**MODULE 1**

**Introduction to Block chain**

Blockchain is the new wave of disruption that has already started to redesign business, social and political interactions, and any other way of value exchange. Again, it is not just a change, but a rapid phenomenon that is already in motion. More than 40 top financial institutions and many different firms across industries have started to explore blockchain to lower transaction cost, speed up transaction time, reduce the risk of fraud, and eliminate the middleman or intermediary services.

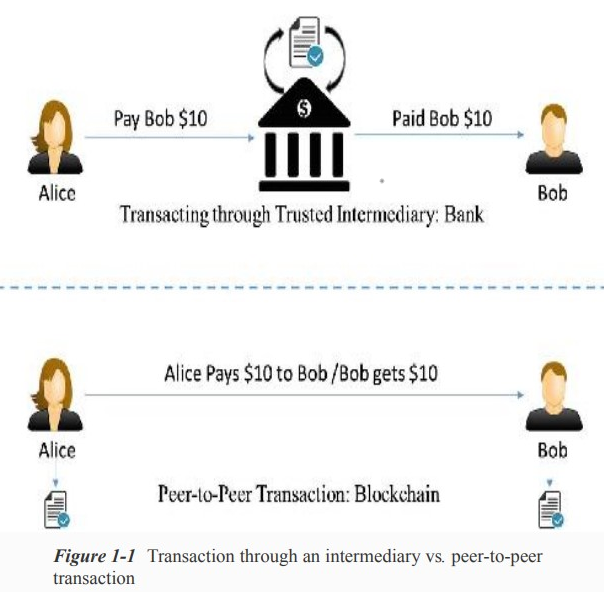
Let us take a closer look at the banking system and its evolution. Starting from the olden days of barter system till fiat currencies, there was no real difference between a transaction and its settlement because they were not two separate entities. As an example, if Alice had to pay $10 to Bob, she would just hand over a $10 note to Bob and the transaction would just get settled there. No bank was needed to debit $10 from Alice’s account and credit the same to Bob’s account or to serve as a system of trust to ensure Alice does not cheat Bob. However, transacting directly with someone who is physically not present close by was difficult. So, banking systems evolved with many more service offerings and enabled transactions from every corner of the world. With the help of the Internet, geography was no more a limitation and banking became easier than ever. Not just banking for that matter: the Internet facilitated many different kinds of value exchange over the web. Technology enabled someone from India to make a monetary transaction with someone in the United Kingdom, but with some cost. It takes days to settle such transactions and is expensive as well. A bank was always needed to impose trust and ensure security for such transactions between two or more parties. What if technology could enable trust and security without these intermediary and centralized systems? Somehow, this part (of technology imposing trust) was missing all through, which resulted in development of centralized systems such as banks, escrow services, clearing houses, registrars and many other such institutions. Blockchain proves to be that missing piece of the Internet revolution puzzle that facilitates a trust less system in a cryptographically secured way.

Banks formed the centralized institutions that maintained the transaction records, governed interactions, enforced trust and security, and regulated the whole system. The whole of commerce relies on these financial institutions, which serve as the trusted third parties to process payments. The mediation of financial institutions increases cost and time to settle a transaction, and also limits the transaction sizes. The mediation was needed to settle disputes, but that meant that completely non-reversible transaction was never possible. This resulted in a situation where trust was needed for someone to transact with another. Certainly, this bureaucratic system had to change to keep up with the economy’s expected digital transformation. So, a cryptocurrency called Bitcoin was invented which was enabled by the underlying technology— blockchain. Bitcoin is just one monetary use case of blockchain that addresses the inherent weakness of trust-based models.

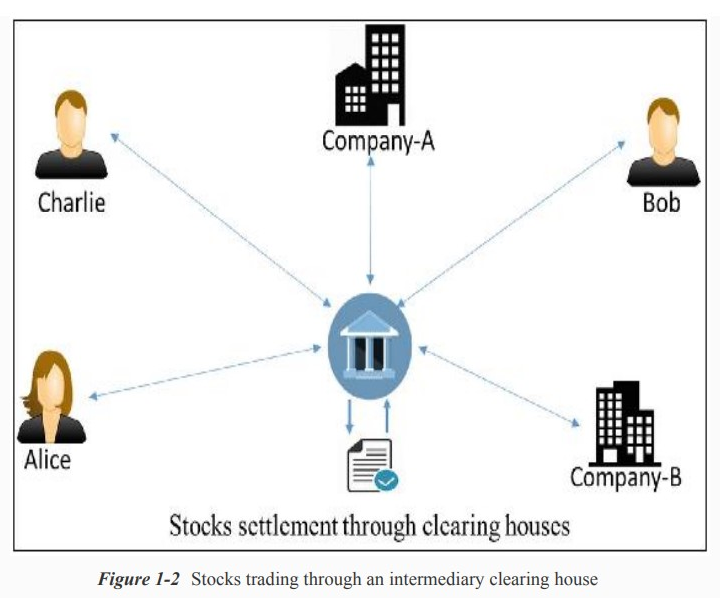
**What is Blockchain?**

The Internet has revolutionized many aspects of life, society, and business. However, the way people and organizations execute transactions with one another has not changed much in the past couple of decades. Blockchain is believed to be the component that completes the Internet puzzle and makes it more open, more accessible, and more reliable. To understand blockchain, you have to understand it from both a **business perspective** and **technical perspective**. Let us first understand it in a business transaction context to get the **“what”** of it, and then look into the technicality to understand the **“how”** of it.

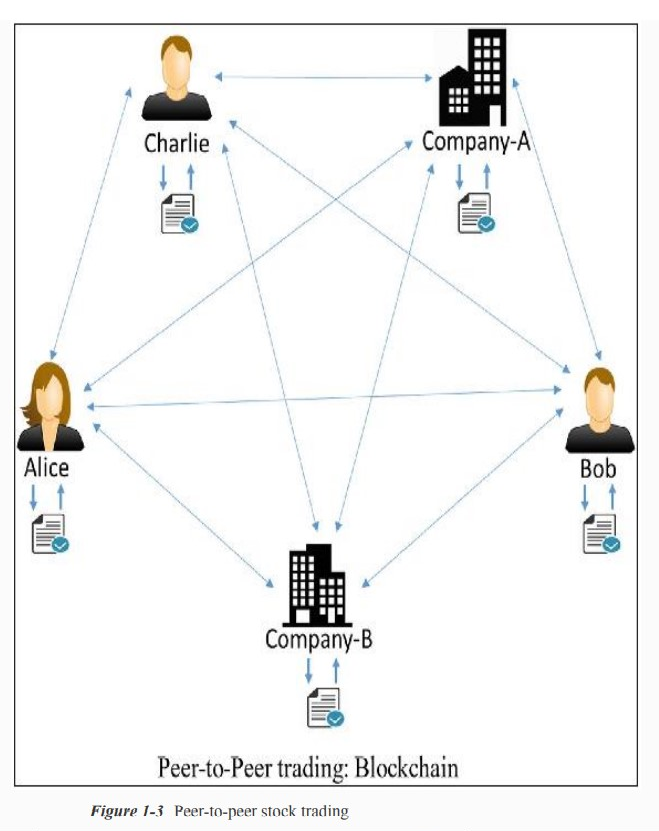
Blockchain is a system of records to transact value (not just money!) in a peer-to-peer fashion. What it means is that there is no need for a trusted intermediary such as banks, brokers, or other escrow services to serve as a trusted third party. For example, if Alice pays to Bob $10, why would it go through a bank? Take a look at the Figure 1-1.



Let us look at a different example now. A typical stock transaction happens in seconds, but its settlement takes weeks. Is it desirable in this digital age? Certainly not!



If someone wants to buy some stocks from a company or a person, they can just directly buy it from them with instant settlement, with no need for brokers, clearing houses, or other financial institutions in between. A decentralized and peer-to-peer solution to such a situation can be represented as in Figure 1-3.

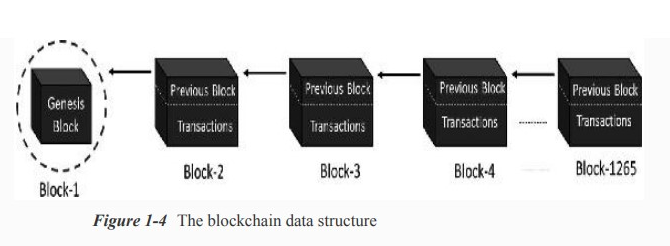


Transaction and settlement are not two different entities in a blockchain setting. The transactions are analogous to, say, fiat currency transactions where if someone pays another a $10 note, they do not own it anymore and that $10 note is physically transferred to the new owner.

**Salient Features:**

* Blockchain is a peer-to-peer system of transacting values with no trusted third parties in between.
* It is a shared, decentralized, and open ledger of transactions. This ledger database is replicated across a large number of nodes.
* This ledger database is an append-only database and cannot be changed or altered. It means that every entry is a permanent entry. Any new entry on it gets reflected on all copies of the databases hosted on different nodes.
* There is no need for trusted third parties to serve as intermediaries to verify, secure, and settle the transactions.
* It is another layer on top of the Internet and can coexist with other Internet technologies.
* Just the way TCP/IP was designed to achieve an open system, blockchain technology was designed to enable true decentralization. In an effort to do so, the creators of Bitcoin open-sourced it so it could inspire many decentralized applications.

A typical blockchain may look as shown in Figure 1-4.



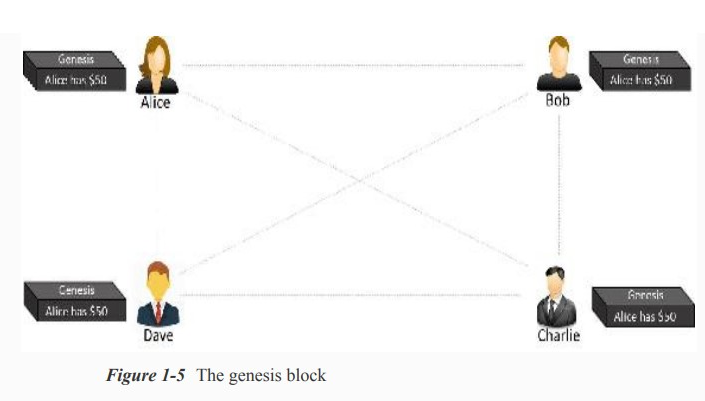
Every node on the blockchain network has an identical copy of the blockchain shown in Figure 1-4, where every block is a collection of transactions, hence the name. As you can see, there are two major parts in every block. The “header” part links back to the previous block in the chain. What it means is that every block header contains the hash of the previous block so that no one can alter any transaction in the previous block. The other part of a block is the “body content” that has a validated list of transactions, their amounts, the addresses of the parties involved, and some more details. So, given the latest block, it is feasible to access all the previous blocks in a blockchain.

**How Blockchain works?**

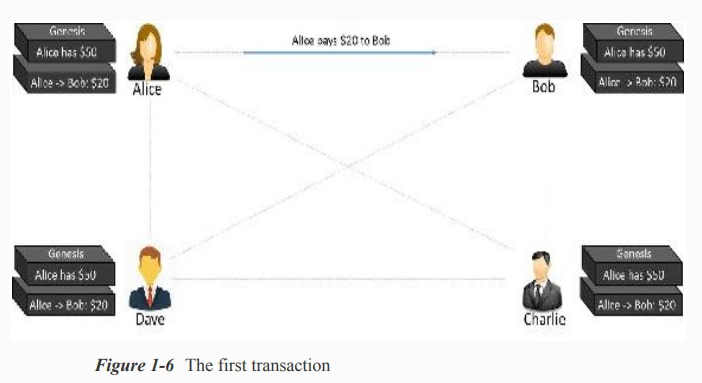
Let us consider a practical example and see how the transactions take place and the ledger gets updated across the network, to see how this system works: Assume that there are three candidates—Alice, Bob, and Charlie—who are doing some monetary transactions among each other on a blockchain network. Let us go through the transactions step by step to understand blockchain’s open and decentralized features.

