BLOCKCHAIN

SHAMS ALI

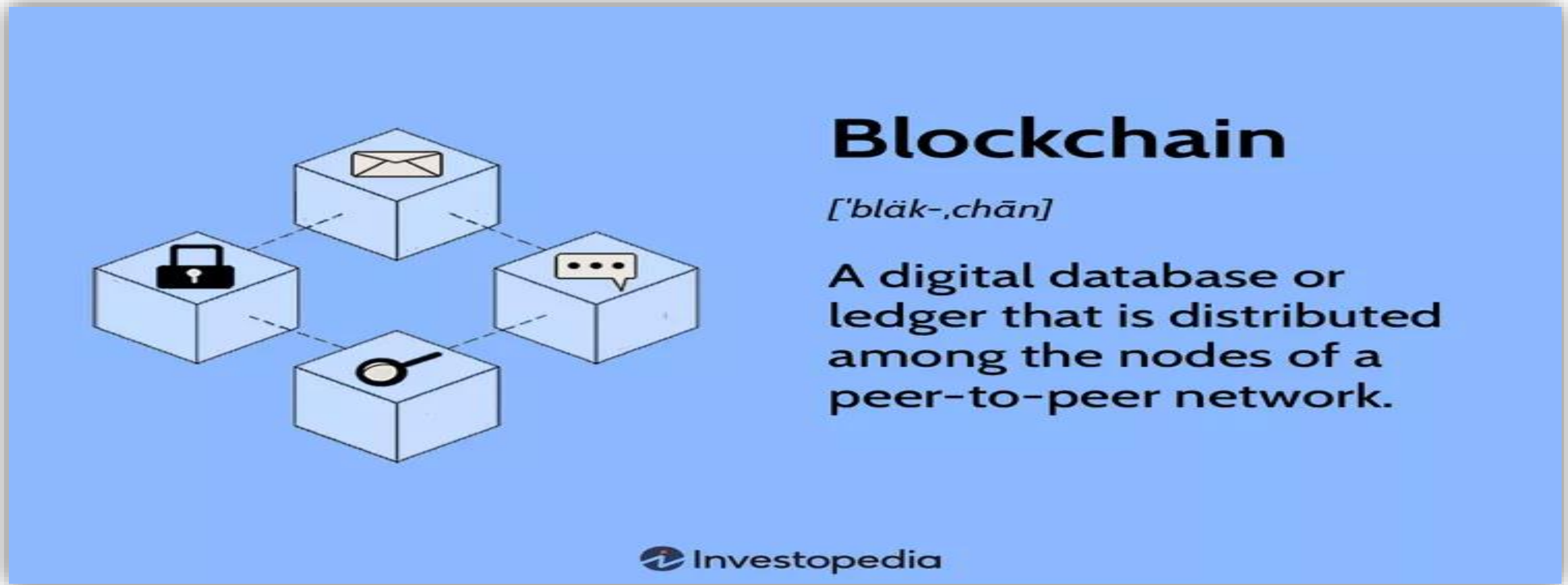
BSIT51F22S016

BSIT(SS1)

What Is a Blockchain?

- A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—the term used to describe the inability to be altered.

- Because there is no way to change a block, the only trust needed is at the point where a user or program enters data. This aspect reduces the need for trusted third parties, which are usually auditors or other humans that add costs and make mistakes.



Blockchain

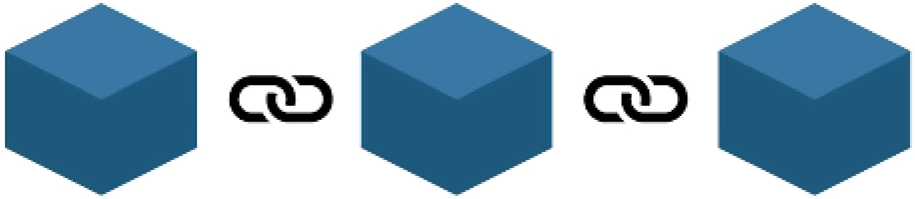
['bläk-,chān]

A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

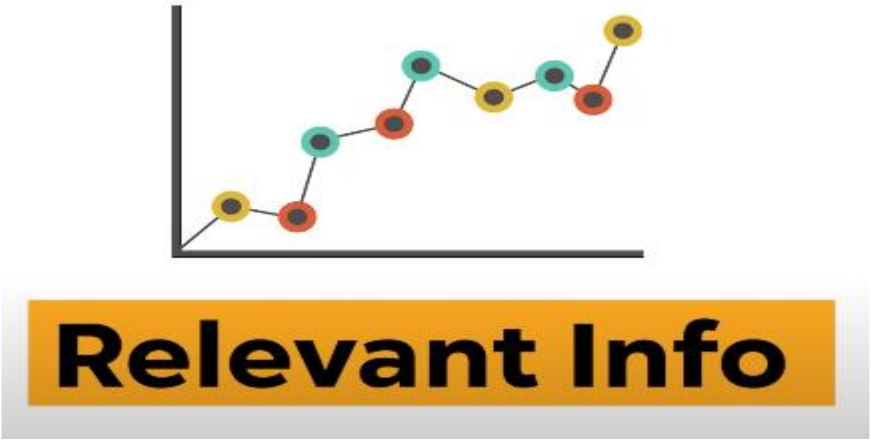
Investopedia

HOW DATA STORED IN BLOCKCHAIN?

