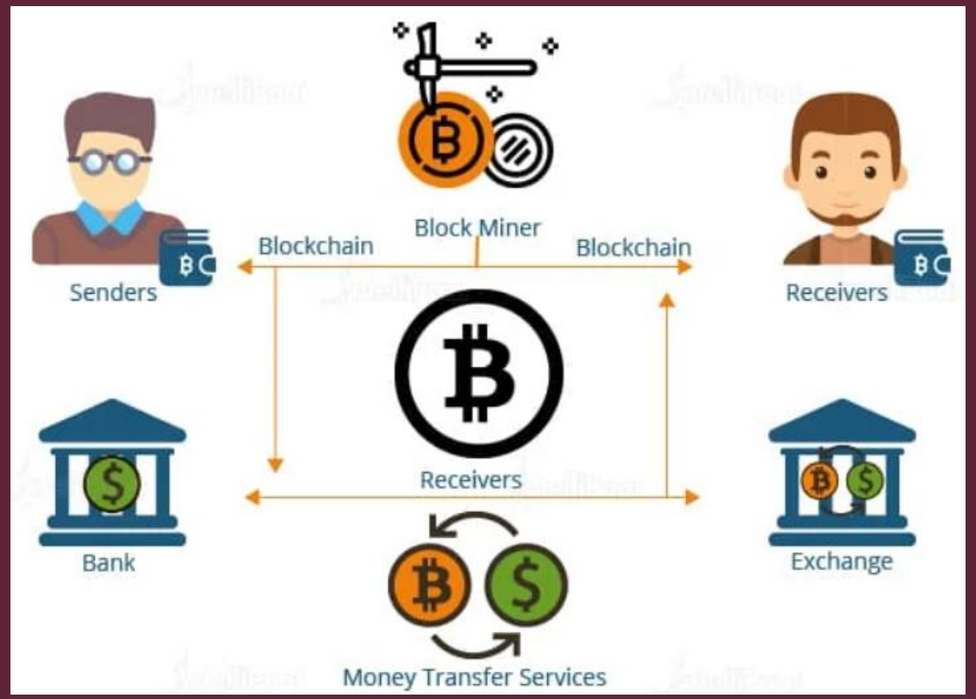
Bitcoin: Overview and Cryptographic Keys

Introduction To Bitcoin

- Bitcoin is the first real-world application of blockchain technology.
- **Decentralized Digital Currency:** Introduces the world's first fully decentralized digital currency with a secure and stable network.
- **Historical Foundations:**
  - Built on decades of research in cryptography, digital cash, and distributed computing.
- **Evolving Financial Landscape:**
  - Beyond just a currency, Bitcoin has inspired financial products like Bitcoin Futures on major exchanges.