**Step-1:**

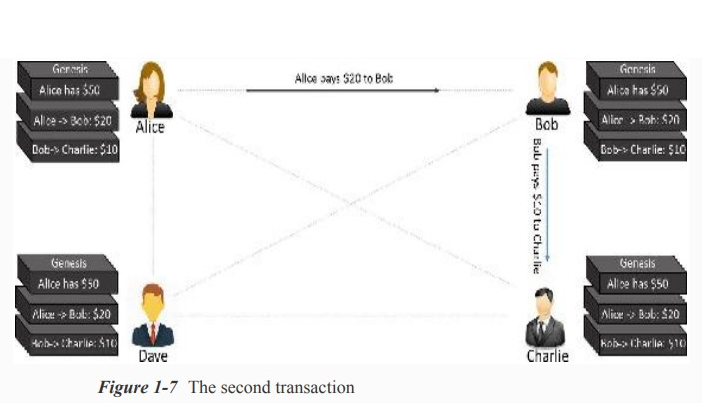
Let us assume that Alice had $50 with her, which is the genesis of all transactions and every node is aware of it, as shown in Figure 1-5.



**Step-2:** Alice makes a transaction by paying $20 to Bob. Observe how the blockchain gets updated at each node, as shown in Figure 1-6.



**Step-3:** Bob makes another transaction by paying $10 to Charlie and the blockchain gets updated as shown in Figure 1-7.

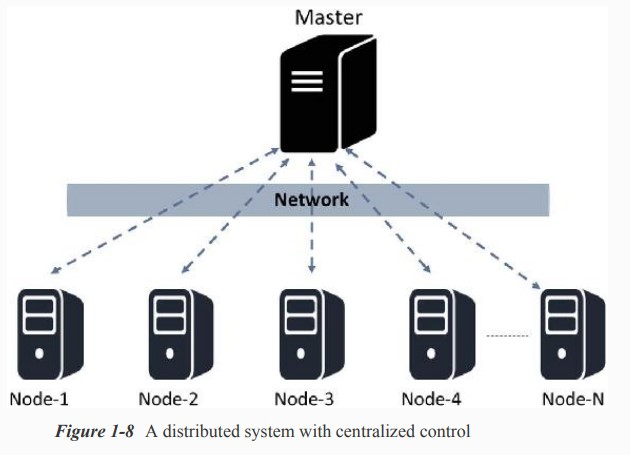


Note that the transaction data in the blocks is immutable. All transactions are fully irreversible. Any change would result in a new transaction, which would get validated by all contributing nodes. Every node has its own copy of blockchain.

If there are many questions popping up in your mind, such as “What if Alice pays the same amount to Dave to double-spend the same amount, or what if she is making a payment without having enough funds in her account?” “How is the security ensured?” and so on, we are going to cover those details in the following chapters.

**Centralized Vs. Decentralized Systems**

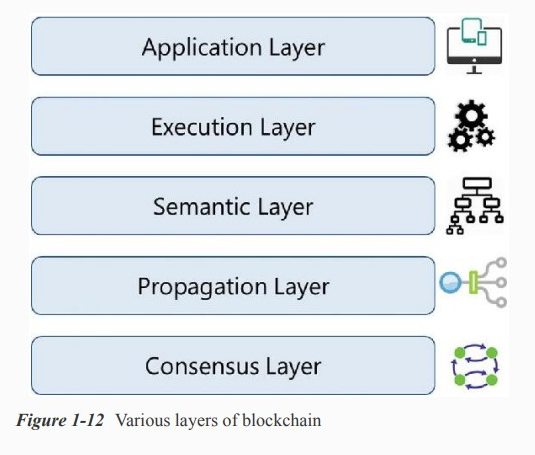
The very reason we are looking into the debate on centralization vs. decentralization is because blockchain is designed to be decentralized, defying the centralized design. Note that whether a system is centralized or decentralized, it can still be distributed. A centralized distributed system is one in which there is, say, a master node responsible for breaking down the tasks or data and distribute the load across nodes. On the other hand, a decentralized distributed system is one where there is no “master” node as such and yet the computation may be distributed. Blockchain is one such example. Figure 1-8 is a pictorial representation of how a centralized distributed system may look.



Though the computation is faster in such designs because of distributed computing, it also suffers from limitations due to centralization.

**Layers of Blockchain**

The public blockchain variants such as Ethereum are in the process of maturing, and building complex applications on top of these blockchains may not be a good idea. Keep in mind that blockchain is never just a piece of technology, but a combination of business principles, economics, game theory, cryptography, and computer science engineering. Most of the real-world applications are quite complex in nature, and it is advisable to build blockchain solutions from the ground up. To start with, let us just recollect our basic understanding of the TCP/IP protocol stack. The layered approach in the TCP/IP stack is actually a standard to achieve an open system. Having abstraction layers not only helps in understanding the stack better, but also helps in building products that are compliant to the stack to achieve an open system. Also, having the layers abstract from each other makes the system more robust and easy to maintain. Any change to any of the layers doesn’t impact the other layers. Again, the TCP/IP analogy is not to be confused with the blockchain layers. TCP/IP is a communication protocol that every Internet application uses, and so is blockchain. There are no agreed global standards yet that would clearly segregate the blockchain components into distinct layers. A layered heterogeneous architecture is needed, but for now that is still in the future. So, we will try to formulate blockchain layers to be able to understand the technology better and build a comparative analogy between hundreds of blockchain/Cryptocurrency variants out there in the market. Take a look at the high-level, layered representation of blockchain in Figure 1-12.



There cannot be too many or too few layers; it is going to be a trade-off driven among complexity, robustness, adaptability, etc., to name a few. The purpose again is not really to standardize blockchain technology, but to build a better understanding. Note that all these layers are present on all the nodes.

In later modules, we will be building a decentralized application from scratch and learning how blockchain functions on all these layers with a practical use case.

1. **Application Layer**

Because of the characteristics of blockchain, such as immutability of data, transparency among participants, resilience against adversarial attacks etc., there are multiple applications being built. Certain applications are just built in the application layer, taking for granted any available “flavor” of blockchain, and some applications are built in the application layer and are interwoven with other layers in blockchain. This is the reason the application layer should be considered a part of blockchain. This is the layer where you code up the desired functionalities and make an application out of it for the end users. For the applications that treat blockchain as a backend, those applications might need to be hosted on some web servers. Ideally, good blockchain applications do not have a client–server model, and there are no centralized servers that the clients access, which is just the way Bitcoin works. You probably have heard or already learned about the off-chain networks. The idea is to build applications that wouldn’t use blockchain for anything and everything, but use it wisely. In other words, this concept is to ensure that the heavy lifting is done at the application layer, or bulky storage requirements are taken care of off the chain so that the core blockchain is light and effective and the network traffic is not too much.

1. **Execution Layer**

The Execution Layer is where the executions of instructions ordered by the Application Layer take place on all the nodes in a blockchain network. The instructions could be simple instructions or a set of multiple instructions in the form of a smart contract. In either case, a program or a script needs to be executed to ensure the correct execution of the transaction. All the nodes in a blockchain network have to execute the programs/scripts independently. Deterministic execution of programs/scripts on the same set of inputs and conditions always produces the same output on all the nodes, which helps avoid inconsistencies. In the case of Bitcoins, these are simple scripts that are not Turing-complete and allow only a few set of instructions. Ethereum and Hyperledger, on the other hand, allow complex executions. Ethereum’s code or its smart contracts written in solidity gets compiled to Bytecode or Machine Code that gets executed on its own Ethereum Virtual Machine. Hyperledger has a much simpler approach for its chaincode smart contracts. It supports running of compiled machine codes inside docker images, and supports multiple high-level languages such as Java.

1. **Semantic Layer**

The Semantic Layer is a logical layer because there is an orderliness in the transactions and blocks. A transaction, whether valid or invalid, has a set of instructions that gets through the Execution Layer but gets validated in the Semantic Layer. If it is Bitcoin, then whether one is spending a legitimate transaction, whether it is a double-spend attack, whether one is authorized to make this transaction, etc., are validated in this layer. It is the semantic layer that defines how the blocks are linked with each other. Every block in a blockchain contains the hash of the previous block, all the way to the genesis block. Though the final state of the blockchain is achieved by the contributions from all the layers, the linking of blocks with each other needs to be defined in this layer. Depending on the use case, you might want to code up an additional functionality in this layer.

1. **Propagation Layer**

The previous layers were more of an individual phenomenon: not much coordination with other nodes in the system. The Propagation Layer is the peer-to-peer communication layer that allows the nodes to discover each other, and talk and sync with each other with respect to the current state of the network. When a transaction is made, we know that it gets broadcast to the entire network. Similarly, when a node wants to propose a valid block, it gets immediately propagated to the entire network so that other nodes could build on it, considering it as the latest block. So, transaction/block propagation in the network is defined in this layer, which ensures stability of the whole network. By design, most of the blockchains are designed such that they forward a transaction/block immediately to all the nodes they are directly connected to, when they get to know of a new transaction/block. In the asynchronous Internet network, there are often latency issues for transaction or block propagation. Some propagations occur within seconds and some take more time, depending on the capacity of the nodes, network bandwidth, and a few more factors.

1. **Consensus Layer**

The Consensus Layer is usually the base layer for most of the blockchain systems. The primary purpose of this layer is to get all the nodes to agree on one consistent state of the ledger. There could be different ways of achieving consensus among the nodes, depending on the use case. Safety and security of the blockchain is ascertained in this layer. In Bitcoin or Ethereum, the consensus is achieved through proper incentive techniques called “mining.” For a public blockchain to be self-sustainable, there has to be some sort of incentivization mechanisms that not only helps in keeping the network alive, but also enforces consensus. Bitcoin and Ethereum use a Proof of Work (PoW) consensus mechanism to randomly select a node that can propose a block. Once that block is proposed and propagated to all the nodes, they check to see if it a valid block with all legitimate transactions and that the PoW puzzle was solved properly; they add this block to their own copy of blockchain and build further on it. There are many different variants of consensus protocols such as Proof of Stake (PoS), deligated PoS (dPoS), Practical Byzantine Fault Tolerance (PBFT), etc.

**Blockchain Vs. Bitcoin**

1. **Blockchain**

In Blockchain every block contains a cryptographic hash of the previous block, a timestamp, and transaction information. In other words, blockchain is a distributed database technology, which restricts bitcoin or any digital asset. It enables multiple parties to transact, share valuable data, and pool their resources in a secure yet tamper-proof manner. Data contained within the blockchain is distributed across many computers and is therefore decentralized. Due to decentralized nature, blockchains are incredibly secure as there is no single point of attack.

