BITCOIN

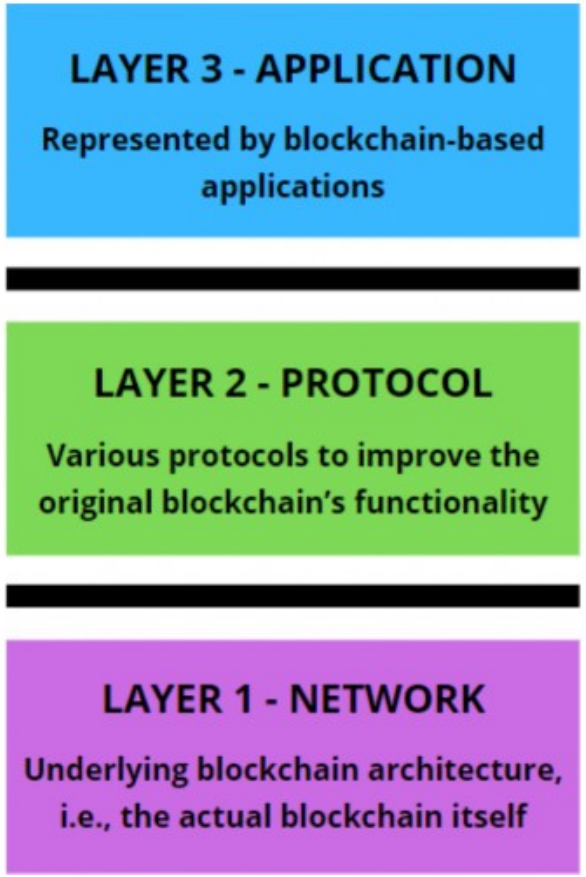
Bitcoin ?

- Bitcoin is a peer to peer electronic cash, a digital money that can be transferred between people or computers without any trusted middleman(such as a bank or government), and whose issuance is not under the control of any single party on which everyone trusts.
- Bitcoin tries to get rid of the requirement of trust by using cryptographic math to verify the facts and transactions.

Emergence of Bitcoin (BTC)

- Bitcoin was invented in 2008 by a person or group known by the false name of Satoshi Nakamoto.
- No one knows the identity of this individual.
- In the paper, Satoshi expressed dissatisfaction that banks repeatedly breached the trust of people who deposit money with them by lending the money in credit bubbles while keeping very little as a reserve.

Bit coin Architecture



Network Layer : is the fundamental BTC blockchain, complete with all of its essential parts and functionalities.
Layer 1 on Bitcoin consists of the real ledger of Bitcoin transactions, network nodes, and the Proof of Work block verification process (PoW). Layer 1 Bitcoin is, in essence, the actual BTC network as it was first presented in 2009.

- **Protocol Layer:** refers to protocols that are constructed on top of layer 1 with additional functionality.
- Faster processing times and less transaction costs are typically part of this added capabilities. The majority of layer 2 systems gain technical efficiency by processing the majority of transactions off-chain, and then sending the finished transactions in batch mode to the underlying layer 1 ledger.
- **Application Layer :** is a common designation. It is a layer where DApps and the protocols that make the apps possible are hosted. While other blockchains, like Ethereum or Solana (SOL), are well-suited to hosting layer 3 applications, Bitcoin is not.

Advantages of Bitcoin (BTC)

- **Bitcoin transactions don't incur banking fees**
  - No /minimum maintenance fees, deposit fees, and many others.
- **Bitcoin international payments include very low transaction cost**
  - No intrusion of government involvement and intermediary institutions.
  - Only exchange costs and fees are involved with foreign purchases and typical wire transfers.
  - Eradicates the annoyance of waiting times and customary authorization needs.
- **Transactions through bitcoin are secure and mobile**
  - Anyone with internet access can buy bitcoin from anywhere in the globe.
  - No personal information is required to finish any transaction, thus it decreases risk of identity theft.

Advantages of Bitcoin (BTC)

- **P2P and anonymous transactions**
  - Only by using a blockchain address can a transaction be identified, therefore it is not entirely anonymous.
  - Anyone on the network can send or receive payments from users anywhere in the world.
- **Security Against Payment Fraud**
  - It makes use of cryptographic protocols and an algorithm. They are therefore impossible to be forged.
- **Immediate settlement and direct transfer**
  - No involvement of a third party to facilitate the transactions.
- **Greater Liquidity**
  - In contrast to other crypto, bitcoin retains the majority of its value when converted to other real-world currencies.

