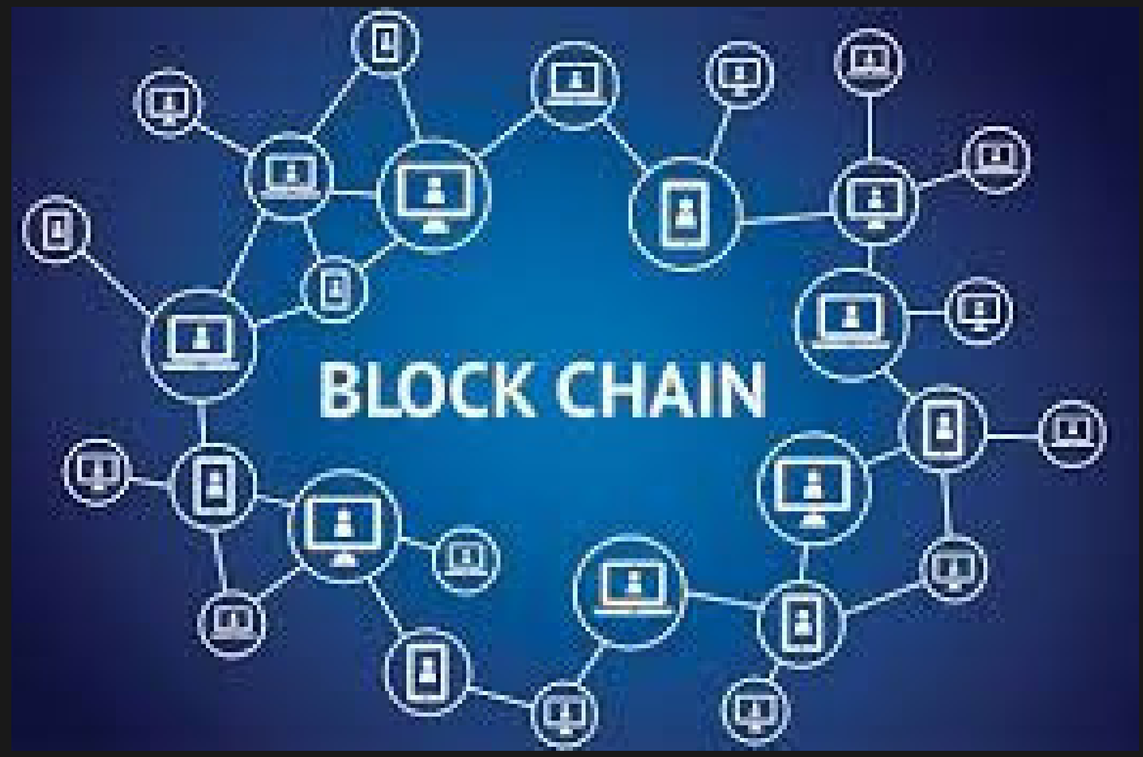
Blockchain In Cryptocurrency

By:
Aditi Kanojia (19030121003)
Amal Pillai (19030121009)
Sradha S Kumar (19030121089)
Umang Agarwal (19030121093)

What is Blockchain ?

A blockchain is a computer file for storing data. it's an open,
distributed database. The data is distributed
across many computers, and the whole blockchain is entirely decentralised. This means no one person or entity has control over the blockchain; this is a radical departure from the centralised databases that are controlled and administered by businesses and other entities.



Features of Blockchain

- Immutability.: What that means is that if you have stored data on the blockchain it is guaranteed that data cannot be changed later.

- Decentralized. :Which means that no single entity has control. Blockchain needs a group of nodes to be able to serve that work as points where all the data is stored in a decentralized manner. And these nodes work together to make sure that the correct provenance of data is maintained, which means that the correct timeline of data is maintained.

- Digital Ledger : It is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

- Enhances Security : Network automatically checks and updates itself every few minutes, this helps in providing a self-reviewing system. It helps in providing a very robust system.

- Consensus : It thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.

Why is blockchain used ?

- Increase Business Velocity — With blockchain, you can optimize business decisions by providing real-time information visibility across your company's ecosystem.

- Reduce Operation Costs — Use blockchain to accelerate transactions and eliminate cumbersome offline reconciliations by using a trusted shared fabric of common information. Blockchains help you eliminate intermediaries and related costs, possible single points of failure, and time delay by using a peer to peer business network.

- Reduce the cost of fraud and regulatory compliance — Blockchain allows you to gain the security of knowing that business critical records are made tamper-proof with securely replicated, cryptographically linked blocks that protect against single point of failure and insider tampering.

