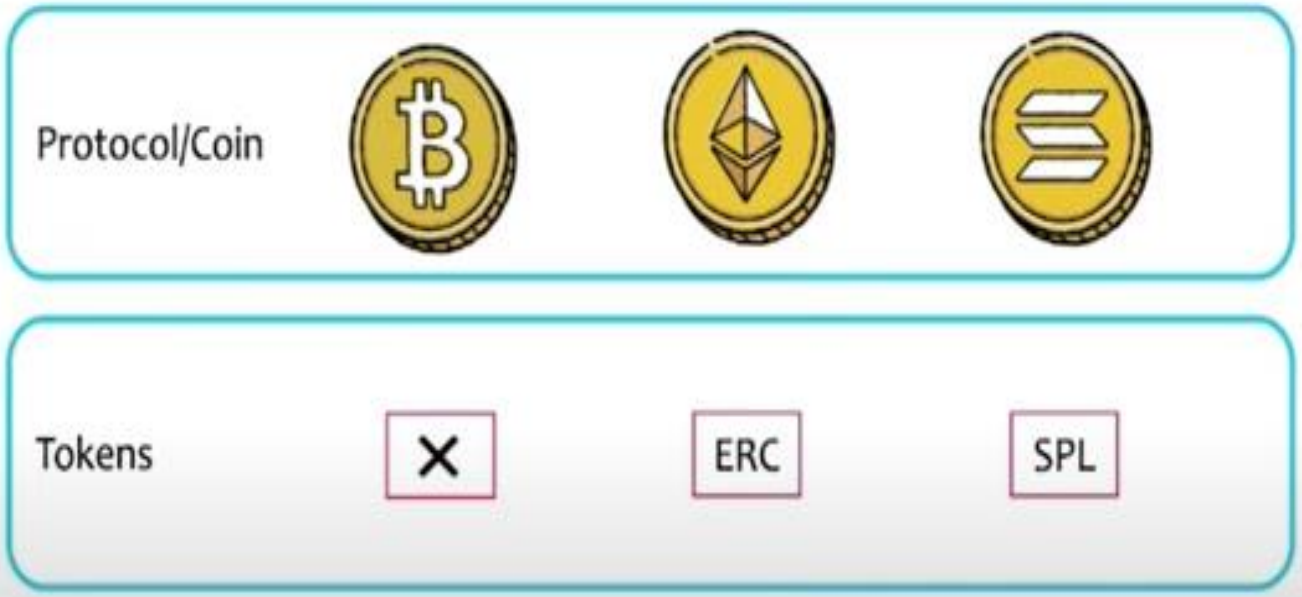
UNIT II - BITCOIN

CREATION OF BITCOIN

- **Bitcoin Introduction.**
- Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world.
- Bitcoin uses peer-to-peer technology to operate with no central authority.

- **Main Operations:**
- **Transaction Management:** Transfer bitcoins from a user to another across the world.
- **Money Issuance:** No central authority regulates monetary base.

How to create our own Cryptocurrency



- Protocol/coin
- Creation of your own Blockchain.
- Modification of existing blockchain.
- Which may be complex, high knowledge, time consuming.

- Tokens
- Type of cryptocurrency that represent an asset or specific use and resides on blockchain.
- Ex: coinmarketcap.com

CATEGORIZATION OF CRYPTOCURRENCY

COIN

TOKEN

EXAMPLES:

Bitcoin

Ethereum

Ripple

Litecoin

Cardano

Iota

EXAMPLES:

Tron

Byton

Vechain

Ox

Omisego

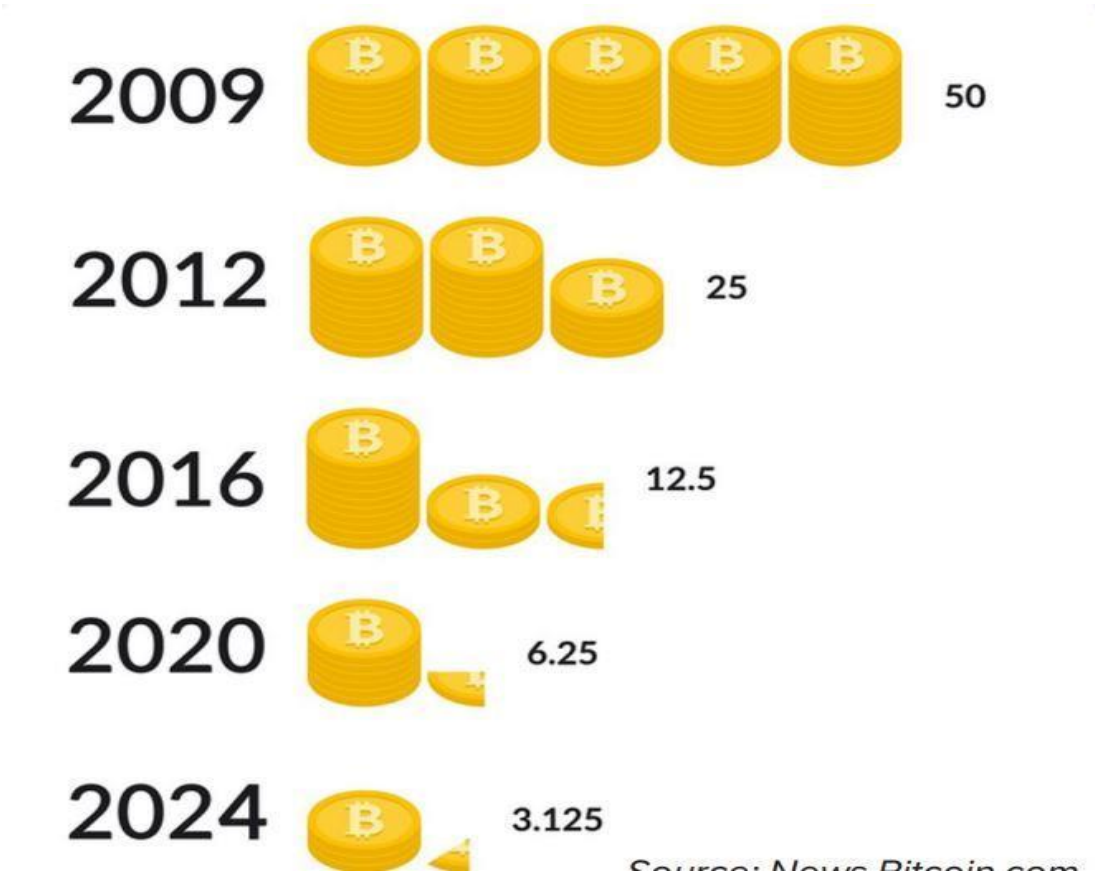
Augur

Creation of Bitcoin

- **Controlled Supply:** In this currency is created by the nodes of a peer-to-peer network.
- The Bitcoin generation algorithm defines, in advance, how currency will be created and at what rate.
- Any currency that is generated by a malicious user that does not follow the rules will be rejected by the network and thus is worthless.
- New bitcoins are generated during **mining** when a user discovers a new block.

- The number of bit coins generated per block is set to decrease geometrically with a 50% reduction for every 21 millions blocks,or approximately 4 years.
- This reduce with time amount of bitcoins generated per block
- Theoretical limit for total bitcoins
- Miners will get less reward for mining bitcoin as the time progresses. Hence, the transaction fees will increase to encourage the miners to complete transaction quickly.