Bitcoin Origin & Definition

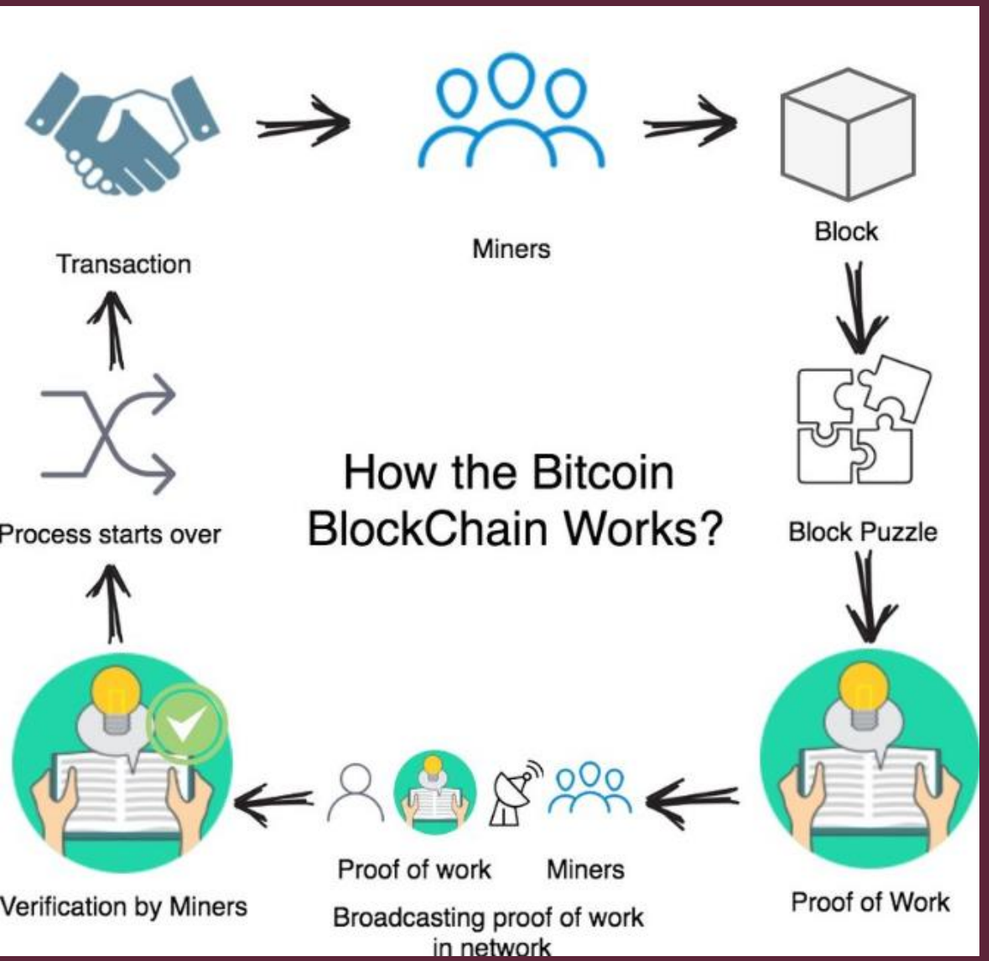
- In 2008, Bitcoin was introduced through a paper, Bitcoin: A Peer-to-Peer Electronic Cash System by **Satoshi Nakamoto.**

- The first key idea introduced in the paper was of a purely peer-to-peer electronic cash that does need an intermediary bank to transfer payments between peers.

- Ideas such as BitGold, B-money, hashcash, and cryptographic time stamping provided the foundations for bitcoin invention.

- Bitcoin is a combination of peer-to-peer network, protocols, software that facilitate the creation and usage of the digital currency named bitcoin. Nodes in this peer-to-peer network talk to each other using the Bitcoin protocol.

Bitcoin : A bird's-eye view



Let’s see how the Bitcoin network looks from a user's point of view.

The main components of a Bitcoin network are -

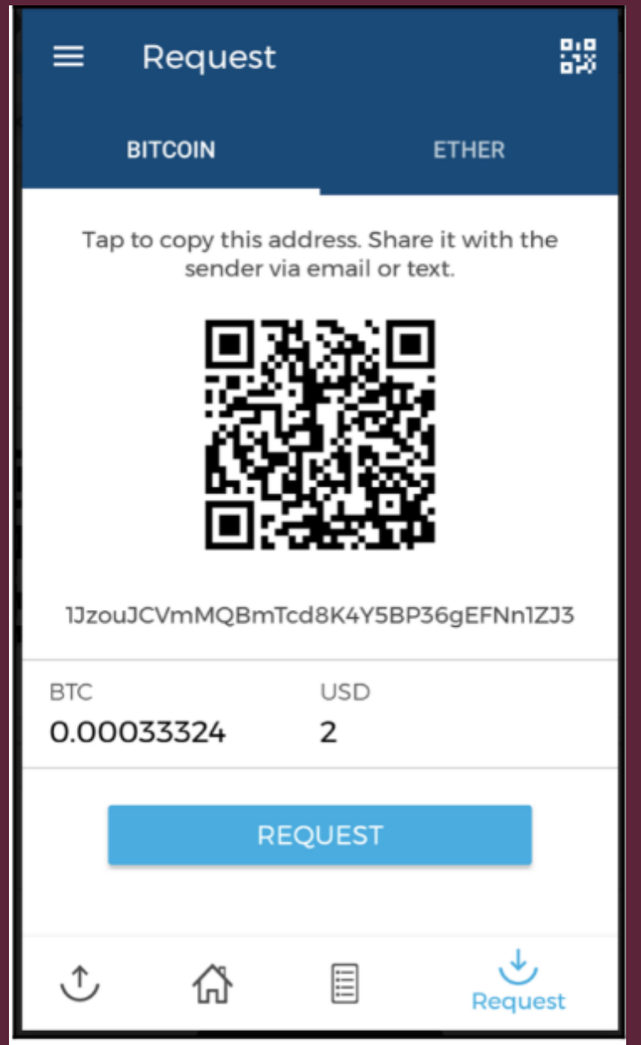
- Digital keys
- Addresses
- Transactions
- Blockchain
- Miners
- The Bitcoin network
- Wallets (client software)