1. GREATER TRANSPARENCY

2. ENHANCED SECURITY

3. IMPROVED TRACEABILITY

4. REDUCED COSTS

Advantages

Disadvantages

1. LESS SECURE
2. PRIVATE KEYS
3. STORAGE
4. INEFFICIENT

TYPES OF BLOCKCHAIN

Public Blockchain Networks

Private Blockchain Networks

Permissioned Blockchain Networks

Consortium Blockchain Networks

THE BITCOIN BLOCKCHAIN

Bitcoin is a cryptocurrency invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto.

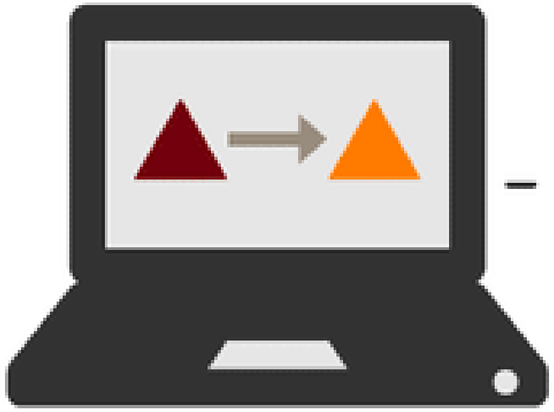
The blockchain behind the bitcoin is the public ledger of every transaction that has taken place.

Nodes in the blockchain network acts as a decentralized database storing the transactions w.r.t bitcoin cryptocurrency thus acting as a public ledger.
It takes approximately 10 minutes to add a transaction/block to the bitcoin blockchain.

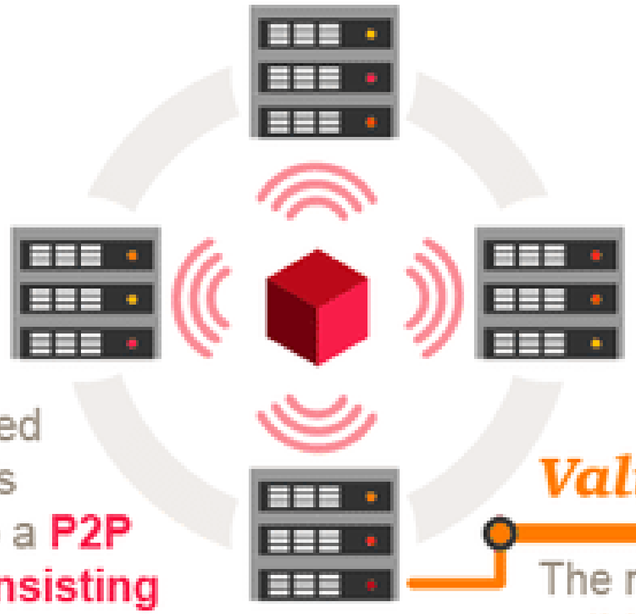
Many other cryptocurrencies also implements blockchain some examples are -:
ether used by etherum, XRP, etc

HOW TRANSACTION IS DONE

How it works:



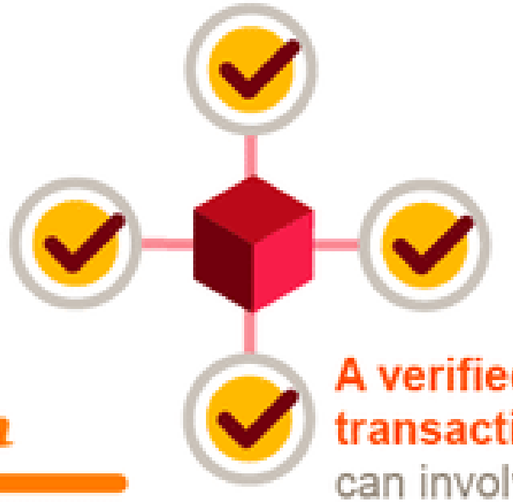
Someone requests a transaction.