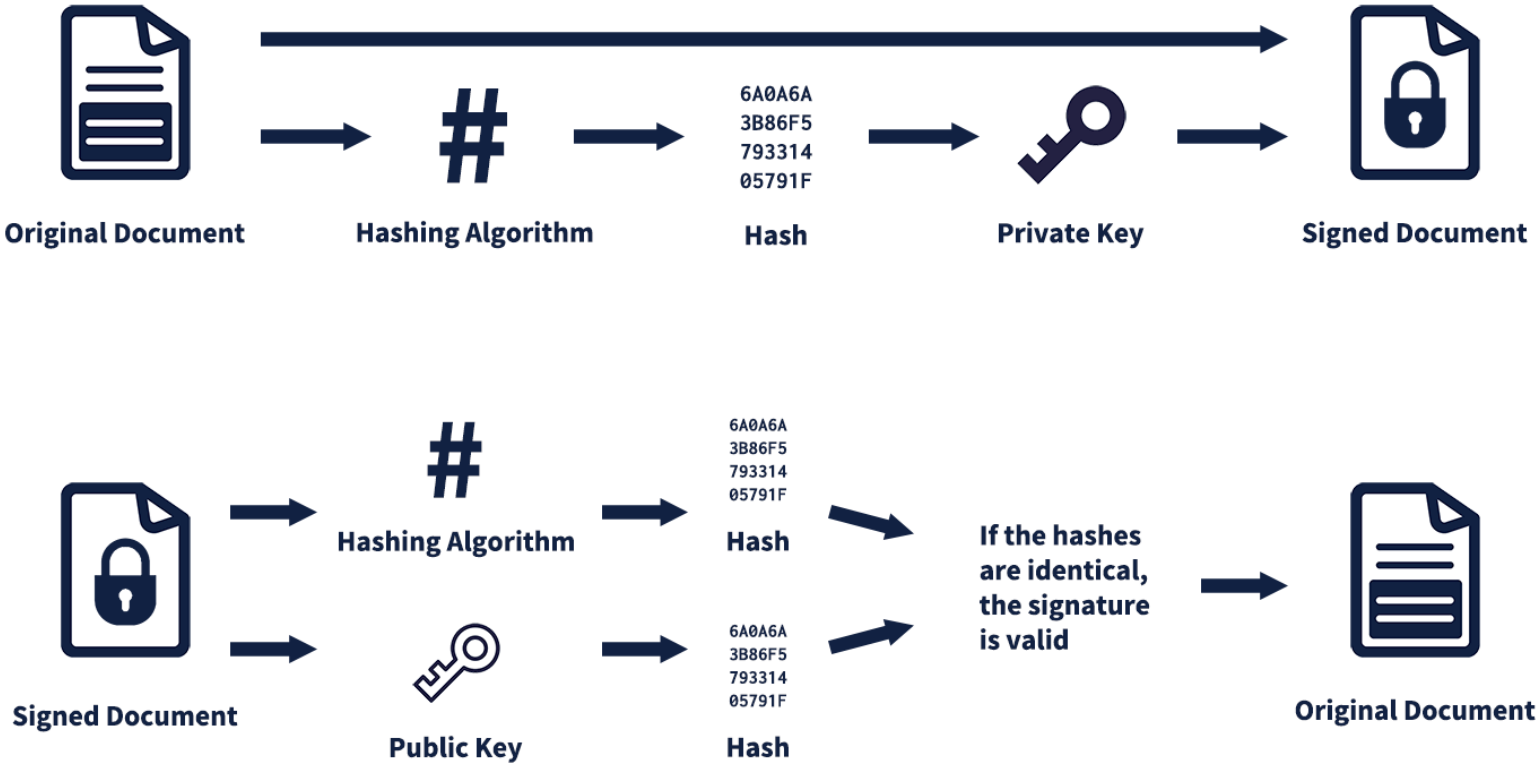
The process, occurring every four years, reduces the reward miners receive for validating transactions by 50%.



- **Transactions:**
- Bitcoin uses **public key cryptography** to verify the digital signature.
- Every user can have one or more wallet addresses but every address will always have a pair of public and private keys.

- **Example of transaction:** Suppose Alice wants to send some bitcoins to Bob. Then, the following will take place:
- Bob sends his address to Alice.
- Alice adds Bob’s address and the amount of bitcoins to transfer to a message: a ‘transaction’ message.
- Alice signs the transaction with her private key, and announces her public key for signature verification.
- Alice broadcasts the transaction on the Bitcoin network for all to see.
- The first are done manually by humans. Last are taken care by Bitcoin client software itself.

