**School of Continuing and Distance Education**

**JNTU Hyderabad**

**Blockchain Technology**

**( Submitted by N Ravinder Reddy)**

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

* Immutable. Immutability means that the blockchain is a permanent and unalterable network. ...
* Distributed. All network participants have a copy of the ledger for complete transparency.
* Decentralized.
* Secure.
* Consensus.
* Unanimous.

Blockchain is a distributed database of records or public ledger of transactions that have been carried out on the network.

To paint a picture, let’s say that four business partners, Alice, Bob, Tom, and Hardy, are starting a chain of stores. Each of them owns one store and they have four stores in total. The partners decide to store the profits and sales made from each store in a database (e.g., MySQL).

The database is vulnerable to any of a number of potential snafus, included but not limited to the following.

* The database could be compromised by a malicious actor
* Due to its centralized nature, a crash or failure of the database would affect all records
* A malicious or unwitting actor could alter records in the database
* An authorized party could enter records into the database without validating its authenticity
* One partner might accidentally alter or delete data entered by another partner

Considering the myriad security risks, Alice, Bob, Tom, and Hardy wisely opt to use blockchain technology in their database.

Now each partner has a copy of the records or the database. If a record is entered into one database, it is broadcast to all the others, which must vet the record before it is entered into the user’s record. Once it is vetted by all the participants, then the record is entered into the user’s database and the new copy is sent to all of them in the node.

Using blockchain has made the team’s work:

1. Transparent
2. Secure
3. Immutable
4. Decentralized



**Database uses centralized storage of data**. Blockchain uses decentralized storage of data. Database needs a Database admin or Database administrator to manage the stored data. There is no administrator in Blockchain

**Database:**
Generally a database is a data structure which is used for storing information. It is a organised collection or storage of data which is able to store a new data or access a existing data. The data stored in a database can be organized 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.

**Blockchain ledgers:**

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 decentralized control and eliminates the risks of modification of data by other parties with sufficient access to the system.

Underlying **distributed ledgers** are the same technology that is used by blockchain, which bitcoin uses as its distributed ledger. A distributed ledger can be described as a ledger of any transactions or contracts maintained in a decentralized form across different locations and people.

There are **four main types** of blockchain networks: public blockchains, private blockchains, consortium blockchains and hybrid blockchains. Each one of these platforms has its benefits, drawbacks and ideal uses.

Key differences between Blockchain and a Database are:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| Database | Blockchain |
|  |  |
| Database uses centralized storage of data. | Blockchain uses decentralized storage of data. |
| Database needs a Database admin or Database administrator to manage the stored data. | There is no administrator in Blockchain. |
| Modifying data requires permission from database admin. | Modifying data does not require permission. Users have a copy of data and by 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 ertain functionalities. | Blockchain is ideal for transaction platform but it slows down when used as databases, specially with large collection of data. |

 |

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

Unlike traditional databases, distributed ledgers have no central data store or administration functionality. In a distributed ledger, each node processes and verifies every item, thereby generating a record of each item and creating a consensus on its veracity.

Distributed ledgers use independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). Blockchain organizes data into blocks, which are chained together in an append-only mode.

Main Characterics

1. Transparent
2. Secure
3. Immutable
4. Decentralized





**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.**

of blockchain should be used for the security of donations in a charity organization.

Charity is a critical part of a democratic society. It is known that there are many incidents take place in this world which causes tragic loss whether it can be related to wealth or life and cause extensive damage every year. To recover from various types of losses many require help from organizations who providing services which can be financial aid to basic necessities. People are now becoming gluttonous to contribute to the society. So, Charity is a highly growing sector in today’s world and it has evolved from its traditional organizational concepts to a decentralized crypto-currency based system.

The traditional system suffers from various problems such as lack of transparency, lack of trust between donors and corruption. Blockchain is a remarkably transparent and decentralized way of maintaining this kind of different charity-based transactions. So, we are going to propose a blockchain based decentralized system that acts as a platform to donate money for donors to beneficiaries and this entire system taking place under maximum security and fulfilled trust. Fake charities try to take advantage of our generosity and compassion for others in need. Scammers will steal your money by acting as a genuine charity. These scams not only cost you money but they also divert much needed donations away from legitimate charities and causes. Following statistics will state the broader view about this crisis related to frauds in charity.

The blockchain system can bring transparency to online charity trusts. Contributors can see the journey of the donation in real time and confirm if it’s reaching the deserving hands or not. With the addition of blockchain into charities, donors would no longer be unaware of what’s being done with their money. donation information would be stored in blocks. Each data block contains the hash code of a previous block and their own hash. This hash is generating for each new transaction. Hash is nothing but the string of numbers and letters. And suppose if we make a small change in the transaction, a new hash is generated immediately. So that we can immediately understand that something went wrong or someone tries to malpractice. Like this blockchain technology works.

