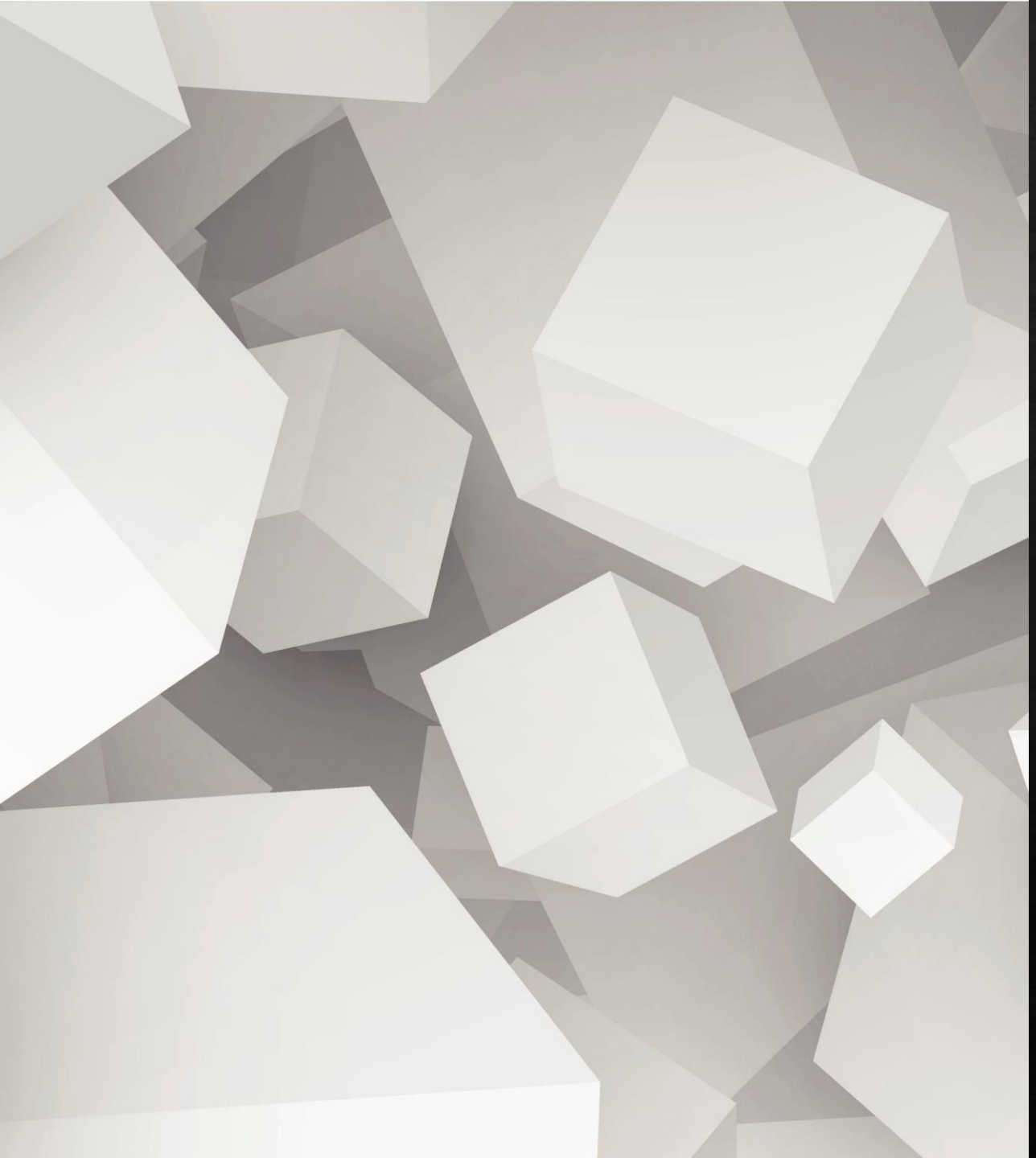
CAPSTONE

Domain - Cybersecurity



Title

- Fisal
- Akshatha p
- Rachappa
- praveen

Why choose blockchain?

- **Decentralization:** The decentralized nature of blockchain ensures that there is no single central entity governing data-related decisions.
- **Security:** Decentralized cloud data is difficult to attack as there are multiple nodes in the network with the same copy of data and any hacker must have to change data on the majority of nodes on the network to make the change look legitimate.
- **Distributed:** Blockchain is a distributed ledger where independent computers record, share, and synchronize the transactions instead of keeping data centralized in one location.

How to use blockchain for data storage ?