1. **Bitcoin**

The Bitcoin Network is the network of computers throughout the world that are connected together, to actually process Bitcoin payment transactions between Bitcoin accounts. These computers are referred to as miners and are owned by individual people and companies around the world. The Bitcoin Network is very secure. There is no possibility of ‘Double Spending’ and the system has been specifically designed and coded to make creating counterfeit Bitcoin or fake transactions impossible. Bitcoin is one of the earliest cryptocurrencies to use blockchain technology in facilitating peer-to-peer payments. Through a decentralized network, bitcoin offers a reasonably low transaction fee compared to popular payment gateways.

| **S.No.** | **Basis of Comparison** | **Blockchain** | **Bitcoin** |
| --- | --- | --- | --- |
| 1. | What is it? | A Distributed Database | A cryptocurrency |
| 2. | Main Aim | To provide a low cost, safe and secure environment for peer to peer transactions | To simplify and increase the speed of transactions without much of government restrictions. |
| 3. | Trade | Blockchain can easily transfer anything from currencies to property rights of the stock | Bitcoin is limited to trading as a currency. |
| 4. | Scope | It is more open to changes and hence has the backing of many top companies. | The scope of bitcoin is limited. |
| 5. | Strategy | Blockchain can be adapted to any changes and hence it can cater to different industries. | Bitcoin focuses on lowering the cost of influencers and reducing the time of transactions but is less flexible. |
| 6. | Status | As blockchain works with various businesses, it should have compliance with KYC and other norms. Hence blockchain is transparent. | Bitcoin likes to be anonymous and hence even though we can see the transactions in the ledger, they are numbers that are not in a particular sequence. |

* **Key Differences**

To finish up, let’s recap why blockchain and Bitcoin are two completely separate things:

* Bitcoin is a cryptocurrency, while blockchain is a distributed database.
* Bitcoin is powered by blockchain technology, but blockchain has found many uses beyond Bitcoin.
* Bitcoin promotes anonymity, while blockchain is about transparency. To be applied in certain sectors (particularly banking), blockchain has to meet strict Know Your Customer rules.
* Bitcoin transfers currency between users, while blockchain can be used to transfer all sorts of things, including information or property ownership rights.

**Practical Applications**

In this section, we will look at some of the initiatives that are already being taken across industries such as finance, insurance, banking, healthcare, government, supply chains, IoT (Internet of Things), media and entertainment to name a few. The possibilities are limitless. A true sharing economy, which was difficult to achieve in centralized systems, is possible using blockchain technology (e.g., peer-to-peer versions of Uber, AirBNB). It is also possible to enable citizens to own their identity (Self-Sovereign Digital Identity) and monetize their own data using this technology. For now, let us take a look at some of the existing use cases.

* Any type of property or asset, whether physical or digital, such as laptops, mobile phones, diamonds, automobiles, real estate, e-registrations, digital files, etc. can be registered on blockchain. This can enable these asset transactions from one person to another, maintain the transaction log, and check validity or ownerships. Also, notary services, proof of existence, tailored insurance schemes, and many more such use cases can be developed.
* There are many financial use cases being developed on blockchain such as cross-border payments, share trading, loyalty and rewards system, Know Your Customer (KYC) among banks, etc. Initial Coin Offering (ICO) is one of the most trending use cases. ICO is the best way of crowdsourcing today by using cryptocurrency as digital assets. A coin in an ICO can be thought of as a digital stock in an enterprise, which is very easy to buy and trade.
* Blockchain can be used to enable “The Wisdom of Crowds” to take the lead and shape businesses, economies, and various other national phenomena by using collective wisdom! Financial and economic forecasts based on the wisdom of crowds, decentralized prediction markets, decentralized voting, as well as stocks trading can be possible on blockchain.
* The process of determining music royalties has always been convoluted. The Internet-enabled music streaming services facilitated higher market penetration, but made the royalty determination more complex. This concern can pretty much be addressed by blockchain by maintaining a public ledger of music rights ownership information as well as authorised distribution of media content.
* This is the IoT era, with billions of IoT devices everywhere and many more to join the pool. A whole bunch of different makes, models, and communication protocols makes it difficult to have a centralized system to control the devices and provide a common data exchange platform. This is also an area where blockchain can be used to build a decentralized peer-to-peer system for the IoT devices to communicate with each other. ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) is a joint initiative from IBM and Samsung that has developed a platform that uses elements of the Bitcoin’s underlying design to build a distributed network of devices—a decentralized IOT. ADEPT uses three protocols: BitTorrent for file sharing, Ethereum for smart contracts, and TeleHash for peer-to-peer messaging in the platform. The IOTA foundation is another such initiative.
* In the government sectors as well, blockchain has gained momentum. There are use cases where technical decentralization is necessary, but politically should be governed by governments: land registration, vehicle registration and management, e-Voting, etc. are some of the active use cases. Supply chains are another area where there are some great use cases of blockchain. Supply chains have always been prone to disputes across the globe, as it was always difficult to maintain transparency in these systems.

**Basics of Public and Private Keys**

Public and private keys are an integral part of Bitcoin and other cryptocurrencies. They allow you to send and receive cryptocurrency without requiring a third party to verify the transactions. These keys are a part of the public-key cryptography (PKC) framework. You can use these keys to send your cryptocurrency to anyone, anywhere, at any time. The public and private keys fit together as a key pair. You may share your public keys in order to receive transactions, but your private keys must be kept secret. If anyone has access to the private keys, they will also have access to any cryptocurrency associated with those keys.

1. **Public Key Cryptography (PKC)**

Public-key cryptography (PKC) is a technology often used to validate the authenticity of data using asymmetric encryption. PKC was first used primarily to encrypt and decrypt messages in traditional computing. Cryptocurrencies now use this technology to encrypt and decrypt transactions. Without PKC, the technology underpinning cryptocurrencies would be practically impossible.

The key to PKC is “trapdoor functions,” one-way mathematical functions that are easy to solve in one way, but nearly impossible to crack in the reverse. While it might be possible, it would likely take a supercomputer — and thousands of years — to reverse engineer these functions.

1. **Public Key**

A public key allows you to receive cryptocurrency transactions. It’s a cryptographic code that’s paired to a private key. While anyone can send transactions to the public key, you need the private key to “unlock” them and prove that you are the owner of the cryptocurrency received in the transaction. The public key that can receive transactions is usually an address, which is simply a shortened form of your public key. Therefore, you can freely share your public key without worry. You may have seen donation pages for content-creators or charities with the public keys for their crypto addresses online. While anyone can donate, you’d need the private key to unlock and access the donated funds.

1. **Private Key**

Here is one crucial piece of advice to remember: Never share your private key with anyone. A private key gives you the ability to prove ownership or spend the funds associated with your public address. A private key can take many forms:

* 256 character long binary code
* 64 digit hexadecimal code
* QR code
* Mnemonic phrase

Regardless of its form, a private key is an astronomically large number, and it’s large for a good reason. While you can generate a public key with a private key, doing the opposite is practically impossible because of the one-way “trapdoor” function. You can have any number of public keys connected to a private key.

1. **Digital Signing of a Transaction**

For a transaction on the blockchain to be complete, it needs to be signed. The steps for someone to send you a transaction are:

* A transaction is encrypted using a public key. The transaction can only be decrypted by the accompanying private key.
* Next, the transaction is signed using the private key, which proves that the transaction hasn’t been modified. The digital signature is generated through combining the private key with the data being sent in the transaction.
* Finally, the transaction can be verified as authentic using the accompanying public key.

You digitally sign a transaction to prove you’re the owner of the funds. Nodes check and authenticate transactions automatically. Any unauthenticated transactions get rejected by the network. An authentic, mined transaction on the blockchain is irreversible.

1. **Where are the “Private Keys?”**

Your private keys are in a cryptocurrency wallet, which is typically mobile or desktop software or a specialized hardware device. Your private keys are not on the cryptocurrency blockchain network. If you keep cryptocurrency on an exchange, then the exchange is the custodian of your private keys; you’re trusting it with your keys in the same way you’d trust a bank’s vault to hold your gold.

If you transfer your cryptocurrency from an exchange to a non-custodial wallet, then you are in control of your keys. Because of the configuration and functionality of cryptocurrency wallets, you’ll likely never handle the private keys directly as wallets generally manage them for you automatically. Typically, you’re given a seed phrase that encodes your private keys as a back-up.

1. **Public and Private Keys Control Crypto**

How public and private keys work together is fundamental to understanding how cryptocurrency transactions function. When you say you have cryptocurrency, what you’re really saying is you have a private key that proves ownership of that cryptocurrency. Since it’s stored on the blockchain, anyone can verify you as the owner with your public key.

The choice of “holding your own keys” or trusting a custodian depends on your philosophy, risk-tolerance, and a host of other factors. If you hold your own private keys, consider modern HD wallets, which can do a great job of managing your private keys, and remember to never share them. If you choose a custodial solution like an exchange, make sure you choose a trusted, reputable company that places a high emphasis on security and regulation.

**Pros and Cons of Blockchain**

Let’s look at the most significant blockchain advantages and why businesses and individuals are eager to adopt the technology. Some disadvantages are also put forward.

**Advantages:**

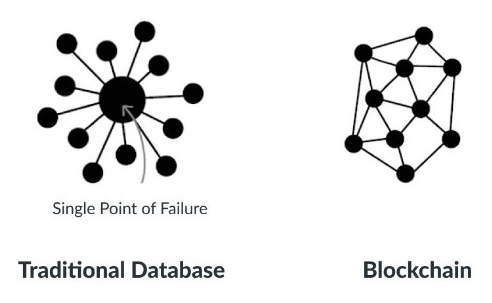
1. Decentralized Trust

One of its biggest strengths is that you no longer need to trust a third party to make any transaction. People using blockchain worldwide are confident that no single party is manipulating transactions, viewing personal information or performing any other activity breaching their privacy and security. That doesn’t mean blockchain-based applications are always secure—that depends on how good developers are at creating secure code—but it does mean there are opportunities for better security than conventional applications. With blockchain, you can feel more confident about your data and identity. You only share what you want; companies cannot see your data without your permission. You can also feel more confident about getting paid for providing services. With blockchain, payment is instant; there’s no need to wait days for money orders or checks to clear.

1. Low Operational Cost

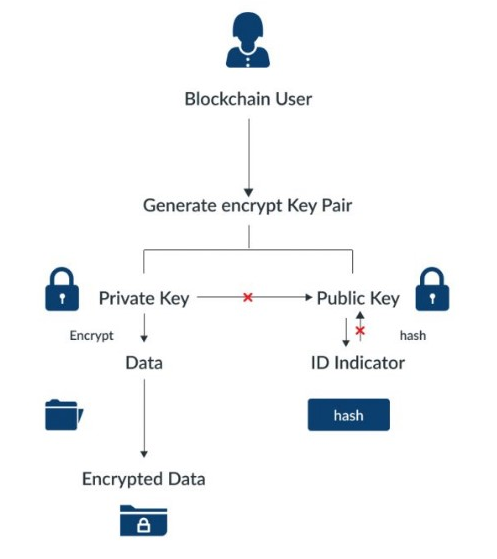
Blockchain reduces overhead costs as it has no centralized authority or servers to maintain operations. There is no payment processing or banking fees as it opts for peer-to-peer transactions without third-party approval. It embeds documents, agreements, or transactions within the system. Blockchain encryptions are more secure against identity theft than conventional payment systems.

1. No Single Point of Failure



With blockchain technology, there’s no single point of failure. If a hacker were to gain access to your business’s server or database, they could very easily wipe out your entire network—all at once. Blockchain technology is not centralized; instead, it is in distributed form. It saves your data if the network goes down as hackers cannot break into the central grid and affect any connected account. You can create passwords up to 100 characters long, making it impossible for hackers to guess or decode. It gives better security than regular networks with the option of up to 8-character long passwords (including letters and numbers).