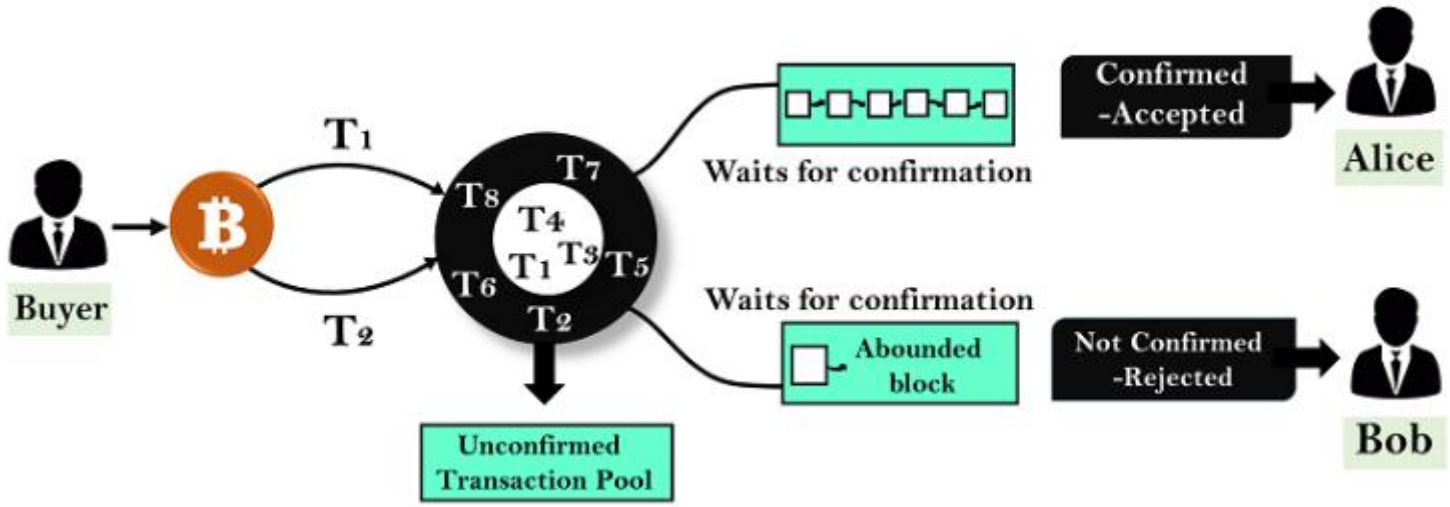
Private key encrption and public kay decryption



- **Handling Double Spending:**

- When the same money is spent more than once, it is called Double Spending.
- For example, Alice has 50 bitcoins and she sent 50 bitcoins to Bob and 50 bitcoins to Eve simultaneously.
- Then, only one of the transaction will be successful because double spending is not allowed in Bitcoin.

Let us suppose you have 1 BTC and try to spend it twice. You made the 1 BTC transaction to Alice. Again, you sign and send the same 1 BTC transaction to Bob



- Bitcoin prevents double spending by following ways:
- Details about the transaction are sent and forwarded to all or as many other computers as possible.
- A constantly growing chain of blocks that contains a record of all transactions is collectively maintained by all computers (each has a full copy).
- To be accepted in the chain, transaction blocks must be valid and must include proof of work (one block generated by the network every 10 minutes).

Address generation

- Blockchain addresses are typically generated using a mathematical algorithm known as a hashing function. This algorithm takes an input, such as a **public key** or **private key**, and generates a unique output string of alphanumeric characters that serve as the blockchain's **unique address**.

- The process of generating a blockchain address varies depending on the specific cryptocurrency network, but it generally follows a similar set of steps: chain's **unique address**.

- **Private Key Generation:** The first step in generating a blockchain address is to create a private key, which is a randomly generated string of characters used to sign transactions and verify ownership of the digital wallet.
- **Public Key Generation:** Once a **private key** is generated, a corresponding public key is created using a mathematical algorithm. The **public key** is a **unique identifier** used to derive the blockchain address.
- **Hashing:** The public key is then hashed using a hashing algorithm such as SHA-256 or RIPEMD-160 to generate the final blockchain address.
- **Checksum:** Some blockchain networks add a checksum to the address to ensure that the address is valid and prevent **transaction** errors.

- **Anonymity:**
- There are no specific usernames, emails, passwords to hold bitcoins.
- Each balance is simply associated with an **address and its public-private key pair.**
- Transacting parties do not need to know each other's identity in the same way that a store owner does not know a cash-paying customer's name.
- A Bitcoin address mathematically corresponds to a public key and looks like this: 1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz.
- A single person can have multiple addresses making it difficult to know what amount of bitcoins the person holds.