Sending a payment to someone

This is an example of how money can be sent using Bitcoin network.There are several steps that are involved in this process.

1. First, the payment is initiated either when the recipient sends their Bitcoin address (via email, SMS etc) or when the sender starts the transfer. In both cases, the beneficiary's address is required.

1. The sender enters or scans a QR code with the receiver's address, amount, and description, which the wallet decodes into a payment prompt.



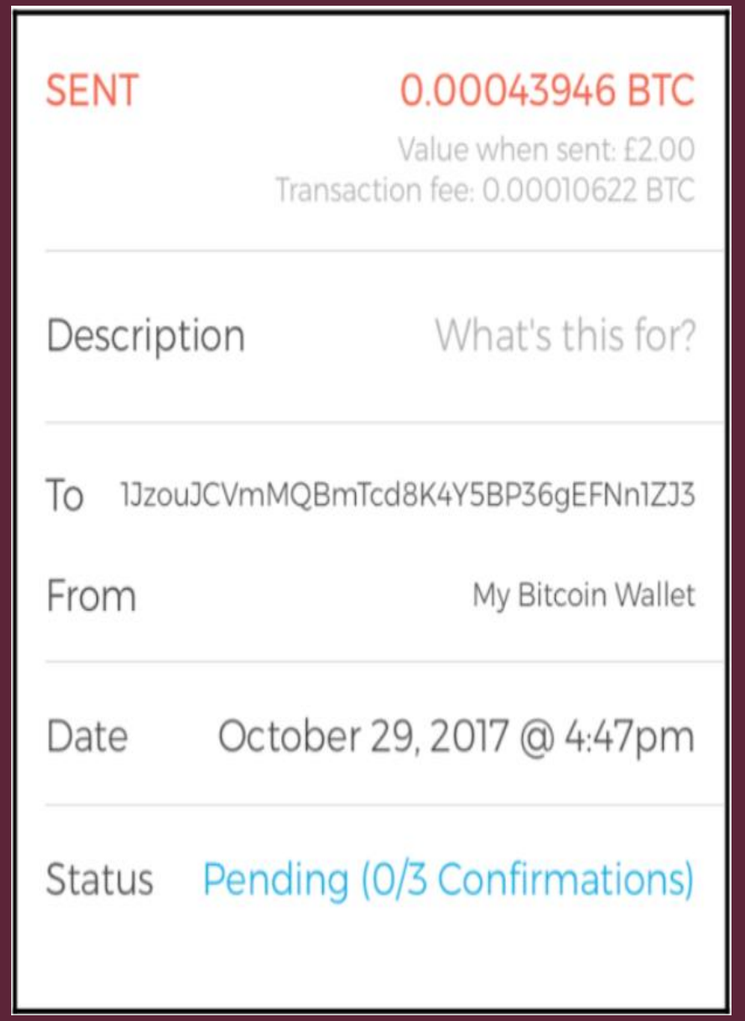
bitcoin payment request (using Blockchain wallet)

Sending a payment to someone

3. In the wallet application of the sender, this transaction is constructed by following some rules and broadcasted to the Bitcoin network. This transaction is digitally signed using the private key of the sender before broadcasting it.