1 BTC = 2,379,506.582493 INR Jul 25, 2023 01:22 UTC.

Bitcoin’s (Btc Price) Performance Over the Years

Bitcoin

- Bitcoin can be defined in various ways; it's a protocol, a digital currency, and a platform. It is a combination of peer-to-peer network, protocols, and software that facilitate the creation and usage of the **digital currency named bitcoin**.
- Double spending problem arises when, for example, a user sends coins to two different users at the same time and they are verified independently as valid transactions

Bitcoin: keys and addresses

- **Elliptic curve** cryptography is used to generate public and private key pairs in the Bitcoin network.
- The bitcoin address is created by taking the corresponding public key of a private key and hashing it twice, first with the SHA256 algorithm and then with RIPEMD160.
- 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

Bitcoin: keys and addresses

- Currently, there are two types of addresses,
  - P2PKH starting with 1
  - P2SH starting with 3
- In the early days, bitcoin used **direct Pay-to-Pubkey**, which is now superseded by P2PKH.
- However, direct Pay-to-Pubkey is still used in bitcoin for coin base addresses.
- Addresses **should not be used more than once**; otherwise, privacy and security issues can arise.
- Avoiding address reuse circumvents **anonymity issues** to an extent

Public keys in bitcoin

- In public key cryptography, public keys are generated from private keys.
- Bitcoin uses ECC based on the SECP256K1 standard. A private key is randomly selected and is 256-bit in length.
- Public keys can be presented in an uncompressed or compressed format.
- Public keys are basically *x and y coordinates on an* elliptic curve and in an uncompressed format and are presented with a prefix of 04 in a hexadecimal format. *X* and *Y coordinates are both 32-bit in length.*
- *In total, the* compressed public key is 33 bytes long as compared to 65 bytes in the uncompressed format.
- The compressed version of public keys basically includes only the *X part,* since the *Y part can be derived from it.*
- Keys are identified by various prefixes, described as follows:
  - Uncompressed public keys used 0x04 as the prefix
  - Compressed public key starts with 0x03 if the y 32-bit part of the public key is odd
  - Compressed public key starts with 0x02 if the y 32-bit part of the public key is even

