K. K. Wagh Institute of Engineering Education and Research, Nashik.
Department of Computer Engineering Academic
Year 2022-23

Course: Laboratory Practice III	**Course Code: 410246**
Name: Ahire Kalpesh Bapurao	**Class: BE**
Roll No. : 12	**Div: A**

****

Problem Statement:

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

Objective:

Understand and explore the working of Blockchain technology and its applications.

Course Outcome:

CO6: Interpret the basic concepts in Blockchain technology and its applications.

- ## What is Blockchain?

  - A blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority. Potential applications can include fund transfers, settling trades, voting and many other issues.
  - As explained by Wikipedia, “Blockchain was invented by Satoshi Nakamoto”—the pseudonym of an unknown person or persons—“in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin… [which] made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.”
  - A blockchain is a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.
  - A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.
  - Each block contains a hash (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In theory, the method renders the blockchain tamperproof.

- ## The four key concepts behind blockchain are:

1. Shared ledger: A shared ledger is an “append-only” distributed system of record shared across a business network. “With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.”

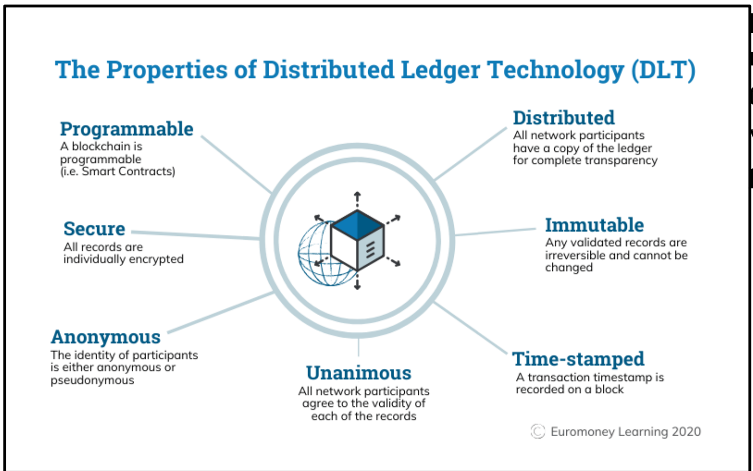
2. Permissions: Permissions ensure that transactions are secure, authenticated, and verifiable. “With the ability to constrain network participation, organizations can more easily comply with data protection regulations, such as those stipulated in the Health Insurance Portability and Accountability Act (HIPAA)” and the EU General Data Protection Regulation (GDPR).
3. Smart contracts: A smart contract is “an agreement or set of rules that govern a business transaction; it’s stored on the blockchain and is executed automatically as part of a transaction.”
4. Consensus: Through consensus, all parties agree to the network-verified transaction. Blockchains have various consensus mechanisms, including proof of stake, multisignature, and PBFT (practical Byzantine fault tolerance).

- **Benefits of Blockchain:**
  - Time savings: Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn’t require verification by a central authority.
  - Cost savings: Transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger.
  - Tighter security: Blockchain’s security features protect against tampering, fraud, and cybercrime.

- **Types of Blockchain**

  1. Public Blockchain

     - A public blockchain is a decentralized distributed system in which an unspecified number of participants can share and mutually verify transaction information occurring in the system. There is no separate managing entity. Anyone can participate anonymously, and there is no restriction on authority.
     - One current application of the public blockchain lies in the foundational technology behind Bitcoin, a well-known cryptocurrency (i.e. virtual money) currently in circulation around the world. Naturally, public blockchains are being actively researched in finance (Ripple Labs Inc 2018, S. Nakamoto 2008).
     - DLT is at the core of public blockchains. Additionally, public blockchain is an open blockchain that enables anyone to create transactions and participate as a node. It also provides high reliability and integrity through the verification of participants’ work.


