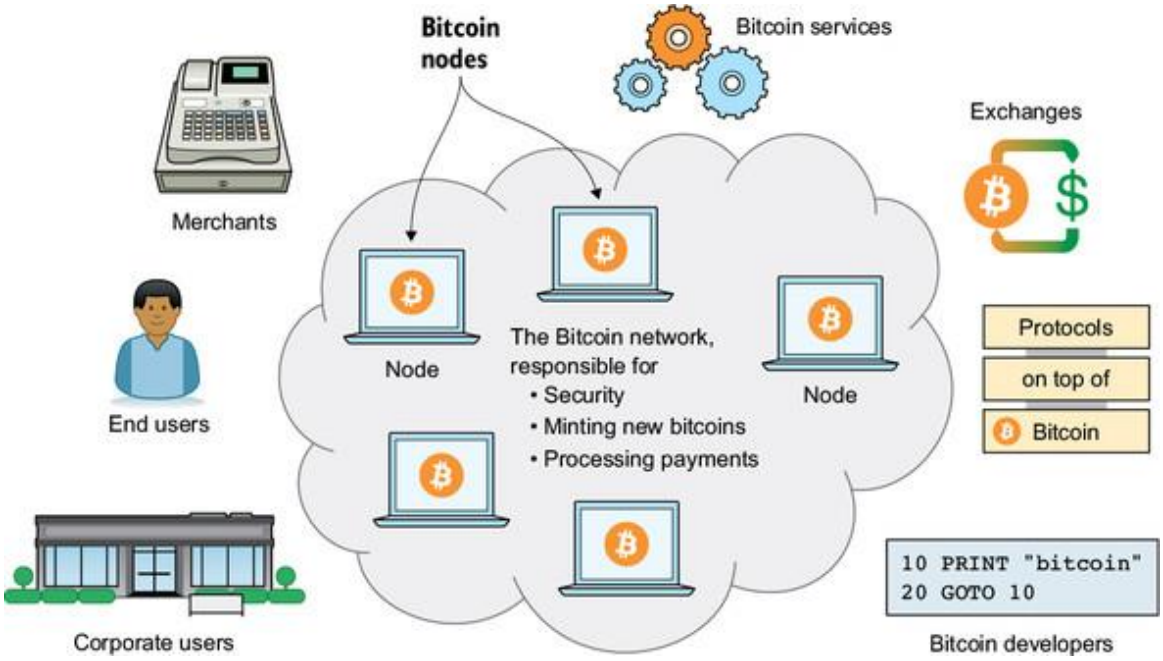
MODULE 4

Introduction to Bitcoin

Bitcoin is a digital cash system. It allows for people to move bitcoins, the currency unit of Bitcoin, between each other without using a bank or any other trusted third party. It resembles traditional bank notes and coins, but it's purely digital and used over the internet. The Bitcoin currency isn't tied to any specific fiat currency like the US dollar. It has free-floating exchange rates against most fiat currencies. You can buy and sell bitcoins for fiat currencies online using one of several exchanges, such as kraken.com, bitstamp.net, or localbitcoins.com.

No government or company controls Bitcoin. Instead, thousands of computers around the globe—the Bitcoin network, collectively keep the system working 24/7. You don't need to register or sign up anywhere to use Bitcoin, you just need internet access and a computer program, like a mobile app, to use it.



Bitcoin network and its ecosystem

Anyone can use or participate in the Bitcoin network without special permission from a bank or similar institution. It is permission less in nature. We can roughly categorize participants in this Bitcoin ecosystem into several groups:

End users—People using Bitcoin for their day-to-day needs, such as savings, shopping, speculation, or salaries

Corporate users—Companies using Bitcoin to solve their business needs, such as paying wages internationally, or use cases similar to those of end users

Merchants—For example, a restaurant or a bookstore accepting Bitcoin payments

Bitcoin services—Companies providing Bitcoin-related services to customers, such as topping up mobile phones, anonymization services, remittance services, or tipping services

Exchanges—Commercial services people can use to exchange their local currency to and from bitcoins

Protocols on top—Systems that operate "on top" of Bitcoin to perform certain tasks, such as payment network protocols, specialized tokens, and decentralized exchanges

Bitcoin developers—People working, often for free, with the open source computer programs that participants of the Bitcoin network use

The Bitcoin network's job is to process Bitcoin payments, secure the ledger of who owns what from unauthorized modifications, and get new bitcoins into circulation at the predetermined rate. The network consists of thousands of computers around the world. We call these computers Bitcoin nodes, or just nodes. Any of the actors mentioned previously can also participate actively in the Bitcoin network by running their own Bitcoin node. You must run your own node if you don't want to trust others to provide you with correct financial information.

Bitcoin consists of the following four key concepts:

- Distributed
- Disintermediated
- Decentralized
- Trustless

i. Distributed

The whole Bitcoin network runs on a particular network of many distributed computers & they share the same workload. It consists of many distributed computers because it is always better to distribute the workload with multiple computers instead of doing all the work on a single centralized computer. In a distributed computer network, the workload is distributed across all the computers. There is no single point mistake or failure & thus, the distributed network becomes more reliable when compared to a single centralized computer.

ii. Disintermediated

When someone sends money online over the internet, we require a third party to connect or link our bank, which will internally manage all the transactions. But in the case of Bitcoin, you don't require any third party to link the bank; in Bitcoin, you are doing the transactions directly to the other party over the network or internet. The network connection confirms that the transaction is valid and verifies if there was a true transfer between the two parties. This concept or process is called Disintermediated.

iii. Trustless

There is no need for any third party in Bitcoin & that's why it is Trustless; it doesn't require any bank to certify or verify the transaction process. In Bitcoin, it uses Distributed Trustless Consensus, which verifies all the nodes accept & agree that a transaction has taken place. This enables all the transactions that have taken place in the Bitcoin.

iv. Decentralized

Decentralized means there is no central repository of data, no management in between overseeing what Bitcoin is doing & there is no central control in Bitcoin. Because of this, there is no single point of failure or central point of failure. That's the reason Bitcoin is decentralized.