The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

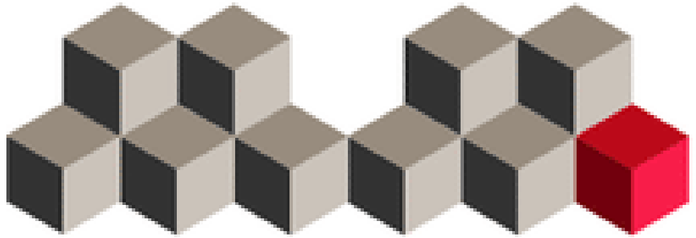
Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**



A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

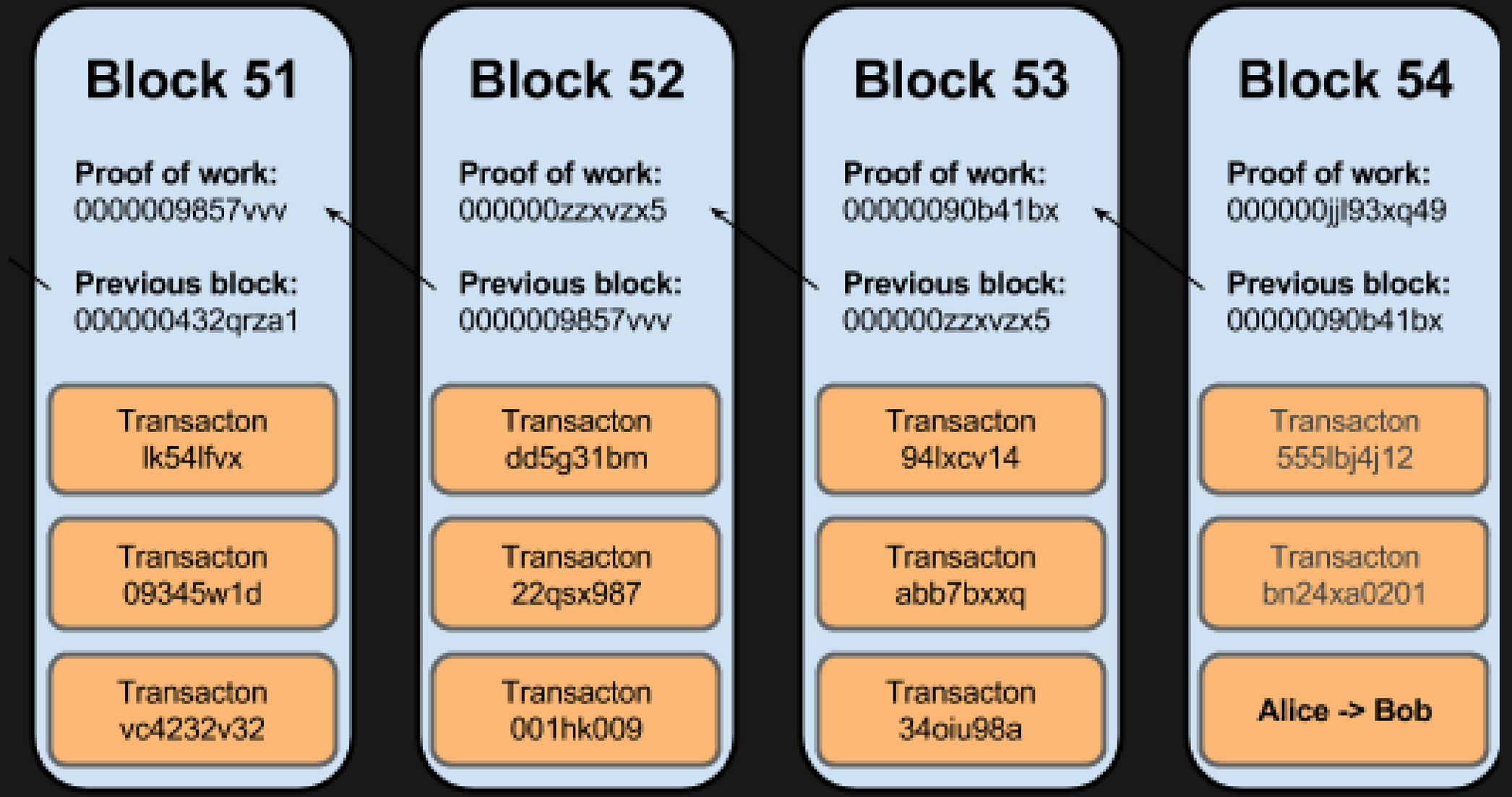
The transaction is complete.