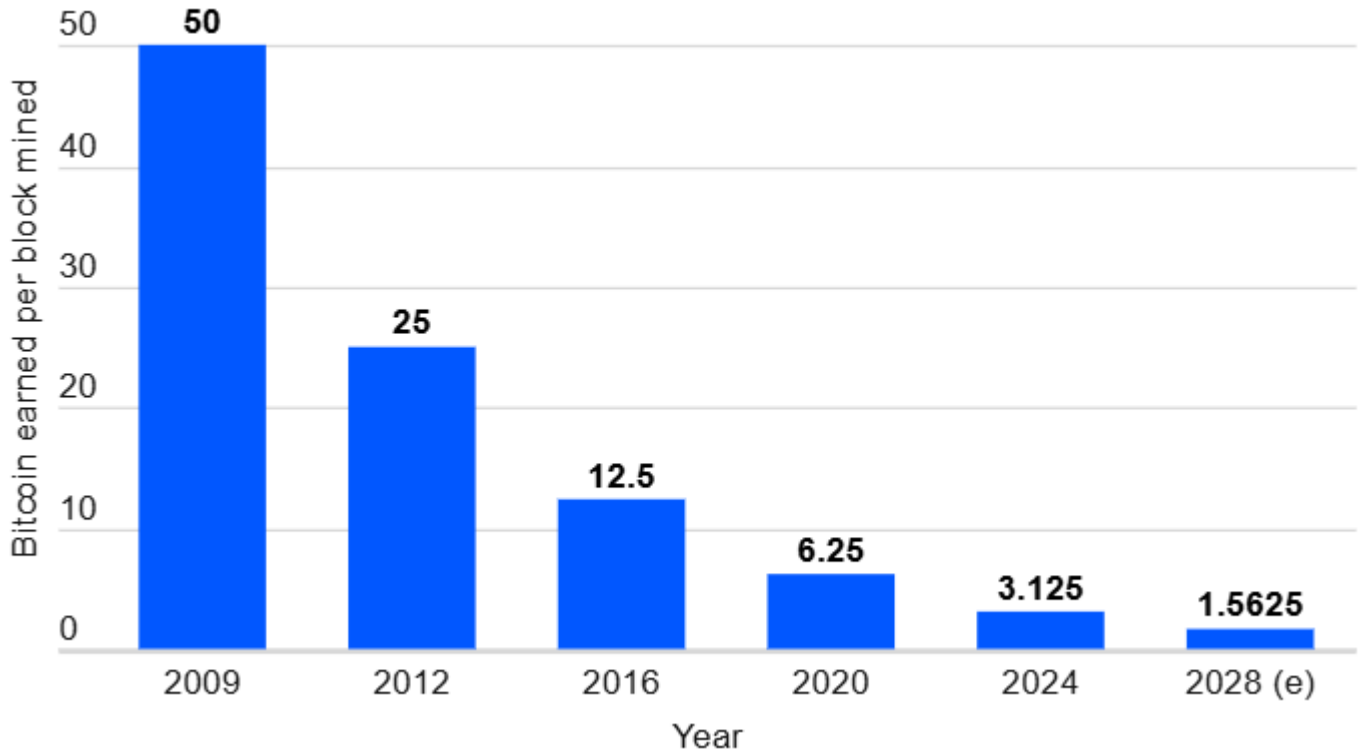
Private Keys in Bitcoin

- Private keys are basically 256-bit numbers chosen in the range specified by the SECP256K1 ECDSA recommendation. Any randomly chosen 256-bit number from 0x1 to 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE

  Eg. BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 is a valid private key.
- Private keys are usually encoded using **Wallet Import Format (WIF) in order to make them easier to copy and** use.
- WIF can be converted into private key and vice versa. **Mini Private Key Format is sometimes used to** encode the key in under 30 **characters** in order to allow storage where physical space is limited.
- 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 utlilizing a set of 58 alphanumeric symbols.

Bitcoin mining rewards over time

The reward for mining 1 block is halved every 210,000 blocks, or about every 4 years



Creation of Coins

- Units of cryptocurrency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins.
- Users can also buy the currencies from brokers, then store and spend them using cryptographic wallets.

How to buy cryptocurrency?

There are typically three steps involved. These are:

Step 1: Choosing a platform

The first step is deciding which platform to use. Generally, you can choose between a traditional broker or dedicated cryptocurrency exchange:

- **Traditional brokers.** These are online brokers who offer ways to buy and sell cryptocurrency, as well as other financial assets like stocks, bonds, and ETFs. These platforms tend to offer lower trading costs but fewer crypto features.
- **Cryptocurrency exchanges.** There are many cryptocurrency exchanges to choose from, each offering different cryptocurrencies, wallet storage, interest-bearing account options, and more. Many exchanges charge asset-based fees.
- When comparing different platforms, consider which cryptocurrencies are on offer, what fees they charge, their security features, storage and withdrawal options, and any educational resources.

Step 2: Funding your account

- The next step is to fund your account so you can begin trading.
- Most crypto exchanges allow users to purchase crypto using fiat (i.e., government-issued) currencies such as the US Dollar, the British Pound, or the Euro using their debit or credit cards – although this varies by platform.
- Crypto purchases with credit cards are considered risky, because cryptocurrencies are highly volatile, and it is not advisable to risk going into debt.

Step 3: Placing an order

Order via your broker's or exchange's web or mobile platform.

- **There are also other ways to invest in crypto.** These include payment services like PayPal, Cash App, and Venmo, which allow users to buy, sell, or hold cryptocurrencies. In addition, there are the following investment vehicles:
- **Bitcoin trusts:** You can buy shares of Bitcoin trusts with a regular brokerage account. These vehicles give retail investors exposure to crypto through the stock market.
- **Bitcoin mutual funds:** There are Bitcoin ETFs and Bitcoin mutual funds to choose from.
- **Blockchain stocks or ETFs:** You can also indirectly invest in crypto through blockchain companies that specialize in the technology behind crypto and crypto transactions. Alternatively, you can buy stocks or ETFs of companies that use blockchain technology.