There are two different ways to store data in a blockchain:

- **On-chain storage:** This is the costly method of storing the data in the blockchain as the data is stored inside each block on the chain. If an attack happens then data can be restored and used.
- **Off-chain storage:** In this type of storage only the metadata is stored in the chain. The entire is not stored in the chain so if any attack happens then it might not be possible to restore the data. This is a cost-efficient method of data storage.

Where is the data stored in a blockchain?

Blockchain data is stored on a decentralized public ledger. The data on the ledger is stored in chunks called blocks, which are chained together using cryptography.

•Every block has a unique cryptographic hash as an identifier along with the previous block in the blockchain.

Each transaction inside a block is timestamped and added to the ledger with each block. Each new block records all transactions and adds them to the previous one. The data stored on Blockchain cannot be altered or removed from the blockchain as it would require alterations on every subsequent block.

•The miner who finds a solution for the proof-of-work puzzle (such as solving an equation by submitting correct answers) is rewarded with newly created bitcoins and has to add that block to the blockchain. But doing this takes time, so miners solve these puzzles using computer processors' power, resulting in competition to solve these puzzles first.

Types of storges provided by blockchain

- **Hashing:** This is a cost-efficient way of storing the data in the blockchain. In this method, only the hash value of the data is stored in the blockchain. The raw data can be stored in the file system and the hash id of the blockchain will be attached to the raw data.
- **TiesDB:** This is an Ethereum-based decentralized application (dApps) to store non-financial data and search through their documents. This allows advanced search and document modifications.
- **BigChainDB:** This database allows developers and enterprises to deploy blockchain proofs-of-concept, platforms, and applications with a blockchain database. This offers immutable data storage, built-in-asset support, low latency, powerful query functionality, and high throughput, thus this is a database with blockchain characteristics.
- **Distributed database:** Distribute databases like MongoDB, Apache, and Rethink DB can be used to store data. They are quick and versatile, but they are not Byzantine verified. This means any hacker can corrupt the entire information base as all the hubs of the information completely trust one another.

Types of storages provided by blockchain

- **Decentralized cloud storage:** Decentralized cloud storages allow for the storage of static data where data is not stored on the company server but instead on the devices of the renters. This storage can be used online thus making them fast and efficient but they are costly too.
- **Interplanetary file system:** This is a blockchain technology that breaks up data into shards and stores them in multiple instances. It is a peer-to-peer solution where the files get downloaded only if the person needs them. Thus, this is the address-dependent storage solution.

Important notes to remember about sharing data through blockchain

Transactions between users are how bitcoins are transferred from one person to another. When a transaction is made, it is written to the blockchain in a certain format and broadcast to all nodes on the network. The data stored in the transactions consist of multiple different fields:

- **Sender's address:** The address of the sender of the transaction.
- **Recipient address:** The address of the recipient of the transaction.
- **Transaction amount:** The amount that was transferred, including a decimal place. This is important because fractions of pennies are not possible in Bitcoin. Therefore, if you send one bitcoin and two cents, it would be equal to one bitcoin and two cents in Bitcoin.
- **Timestamp:** This is a message that tells you which block this transaction was recorded in, as well as its timestamp. Since the blockchain is public, anyone can see all transactions on it; therefore this information can be used to see when payments were made or wallets were funded for specific periods of time

Different ways to store data in blockchain

Blockchain technology can store data in a number of different ways. It all depends on the blockchain, but some examples include:

- **Bitcoin:** In bitcoin the data includes the entire history of all the bitcoin transactions. If one node has an error then it uses thousands of other nodes as a reference point to correct itself.
- **Ethereum:** Ethereum uses a trie data structure to store data. It separates the temporary data from the mined transaction data. The data is added to the transaction trie only when the transaction is confirmed

- There are three types of trie in Ethereum for data storage:
  - **State Trie :** This global state trie is constantly updated and it contains the key-value pair for every account which exists on the Ethereum Network.
  - **Storage Trie :** This stores the contract data. Each Ethereum account has a storage trie and the 256-bit hash value of the storage trie's root node is stored in the global state trie.
  - **Transaction Trie :** Each Ethereum block has its own separate transaction tire. A block contains many transactions
- **Corda:** This is the open-source blockchain platform that doesn't use the global broadcast. It can cut the record-keeping cost while at the same time streamlining the business operations. Here, the communication between the peers can be verified without the need to download the whole data due to the use of graphs and persistent queues.

Reasons to choose blockchain

The blockchain is a revolutionary system for securely recording transactions
The entire point of using a blockchain is distributed trust and the ability to verify transactions in a trustless environment. it can be used to encrypt data with public access. If a user wishes to have complete control over his/her data, he/she will need to keep it local or use an external device.