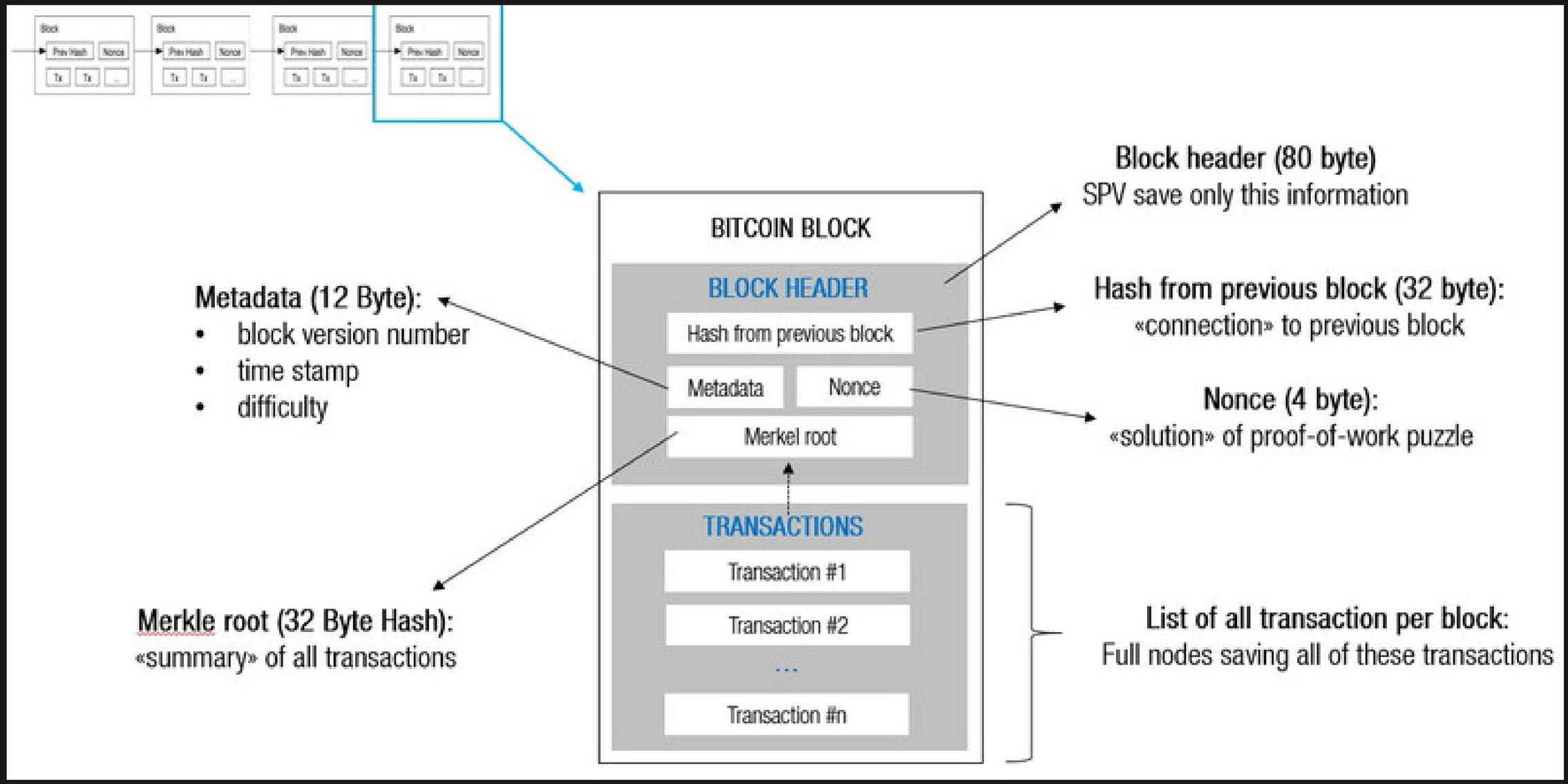
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

