donor browses the charity projects and selects one project to be donated. The system will check the balance of the donor account. If the balance is insufficient, the user will be reminded to deposit. Donations can be completed only if the balance is sufficient.

2.People in need

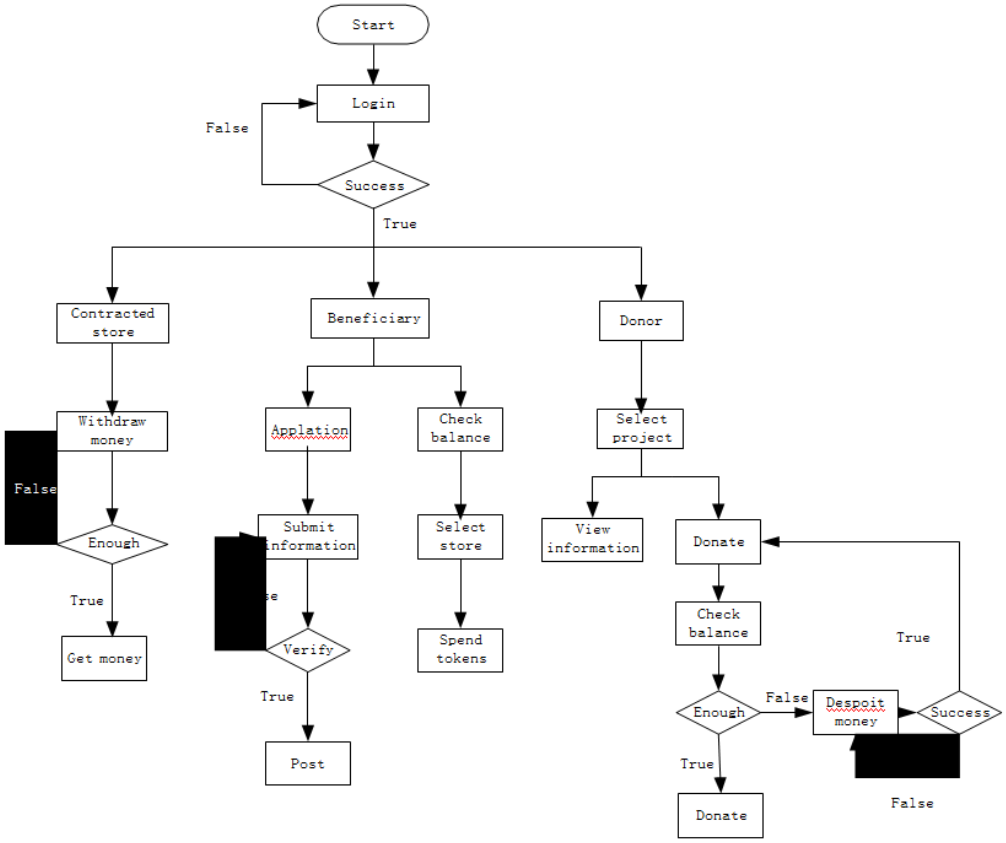
The people who need help should fill in the rescue information which will be uploaded to the charity organization for review, and the approved projects will be posted on the charity platform. The beneficiary can check the account balance to know the project status, and then use the tokens in cooperative shops to obtain services or products.

3.Cooperative shops

The shops provide the corresponding services or goods such as medicines or books to the beneficiaries to obtain tokens. they can exchange tokens for real money from charity organizations.

4.Charity organization

The organization can get a donation from the platform to help other people and apply money to the cooperative shops for token exchange.



Build Smart Contracts

Smart contracts are value streams based on specific terms and conditions. Different from real contracts, smart contracts are completely digital, they are pre-programmed code stored on the blockchain [20]. With the expansion of the blockchain, smart contracts adapt well to the decentralization of the blockchain which can run in the whole network node. The transactions using the smart contract will be recorded on the blockchain without the need for managers. Once conditions are met, the smart contract will be executed automatically. Smart contracts can be used to define transaction logic for charity platforms.

In the Dapp, we have built a smart contract to meet the functions described in the previous section, smart contracts structure is shown in Figure 6. Users can create a charity project using The ProjectList Contract which also supplies the view of all projects recorded on the blockchain. The Project contract is used to describe and store specific charity projects, which provides an interface to operate the charity project and its funds.