1. Enhanced Security and Confidentiality



Being distributed across a global network of computers and protected by cryptography, blockchain technology is inherently more secure than centralized systems. It is tough to tamper with records once they are in there. Any attempt to alter one’s record will reflect immediately because copies and digital signatures are checked against each other automatically. It has an added layer of confidentiality that secures your data from hackers. Transactions are impossible to trace or link back to an individual user. The user can select their names and e-mail addresses during transactions. You get the option to complete your transactions while remaining anonymous. So, you can use blockchain-based services without worrying about advertisers tracking your activity or identity thieves accessing sensitive information such as credit card numbers.

1. Quick Transactions

Blockchain is capable of processing much faster transactions than any traditional bank. As a result, businesses that use blockchain instead of banks can save a considerable amount on fees. Deloitte has predicted that blockchain technology could save companies up to billions in the form of banking fees. Blockchain’s decentralized structure doesn’t require massive data centers and expensive third-party verification. It also limits the number of people involved in monitoring the transactions.

1. Reduces Fraud

Blockchain technology has some attributes that make it ideal for financial institutions to reduce forgery. It records every activity, making it impossible for anyone to make duplicate transactions. Each block stores the financial information, and if any modification is made to a previous block, other nodes on the network reject it.

1. Transparent and Universal Recording System

The transactions in the blockchain are recorded in a public ledger that anyone can view. All can see the amount stored in the wallet but cannot identify its owner. A wallet could be tied to an individual or group. Still, if users want to remain anonymous, they must transfer their Bitcoins to another address (e.g., a different Bitcoin wallet) that isn’t linked with their real identity. But even without anonymity features enabled, blockchain tech provides more transparency than traditional payment methods like credit cards and checks; you don’t need a bank intermediary (or permission from one) to see what or whom you paid or received money from.

1. Better Accessibility

A blockchain allows anyone with a computer and an internet connection to be part of its network. It is decentralized, meaning any single entity can’t control it—and everyone has equal access to it. Anyone can make changes (add information) or add new blocks (to store data) to a blockchain, provided they know how to do so. Even non-tech individuals have the same access to blockchains. This openness makes blockchains much more accessible than traditional institutions like banks and financial services. That doesn’t mean you shouldn’t be wary when dealing with blockchain providers: you should always research your choices before making any significant financial decisions.

1. Prevents Double Spending

Bitcoin transactions are verified by network nodes through cryptography and recorded in a publicly distributed ledger called a blockchain. This ensures safety by eliminating direct access to your money. That’s why some say bitcoin is fungible—its value is equal even if its physical form changes. In other words, bitcoins derive their worth from mathematics alone, unlike fiat currencies like U.S. dollars or euros, which get their value from an organization’s financial standing. Every single bitcoin carries all its transactional histories within that particular blockchain framework.

1. Seamless Integration into Existing Systems

Blockchain offers seamless integration of their current financial systems into the outside networks. It can be done in two ways: Blockchain as a Service (BaaS) and blockchain application platforms. BaaS offers organizations a secure connection to blockchain networks using cloud services, while blockchain application platforms allow anyone – even those without cloud services – to use blockchain technology. The integration process is much more seamless than other means of blockchain access. Blockchain as a Service allows businesses to connect directly with blockchain networks, giving them immediate access to these decentralized ledgers. It doesn’t force you to use one blockchain or another and gives you a higher level of control than some other methods. Additionally, BaaS is typically quicker and easier to set up than other services, making it ideal for organizations that may need blockchains immediately, such as supply chain management applications.

**Disadvantages:**

* Scalability

Blockchain is capable of handling fewer transactions per second. It causes delays in finalizing the massive volume of transactions resulting in poor scalability. However, several methods have been proposed to overcome this shortcoming, but none has been implemented till now.

* Security

Blockchain is publicly accessible as a distributed ledger. It may attract any unknown visitor monitoring your wallet. Though there are several provisions to add privacy and encryption layers to enable your preferred privacy, all are not commonplace yet. Moreover, much of your data is linked directly to your digital identity, so it could potentially expose parts of your private life that you wouldn’t necessarily want online. Security concerns often lead people to trust third-party solutions (like exchanges) over direct blockchain transactions, relinquishing control over personal assets.

* Cost

One of the biggest problems with blockchain technology is that it requires enormous energy. Because miners have to solve complicated math problems to get a payout, they need powerful rigs that consume tons of electricity. As a result, some blockchains are incredibly costly to run, especially for smaller businesses or individuals. You cannot make changes later; if you want your blockchain online, you must pay for it up front!

* Competitiveness

There is a lot of hype surrounding these industries trying to use blockchain. It leads to unnecessary competition between businesses as they opt for this technology and waste their time, money, and efforts even when it is useless for their business. Companies will have no alternative but to invest heavily to keep up with their competitors.

* Speed

The other significant con to blockchain technology is its speed. Unlike a centralized database, blockchains require miners—or people with high-end computers and dedicated software that solve computational puzzles in exchange for new crypto tokens. In simple terms, blockchain transactions take longer than traditional payment methods like cash or credit cards. This can be discouraging if you’re interested in using blockchain technology as a daily payment method.

**Myths about Bitcoin**

Myth 1: Bitcoin Is Anonymous

A common misconception of Bitcoin is that its users are anonymous. However, this is far from true. Because each bitcoin belongs to an address, all bitcoins have a clear and visible history of ownership tracing back to their creation. In addition, the Bitcoin blockchain allows all transactions to be viewed by anyone in the network, so transactions, addresses, and supply can be easily audited by any and all network participants. Addresses however, are merely strings of letters and numbers, and are not inherently connected to a given user or wallet. Both users and wallets can use an arbitrary number of addresses to store bitcoin, and some addresses, called **multisig** addresses, can hold bitcoin belonging to multiple users. Thus, Bitcoin is most accurately defined as pseudonymous rather than anonymous.

* Block explorers are a software tool that allow blockchain transaction data to be audited. They audit transactions by confirming the bitcoin quantity of a bitcoin address on a given date matches the transaction specifications.

Myth 2: Bitcoin Is Not Backed and Has No Inherent Value

While Bitcoin is not backed in the sense that it has a guaranteed rate of exchange for another asset, Bitcoin is backed in the same way that traditional fiat currencies are backed: demand and support from its users. Its value is guaranteed by its market participants and utility. Unlike fiat currencies, the long-term value of Bitcoin is assured by its limited supply. The limited supply of Bitcoin protects against inflation, which has historically crippled many fiat currencies.

Myth 3: The Bitcoin Blockchain Is Insecure

Often, the transparency of the Bitcoin blockchain is misinterpreted as a security failing. However, the public nature of the Bitcoin network allows it to remain secured by the millions of miners, traders, and investors active on the network. In order to corrupt the Bitcoin blockchain, it would be necessary to control at least 51% of all the computing power associated with the network. With millions of computers and users around the world participating in the Bitcoin network, the potential for any one entity to control a majority of the network is incredibly limited.

Myth 4: Bitcoin Is Unregulated and Unsupported by Governments

Major U.S. government figures, including the Federal Reserve, presidential candidates, senators, and state-elected officials, have acknowledged Bitcoin and supported formal regulation. In the United States, Bitcoin is regulated at both the state and federal level. Companies and individual investors that engage with Bitcoin are required to complete rigorous due diligence, comparable to the requirements of those that engage with traditional investment assets. Bitcoin exchanges and brokerages are likewise subject to the exact same regulation as most traditional brokerages and exchanges.

Myth 5: Bitcoin Is Difficult to Understand and the Barriers to Entry Are High

Bitcoin may be an intimidating concept, but the information detailing why and how Bitcoin was creating and how it operates is widely available. Satoshi Nakamoto, the creator of Bitcoin, ensured that the Bitcoin blockchain and its white paper would be publicly accessible so that anyone could participate in the Bitcoin market. In addition, opening a personal wallet for Bitcoin transactions is fast and simple. Finally, Bitcoin is highly divisible into portions of bitcoin known as satoshis, which can be purchased for fractions of a cent.

Myth 6: Bitcoin Has No Utility

Many Bitcoin skeptics view money solely through the lens of its use as a medium of exchange. However, Bitcoin has several inherent properties that provide utility. Firstly, Bitcoin is the most secure database in history. A publicly accessible database with ultimate security and immutability offers many use cases, the foremost being Bitcoin the monetary system. Regulated, day-to-day use-cases for Bitcoin have increased in the last several years. In addition to trading and long-term investing, bitcoin is accepted as a payment method with a growing number of merchants and stores. It also shows potential as an option for debt collateral. In addition, Visa is developing a credit card that offers bitcoin rewards.

Myth 7: Bitcoin Will Never Integrate With The Current Financial System

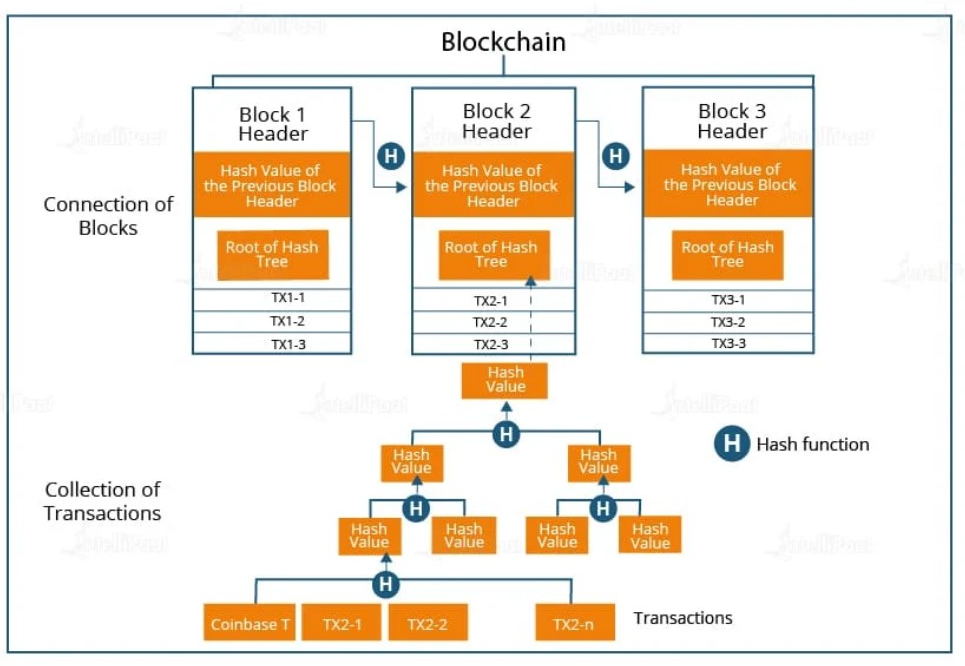
Bitcoin has already proved capable of integrating with our financial system. It is regulated as an investment asset, with the corresponding tax and reporting requirements for individuals and corporations. Bitcoin is a viable payment method with many merchants, no different than fiat currencies. Several companies now allow bitcoin to be invested in retirement accounts, and Bitcoin derivatives populate the stock market.

**MODULE 2**

**Blockchain Architecture**

Whenever a blockchain is introduced with a new blockchain transaction or any new block is to be added to the blockchain, in general, numerous nodes within the same blockchain implementation are required to execute algorithms to evaluate, verify and process the history of the blockchain block.

If most of the nodes authenticate the history and signature of the block, the new block of blockchain transaction is accepted into the ledger and the new block containing data is added to the blockchain. If a consensus is not achieved, the block is denied being added to the blockchain. This distributed consensus model allows blockchains to function as distributed ledgers without requiring any central or unifying authority to validate the blockchain transactions. Thus, the blockchain transaction is extremely secure.