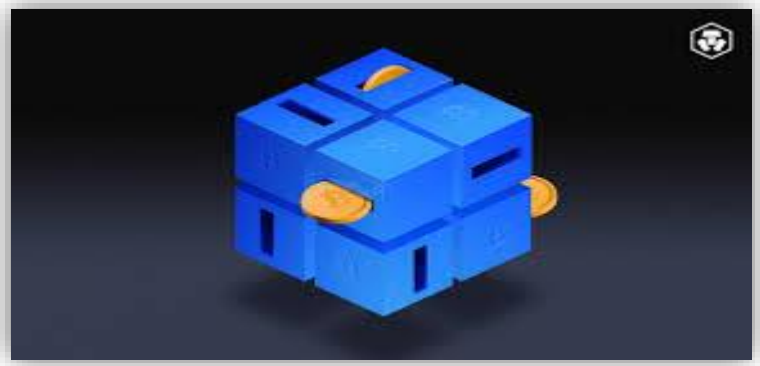
- Single record of database is called block and a blockchain is a chain of related blocks.



- A single block contain an information or data and also a hexadecimal number called the hash.



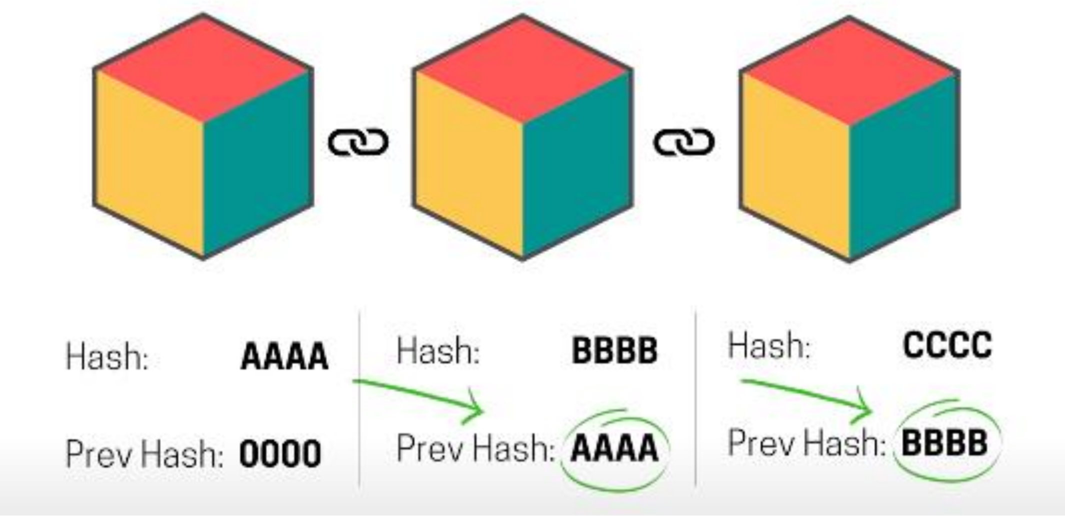
- For example in the use case of bitcoin block is used to store the information of transaction of the transportation of bitcoin from one person to the other.



- Hash is just like a fingerprint that is generated when data is entered in the block.

- A block also contain the prev block hash creating a chain of block just like a linked list.

- The first block that do not store any previous hash is called **GENSIS** block.



Blockchain Transparency

- Because of the decentralized nature of the Bitcoin blockchain, all transactions can be transparently viewed by either having a personal node or using blockchain explorers that allow anyone to see transactions occurring live.
- Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. This means that if you wanted to, you could track a bitcoin wherever it goes.

Is Blockchain Secure?

- Blockchain technology achieves decentralized security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain. After a block has been added to the end of the blockchain, previous blocks cannot be changed.
- A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would reject an altered block because the hashes would not match.
- For instance, imagine that a hacker runs a node on a blockchain network and wants to alter a blockchain and steal cryptocurrency from everyone else. If they were to change their copy, they would have to convince the other nodes that their copy was the valid one.
- They would need to control a majority of the network to do this and insert it at just the right moment. This is known as a 51% attack because you need to control more than 50% of the network to attempt it.

Pros

- Improved accuracy by removing human involvement in verification.
- Cost reductions by eliminating third-party verification.
- Decentralization makes it harder to tamper with.
- Transactions are secure, private, and efficient.

Cons

- Significant technology cost associated with some blockchains.
- Low transactions per second.
- History of use in illicit activities, such as on the dark web.
- Regulation varies by jurisdiction and remains uncertain.
- Data storage limitations.

BENEFITS OF BLOCKCHAINS

1. Accuracy of the Chain

- Transactions approved by distributed computers, minimizing human error.
- Errors isolated to one copy, not accepted by the entire network.

2. Cost Reductions

- Eliminates need for third-party verification, reducing associated costs.
- Bitcoin's decentralized nature leads to limited transaction fees.

3. Decentralization

- Information spread across a network, difficult to tamper with.
- No central location for storing data, enhancing security.

4. Efficient Transactions

- Operates 24/7, accelerating transaction settlement.
- Useful for cross-border trades, bypassing time zone delays.

5. Secure Transactions

- Verified authenticity before adding to blockchain.
- Immutable blocks prevent alteration after confirmation.

6. Transparency

- Open-source nature allows auditing for security.
- Decentralized control with community-driven upgrades.

7. Banking the Unbanked

- Enables financial inclusion regardless of background.
- Provides secure storage, reducing vulnerability to theft.
- Potential for broader applications beyond wealth storage.