

4.5 BLOCKCHAIN TECHNOLOGY

A blockchain is a distributed ledger (storing all the transactions) across a peer-to-peer (P2P) network. *Confused ?*. Hmm. Well, don't be ; just read the following hypothetical situation in order to understand the above statement.

Hasan and Nitin were friends since their school days, During their adulthood, they were also doing business together. All their financial transactions took place through ABCXYZ Bank where both Hasan, Nitin and their clients made financial transactions. One day some common client of Hasan and Nitin hacked their financial data from the Bank and forged it. It led to heavy losses and the trust-violation of clients.

After sometime, Hasan and Nitin decided to continue the same business, but this time, they decided that every time a financial transaction would take place, each connected client would get a printed copy of it. So, all connected clients would get printed copies of each financial transaction taking place and thus would have their own copy of ledger containing details of all financial transactions.

Every time a new transaction takes place, all available financial data is compared with the existing ledger ; if they match, the transaction is considered valid. This happens at all clients' ends.

So, if someone tries to forge data, then its data will not match all copies of decentralized, distributed ledger available with all clients and thus will be rejected.

Hasan and Nitin are happy with this secure form of financial transactions and so are their clients.

Now, in the second style of the financial transactions, you can see that

- ⇒ the financial transactions' ledger is not at a centralized location like a bank, but is distributed and is available to all connected clients.
- ⇒ Every transaction's details (called a **block**) is sent to all the connected clients (peer-to-peer network).
- ⇒ Each new block is chained with earlier existing blocks (forming a **blockchain**) to form a distributed ledger.

This style of financial transactions is called the **blockchain technology**. Now read the very first line of this section again. Now, I am sure the confusion is no more there.

Let us now understand the blockchain technology in technical terms.

4.5.1 Blockchain Technology Keyterms

Before we discuss the working of blockchain technology, it is important to know about the key elements involved.

The key elements involved in the blockchain technology are :

- ⇒ **Blockchain Technology**. It is a decentralised, digitized, public ledger of each of the online transactions (mostly financial, but not always) occurring among a network of peers. (peer-to-peer network)
- ⇒ **Block**. A block refers to a secured data chunk that stores encrypted details of a valid transaction that has occurred online. A block consists of *two* parts :
 - (i) a **header**, which is public to all and
 - (ii) **private details of transaction**, accessible only to the owner of the block.

- ❖ **Blockchain.** It is the group of linked blocks, which are related to each other and are in proper, linear chronological order. It stores the complete trail of transactions.
- ❖ **Public ledger.** All confirmed transactions' linked blocks since the first transaction available in the form of a blockchain called *public ledger*.
- ❖ **Mining.** It is the process of confirming a transaction after validation, and adding it to the *public ledger*.
- ❖ **P2P Network (Peer-to-Peer Network).** The traditional architecture of www is client-server type where the server stores all the information in a centralised database. The P2P network (Peer-to-Peer network) is the type of network used in blockchain technology. It is a distribution network where each participant computer within the network maintains a copy of the data and approves and updates the new entries. Each participant has equal power.

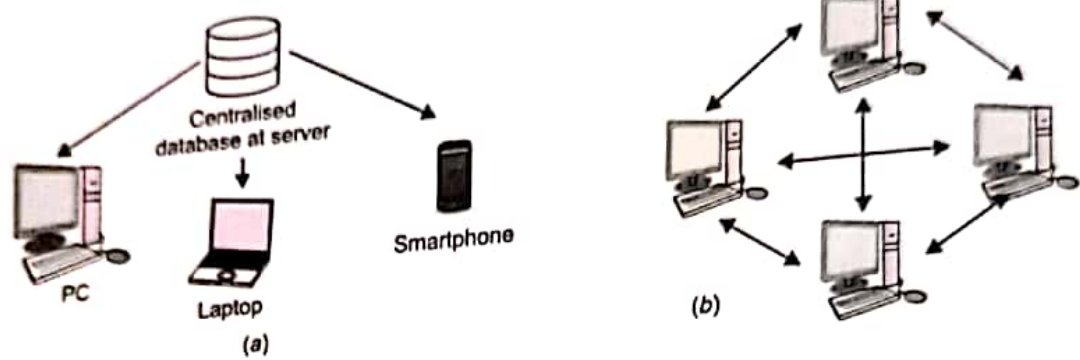


Figure 4.5 (a) Client-Server network architecture of www.
 (b) P2P (Peer-to-Peer) network architecture of blockchain technology.

4.5.2 How Blockchain Technology Works

You know that a block is a secure data chunk storing encrypted details (using cryptography) of a valid transaction. A block is created when a user initiates a transaction. It stores the encrypted details of the transaction taking place.

A block gets connected with blockchain as a permanent database only after validation. A blockchain contains numerous linked blocks which are related to each other in a proper linear chronological order.