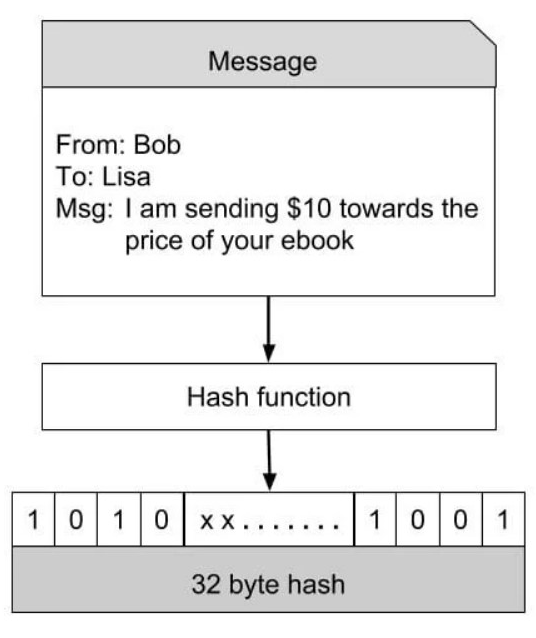


Main aspects of architecture include the blockchain platform, nodes, transactions that makeup blocks, security implementations, and the process of adding new blocks to the chain. The blockchain architecture is undoubtedly complex, but once you get a hold of it you will get acquainted with the same.

With blocks being connected with each other through their respective hash codes, the whole blockchain ecosystem becomes a well-protected one. Whenever a blockchain transaction flag is raised, a blockchain consensus needs to be achieved to update the same in the blockchain. Instead of relying on a third party to mediate transactions, member nodes in the blockchain network stick to a blockchain consensus protocol to agree on the ledger content and cryptographic hashes and digital signatures to ensure the integrity of transactions. Once authenticated, these blockchain transactions are considered successful and irreversible. Transactions rely a lot on hash values and hash functions. These hash functions are mathematical processes that take input data of any size, perform required operations on it, and return the output data of a fixed size. These functions can be used to take a string of any length as input and return a sequence of letters of a fixed length. This functionality of hash functions makes them apt for transaction processing. Regardless of the size of transactions, the final output will always be fixed and untampered.

Under the hood of blockchains, hashing is necessarily a process that helps differentiate between blocks. The process of hashing gives blocks in a blockchain a unique identity. Technically, blocks in a blockchain are identified by their hash, which serves the purposes of both identification and integrity verification. An identification string that also provides its own integrity is called **a self-certifying identifier**. The hashing functions generate public keys. Here’s an example pertaining to hashing for bitcoin blockchains.

Bitcoin uses the SHA-256 hash function that produces a hash code of size 256 bits or 32 bytes.



Bob, while placing an order with Lisa, creates a message which is like the one shown above. This message is hashed through a hash function that produces a 32 byte hash code. The beauty of the hash is that for all practical purposes it can be considered unique for the contents of the message. If the message is modified, the hash value will change. This makes it impossible to reconstruct the original message. Hacking, therefore, is a distant dream with hash functions.

* **Blockchain Nodes**

In simple terms, every participant in a blockchain network is a node. Being a decentralized network where a central authority is absent, there is great value for blockchain nodes. There exist several types of blockchain nodes, and each of them requires specific hardware configurations to get hosted or connected. Basically, there are two types of nodes: full nodes and lightweight nodes. These types comprise a constellation of a variety of nodes that are grouped under them.



**i. Full nodes**: They act as a server in a decentralized network. Their main tasks include maintaining the consensus between other nodes and verifying the transactions. They also store a copy of the blockchain, thus being able to securely enable custom functions such as instant send and private transactions. When making decisions for the future of a network, full nodes are the ones that vote on proposals.

**ii. Pruned Full Nodes:** The specific characteristic here is that these nodes begin to download blocks from the beginning, and once they reach the set limit, the oldest ones are deleted, retaining only their headers and chain placement.

**iii. Archival Full Nodes:** These are what most people refer to when they talk about full nodes. These nodes envision a server that hosts the full Blockchain in its database.

**iv. Lightweight or Simple Payment Verification (SPV) nodes:** On the other hand, they are used in day-to-day cryptocurrency operations. These nodes communicate with the blockchain while relying on full nodes to provide them with the necessary sets of information. They do not store a copy of the blockchain but only query the current status for the last block. Also, they broadcast transactions to other nodes in the network for processing.

**v. Master Nodes:** Compared to full nodes, Master nodes themselves cannot add blocks to the blockchain. Their only purpose is to keep a record of transactions and validate them. Whether Mining or Staking nodes, they’re the ones who write blocks on the blockchain.

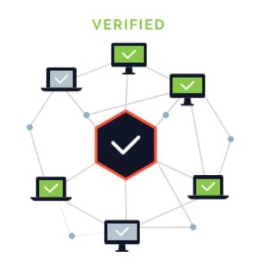
**vi. Mining Nodes:** The mining node competes with other miners to add the next block of transactions to the blockchain in order to be rewarded with fees and newly generated cryptocurrency.

**vii. Staking Nodes:** The nodes which verify the validity of transactions in the blockchains using the Proof of Stake consensus model are called staking nodes. To set up a staking node, users have to lock a certain amount of native tokens of that ecosystem on the blockchain.

**viii. Authority Nodes:** Authority nodes are of use to centralized blockchains. The owners of these networks will decide upon the validators of transactions. In the Delegated Proof of Stake system, for example, the network's users take a vote on who gets to validate the following block.

**Blockchain Consensus**

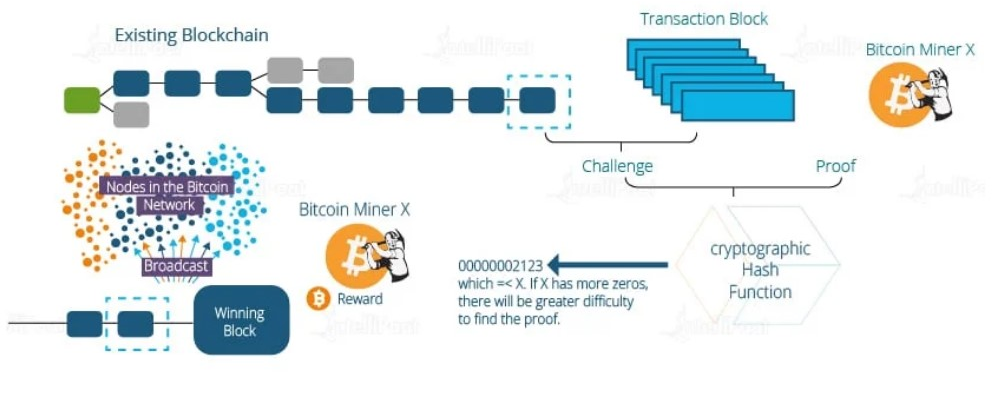
The set of rules by which a blockchain network operates and validates the information of blocks is known as ‘consensus’. Since cryptocurrencies operate on a decentralized P2P network, it won’t be wrong to assume that complications are bound to arise when a decision needs to be taken. This is where consensus comes in handy. While consensus must be achieved by a certain type of node, in P2P networks any user can become a full node and thus gain supremacy over others.

****

When at least 51% of nodes agree on something, the decision is validated on behalf of the whole of the blockchain. This 51% rule may result in threats even. The most common threat to a blockchain is the 51% attack, where more than half of the nodes are concentrated in one entity. This paves the way for the entity to change consensus rules as it sees fit, which could lead to a monopoly.

**Blockchain Proof of Work**

A popular consensus mechanism for blockchains, Proof of Work is a requirement through which expensive computations, also called mining, can be performed in order to facilitate transactions on the blockchain. Although it might be hard for nodes to generate a valid block, it is quite easy for the network to validate the block’s authenticity. This is achieved through hash functions. Since hashes are quite sensitive to changes and even minute modifications will result in a completely different hash output, they can be used to validate and secure blocks.



For a block to be confirmed as valid, miners are required to generate two hashes: a hash of all the transactions in the block and one proving that they have expended the energy required to generate the block by solving a special cryptographic puzzle with a pre-set level of difficulty. The difficulty of solving the puzzle can be automatically adjusted in Proof of Work systems to create a consistent time period for blocks that are to be added to the blockchain.

In summary, a miner creates a block of valid transactions. Further, the miner runs a Proof of Work algorithm on it to find a valid hash. When a valid block is generated, the block is added to the blockchain, and the miner receives network fees and the newly created cryptocurrency.

**Blockchain Versions**

**i. BlockChain 1.0 (Cryptocurrency) –**

BlockChain Version 1.0 was introduced in 2005 by Hall Finley, who implemented DLT (Distributed Ledger Technology) represents its first application based on Crypto currency. This allows Financial Transaction based on BlockChain technology or DTL which is executed with the help of BitCoin. This type of Version is permissionless as any participant will perform valid transaction of Bitcoin. This type is mainly used in Currency and Payments.

**ii. BlockChain 2.0 (Smart Contracts) –**

The new Version of BlockChain come because there is a problem in version 1.0 which was Mining of BitCoin was Wasteful and there was also lack of Scalability of Network in it. So problem is addressed in Version 2.0. In this version, the BlockChain is not just limited to Cryptocurrencies but it will extend up to Smart Contracts.

Thus, Smart Contracts are Small Computers which live in the Chains of Blocks. These Small Computers are free computer programs that executed automatically, and check the condition defined earlier like facilitation, verification or enforcement and reduce transactions cost.

In BlockChain 2.0, BitCoin is replaced with Ethereum. Thus, BlockChain 2.0 was successfully processing high number of Transactions on Public network rapidly.

**iii. BlockChain 3.0 (DApps) –**

After Version 2.0, new version was introduced which includes DApps which is known as Decentralized Apps. A DApp is like a conventional app, it can have frontend written in any language that makes calls to its backend, and its backend code is running on decentralized Peer-To-Peer Network. It makes use of decentralized storage and communication which can be Ethereum Swarm etc.

There are many decentralized Applications like BitMessage, BitTorrent, Tor, Popcorn, etc.

**Blockchain Variants**

There are four main types of blockchain networks: public blockchains, private blockchains, consortium blockchains and hybrid blockchains. Each one of these platforms has its benefits, drawbacks and ideal uses.

1. **Public blockchain**

The first type of blockchain technology is public blockchain. This is where cryptocurrency like Bitcoin originated and helped to popularize distributed ledger technology (DLT). It removes the problems that come with centralization, including less security and transparency. DLT doesn't store information in any one place, instead distributing it across a peer-to-peer network. Its decentralized nature requires some method for verifying the authenticity of data. That method is a consensus algorithm whereby participants in the blockchain reach agreement on the current state of the ledger. Proof of work (PoW) and proof of stake (PoS) are two common consensus methods.

Public blockchain is non-restrictive and permissionless, and anyone with internet access can sign on to a blockchain platform to become an authorized node. This user can access current and past records and conduct mining activities, the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed on the network, and anyone can verify the transactions, find bugs or propose changes because the source code is usually open source.

**Advantages:** One of the advantages of public blockchains is that they are completely independent of organizations, so if the organization that started it ceases to exist the public blockchain will still be able to run, as long as there are computers still connected to it. Some blockchains incentivize users to commit computer power to secure the network by providing a reward. Another advantage of public blockchains is the network's transparency. As long as the users follow security protocols and methods, public blockchains are mostly secure.