Some other features of Bitcoin that make it a unique asset class-

- Censorship resistant

As we know, Bitcoin is decentralized, and Bitcoin is censorship resistant means it is not under any corporate or government entity. This aspect makes Bitcoin very unique from the others. But as we know, Bitcoin is decentralized, and the digital existence of Bitcoin means one can have access to the network, and this access cannot be restricted.

- **Hard Capped**

Bitcoin ensures that it never crosses twenty-one million BTC. This makes Bitcoin limited in supply. Every four years, there is a halving rule applicable in Bitcoin, which is why BTC is still valuable. This is why Bitcoin is called Hard Capped & this is a very important aspect that differentiates Bitcoin from others.

- Immutable

Bitcoin is known as immutable because the blockchain tech used in Bitcoin is immutable. Every transaction done in Bitcoin is stored or collected in a block, and that block is linked to the earlier blocks of transactions.

- **Network Effects**

Bitcoin's value is increasing daily and has become a mainstream investing asset. The ubiquity and value make Bitcoin even more valuable.

Merits and Demerits of Bitcoin

Advantages

1. Store of value

Earning the title of 'digital gold', bitcoin is now accepted as a store of value by many sophisticated investors. As you're probably aware, a store of value is a commodity, asset, or currency that keeps its value over a long period of time — a trait that's especially important during inflationary times.

2. Outsized returns

Bitcoin has been the best performing asset class of the last decade. It even outperformed the second-best performing asset class, the NASDAQ 100, by an order of magnitude. Even small investments have generated outstanding returns for long-term investors.

3. Self-custody

Individuals can self-custody cryptocurrencies like bitcoin. You don't need to rely on a bank, legal documents, or a single entity to take complete ownership of your assets. This makes an incredible impact in countries across the globe without strong property rights, giving individuals more control over their future.

4. Decentralised

Bitcoin is the most decentralised cryptocurrency. What does that mean? It means that the Bitcoin network is distributed across many different computers, known as nodes. Decentralisation is so important because it prevents a single point of failure to attack, making it almost impossible for any organisation or government to take down the network. Notably, Bitcoin was the first ever protocol to solve the Byzantine Generals problem and create a decentralised network with a

shared consensus and that invention gave way to every cryptocurrency that followed, including Ethereum, Litecoin, Dogecoin and Polkadot.

5. Permissionless

Anyone can access the Bitcoin network. It doesn't matter where you live or how much money you have, it's an open peer-to-peer network that everyone can use.

6. Secure

Bitcoin is incredibly secure. Its public key cryptography makes sure every transaction is authentic. Its decentralisation means no centralised power can manipulate it for their benefit. And its irreversibility means nobody can go back and change the data.

7. 24/7

Unlike traditional financial markets, bitcoin doesn't close in the afternoon or over the entire weekend. Bitcoin is tradeable 24/7, 365 days per year. Not to mention, sending bitcoin is faster than a bank transfer. While remittance payments to family overseas can take days, people can send and receive bitcoin in 10 minutes to an hour.

8. Fixed supply

Unlike fiat currencies like the US dollar, governments cannot print bitcoin whenever they want more money. There will only ever be 21 million bitcoins. The importance of that scarcity is highlighted in the stock-to-flow model.

9. Divisible

Each bitcoin is divisible into 100,000,000 satoshis (or sats for short). That means you can use bitcoin to pay for a cup of coffee, for micro-payments online, and 'stack sats' with as little as $10. Being able to use fractions of a bitcoin can make it the peer-to-peer digital currency that it was always intended to be.

10. Inflation hedge

Many sophisticated investors see bitcoin as an inflation hedge who said it's a better inflation hedge than gold. With ongoing money printing from central banks across the world, more and more investors are turning to bitcoin as an inflation hedge.

Disadvantages

1. Volatility

Bitcoin is highly volatile compared to other assets like property. While that's to be expected with any fast-growing asset, and has been a boon for traders, it can be hard at times for long-term investors. As always, risk management is critical in such a market.

2. Competitors

While bitcoin remains the dominant cryptocurrency (with a market cap double the next biggest cryptocurrency), there are more and more coins being created every day. And while it holds the dominant position, other competitors like Ethereum are designing their monetary policy to be more competitive with bitcoin.

3. Awareness

While bitcoin is now being covered by the biggest media companies in the world, there are still many people who aren't aware of it or why it's so transformative to society. For example, while many people are aware that it has been a successful asset to generate wealth with, they don't recognise how it can empower unbanked communities.

4. Learning curve

There's a steep learning curve to fully understand bitcoin, and that can be daunting to beginner investors. Luckily, there are guides that explain what bitcoin is. More and more investors are educating themselves every day.

5. Energy concerns

Bitcoin's proof-of-work consensus system uses energy to help secure the network, with miners running specialised computers and burning energy. While more and more miners are switching to renewable energy and helping drive the green revolution, this wasn't a big focus in bitcoin's early history.

6. Transactions Per Second

Other blockchain networks like Solana and Avalanche operate with much higher Transactions Per Second (TPS) than bitcoin, making them more suitable for high throughput applications. While bitcoin is the dominant store of value in crypto, other blockchains can be better for different use cases.