4. Once the transaction is sent it will appear as shown here in the Blockchain wallet software.

5. At this stage, the transaction has been constructed, signed and sent out to the Bitcoin network. This transaction will be picked up by miners to be verified and included in the block.



Digital Keys - Private

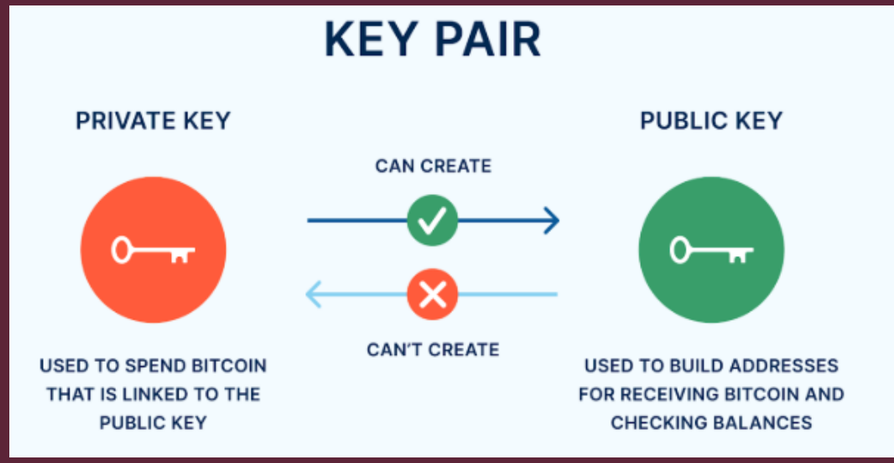
A Casascius physical bitcoin's security hologram paper with minikey and QR code

- A **Digital Key** is a cryptographic key (public or private) used for encrypting, decrypting, signing, or verifying data.
- Private keys are required to be kept safe and normally resides only on the owner's side.
- Private keys are used to digitally sign the transactions proving the ownership of the bitcoins.
- Private keys are fundamentally 256-bit numbers randomly chosen in the range specified by the secp256k1 ECDSA curve recommendation.

*Mini keys are private keys up to 30 characters, starting with 'S', used where space is limited, like physical bitcoins or QR codes. They’re more damage-resistant due to better error correction. Minikeys can be converted to full private keys, but not the other way around. Casascius bitcoins used this format.

Digital keys - Public

- Public keys are visible to all network participants. They are derived from private keys using ECC (secp256k1 standard).
- Public keys are used to verify transactions signed by corresponding private keys.
- Public keys are 256-bits, represented in compressed (33 bytes) or uncompressed (65 bytes) formats.
- Initially, Bitcoin client used uncompressed keys, but starting from Bitcoin core client 0.6, compressed keys are used as standard. This resulted in almost 50% reduction of space used to store public keys in the blockchain.