**Disadvantages:** The network can be slow, and companies can't restrict access or use. If hackers gain 51% or more of the computing power of a public blockchain network, they can unilaterally alter it.

Public blockchains also don't scale well. The network slows down as more nodes join the network.

**Use cases:** The most common use case for public blockchains is mining and exchanging cryptocurrencies like Bitcoin. However, it can also be used for creating a fixed record with an auditable chain of custody, such as electronic notarization of affidavits and public records of property ownership. This type of blockchain is ideal for organizations that are built on transparency and trust, such as social support groups or non-governmental organizations. Because of the public nature of the network, private businesses will likely want to steer clear.

1. **Private Blockchain**

A blockchain network that works in a restrictive environment like a closed network, or that is under the control of a single entity, is a private blockchain. While it operates like a public blockchain network in the sense that it uses peer-to-peer connections and decentralization, this type of blockchain is on a much smaller scale. Instead of just anyone being able to join and provide computing power, private blockchains typically are operated on a small network inside a company or organization. They're also known as permissioned blockchains or enterprise blockchains.

**Advantages:** The controlling organization sets permission levels, security, authorizations and accessibility. For example, an organization setting up a private blockchain network can determine which nodes can view, add or change data. It can also prevent third parties from accessing certain information. Because they're limited in size, private blockchains can be very fast and can process transactions much more quickly than public blockchains.

**Disadvantages:** The disadvantages of private blockchains include the controversial claim that they aren't true blockchains, since the core philosophy of blockchain is decentralization. It's also more difficult to fully achieve trust in the information, since centralized nodes determine what is valid. The small number of nodes can also mean less security. If a few nodes go rogue, the consensus method can be compromised. Additionally, the source code from private blockchains is often proprietary and closed. Users can't independently audit or confirm it, which can lead to less security. There is no anonymity on a private blockchain, either.

**Use cases:** The speed of private blockchains makes them ideal for cases where the blockchain needs to be cryptographically secure but the controlling entity doesn't want the information to be accessed by the public. Other use cases for private blockchain include supply chain management, asset ownership and internal voting.

1. **Hybrid Blockchain**

Sometimes, organizations will want the best of both worlds, and they'll use hybrid blockchain, a type of blockchain technology that combines elements of both private and public blockchain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the blockchain, and what data will be opened up publicly.

Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed, such as by allowing access through a smart contract. Confidential information is kept inside the network but is still verifiable. Even though a private entity may own the hybrid blockchain, it cannot alter transactions.

When a user joins a hybrid blockchain, they have full access to the network. The user's identity is protected from other users, unless they engage in a transaction. Then, their identity is revealed to the other party.

**Advantages:** One of the big advantages of hybrid blockchain is that, because it works within a closed ecosystem, outside hackers can't mount a 51% attack on the network. It also protects privacy but allows for communication with third parties. Transactions are cheap and fast, and it offers better scalability than a public blockchain network.

**Disadvantages:** This type of blockchain isn't completely transparent because information can be shielded. Upgrading can also be a challenge, and there is no incentive for users to participate or contribute to the network.

**Use cases:** Hybrid blockchain has several strong use cases, including real estate. Companies can use a hybrid blockchain to run systems privately but show certain information, such as listings, to the public. Retail can also streamline its processes with hybrid blockchain, and highly regulated markets like financial services can also see benefits from using it. Medical records can be stored in a hybrid blockchain. The record can't be viewed by random third parties, but users can access their information through a smart contract. Governments could also use it to store citizen data privately but share the information securely between institutions.

1. **Consortium Blockchain**

The fourth type of blockchain, consortium blockchain, also known as a federated blockchain, is similar to a hybrid blockchain in that it has private and public blockchain features. But it's different in that multiple organizational members collaborate on a decentralized network. Essentially, a consortium blockchain is a private blockchain with limited access to a particular group, eliminating the risks that come with just one entity controlling the network on a private blockchain.

In a consortium blockchain, the consensus procedures are controlled by preset nodes. It has a validator node that initiates, receives and validates transactions. Member nodes can receive or initiate transactions.

**Advantages:** A consortium blockchain tends to be more secure, scalable and efficient than a public blockchain network. Like private and hybrid blockchain, it also offers access controls.

**Disadvantages:** Consortium blockchain is less transparent than public blockchain. It can still be compromised if a member node is breached, the blockchain's own regulations can impair the network's functionality.

**Use cases:** Banking and payments are two uses for this type of blockchain. Different banks can band together and form a consortium, deciding which nodes will validate the transactions. Research organizations can create a similar model, as can organizations that want to track food. It's ideal for supply chains, particularly food and medicine applications.

Blockchain technology is becoming more popular and rapidly gaining enterprise support. Every one of these types of blockchain has potential application that can improve trust and transparency and create a better record of transactions.

**Blockchain Vs. Shared Database**

Both blockchains and databases have a similar goal of maintaining a consistent copy of a particular dataset across a number of nodes. Maintaining consensus on the data that is stored, as well as keeping redundant copies of this dataset, are the major similarities between the technologies. Blockchain is a peer to peer decentralized distributed ledger technology whereas databases are centralized ledger which stores data in a structured way and is managed by an administrator.

* Authority – Blockchain is decentralized and has no centralized approach. But, private blockchains may utilize some form of centralization whereas databases are controlled by the administrator and are certified in nature.
* Architecture – Blockchain uses a distributed ledger network architecture whereas database utilises a client-server architecture.
* Data Handling – Blockchain utilizes Read and Write operations whereas the database supports CRUD (Create, Read, Update and Delete) operations.
* Integrity – Blockchain data supports integrity whereas malicious actors can alter database data.
* Transparency – Public blockchain offers transparency whereas databases are not transparent. Only the administrator decides which data can be accessed by the public.
* Cost – Blockchain are comparatively harder to implement and maintain whereas the database being an old technology is easy to implement and maintain.
* Performance – Blockchain involves the verification and consensus methods whereas the databases are extremely fast and offer great scalability.

**Introduction to Cryptocurrencies**

1. **What is Cryptocurrency?**

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

The first cryptocurrency was Bitcoin, which was founded in 2009 and remains the best known today. Much of the interest in cryptocurrencies is to trade for profit, with speculators at times driving prices skyward.

1. **How does Cryptocurrency work?**

Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders. 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. If you own cryptocurrency, you don’t own anything tangible. What you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party.

Although Bitcoin has been around since 2009, cryptocurrencies and applications of blockchain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.

1. **Cryptocurrency Examples**

There are thousands of cryptocurrencies. Some of the best known include:

**Bitcoin:**

Founded in 2009, Bitcoin was the first cryptocurrency and is still the most commonly traded. The currency was developed by Satoshi Nakamoto – widely believed to be a pseudonym for an individual or group of people whose precise identity remains unknown.

**Ethereum:**

Developed in 2015, Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum. It is the most popular cryptocurrency after Bitcoin.

**Litecoin:**

This currency is most similar to bitcoin but has moved more quickly to develop new innovations, including faster payments and processes to allow more transactions.

**Ripple:**

Ripple is a distributed ledger system that was founded in 2012. Ripple can be used to track different kinds of transactions, not just cryptocurrency. The company behind it has worked with various banks and financial institutions.

1. **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**

Once you have chosen your platform, 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, and some exchanges don't support them. Some credit card companies don't allow crypto transactions either. This is because cryptocurrencies are highly volatile, and it is not advisable to risk going into debt — or potentially paying high credit card transaction fees — for certain assets.

Some platforms will also accept ACH transfers and wire transfers. The accepted payment methods and time taken for deposits or withdrawals differ per platform. Equally, the time taken for deposits to clear varies by payment method.

An important factor to consider is fees. These include potential deposit and withdrawal transaction fees plus trading fees. Fees will vary by payment method and platform, which is something to research at the outset.

**Step 3: Placing an order**

You can place an order via your broker's or exchange's web or mobile platform. If you are planning to buy cryptocurrencies, you can do so by selecting "buy," choosing the order type, entering the amount of cryptocurrencies you want to purchase, and confirming the order. The same process applies to "sell" orders.

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.

1. **How to store Cryptocurrency?**

Once you have purchased cryptocurrency, you need to store it safely to protect it from hacks or theft. Usually, cryptocurrency is stored in crypto wallets, which are physical devices or online software used to store the private keys to your cryptocurrencies securely. Some exchanges provide wallet services, making it easy for you to store directly through the platform. However, not all exchanges or brokers automatically provide wallet services for you.

There are different wallet providers to choose from. The terms “hot wallet” and “cold wallet” are used:

* **Hot wallet storage:** "hot wallets" refer to crypto storage that uses online software to protect the private keys to your assets.
* **Cold wallet storage:** Unlike hot wallets, cold wallets (also known as hardware wallets) rely on offline electronic devices to securely store your private keys.

Typically, cold wallets tend to charge fees, while hot wallets don't.

1. **Applications**

When it was first launched, Bitcoin was intended to be a medium for daily transactions, making it possible to buy everything from a cup of coffee to a computer or even big-ticket items like real estate. That hasn’t quite materialized and, while the number of institutions accepting cryptocurrencies is growing, large transactions involving it are rare. Even so, it is possible to buy a wide variety of products from e-commerce websites using crypto. Here are some examples:

**Technology and e-commerce sites:**

Several companies that sell tech products accept crypto on their websites, such as newegg.com, AT&T, and Microsoft. Overstock, an e-commerce platform, was among the first sites to accept Bitcoin. Shopify, Rakuten, and Home Depot also accept it.

**Luxury goods:**

Some luxury retailers accept crypto as a form of payment. For example, online luxury retailer Bitdials offers Rolex, Patek Philippe, and other high-end watches in return for Bitcoin.

**Cars:**

Some car dealers – from mass-market brands to high-end luxury dealers – already accept cryptocurrency as payment.

**Insurance:**

In April 2021, Swiss insurer AXA announced that it had begun accepting Bitcoin as a mode of payment for all its lines of insurance except life insurance (due to regulatory issues). Premier Shield Insurance, which sells home and auto insurance policies in the US, also accepts Bitcoin for premium payments.

If you want to spend cryptocurrency at a retailer that doesn’t accept it directly, you can use a cryptocurrency debit card, such as BitPay in the US.

**MODULE 3**

**Hashing in Blockchain**

Blockchain technology is an intricate web of several technological innovations working together. Among the most important pieces of the blockchain puzzle is hashing.

Hashing is a cryptographic function that converts a string of characters of any length into a unique output, or hash, of fixed length. This means that no matter what combination of symbols are used as the input, they will always produce a one-of-a-kind string of digits and characters.

A Bitcoin hash looks like this:

00000000000000000025e2ba026a8ad462b9a693d80fd0887def167f5f888a11

(hash of block 540807)

1. **Hashing Essentials**

* Hashing is a method for cryptographically encoding data.
* It produces a fixed-length output from any input.
* The same input always produces the same hash.
* The input cannot be reconstructed from the hash.
* Modern hash functions make it virtually impossible to produce the same output from two different inputs.

1. **Hashing in Cryptocurrencies**

Hashing is an integral part of all blockchain-based transactions, including the trading of cryptocurrency. Hash functions are necessary in everything from mining blocks to signing transactions to generating private keys.

Bitcoin SHA-256

Bitcoin Cash SHA-256

Ethereum keccak256

Litecoin scrypt

Ripple SHA-512

A hash function is a mathematical algorithm used to calculate the hash. Different cryptocurrencies use different hash functions but all of them follow the same basic principles of hashing.