BLOCKCHAIN OF BITCOIN



CONTENTS OF A BITCOIN BLOCK

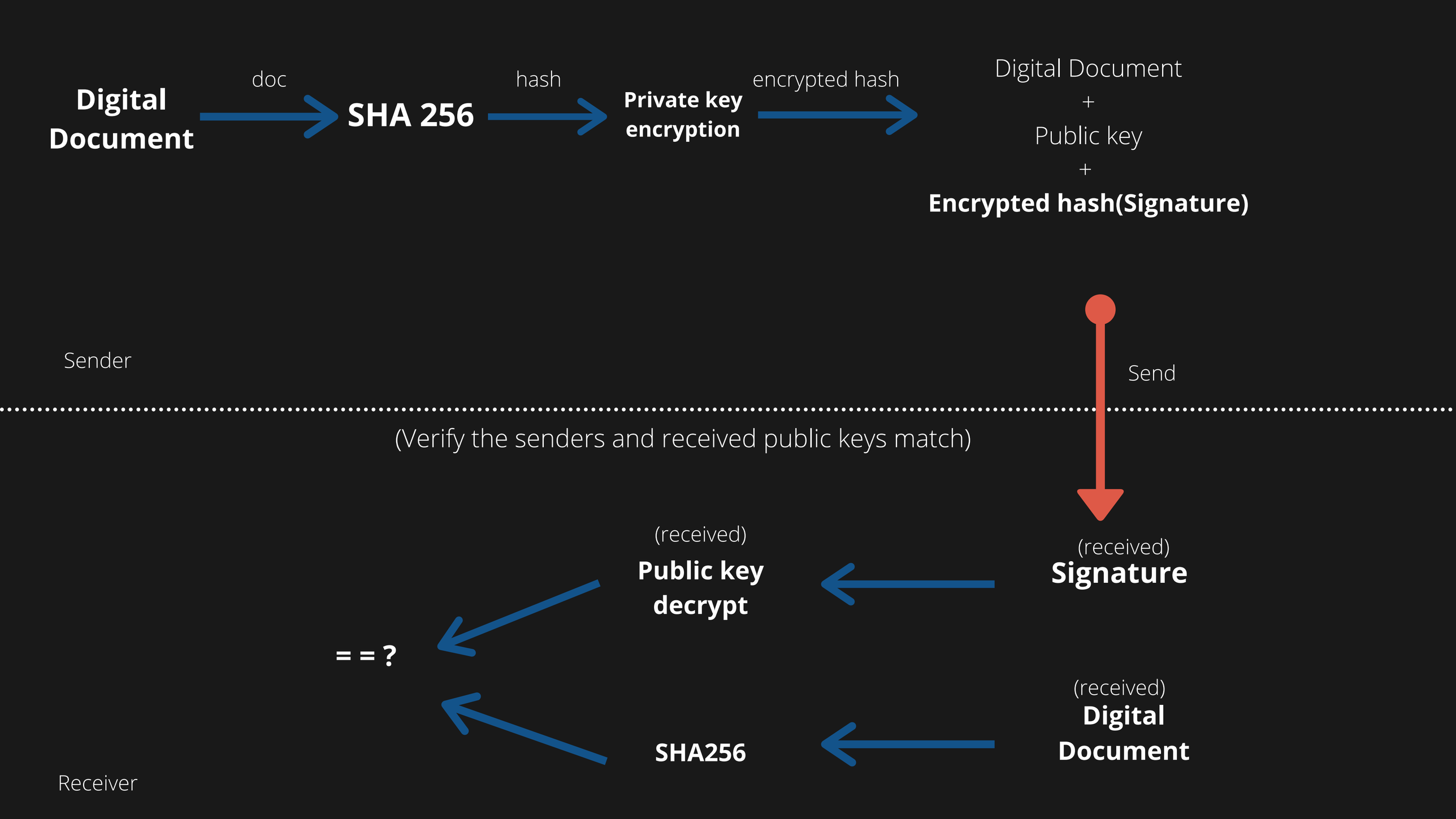


The role of Public key encryption in bitcoin blockchain

In bitcoin, we use public key cryptography to create a key pair that controls access to bitcoin. The key pair consists of a private key and derived - from it a unique public key. The public key is used to receive funds, and the private key is used to sign transactions to spend the funds.

WHY USE ASYMMETRIC CRYPTOGRAPHY (PUBLIC/PRIVATE KEYS)?

Why is asymmetric cryptography used in bitcoin? It's not used to "encrypt" (make secret) the transactions. Rather, the useful property of asymmetric cryptography is the ability to generate digital signatures. A private key can be applied to the digital fingerprint of a transaction to produce a numerical signature. This signature can only be produced by someone with knowledge of the private key. However, anyone with access to the public key and the transaction fingerprint can use them to verify the signature. This useful property of asymmetric cryptography makes it possible for anyone to verify every signature on every transaction, while ensuring that only the owners of private keys can produce valid signatures.


Digital Document
doc
SHA 256
hash
Private key encryption
encrypted hash
Digital Document
+
Public key
+
Encrypted hash(Signature)
Sender
Send
(Verify the senders and received public keys match)
(received)
Public key decrypt
(received)
Signature
= = ?
(received)
Digital Document
SHA256
Receiver

Let's get some action now!

https://www.blockchain.com/explorer

Thank you!