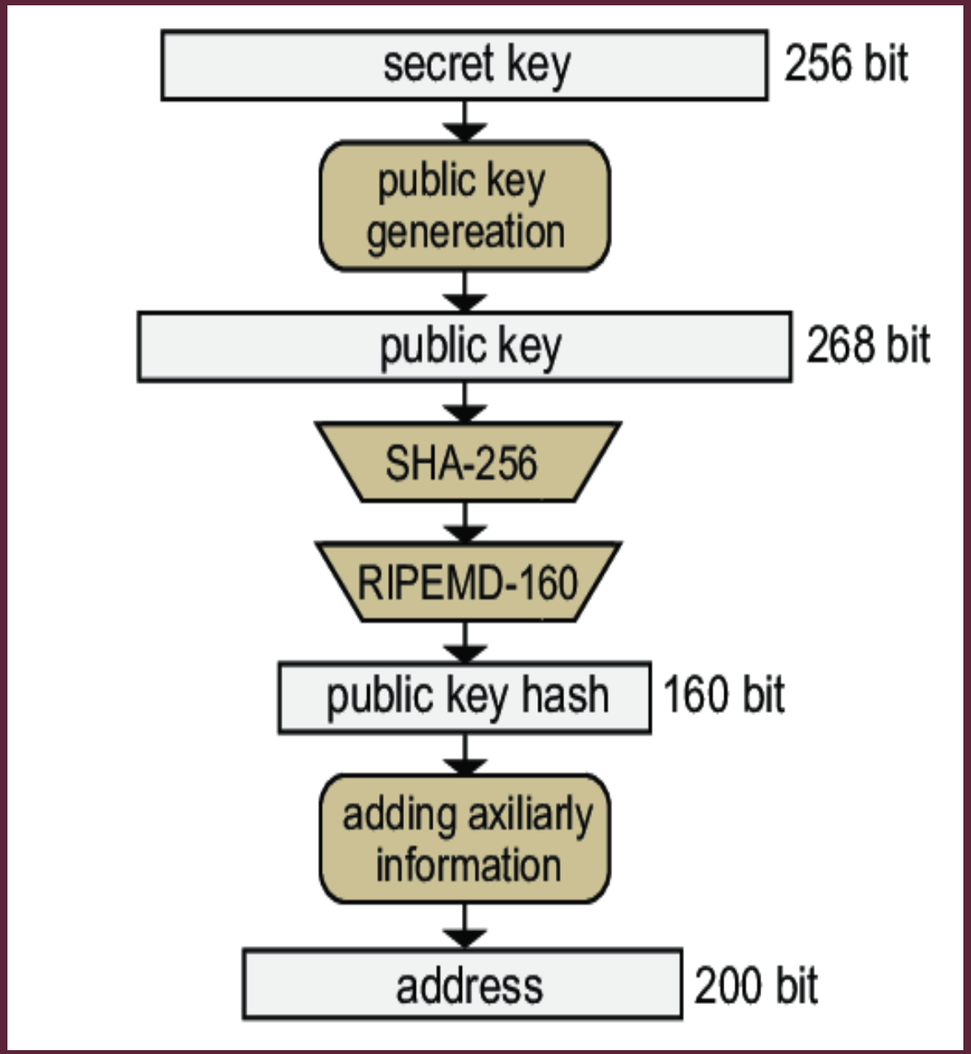
Addresses in Bitcoin

- A bitcoin address is created by taking the corresponding public key of a private key and hashing it twice, first with the SHA-256 algorithm and then with RIPEMD-160.
- The resultant 160-bit hash is then prefixed with a version number and finally encoded with a Base58Check encoding scheme.
- The bitcoin addresses are 26-35 characters long and begin with digit 1 or 3.
- A typical bitcoin address looks like a string shown here:

  1ANAguGG8bikEv2fYsTBnRUmx7QUcK58wt

Generating Address of a Bitcoin

- Randomly Generating Private Key
- Generating Public Key from Private Key
- Apply the SHA-256
- Appling RIPEMD-160 Hashing
- Adding Network Version Byte
- Compute the CheckSum
- Appending Checksum to Data



Base58Check encoding

- Bitcoin addresses are encoded using the Base58Check encoding. This encoding is used to limit the confusion between various characters, such as 0OIl as they can look the same in different fonts.
- The encoding basically takes the binary byte arrays and converts them into human-readable strings.
- This string is composed by utilizing a set of 58 alphanumeric symbols.

Vanity Address

A **vanity address** in Bitcoin is a personalized Bitcoin address that includes a specific, user-chosen pattern or characters, usually at the beginning of the address.

Vanity public address encoded in QR

Multisignature Address

- **Multisignature (Multisig) Addresses** in Bitcoin require multiple private keys to authorize a transaction instead of just one. This adds an extra layer of security and control.

- This is also known as M-of-N MultiSig. Here M represents threshold or the minimum number of signatures required from N number of keys to release the bitcoins.

Thank you!