1. **Main Properties of Hashing**

* **Hashing produces outputs of fixed length**

Hashing will always produce a unique, fixed-length output from any input. Let us take a look at what that means with a couple of examples.

Input: hello

Output: 2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824

Input: It’s a good day to HODL

Output: 6B89D5D4AD6A3364410DD9BAB95FD250EF4A663D9D3C47CBD7388535A5912E03

Input: The entire novel of Oliver Twist

Output: 4F144CC612CA27E2DD6DFD6663F68BABC3B758D602B5102BF14E717E823EB741

Here, the SHA-256 hash function is used to generate the hashes of two different inputs. In all three cases, the hash is completely unique, but its length remains the same. SHA-256 generates hashes that are 256 bits long, usually represented as 64 symbols comprised of numbers 0–9 and letters A–F. No matter how short or how long the input is – be it a single word (hello) or even a whole novel (Oliver Twist by Charles Dickens) – the hash is fixed at 64 characters.

* **Hashing is deterministic**

The same input will always produce the same output. If you use SHA-256 to generate a hash from “fun”, you will always get the output seen in the table below. Even changing one letter, however, will produce a completely different hash.

Input: fun

Output: 00C4285274FCC5D6FBA2EE58DAF0D8C2B9B825B68D35D65D0E90A9BB333A51B5

Input: sun

Output: 27756F050E14A1CB1C1EE867F0EACE9EA4D9FCB81B8BEE089469F1EBD5FD7B17

* **Hashing is a one-way function**

It is infeasible to determine what the input was from any given output. That is to say, it is virtually impossible to reverse the hash function with contemporary technology. The only way to determine what the input was is trying out random strings until you find the right one. This method is known as brute force.

Using brute force to reverse the hash back to the original string is easier said than done. No computer in existence is powerful enough to find the solution in any reasonable amount of time, nor are we ever likely to build one that will. Even IBM Summit, currently the fastest computer in the world, capable of making several trillion calculations per second, would need many years and an astounding amount of electricity to find the answer for a single hash.

* **Hashing is resistant to collisions**

A collision occurs when a hashing mechanism produces the same output for two different inputs. This is possible in theory for hashing, as the number of unique hashes is limited but the number of inputs is not. However, the probability of collisions is extremely small. Hashing is thus said to be resistant, but not immune, to collisions.

SHA-256, the algorithm used by Bitcoin, outputs hashes that are 256 bits long (a 256 digit-long string of 1s and 0s). This means there are a total of 2256 unique hashes that it can produce. As soon as the number of inputs is larger than the number of all possible outputs, let us say 2256+1, at least two of the inputs will have the same output – that’s a collision.

So does that mean hashing is exploitable? No, not at all. 2256 is an enormous number. The sheer size of this number means the likelihood of a collision occurring is utterly miniscule.

**Concept of Double Spending**

Double-spending is the risk that a cryptocurrency can be used twice or more. Transaction information within a blockchain can be altered if specific conditions are met. The conditions allow modified blocks to enter the blockchain; if this happens, the person that initiated the alteration can reclaim spent coins.

To understand double-spending, it helps to review how the blockchain works first. When a block is created, it receives a hash—or encrypted number—that includes a timestamp, information from the previous block, and transaction data. This information is encrypted using a security protocol like the SHA-256 algorithm used by Bitcoin. Once that block's information is verified by miners (in proof-of-work consensus), it is closed, and a new one is created with the timestamp, transaction information, and previous block's hash. A Bitcoin is awarded to the miner whose machine verified the hash.

For someone to double spend, a secret block has to be mined that outpaces the creation of the real blockchain. They would then need to introduce that chain to the network before it caught up—if this happened, then the network would recognize it as the latest set of blocks and add it to the chain. The person that did this could then give themselves back any cryptocurrency they had spent and use it again.

* **Preventing Double Spending**

Double spending remains a risk; however, it is minimized by the blockchain. The likelihood of a secret block being inserted into the blockchain is very slim because it has to be accepted and verified by the network of miners. The only chance a miner with illicit intentions has of inserting an altered block is to attempt to get another user to accept a transaction using their secret block and cryptocurrency. Even then, the likelihood that the modified block will be accepted is very slim. The blockchain and consensus mechanism move so quickly that the modified block would be outdated before it was accepted. Even if it was accepted, the network would still have passed up the information in the block and would reject it. Cryptocurrency transactions take some time to verify because the process involves randomly selecting numbers to solve the complex hash—this also takes up a great deal of computational power. It is, therefore, exceedingly difficult to duplicate or falsify the blockchain because of the immense amount of computing power needed to stay ahead of all of the other miners on the network.

* **Double Spending Attacks**

The most significant risk for blockchains comes in the form of a 51% attack, which can occur if a miner controls more than 50% of the computing power that validates the transactions, creates blocks, and awards cryptocurrency. If this user—or users—controls a majority of the hashing in the blockchain, they will be able to dictate transaction consensus and control the award of currency. In more popular cryptocurrencies such as Bitcoin, this is very unlikely due to the number of miners and hashing difficulty it has reached; however, new or forked cryptocurrencies with smaller networks are susceptible to this attack. Most commonly, the unconfirmed transaction attack is used to fool cryptocurrency users. If you see one of these transactions, you shouldn't accept it because it can cause an attempted double-spend attack.

**Mining**

Blockchain mining is a peer-to-peer computer process and is used to secure and verify bitcoin transactions. Mining involves blockchain miners who add bitcoin transaction data to Bitcoin’s global public ledger of past transactions. In the ledgers, blocks are secured by blockchain miners and are connected to each other forming a chain.

When we talk in-depth, as opposed to traditional financial services systems, Bitcoins have no central clearing house. Bitcoin transactions are generally verified in decentralized clearing systems wherein people contribute computing resources to verify the same. This process of verifying transactions is called mining. It is probably referred to as mining as it is analogous to mining of commodities like gold—mining gold requires a lot of effort and resources, but then there is a limited supply of gold; hence, the amount of gold that is mined every year remains roughly the same. In the same manner, a lot of computing power is consumed in the process of mining bitcoins. The number of bitcoins that are generated from mining dwindles over time. In the words of Satoshi Nakamoto, there is only a limited supply of bitcoins. Only 21 million bitcoins will ever be created.

At its core, the term ‘Blockchain mining’ is used to describe the process of adding transaction records to the bitcoin blockchain. This process of adding blocks to the blockchain is how transactions are processed and how money moves around securely on Bitcoins. This process of blockchain mining is performed by a community of people around the world called ‘Blockchain miners.’

Anyone can apply to become a blockchain miner. These Blockchain miners install and run a special blockchain mining software that enables their computers to communicate securely with one another. Once a computer installs the software, joins the network, and begins mining bitcoins, it becomes what is called a ‘node.’ Together, all these nodes communicate with one another and process transactions to add new blocks to the blockchain which is commonly known as the bitcoin network. This bitcoin network runs throughout the day. It processes equivalent to millions of dollars in bitcoin transactions and has never been hacked or experienced downtime since its launch in 2009.

1. **Types of Mining**

The process of mining can get really complex and a regular desktop or PC cannot cut it. Hence, it requires a unique set of hardware and software that works well for the user. It helps to have a custom set specific to mining certain blocks.

The mining process undertaking can be divided into three categories:

**a. Individual Mining**

When mining is done by an individual, user registration as a miner is necessary. As soon as a transaction takes place, a mathematical problem is given to all the single users in the blockchain network to solve. The first one to solve it gets rewarded. Once the solution is found, all the other miners in the blockchain network will validate the decrypted value and then add it to the blockchain thus verifying the transaction.

**b. Pool Mining**

In pool mining, a group of users works together to approve the transaction. Sometimes, the complexity of the data encrypted in the blocks makes it difficult for a user to decrypt the encoded data alone. So, a group of miners works as a team to solve it. After the validation of the result, the reward is then split between all users.

**c. Cloud Mining**

Cloud mining eliminates the need for computer hardware and software. It’s a hassle-free method to extract blocks. With cloud mining, handling all the machinery, order timings, or selling profits is no longer a constant worry. While it is hassle-free, it has its own set of disadvantages. The operational functionality is limited with the limitations on bitcoin hashing. The operational expenses increase as the reward profits are low. Software upgrades are restricted and so is the verification process.

1. **Mining Bitcoins**

**a. Mining Bitcoins in Cloud**

***Obtain a bitcoin wallet:*** Bitcoins are stored in digital wallets in an encrypted manner. This will keep your bitcoins safe.

***Secure the wallet:*** Since there is no ownership of bitcoins, anyone who gains access to your blockchain wallet can use it without any restriction. So, enable two-factor authentication and store the wallet on a computer that does not have access to the Internet or store it on an external device.

***Choose a cloud mining service provider:*** Cloud mining service providers allow users to rent processing or hashing power to mine bitcoins remotely. Popular cloud mining service providers are Genesis Mining and HashFlare.

***Choose a cloud mining package:*** To choose a package, you will need to decide on how much you are willing to pay and keep your eyes open to the hashing power the package will offer. Cloud mining companies will mostly envisage the Return on Investment (ROI) based on the current market value of Bitcoins.

***Pick a mining pool:*** This is the best shot you can get to earn bitcoins easily. There are many mining pools which charge a mere 2 percent of your total earnings. Over here, you will have to create workers which are basically subaccounts that can be used to track your contributions to the pool.

***Put your earnings in your own secure wallet:*** Whenever you witness an ROI, simply withdraw your earnings and put them in your own secure wallet.

**b. Mining Bitcoins on your own**

***Purchase custom mining hardware:*** You need to purchase an Application-specific Integrated Circuit (ASIC) miner to mine bitcoins. While purchasing an ASIC Blockchain miner, you should consider its efficacy in hashing power and take note of its pricing policies.

***Purchase a power supply:*** Blockchain miners consume a lot of power. So, get a dependable power supply that is compatible with the ASIC miner that you purchase.

***Obtain a bitcoin wallet:*** Bitcoins are stored in digital wallets in an encrypted manner. This will keep your bitcoins safe.

***Secure the wallet:*** Since there is no ownership on bitcoins, anyone who gains access to your wallet can use it without any restriction. So, enable two-factor authentication and store the wallet on a computer that does not have access to the Internet or store it in an external device.

***Pick a mining pool:*** This is the best shot you can get to earn bitcoins easily. There are many mining pools that charge a mere 2 percent of your total earnings. Over here, you will have to create workers which are basically subaccounts that can be used to track your contributions to the pool.

1. **Uses of Blockchain Mining**

**a. Validating Transactions**

Bitcoin transactions take place in huge figures every day. Cryptocurrencies function without a central administrator and the insecurity can be substantial with the transactions that transpire. So, what is the authentication method with such cryptocurrencies? With each transaction, new blocks are added to the blockchain in the network and the validation lies in the mining results from the blockchain miners.

**b. Confirming Transactions**

Miners work the blockchain mining process to confirm whether the transaction is authentic or not. All confirmed transactions are then included in the blockchain.

**c. Securing Network**

To secure the transaction network, bitcoin miners work together. With more users mining the blockchain, blockchain network security increases. Network security ensures that there are no fraudulent activities happening with cryptocurrencies.