Fork and Segwit

i. Blockchain Fork

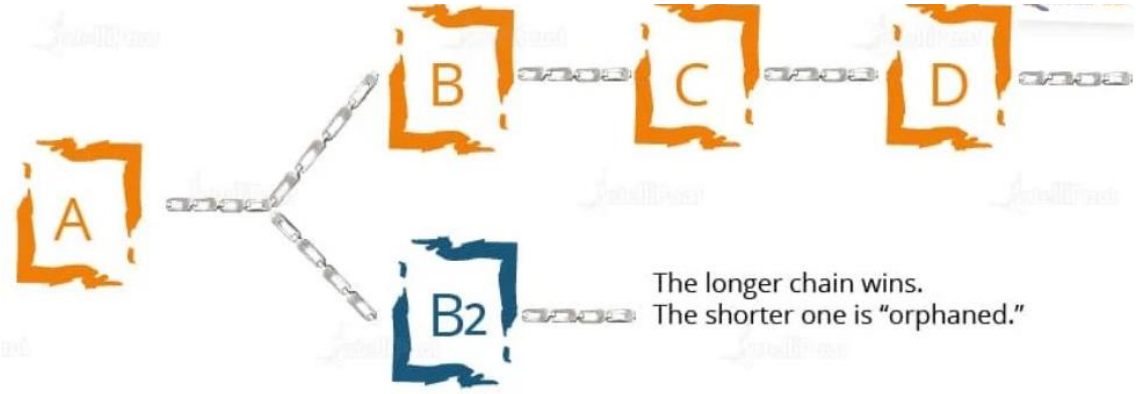
A fork is a **change to the blockchain protocol.** It is essentially a divergence from the previous version of blockchain.

There are three major reasons why blockchain forks occur:

- Adding new functionalities
- Fixing security issues
- Reversing transactions

The decentralized nature of public blockchains means that the participants on the network must be able to come to an agreement as to the shared state of the blockchain. The unanimous consensus among the network nodes results in a single blockchain that contains verified data that the network asserts to be correct. However, many times, the nodes in the network cannot come to a unanimous consensus regarding the future state of the blockchain. This event leads to forks, meaning that it leads to a point in which the ideal single chain of blocks is split into two or more chains, that are all valid.

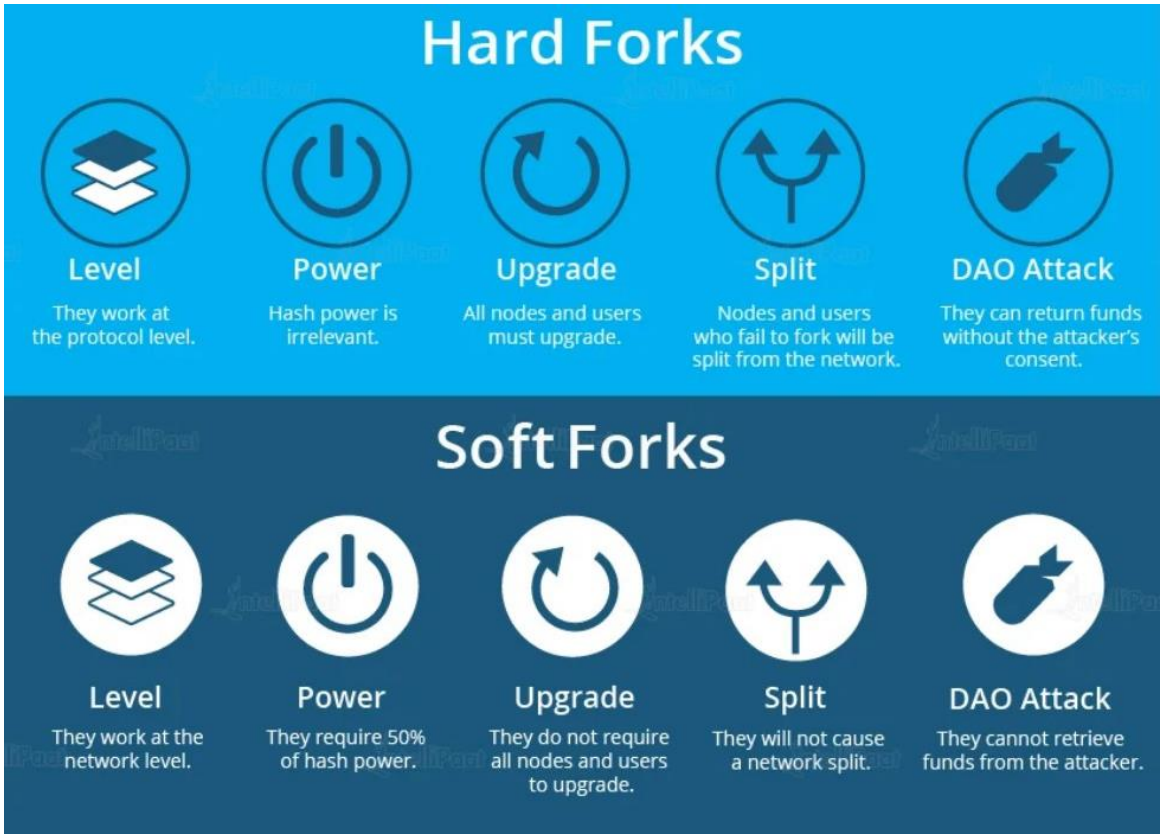
When an upgrade is made to a blockchain's underlying protocol leading to Fork, depending on the severity of the changes made in the upgrade, miners (those that operate nodes, validate transactions and add new blocks to the chain) can choose or not choose to also upgrade their nodes' software to implement those changes. If the changes to the protocol are minor (e.g adding small features or improvements to the existing protocol) then the majority of miners will often opt-in to this change by upgrading their nodes and continuing to validate transactions as normal.



Types of Forks

There are two types of forks:

- Hard forks
- Soft forks



Hard Forks

When there is a change in the software that runs on full nodes to function as a network participant, the new blocks mined based on the new rules in the blockchain protocol are not considered valid by the old version of the software. When hard forks occur, new currency comes into existence. An equivalent quantity of currency is distributed to the full nodes that choose to upgrade their software so that no material loss occurs. The final decision to join which chain rests with the full nodes. If the full nodes choose to join with the new chain, the software is upgraded

to make newer transactions valid, while the nodes that do not choose to upgrade their software continue to work the way they used to work.

