Assignment 5

Title:

Write a survey report on types of Blockchains and its real time use cases.

Aim:

Write a survey report on types of Blockchains and its real time use cases.

Theory:

A **blockchain** is a type of distributed ledger technology (DLT) that consists of growing list of records, called *blocks*, that are securely linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a *chain* (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

A blockchain was created by a person (or group of people) using the name (or pseudonym) Satoshi Nakamoto in 2008to serve as the public distributed ledger for bitcoin cryptocurrency transactions, based on previous work by Stuart

Haber, W. Scott Stornetta, and Dave Bayer.The identity of Satoshi Nakamoto remains unknown to date. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain may be considered a type of payment rail.

Private blockchains have been proposed for business use. *Computerworld* called the marketing of such privatized blockchains without a proper security model "snake oil"; however, others have argued that permissioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

Blockchain can be defined as an immutable distributed digital ledger, which is secured using advanced cryptography, replicated among the peer nodes in the peer-to-peer network, and uses consensus mechanism to agree upon the transaction log, whereas control is decentralized. With this definition, paper identifies following concepts as the core concepts to unwrap the meaning of blockchain—immutable, distributed, digital ledger, cryptography, peer-to-peer network, consensus mechanism, decentralization. In accounting, a ledger is a place to record and store all the transactions with regard to an entity.Blockchain transaction ledger is pretty unique to other ledgers in a manner, which ensures that transaction log is computationally impractical to change, as long as honest nodes in the network control the majority of CPU power, thus making it immutable.

The origins of ledger can be traced back to over 5000 years ago in Mesopotamia. The Earliest and simplest form of recording transactions is called single entry accounting, which enters transactions into a list to keep track of adding or deducting assets. The single entry accounting was managed by owners or family members, as this kind of recordings are error-prone as well as difficult to track down, when recorded fraudulently. Double entry accounting added a clear strategy to identify and remove errors, where there are two entries recorded against each transaction, so that the ledger is balanced all the time. Grigg proposed triple entry accounting in 2005, an alternative to traditional double entry accounting, which secures transactions using cryptography in order to make it difficult to change. Blockchain implements triple entry accounting concept to permanently store transactions in blockchain, ensuring that the sender has authority to execute non-reversible transactions using public-key cryptography.

A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called *blocks* that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double-spending. A blockchain has been described as a *value-exchange protocol*. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Logically, a blockchain can be seen as consisting of several layers:

- infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

Blockchain Types

According to our survey findings, blockchains can be categorized into two main types namely **permissionless blockchains and permissioned blockchains**. **Permissionless Blockchains**

Permissionless blockchains do not enforce any restrictions on its nodes; anyone can openly read data, inspect data, and participate in validation and writing of the data in accordance with the consensus protocol of the particular blockchain. Bitcoin, Ethereum and many other cryptocurrencies run on permissionless blockchains. These blockchains are considered fully decentralized and secured using advanced cryptography, whereas economic incentives are provided for users who work to keep the integrity of the network. Due to the security considerations and strict restrictions, transaction throughput of a permissionless blockchain is comparatively lesser than one of a permissioned blockchain. Permissionless blockchains are fully decentralized and transparent.

- **Permissioned Blockchains:**
- Permissioned blockchains restrict the writing access for a limited set of participants, and a consensus mechanism is used to validate the writing of data among its privileged participants. Read access could either be open to anyone or closed to the public based on the requirement of the permissioned blockchain. This type of blockchains has evolved as an alternative to initial permissionless blockchains, to address the requirement for running blockchain technology among a set of known and identifiable participants that have to be explicitly responsible to the blockchain network, while participants need not be fully trusting each other. The permissioned blockchains are mainly useful for business and social applications, which requires blockchain distributed ledger

technology without the need of a in centifying cryptocurrency. Based on the read access mentioned, permissioned blockchains are further divided as open and closed—open permissioned blockchains are partially decentralized, anyone can read its data, whereas closed permissioned blockchains are fully centralized, data is visible only to the participants. Closed permissioned blockchains can be argued as restricted distributed databases which are facelifted with the blockchain term. The initial idea of introducing blockchain concept was to remove centralization and add transparency to everyone to read and update its data. For example, a supply chain management system for a private organization can be implemented without the concepts of blockchain. In order to support our argument on closed permissioned blockchains, we have presented a characteristic comparison of different blockchain types compared with restricted distributed database system. The comparison shows that all of the characteristics in closed permissioned blockchains are comparatively similar to that of restricted database systems. In addition to this categorization, there is also another blockchain categorization called public, consortium, and private blockchains In simple terms, public blockchains are permissionless blockchains, whereas consortium and private blockchains fall into permissioned blockchains.