1) Donor: In this module, user can register in our system as a donor using credentials and unique wallet address. Only after admin verifies the donor account, he can view the campaigns and their details. And after selecting project for donation, he/she proceed for donation. For the donation purpose donor will request for our custom build token i.e., MOSS. The value for each MOSS is pre-defined in the code of smart contract. That value will never change. Suppose that 1MOSS = 2 Rupees, then if donor want 1000 MOSS, he has to pay 2000 Indian Rupees. When donor will upload his/ her transaction’s screen-shot then only system will cross verify the transaction request made by the donor for the tokens. If this gets successful then admin will issue the respected no of tokens to the donor’s wallet address. After that the system will check the balance of donor’s account. Donation can be complete if balance is sufficient.

2) Beneficiary: In this module, user can register in system as a beneficiary using credentials and unique wallet address. After registration, admin will look for the beneficiary registration request. And do the KYC. Here admin will do the KYC for the cross-verification purpose. Once the KYC is done then only beneficiary can access the system and can-do further things such as creating campaigns etc. beneficiary can create campaigns with their details such as images, goals, required amount, duration. beneficiary can view all transactions related to campaigns. Beneficiary can get report of their own campaigns in which he/she will get information related to donated amount and their information. The key point here is that one beneficiary can only make one campaign at a time. This is done to avoid the confliction of wallet addresses.

3) Admin: This is the most important and essential module of the entire project. Because this is the module in which donor can be verified, beneficiary can be verified, campaigns can be approved, tokens can be issued. Admin can also do the KYC for the donor as well as beneficiary. The most important thing of entire project is our MOSS tokens. Admin can issue these tokens to the donor.

4) MetaMask: Metamask is a wallet that exists solely on your computer and gives you full control of your funds. Metamask is a crypto wallet- it allows you to store and transact Ethereum or any other Ethereum-based (ERC- 20) tokens. You do not register it on a website, but rather install it as an extension to your Chrome or Firefox browser. Since September 2020, it has also been available to install on a mobile app for Android and iPhone. Metamask stores your private key locally on your computer, within the browser data in particular. This is a huge step up in security terms but it is still conceivable that somebody might hack your PC and get the key. Perhaps the only safer options would be hardware wallets like Ledger or paper stored wallets, which are less convenient for frequent use. Indeed, it is possible to connect Metamask to hardware wallets like Trezor and Ledger. This is an ultimat combo – 100% security combined with Metamask’s functionality. In short Metamask is a smarter wallet choice. Here in our project, we have used MetaMask for the same purpose that is for making transactions. Donor as well as beneficiary will make wallet on MetaMask and will give its wallet address to the system. Then the respected system will fetch all the details with respect to that wallet address and do further transactions.

5) Blockchain Node/ Smart Contract: Blockchain nodes are network stakeholders and their devices that are authorized to keep track of the distributed ledger and serve as communication hubs for various network tasks. A blockchain node’s primary job is to confirm the legality of each subsequent batch of network transactions, known as blocks. In addition, allocating a unique identifier to each node in the network helps to distinguish a node from other nodes in the network easily. We have developed our own blockchain network by using the concept called as smart contracts. Smart contracts are smart because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises specified in digital form, including protocolswithin which the parties perform on these promises. These contracts are written in on programming language that is Solidity. We have used the same programming language in our project. Codes or more specifically we can say functions which we are going to use in our smart contracts are already predefined in the solidity, we just have to modify them according to our need. In our smart contract we have taken the parameters such as sender’s address, receiver’s address, amount etc. according to these parameters our transaction happens. Also, the tokens that we have made which is MOSS. That is also made in smart contract



System Architecture

1) With the addition of blockchain into charities, donors would no longer be unaware of what’s being done with their money. Donation information would be stored in blocks along with donor information.

2) Since blockchain is a public ledger that is viewable by anyone, charity fraud would be very difficult to commit; donors are able to carefully monitor their funds and ensure that no data is tampered with.

3) Blockchain technology can help charities manage their funds more closely and serve as a marketing strategy, removing the need for these middlemen.

4) Smart contracts are applications that run on blockchain technology that have rules and conditions programmed into them and initiate certain events when these conditions are met. In the case of philanthropy, these contracts can represent agreements between the giver and the charitable organization. This brings a lot of opportunities for all the parties involved in the donation process and can make it fully automated and uncompromising.

5) charities can accept payments securely, transparently, and globally without the need to pay currency exchange fees