Example: Suppose, there is a new update in the Ethereum Blockchain in which the consensus protocol will change from a type of proof-of-work to a type of proof-of-stake. The full nodes that install the update will use the new consensus protocol, and the ones that do not choose to install the update will become incompatible in the blockchain.

Soft Forks

When there is a change in the software that runs on full nodes to function as a network participant, new blocks are mined based on new rules in the blockchain protocol and are also considered valid by the old version of the software. This feature is also called backward compatibility.

Example: Suppose, there is a new update in the Ethereum blockchain in which the consensus protocol will change from a type of proof-of-work to a type of proof-of-stake. The full nodes that will install the update will use the new consensus protocol, and the ones that choose not to install the update will still stay compatible with the other nodes in the blockchain.

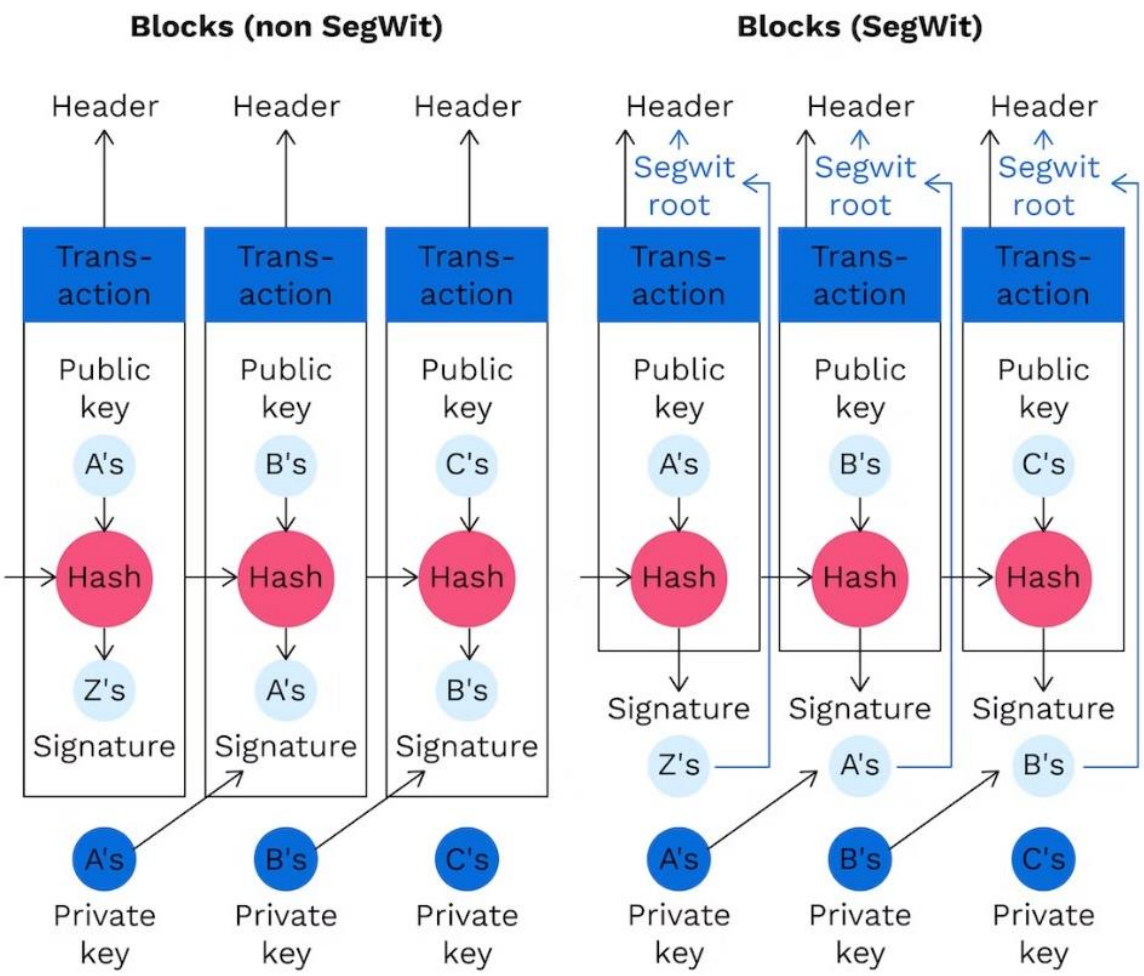
ii. SegWit

SegWit was an update to the Bitcoin protocol and stands for “segregated witness consensus layer”, a technological feature created to optimise transactions in 2015. SegWit is a change in Bitcoin’s protocol. SegWit was pushed through in a soft fork of the original Bitcoin network. Presently, SegWit is a scaling solution used by several different cryptocurrency networks including Litecoin.

The main purpose of SegWit is to improve transaction throughput on a blockchain network. It is worth noting that the first cryptocurrency to implement the SegWit layer was not Bitcoin, but Litecoin.

In essence, SegWit reduces the weight of transactions in a block on the blockchain by segregating a transaction into two sections; effectively increasing the amount of transactions one can include in a block of the same size. The first part of a transaction contains the wallet addresses of the sender and receiver and the second part contains the “witness data” containing transaction signatures. SegWit removes the “witness data” from the main block, therefore notably reducing transaction size. The transactions consequently require less space, enabling more transactions per block and greatly increasing the capacity of the Bitcoin network.

Further, SegWit provided the fix to a flaw in the Bitcoin protocol which let users change transaction hashes of transactions. The change of just one character in a digital signature results in an entirely different transaction hash. As the signature is moved out of the transaction data into the segregated witness data, it is no longer possible to change the transaction ID. Consequently, SegWit is a solution to transaction malleability.