There are 4 types of blockchain:

1. Public Blockchain

These blockchains are completely open to following the idea of decentralization. They don’t have any restrictions, anyone having a computer and internet can participate in the network.

- As the name is public this blockchain is open to the public, which means it is not owned by anyone.

- Anyone having internet and a computer with good hardware can participate in this public blockchain.
- All the computer in the network hold the copy of other nodes or block present in the network
- In this public blockchain, we can also perform verification of transactions or records

2. Private Blockchain

These blockchains are not as decentralized as the public blockchain only selected nodes can participate in the process, making it more secure than the others.

- These are not as open as a public blockchain.
- They are open to some authorized users only.
- These blockchains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.

3. Hybrid Blockchain

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

- It is a combination of both public and private blockchain.
- Permission-based and permissionless systems are used.
- User access information via smart contracts
- Even a primary entity owns a hybrid blockchain it cannot alter the transaction

4. Consortium Blockchain

It is a creative approach that solves the needs of the organization. This blockchain validates the transaction and also initiates or receives transactions.

- Also known as Federated Blockchain.
- This is an innovative method to solve the organization’s needs.
- Some part is public and some part is private.
- In this type, more than one organization manages the blockchain.

Applications of Blockchain

1. Asset Management

Blockchain plays a big part in the financial world and it is no different in asset management. In general terms, asset management involves the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments. Normal trading processes in asset management can be very expensive, especially if the trading involves multiple countries and cross border payments. In such situations, Blockchain can be a big help as it removes the needs for any intermediaries such as the broker, custodians, brokers, settlement managers, etc. Instead, the blockchain ledge provides a simple and transparent process that removes the chances of error.

2. Cross-Border Payments

Have you ever tried to make cross-border payments in different currencies from one country to another? This can be a long complicated process and it can take many days for the money to arrive at its destination. Blockchain has helped in simplifying these cross border payments by providing end-to-end remittance services without any intermediaries. There are many remittance companies that offer Blockchain services which can be used to make international remittances within 24 hours.

3. Healthcare

Blockchain can have a big impact on healthcare using smart contracts. These smart contacts mean that a contract is made between 2 parties without needing any intermediary. All the parties involved in the contract know the contract details and the contract is implemented automatically when the contract conditions are met. This can be very useful in healthcare wearing personal health records can be encoded via Blockchain so they are only accessible to primary healthcare providers with a key. They also help in upholding the HIPAA Privacy Rule which ensures that patient information is confidential and not accessible to everyone.

4. Cryptocurrency

Perhaps one of the most popular applications of Blockchain is in Cryptocurrency. Who hasn’t heard about bitcoin and it’s insane popularity. One of the many advantages of cryptocurrency using blockchain as it has no geographical limitations. So crypto coins can be used for transactions all over the world. The only important thing to keep in mind is exchange rates and that people may lose some money in this process. However, this option is much better than regional payment apps such as Paytm in India that are only relevant in a particular country or geographical region and cannot be used to pay money to people in other countries.

5. Birth and Death Certificates

There are many people in the world who don’t have a legitimate birth certificate especially in the poorer countries of the world. According to UNICEF, one-third of all the children under the age of five don’t have a birth certificate. And the problem is similar to death certificates as well. However, Blockchain can help in solving this problem by creating a secure repository of birth and death certificates that are verified and can only be accessed by the authorized people.

6. Online Identity Verification

It is not possible to complete any financial transactions online without online verification and identification. And this is true for all the possible service providers any user might have in the financial and banking industry. However, blockchain can centralize the online identity verification process so that users only need to verify their identity once using blockchain and then they can share this identity with whichever service provider they want. Users also have the option to choose their identity verification methods such as user authentication, facial recognition, etc.

7. Internet of Things

Internet of things is a network of interconnected devices that can interact with others and collect data that can be used for gaining useful insights. Any system of "things" becomes IoT once it is connected. The most common example of IoT is perhaps the Smart Home where all the home appliances such as lights, thermostat, air conditioner, smoke alarm, etc. can be connected together on a single platform. But where does Blockchain come into this? Well, Blockchain is needed for providing security for this massively distributed system. In IoT, the security of the system is only as good as the least secured device which is the weak link. Here Blockchain can ensure that the data obtained by the IoT devices are secure and only visible to trusted parties.

Conclusion:

Blockchain is a relatively new technology that is still not widespread in all industries but it is slowly gaining more momentum. Once Blockchain becomes more widespread, it could become a powerful tool for the democratization of data that will encourage transparency and ethical business tactics