The Properties of Distributed Ledger Technology (DLT)
Programmable
A blockchain is programmable (i.e. Smart Contracts)
Distributed
All network participants have a copy of the ledger for complete transparency
Secure
All records are individually encrypted
Immutable
Any validated records are irreversible and cannot be changed
Anonymous
The identity of participants is either anonymous or pseudonymous
Unanimous
All network participants agree to the validity of each of the records
Time-stamped
A transaction timestamp is recorded on a block
© Euromoney Learning 2020

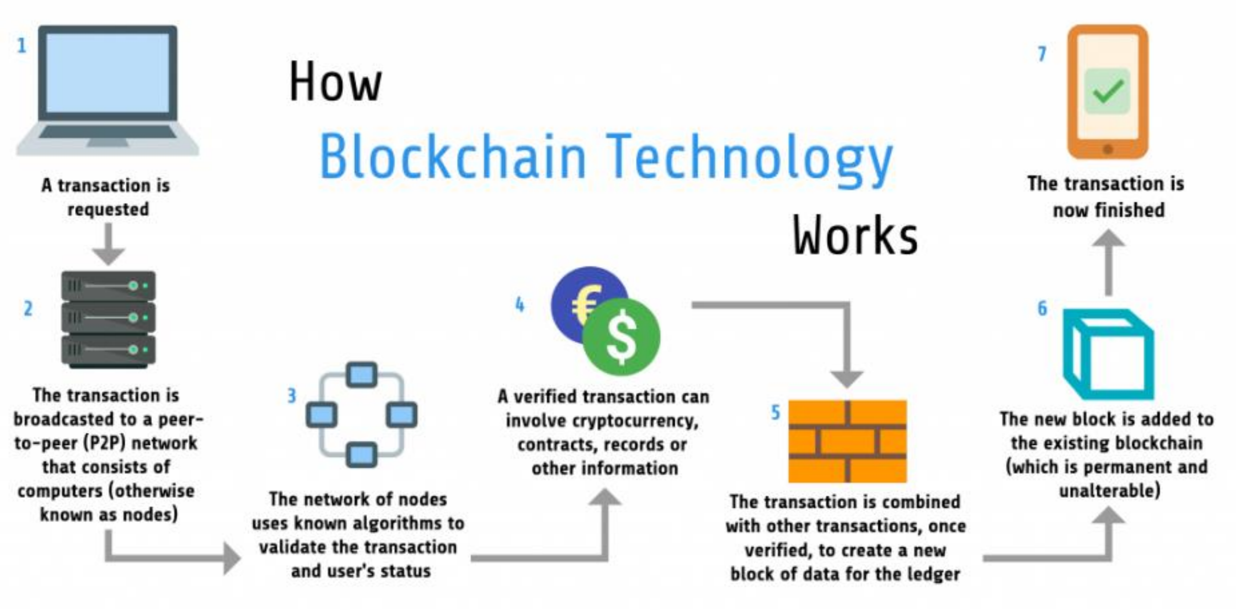
- Despite these strengths, however, there is a disadvantage: recording and processing speeds may decrease as the transaction records of all participants are stored and shared.

2. Private Blockchain

- A private blockchain is related to a public blockchain; yet, it differs in that it limits participation to only those individuals that the service provider (enterprise or organization) has approved. A private blockchain is a centralized blockchain.
- This type employs blockchain technology in a centralized structure as a method to enhance security and transaction speed. Unlike a public blockchain, the private type is managed independently by one entity. Only the nodes that have been verified through the authentication method created on the network can participate in this type of blockchain. Thus, to access transactions, each participant must have received appropriate permissions.
- In a private blockchain, only those entities that take legal responsibilities can create transactions, and only approved and verified entities may validate transaction histories and data as well as approve transactions. In private blockchains, the time for block creation cycles or verification is short because only authorized nodes participate.
- This renders the approval and verification progress of other unauthorized nodes unnecessary. However, since the users of private blockchains must depend entirely on the service provider, the reliability of private blockchains is limited in comparison to public blockchains.

3. Consortium Blockchain

- A consortium blockchain is one in which only those users who satisfy certain requirements or have been agreed on in advance (e.g. companies, organizations) may participate.
- The levels of authorization assigned to users in this blockchain type differ: for example, allowing only some participants to see all or part of transaction information or performing transactions with the authority to add new blocks to some other participants.
- It is a semi-centralized blockchain composed of many companies or organizations as joint entities. As with private blockchains, only the nodes (computers) of authorized users can participate in this type of blockchain.