SegWit and Block Size

Advantages: SegWit is a feature of the Bitcoin protocol that has now been adopted by most Bitcoin-based services. Users of Bitcoin and cryptocurrency exchanges can easily verify with a quick Google search, that the exchange they are using supports SegWit transactions. However, SegWit's benefit to Bitcoin goes beyond simply making blocks smaller and making the network faster.

Disadvantages: Despite the fact that SegWit transaction adoption in the Bitcoin network is increasing and reached an all-time high of more than 65% at the beginning of 2020, possible adaptations of the Bitcoin network take a much longer. On the other hand, not everyone supports SegWit transactions.

Sending and Receiving Bitcoins

Sending and receiving bitcoin is one of the core building blocks of any bitcoin application. Sending and receiving bitcoins securely over the internet gives you a bitcoin value. To send and receive bitcoin, you need to have a wallet where you need to put the public address of the sender and recipient. The process of sending and receiving bitcoin can differ between wallet to wallet, but the general steps are given below.

Step-1 Log-in into your wallet.

Step-2 Go to Send and Receive icon.

Step-3 Choose whether you want to send or receive bitcoin.

Step-4 Send bitcoin: Enter the public address of the recipient and choose the amount which you want to send. Once you decide the amount, confirm the amount to avoid mistakes, then click on send transaction, and verify the transaction one last time for confirming your public address and sender's public address.

Step-5 Receive bitcoin: To receive bitcoin, you need to share your public wallet address with the sender. You can also do this by letting them scan a QR code.

For example, Alice wants to send five bitcoins to Ben. She is sending five bitcoins because she may have bought a product or paying him for services. For sending those five bitcoins, Alice needs to have five bitcoins in her wallet, and can also be able to receive bitcoins in her wallet. Now she could have bought bitcoins, or she could have received bitcoins as payment. Here, we are assuming that Alice has 20 bitcoins in her wallet. When the wallet is created, it assigns two keys. One is the public key which is used to receive bitcoins. And second is the private key which is used to sign and authorize to send or spend those bitcoins to other people. We know that Alice has the private key to her wallet, so she is able to spend those bitcoins.

Ben can receive five bitcoins if he has a wallet of his own, which allows him to get bitcoins from anyone else. Ben also has a private key for his wallet that will enable him to spend those bitcoins that he has in his wallet. Ben's private key is completely different from Alice's private key. Now, if Ben wants to receive five bitcoins from Alice, he needs to provide his Bitcoin address to Alice. The bitcoin address is used for receiving money, which is a hashed version of the public key. Ben has the option to generate a new bitcoin address for every single transaction if he wants. Creating the new bitcoin address for every transaction is a good security recommendation in terms of privacy. Ben can share his bitcoin address in two ways. He can share an alphanumeric code which starts with the number one and ends in the letter H, and another one is the QR code. The alphanumeric code is always different for every single bitcoin address, and these addresses are typically between 26 to 35 characters in length. The bitcoin address which you see numerically is the Ben address used to receive bitcoins from Alice.

Now, when Alice sends the five bitcoins to that address, she creates a transaction. She is able to do this transaction because she can access the private key and can authorize to transfer five bitcoins on Ben's bitcoin address. So, a new transaction shows that from Alice's wallet, five bitcoins are being sent to Ben's wallet. The transaction at that point gets sent out into the network, and the miners begin mining blocks. When the first block comes in and includes that transaction in it, then the transaction is said to be confirmed.

All transactions must pay a fee to be included in the blockchain. The fee rate determines how quickly your transaction will be confirmed, and it is measured in satoshis per byte of data in the transaction or sats/vByte. There are a number of factors which determine the speed at which a transaction settles on the blockchain, including traffic on the network and the fee rate set by the user. Typically, a Bitcoin transaction takes anywhere from 10 minutes to several hours to clear.

Most wallets allow the user to determine the fee rate, so, if you need a transaction to clear quickly, you should pay a higher fee. On the other hand, if you are comfortable waiting a few days or weeks

for a transaction to clear, you can pay a low fee. The lowest fee rate possible is 1 sat/vByte. A vByte is a unit of measure for the weight of blocks and transactions. The vByte was introduced by the SegWit upgrade. A vByte is equivalent to 4 weight units, and thus, a block is limited to being 1 vMegabyte large, or 4 million weight units.

Choosing Bitcoin Wallet

To select a reliable Bitcoin wallet, one should judge it based on the following criteria:

- Hot/Cold Wallet: Whether a wallet is a hot(Online storage) or cold(offline storage).
- Control private keys: A wallet where you own and control your keys.
- Backup & security features: Here, you can seed backup keys and pin codes.
- Developer community: It has an active development community for maintenance.
- Compatibility: It can be compatible with different operating systems.
- HD Wallet: It is a wallet that generates new addresses itself.
- KYC: A wallet that doesn't require KYC.

There are different types of wallets that we can choose from.

Mobile wallet

In the mobile wallet, you can run any type of application, whether it is on Android, iOS, Windows, or even on Blackberry. They are significantly smaller and simpler and serve as a convenient on-the-go wallet for daily usage. Popular Mobile wallets are Bitpay, BTC.com, Edge, Electrum, Mycelium, Bitcoin Wallet, etc.

Desktop wallet

In the desktop wallet, you can run it on your desktop or laptop computer for Windows, Mac, and Linux. Generally, they are secure, but sometimes they are vulnerable to various malware and computer viruses. Popular Desktop wallets are Bitcoin Core, Bitcoin Knots, mSIGNA, Armory, etc.

Hardware wallet

In a hardware wallet, there are devices which contain your private keys. The hardware wallets are the most secure wallets, but it will also cost money. Popular hardware wallets are BitBox, Keepkey, Trezor, Ledger Nano S, etc.

Web wallet

The web wallets are online wallets that are considered less secure than other types of wallets, yet they can be highly convenient. Popular web wallets are Guarda, Coinbase, GreenAddress, Binance, etc.