To see Blockchain in action

Scan QR Code

Each block contains a **hash** of the previous block. Hashing is a strong encryption mechanism. Hashing not only encrypts, it makes forgery impossible because hashing cannot be reversed. Thus, a blockchain has complete information about different user addresses as well as their balances right from the origins set to the very recent completed block. Every node of the P2P network has access to the blockchain.

The blockchain technology ensures that all transactions are always available since their creation and no transaction can be deleted.

Blockchains have found their applications in *healthcare, voting mechanisms, banking sector, finances, Asset management, insurance claim processing, passports, property registrations* and

Figure 4.5 explains how blockchain technology works.

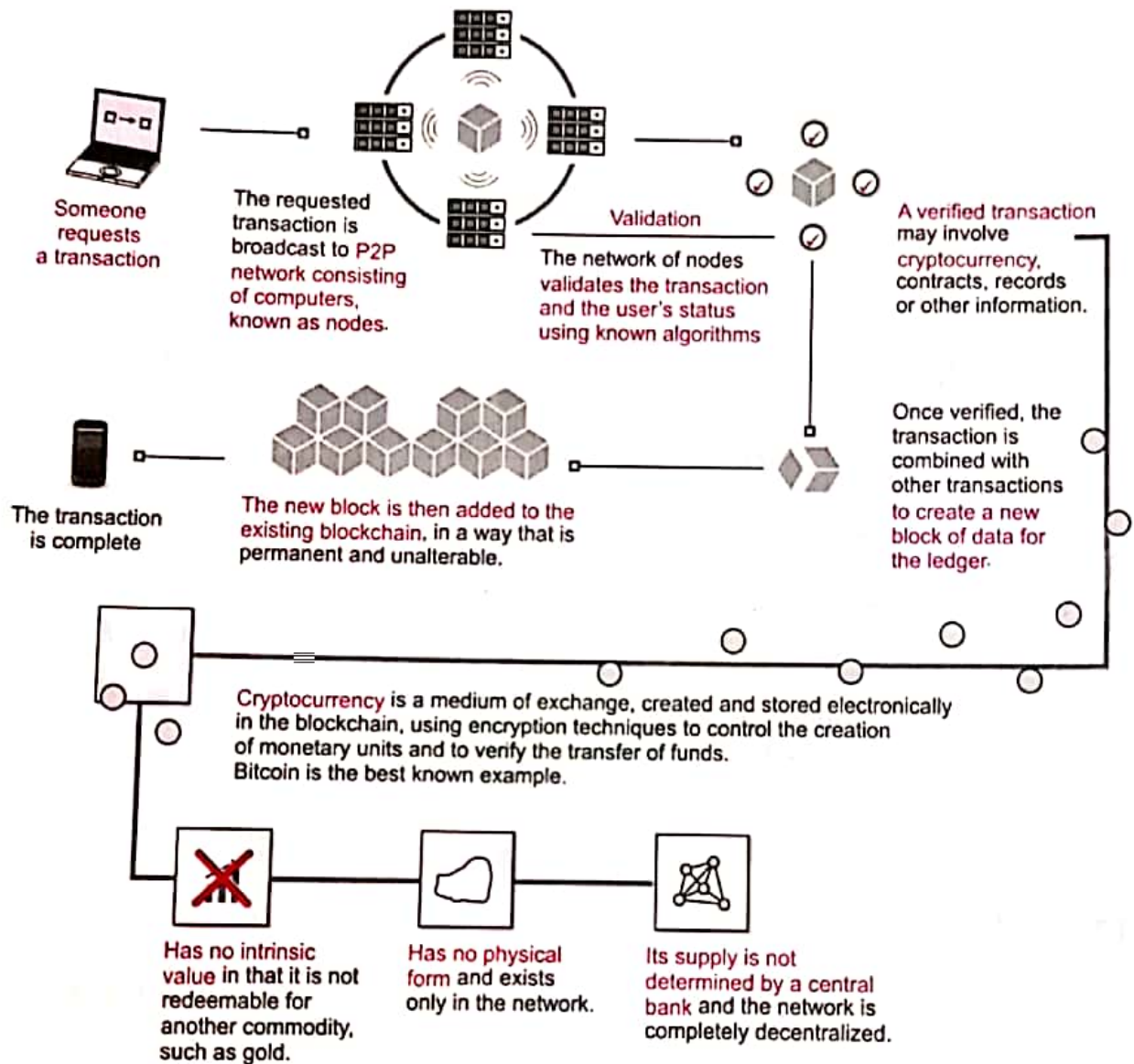


Figure 4.6 How blockchain technology works.

Benefits of Blockchain Technology

- ⇒ Increased time effectiveness due to the real-time transactions.
- ⇒ Direct Transactions eliminate the overheads and intermediary costs.
- ⇒ Reduced risks related to cybercrimes, frauds and tampering.
- ⇒ More transparent processes with a proper record creation and tracking.
- ⇒ Highly secure due to cryptographic and decentralized Blockchain protocols.

NOTE

Many people assume that blockchain and cryptocurrency are the same. Blockchain is the underlying technology of cryptocurrency like Bitcoin.