****

**Assignment 02**

**Course: cse390**

**Name: Shaikat Majumder**

**ID: 18101630**

**Section\_ 02**

**Blockchain for Dummies:**

**What is a blockchain:**

Simply put, blockchain is a distributed ledger system that keeps a record of some transaction in a distributed or decentralized system for the parties in the system to authenticate the validity of that transaction. Till now, a trusted secondary party was involved in any transaction digitally to make sure of the validity of the transaction. These parties are financial institutions or banks.

**Why use blockchain?**

Blockchain brings with it an array of advantages over the current system. The blockchain is a single source of truth for all the transactions in the system and no other intermediary is required. Perhaps the most important advantage and utility of the blockchain is that the records are absolutely transparent and are always accessible to be viewed by the public in the system. This means that the reliability and transparency of the transaction and hence the data is preserved and this system becomes extremely secure as a public ledger to be used cross-industry for several purposes. Due to this extremely secure nature of blockchain, frauds are zero to none and this transparent system can be scaled to vast industries.

**Applications and future of blockchain:**

**Cryptocurrency:**

Due to the secure, transparent, and scalable nature of blockchain, it is initially being used extensively in cryptocurrencies. Even the name “crypto” comes from the cryptographic hashing system of the blockchain. Cryptocurrencies are currencies developed in the blockchain architecture that can be bought and sold securely.

**Ethereum blockchain:**

The Ethereum project came to life after the Russian-Canadian developer Vitalik Buterin published a white paper regarding Ethereum. Instead of making transactions regarding coins, Ethereum had the key difference that it kept a record of the execution of computer codes. Tokens can be created by the developers that can be any type of digital asset. Exciting new technologies like the NFT(nonfungible token) were introduced afterward.

**Web 3.0:**

With the future of the internet being web 3.0, further technologies such as artificial intelligence and blockchain will be incorporated into the internet. The introduction of a blockchain system on the internet will mean a more transparent internet via using the transparent protocols of blockchain. Decentralization of data and processes will also prevent intermediary parties from taking advantage of user data and hence provide for a more reliable and secure internet experience. Blockchain-based internet protocols, especially social media protocols are already in development that allows user to control and manage their own data. Blockchain-based peer-to-peer file-sharing systems are also in development. This allows data to be shared automatically using the secure blockchain system without any intermediary parties cutting both time and costs.

**Conclusion:**

The use of blockchain is one that will become a standard in the coming future. It is a simple and efficient technology, one that can be understood by anyone on the internet. The adoption of this technology and the required protocols and additional standards of use will be required to be developed in time. Due to a huge technology stack being developed on top of the internet this process of developing blockchain-based systems will be a big challenge.

**Blockchain for Techies:**

**What is a blockchain?**

Blockchain is a system by which data and processes can be decentralized as opposed to the client-server model. The term blockchain was coined a few years ago with the whitepaper on the blockchain. The whitepaper exclusively talked about the use of blockchain for online transactions and the use of a decentralized ledger-based system for recording the transactions. The name of the currency generated via this blockchain process is called cryptocurrency since cryptography is used to keep the transaction and other data encrypted in the system.

**The client-server model:**

The client-server model says that the data and the processing codes are stored in a single server that is in a geographic location. All the users must request this single server for retrieving their data and for running any processes. The same goes for online transactions whereby aan intermediary like a bank has a server from which all the data and the tranaction processes are run. Keeping an intermediary adds to the tranaciton time and also increases the cost due to the bank charging a tranaciton fee. Added on top of this is the problem of a single point of failure. Whereby the server might crash or the data might be corrupted.

**The peer to peer distributed model:**

The blockchain model is a decentrlaised model. This is a distributed peer to peer model as multiple peer nodes or blocks exist which are connected to each other via some encrypted data. The data is used to compute the largest treated chain the blockchain and hence the blockchain grows in size in the most trusted and largest chain. This prevents the ability to bypass a trusted longest chain as the majority of the participants in the chain are trusted and hence the blockchain is secure. Generally, blockchain such as cryptocurrency-based blockchains has nodes or blocks and miners as their components. Miners create new blocks via computing complex hash require powerful computer memory. After successful computation, the transaction is confirmed and new blocks are added.

**Consensus Mechanisms and Smart contracts:** One of the most intricate and core parts of the blockchain system is the consensus mechanism. For any sort of change to occur in a blockchain such as the transactions to occur the majority of the rusted blocks must agree to the transaction.. This is maintained by the consensus mechanism which is automatically handled via pieces of instructions and codes called smart contracts. There are several types of consensus mechanisms such as proof-of-trust, proof-of-stake,proof-of-credibility, etc.

**Types of blockchain:**

**Public blockchain**

Public blockchains are one where anyone can join the system. Hence is the name is public. A public blockchain is such as the dogecoin and the bitcoin where anyone can join the chain. Cryptocurrencies are examples of public blockchains.

**Private blockchain**

Private blockchains are one where only certain participants can join based on the type of data and processes being dined by that system. The general public is not allowed to enter this blockchain.

**Enterprise blockchain:** Enterprise blockchains are examples of private blockchain. One type of enterprise blockchain can be only for sharing employee data and information. An example is hyper ledger fabric.

**Hybrid blockchain:**

Hybrid blockchains are a mix of public and private blockchains. Some functionality is reserved in the private consortium and some of them are open to the public.

**Benefits of using blockchain architecture:**

Blockchain cuts down the problem of multiple types of server and data centralization-based frauds and corruption. Furthermore, it also cuts down on cyberattacks on the system.

| **Centralized client-server** | **Blockchain** |
| --- | --- |
| Less secure for data | More secure for data |
| Prone to a single point of failure | No single point of failure |
| Prone to cyber attacks | Less or negligible chance of cyber attacks |
| Data is centralized and can be altered by admin | Data is decentralized and cannot be altered without consensus. |