There are multiple different wallet options available. It is not necessary to have only one wallet. You can have multiple wallets for different needs. It helps you to spread the risk by not keeping all of your personal crypto's in one location but across different locations(wallets). You can create a wallet in any of these options that you find. You can also open up another wallet elsewhere and can send coins to a different wallet.

Converting Bitcoins to Fiat Currency

Bitcoin is basically a cryptocurrency that is stored in a virtual wallet. It is a digital currency that is currently used as a form of payment. The transactions related to bitcoins take place in the blockchain network. Every bitcoin is stored in a virtual wallet and the transaction involves the transfer of bitcoin from one wallet to another. Bitcoins can be sent from peer to peer irrespective of geographical location without any mediator in between. It works in a decentralized way, meaning nobody can interfere with the digital money, only the concerned person is responsible for the bitcoins.

Fiat currency is the currency that is issued by the government. In other terms, it is the cash, coins we generally have, that is the physical form of currency. Fiat currency ranges from USD, EUR, INR, etc.

There are lots of reasons why one might want to exchange Bitcoin for fiat currency:

- To get a profit from the favourable market conditions like bull run on bitcoins price.
- Get more flexibility with the money.
- Fiat currency is the most common form of currency worldwide.
- Pay a bill.

There are many ways to convert bitcoin to fiat currency. The methods are listed below-

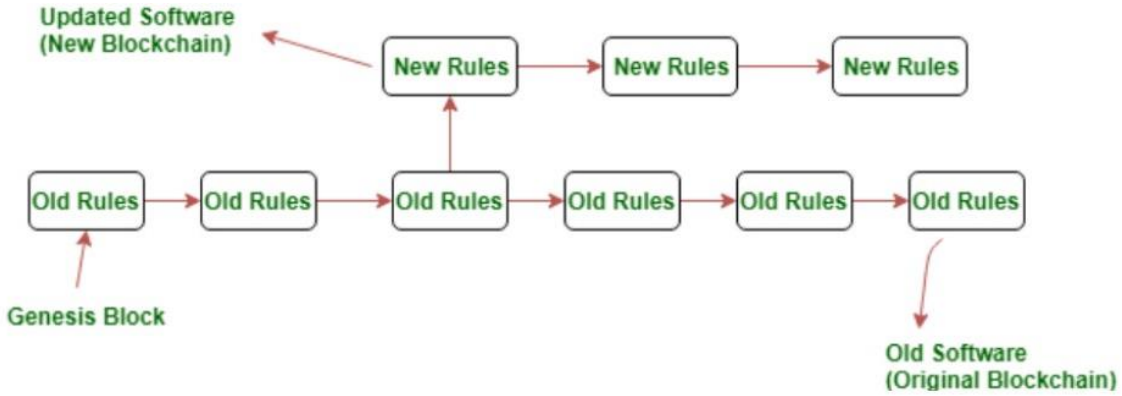
- **Cryptocurrency Exchanges:** This is the most widely used method to convert bitcoin to fiat currency. It is similar to a money exchange center which is needed when a person moves from one country to another. Cryptocurrency exchanges basically convert your cryptocurrency that is bitcoin into your local currency such as rupees, US dollars, euros. The main disadvantage of this method is the delay in withdrawing fiat currency even after completing the transaction. Cryptocurrency Exchanges have an inbuilt crypto converter feature that displays how much fiat currency one could get with the bitcoins that person has. There are multiple exchanges available like Gemini, coinbase, binance, etc. This has a user-friendly interface that eases the whole process of bitcoin conversion. During bull run time, these exchanges are affected negatively and face technical difficulties. Coinbase seems a suitable option as it has improved over its downtime problem by increasing the infrastructure capability. Coinbase exchange sends the converted fiat money directly into your bank account without much hassle.
- **Bitcoin Debit Card:** Possessing a Bitcoin Debit Card is the fastest way to convert bitcoin to cash or fiat currency. The online website is provided as a user interface where the user deposits the bitcoins and the website automatically converts those into required fiat currency. Bitcoin debit cards are used wherever debit cards are accepted, the only difference being, funds are transferred from a crypto wallet rather than from a bank account. The main disadvantage is the providers of Bitcoin debit cards takes transaction charge on every purchase and also limits the total amount of transaction per debit card.in order to register for the Bitcoin debit cards, one needs to go to the bank and do KYC.
- **Peer-to-Peer Exchanges:** It is known that bitcoin doesn't have any centralized authority, therefore any fund can be transferred from one peer to another. This basically involves finding a buyer who will buy your bitcoins and in return, would give cash for that. But one thing to be noted is that transactions in bitcoins are irreversible. So, choose a trustworthy buyer on whom you are sure of getting the cash after a bitcoin transaction.
- **Bitcoin ATMs:** It is also known as a Bitcoin Teller Machine (similar to ATM). BTM acts similar to an ATM, allowing to withdraw cash. QR code and added security features like text messages are there to ensure smooth and secure transactions. BTMs allow you to buy as well as sell bitcoins.it provides a very fast and convenient way to take cash out of

a bitcoin wallet. BTMs are available in developed cities of the world and more are under construction after the boom of the digital currency era. The drawback of BTMs is they charge a heavy amount on conversion and also sets a maximum transaction limit.

- **Metal Pay:** It is a money transfer app that allows cryptocurrency holders to cash out. The need for this app is to complete KYC before filling up the bank details. After filling in bank details, the customer can buy, sell, send, receive as well as convert cryptocurrencies. Metal pay has the capability to convert at least 24 cryptocurrencies including bitcoins.