How
Blockchain Technology
Works
1
A transaction is requested
2
The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)
3
The network of nodes uses known algorithms to validate the transaction and user's status
4
A verified transaction can involve cryptocurrency, contracts, records or other information
5
The transaction is combined with other transactions, once verified, to create a new block of data for the ledger
6
The new block is added to the existing blockchain (which is permanent and unalterable)
7
The transaction is now finished

• Applications of Blockchain

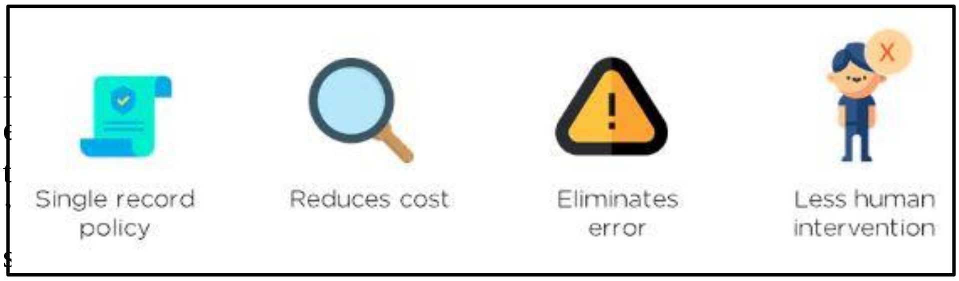
1. **Blockchain in Supply Chain Management**

   - Imagine you've ordered some apples from an online shop. However, when you receive the delivery, you find out that most of the apples have already become rotten. Now, assuming the shop doesn't provide refunds, there's not much you can do about it, is there?

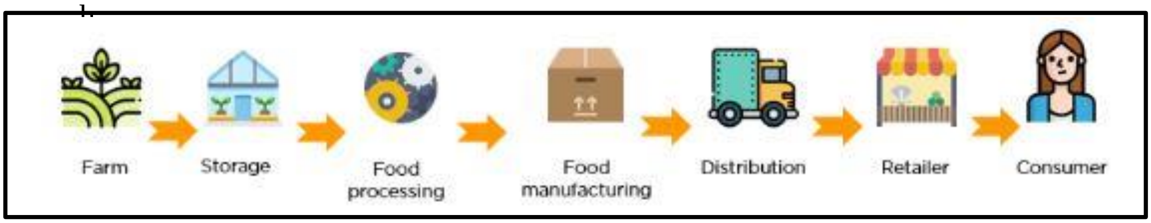
   - But what if there was a way that this whole thing could have been avoided?

   - Such problems can be avoided with blockchain technology, as it facilitates traceability across the entire supply chain. [Blockchain technology]() can be used to track all types of transactions in a very secured and transparent manner.

   - These benefits include:



   - I e t . s h.



a

look at an example of supply chain management:

2. Health Records

- Blockchain technology has huge applications in the healthcare sector, where a large amount of very important medical data must be stored and shared across the globe.
- The use of blockchain in health records has a series of potential benefits and pitfalls. The idea of decentralised healthcare data seems an obvious and useful system that could save lives and improve patient care.
- The way that this system could work would see a patient essentially own their health records. They can then grant or deny access to doctors or researchers, preventing unauthorised access, third party resale and tampering.
- The problem comes when you consider the scalability of something like blockchain into an already complicated and messy system, and the privacy of the stored data.

3. Banking

- When it comes to the Banking sector, there can be a number of use cases of Blockchain technology in Banking beyond the exchange of digital currencies.
- Some of those prominent ones which involve blockchain and cryptocurrencies to one extent or the other are:
  - Fraud Reduction – By bringing all the information on a distributed ledger with a timestamp and batches of specific transactions with a link to another block, the blockchain use cases in banking will make it impossible for the hackers to break into the system without the timestamp of the breach getting highlighted.
  - KYC – It is estimated that banks spend somewhere around $60 million up to $500 million per year in their 'Know Your Customer' project. These practices are followed to lower the money laundering instances and to keep terrorists out of the banking ecosystem. If the KYC process is brought on Blockchain, the verification time and associated cost will get lowered by manifold.

4. Internet of Things

- The mesh of connected devices, while connecting all the phases of a user's life with each other, also brings it to a vulnerable position.
- When you operate in a connected ecosystem, the moment your one device gets hacked the chances of your connected devices to get attacked also increases by manifold.
- Through Blockchain infused IoT adds the capability for you to exchange data on the platform instead of a third party.
- Also, since the devices are addressable with the benefits of the technology, businesses get access to the usage history of the connected devices, which comes in handy at the time of troubleshooting.

Some other blockchain applications include:

- **Insurance:** With the help of blockchain, insurance companies can eliminate forgeries and prevent false claims
- **Real estate:** Deploying blockchain technology in real estate increases the speed of the conveyance process and eliminates the necessity for money exchanges