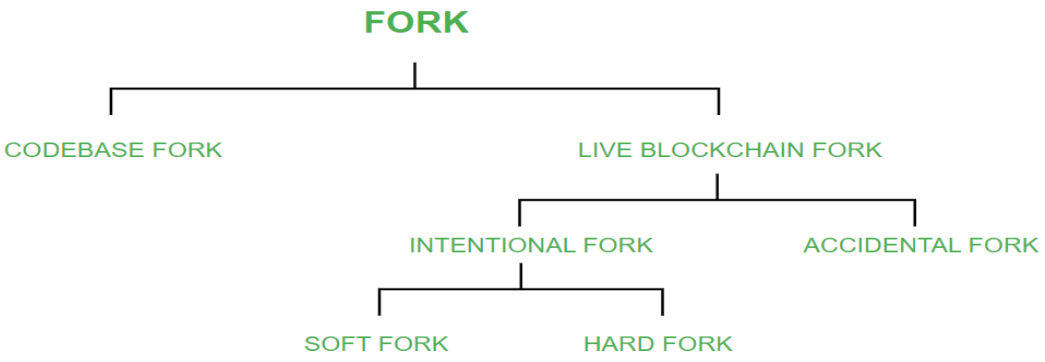
More understanding about Forks

In simple terms, Forks in blockchain means copying the code and modifying it to create a new software or product. In open-source projects, Forks are very common and used widely. So, cryptocurrencies like Ethereum and Bitcoin are decentralized and open software so that anyone can contribute. As they are open-sources they rely on their communities to make the software more secure and reliable. Also open source with the help of fork can make user interface more interactive and look good, helping in gaining more users worldwide. In open source, the code is visible to everyone, anyone can modify, edit, and access it. There are no copyright claims for such actions.



Example of Blockchain Fork

i. More specific categorization of Forks



Basically forks are divided into two categories i.e. Codebase Fork and Live Blockchain Fork. And then Live Blockchain Fork is divided into further two parts i.e. Intentional Fork and Accidental Fork,

as you can see in the above mentioned figure. The Intentional fork is then further divided into two parts i.e. Soft Fork and Hard Fork.

TYPES OF FORKS:

CODEBASE FORK: In codebase blockchain fork you can copy the entire code of a particular software. Let us take BITCOIN as an example. Suppose you copied the whole blockchain code and modified it according to your need, say that you decreased the block creation time, made some crucial changes and created a faster software than BITCOIN and want to publish / launch. In these ways, a new BLOCKCHAIN will be created from an empty blank ledger. It's a fact that many of these ALT COINS which are now running on the blockchain have been made in this way only by using the codebase fork i.e. they have made little changes in the code of BITCOIN and created their whole new ALT COIN.

LIVE BLOCKCHAIN FORK: Live Blockchain fork means a running blockchain is been divided further into two parts or two ways. In live blockchain, at a specific page the software is same and from that specific point the chain is divided into two parts. So in context to this fork the Live Blockchain Fork can occur because of two reasons:

- **ACCIDENTAL FORK / TEMPORARY FORK:** When multiple miners mine a new block at nearly the same time, the entire network may not agree on the choice of the new block. Some can accept the block mined by one party, leading to a different chain of blocks from that point onward while others can agree on the other alternatives (of blocks) available. Such a situation arises because it takes some finite time for the information to propagate in the entire blockchain network and hence conflicted opinions can exist regarding the chronological order of events. In this fork, two or more blocks have the same block height. Temporary forks resolve themselves eventually when one of the chain dies out (gets orphaned) because majority of the full nodes choose the other chain to add new blocks to and sync with.
  Example: Temporary forks happen more often than not and a usual event that triggers this fork is mining of a block by more than one party at nearly the same time.

- **INTENTIONAL FORK:** In intentional fork the rules of the blockchain are changed, knowing the code of the software and by modifying it intentionally. This gives rise to two types of forks which can occur based on the backwards-compatibility of the blockchain protocol and the time instant at which a new block is mined. So Intentional fork can be of two types:

  - **SOFT FORK:** When the blockchain protocol is altered in a backwards-compatible way. In soft fork you tend to add new rules such that they do not clash with the old rules. That means there is no connection between the old rules and new rules. Rules in soft fork are tightened. When there is a change in the software that runs on the nodes (better called as 'full nodes') to function as a network participant, the change is such that the new blocks mined on the basis of new rules (in the Blockchain protocol) are also considered valid by the old version of the software. This feature is also called as backwards-compatibility.

    Example: The Bitcoin network's SegWit update added a new class of addresses (Bech32). However, this didn't invalidate the existing P2SH addresses. A full node with a P2SH type address could do a valid transaction with a node of Bech32 type address.

  - **HARD FORK:** When the blockchain protocol is altered in a non-backwards-compatible way. Hard fork is opposite of Soft fork, here the rules are loosened. When there is a change

in the software that runs on the full nodes to function as a network participant, the change is such that the new blocks mined on the basis of new rules (in the Blockchain protocol) are not considered valid by the old version of the software. When hard forks occur, new currency come into existence (with valid original currency) like in the case of Ethereum (original : Ethereum, new : Ethereum Classic) and Bitcoin (original : Bitcoin, new : Bitcoin cash). Equivalent quantity of currency is distributed to the full nodes who choose to upgrade their software so that no material loss occurs. Such hard forks are often contentious (generating conflicts in the community). The final decision to join a particular chain rests with the full node. If chosen to join the new chain, the software has to be upgraded to make newer transactions valid while the nodes who do not choose to upgrade their software continue working the same.

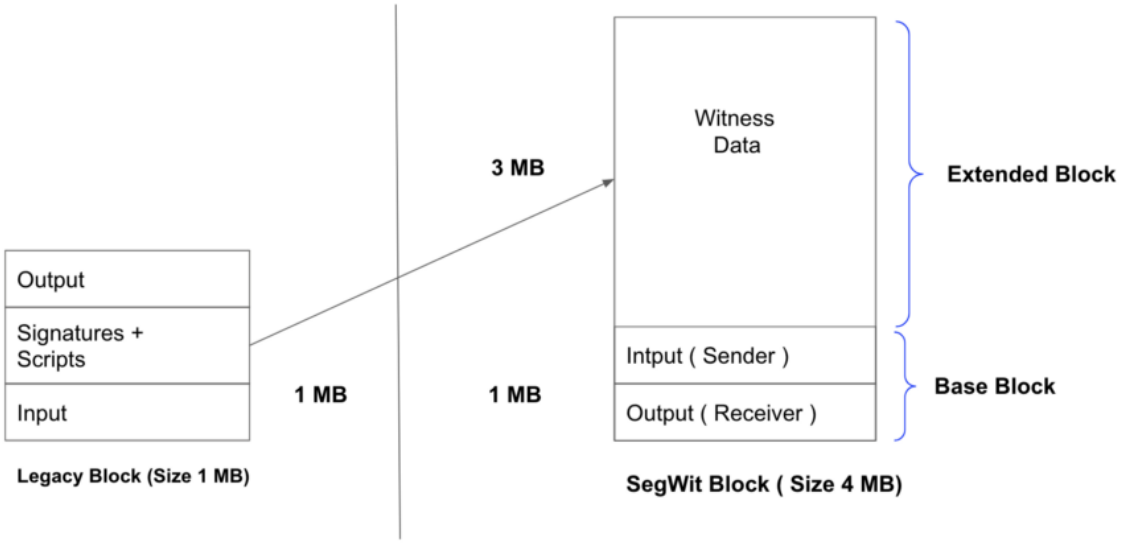
Example: The new Casper update in the Ethereum Blockchain in which the consensus protocol will change from a type of Proof of Work (PoS) to a type of Proof of Stake (PoS). The nodes which install the Casper update will use the new consensus protocol. Full nodes that do not choose to install the Casper update will become incompatible with the full nodes that do.

The working procedure of SegWit

i. Block Size Increase:

Segwit proposes how bitcoin blocks should be structured. Non-segwit blocks are also known as legacy blocks and usually of 1MB size. Inside this 1MB block, data, signatures etc. are stored.

On the other side, Segwit block size is up to 4MB. This is because it consists of base transaction block and an extended block. So Segwit, just like Bitcoin Cash, is indeed a block size increase.



SegWit block structure achieves two primary goals.

- Segwit block structure moves the digital signature outside of the base transaction block. So, if someone changes the signature on the transaction, it will not affect the transaction id. This, in effect, solves the transaction malleability issue.
- It's minimizing the base transaction data in the block. Since the witness data takes up to 65% of the transaction size, moving it outside the base transaction block allows more transactions to fit inside a 1MB block.

ii. Segwit is a Soft Fork:

Bitcoin specifically states that block size can't exceed 1MB. So the bitcoin developer finds the solution without hard fork. A solution of a 1MB block with an “extension” of another 3MB is still acceptable under the existing protocol. So, introduction of SegWit is treated as a Soft Fork. The legacy node can accept 1MB block and the Segwit node can accept 3 MB extended total of 4 MB blocks. This is called a soft fork.

iii. Measuring Block:

Legacy Block measure by size, and SegWit block measure by weight. A SegWit transaction was divided into two parts:

- **Segwit Part of Transaction:** The witness of a transaction is classified as segwit part of a transaction.
- **Non-Segwit Part of Transaction:** All the other parts of transactions except witness are classified as Non-Segwit part of a transaction.

A simple formula defines the weight of any transaction:

3*(non-segwit-part-of-transaction) + 1*(segwit-part-of-transaction)

But, first, let's see the mathematics equation of block measure.

legacy_block_size = ∑(size_of_non-segwit-data_of_each_transaction)

segwit_block_size = legacy_block_size + ∑(size_of_segwit-data_of_each_transaction)

For a block, **non_segwit_weight** and **segwit_weight** is defined as

non_segwit_weight = 3*∑(size_of_non-segwit-data_of_each_transaction)

segwit_weight = 1*∑(size_of_segwit-data_of_each_transaction)

block_weight = non_segwit_weight + segwit_weight

For a block to be valid on the chain

legacy_block_size <= 1 MB

block_weight <= 4MBU

Transaction Malleability

Bitcoin transaction malleability is an attack wherein someone changes a TX ID before it is confirmed or validated by the network. Once a part of that TX ID is changed, that ripple effect

affects the hash—and if the hash is altered, the transaction can't be confirmed. This change in the hash can create problems, especially for people making use of an exchange.

For example, let's say Diana runs a BTC exchange, with Bella having funds stored within that exchange. One day, Bella decides to withdraw her BTC and asks Diana to send it to her address. As soon as Diana sends the bitcoin, a transaction is created on the blockchain. However, before it's added to the current block, it will have to be confirmed by miners.

What if Bella decides to pretend that Diana never sent over the BTC? She can use the bitcoin malleability issue to replicate Diana's original transaction by slightly tweaking the transaction details—effectively changing the hash. Bella then retransmits that transaction with a new ID.

There's a chance that Bella's transaction (the new ID) will be confirmed first and therefore, regarded as valid. If that happens, Bella can then complain that she never received the BTC and when Diana checks the blockchain for her original TX ID, she won't find it. Diana will then send more BTC, effectively paying double to what she was supposed to send out.

However, these issues of bitcoin malleability aren't always malicious. Sometimes, they're accidental. Some people use custom software to handle their own BTC and that can cause problems. Other wallets might not be compatible, forcing them to "fix" the TX ID. The ID is then formatted and changed, causing the malleability issue once again.

So what happens to the people who fall victim to this issue? In some cases, their transactions are stuck in limbo. In other cases, their wallets might think they still have those coins to spend. Although it might not be an enormous deal to the casual trader sitting at home, this issue could significantly affect merchants who offer goods and services in exchange for BTC. These merchants probably won't want to accept a transaction without confirmations if there's a small chance that a miner might malleate it.