**Proof of Work (PoW)**

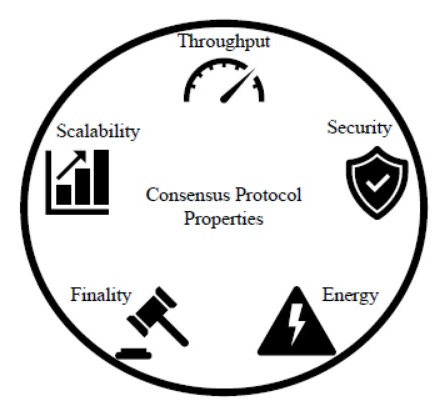
Proof-of-Work (PoW) in the blockchain is a consensus mechanism that allows miners to add a new block to the network based on calculations made to find the perfect hash. Network participants verify the transactions added by the new block.

For a decentralized network like Blockchain, keeping all network participants in sync is essential. However, it seems far-fetched for everyone to agree on one thing. Blockchain uses a consensus mechanism to create governance among all network participants.

1. **Consensus Mechanism**

Consensus means reaching a decision that all network participants agree on. For example, a group of friends agrees to play soccer without conflict. Reaching a decision to play football together is a state of consensus or mutual agreement here.

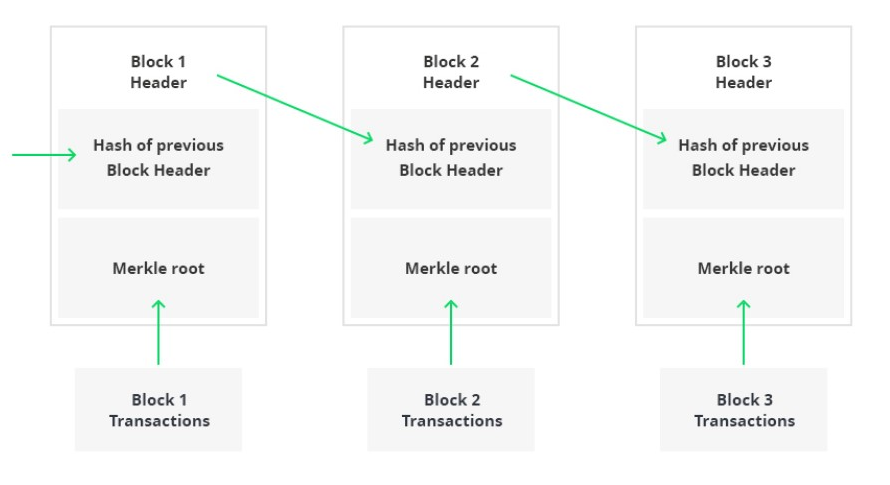
In the case of Blockchain, at least 51% of nodes or network participants agree on the upcoming change. If this happens, the network is updated with the new change. Otherwise, they reject the change by mutual agreement.



The Proof-of-Work (PoW) consensus mechanism is the oldest yet most popular. The idea emerged in 1993 when Moni Naor and Cynthia Dowrk published a paper exploring the potential of algorithms to prevent fraud.

PoW plays a significant role in the development of Blockchain technology. The goal is to create an authentication system that is hard to crack. The decentralized network works on the principle of distrust but cooperation. Blockchain (decentralized network) is a chain of linearly connected blocks containing information secured by cryptography. Here, each block contains the hash of its previous block to stay connected.

Additionally, each block contains several other information such as timestamp, block height, transaction records, Merkle Root Hash, block hash, previous block hash, difficulty level, and many more in the block header. The second part contains a set of financial transactions, the hash of which is eventually converted to a Merkle root. So Blockchain is defined as the chain of blocks of transactions.



Adding a new block to the chain is considered a new update to the current system. It, therefore, requires permission from network participants. In order to decide whether to add a new block or not, Proof-of-Work (PoW), a consensus mechanism, is used. Only verified transactions are added to the network.

In contrast, not all blocks are valid. Most proposed block networks are considered invalid. The Blockchain protocol defines the validity of a block. The blockchain network has an arbitrary “Difficulty” setting managed by the protocol that changes how hard it is to mine a block. Mining here means adding a new block.

Miners design new blocks in the chain. They are externals who want to add their block to the network. The work required to develop a valid block is where the value comes from. Miners receive rewards in proportion to their share of the computing power they spend mining a new block. The miner proves the work done by mining a valid block.

The difficulty level can vary in blockchains such as the Bitcoin network or Ethereum to ensure that blocks are created at regular intervals.

1. **How does PoW algorithm work?**

The Proof-of-Work (PoW) consensus algorithm works by requiring each miner to overcome a difficulty level to prove the validity of a block. A block is marked as “valid” only if the hash value of the entire block is lower than the difficulty hash.

**Block Hash < Hash Difficulty**

The block contains important transaction information that cannot be changed. So miners change the nonce to get the hash below the difficulty threshold. A nonce is a part of a block that can be changed to limit the difficulty level.

**Let’s take an example to understand the working of PoW**

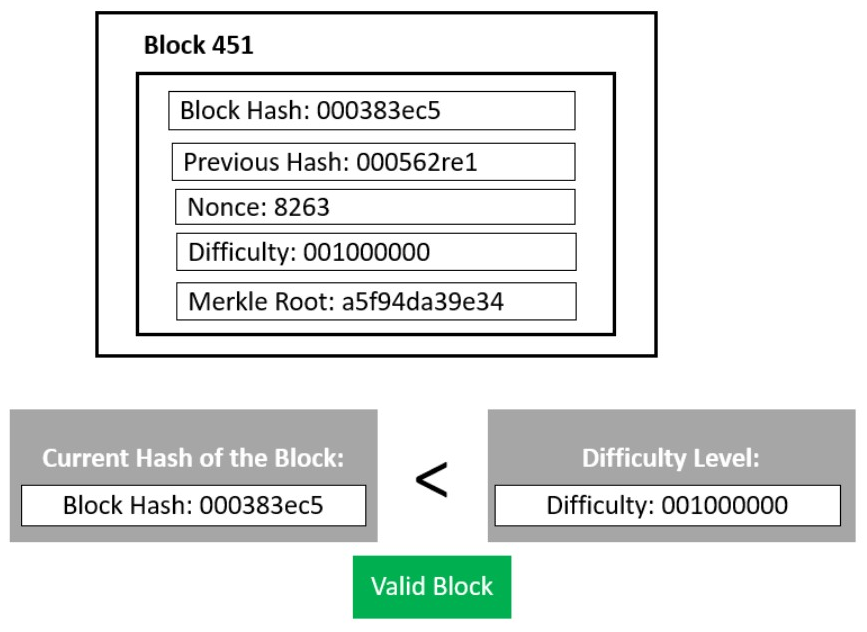
Harry is a Bitcoin miner who wishes to add his block of Bitcoin (digital currency) transactions to the network. However, for his block to be valid, he must change the block until the hash of his block falls below the difficulty threshold.

Let’s say:

**Harry block Hash:** 817de9e0c

**Hash difficulty:** 001000000

**Nonce:** 8263



**Harry will change the nonce until he gets the first 3 digits as zeros.**

After continuously changing the nonce for hours, he finally got the hash.

**Harry block Hash:** 000383ec5

**Hash difficulty:** 001000000

**Nonce:** 6778

The difficulty threshold has now been reached. **Block Hash < Hash Difficulty.**

Therefore, Harry’s block will be marked as valid and added to the blockchain. For mining a block in the Bitcoin blockchain, Harry gets a few Bitcoins as a block reward for spending the computing power to find a valid hash.

This process is completely based on chance. So the miner’s job is to change the nonce value until the total hash of the block is lower than the difficulty hash.

1. **Advantages of Proof-of-Work**

Below are the advantages of the Proof-of-Work (PoW) mechanism:

* A hard-to-find solution. Still, easy verification.
* As an initial consensus mechanism, PoW does not need initial stakes of coins before mining. One can start with 0 coins and it will only be positive.
* Ease of implementation compared to other blockchain consensus mechanisms.
* It is fault tolerant. It means that the failure of one component will not shut down the entire blockchain network.
* Give miners the opportunity to earn by adding a block.
* PoW is the oldest, most trusted, and most popular consensus protocol.

1. **Limitations of Proof-of-Work**

* A lot of energy is wasted because only one miner can finally add their block.
* It requires a lot of computing power and, therefore, massive consumption of resources and energy.
* 51% risk of network attack. A controlling person can get 51% to control the network.
* Spread environmental hazards with attachment machines.
* PoW is a time and energy wipe-out process.
* It required a lot of hardware costs.
* Risk of Denial of Service Attacks by Intruders.

1. **Proof of Work vs. Proof of Stake**

Proof of work and Proof of stake are two discrete consensus mechanisms for cryptocurrency, but there are important differences between them.

Both methods confirm incoming transactions and add them to the blockchain. With Proof of Stake, network participants are known to as “validators” other than miners. One important difference is that instead of solving math problems, validators lock up a set amount of cryptocurrency – their stake – in a smart contract on the blockchain.

In interchange for “staking” cryptocurrency, they get a chance to prove new transactions and earn a reward. However, if they incorrectly verify wrong or fraudulent data, they may lose some or all of their deposit as a penalty.

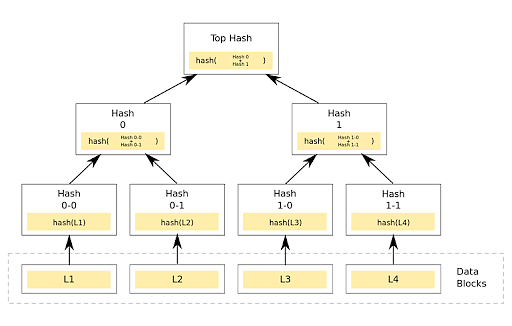
Proof of stake makes it easy to involve more people in blockchain systems as validators. There is no need to buy expensive computing systems and consume huge amounts of electricity to bet cryptocurrencies. All you need are coins.

**Introduction to Merkel Tree**

A hash tree, also known as a Merkle tree, is a tree in which each leaf node is labelled with the cryptographic hash of a data block, and each non-leaf node is labeled with the cryptographic hash of its child nodes' labels. The majority of hash tree implementations are binary (each node has two child nodes), but they can also have many more child nodes.

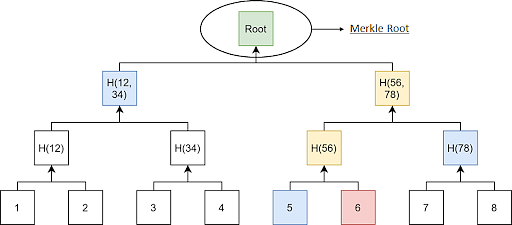
1. **What is a Merkel Tree?**

* Merkle trees, also known as Binary hash trees, are a prevalent sort of data structure in computer science.
* In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.
* It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
* It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.



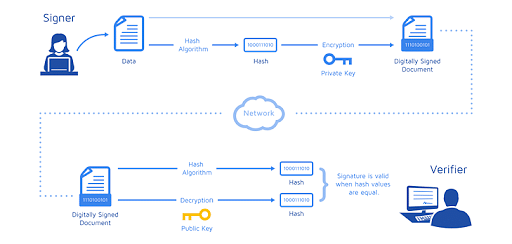
1. **What is a Merkel Root?**

* A Merkle root is a simple mathematical method for confirming the facts on a Merkle tree.
* They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.
* They play a very crucial role in the computation required to keep cryptocurrencies like bitcoin and ether running.



1. **Working of Merkel Trees**

A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether it includes a transaction in the block.



Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains; this hash is known as the Merkle Root or the Root Hash. They're built from the bottom, using Transaction IDs, which are hashes of individual transactions. Each non-leaf node is a hash of its previous hash, and every leaf node is a hash of transactional data.

**Example:**

Consider the following scenario: A, B, C, and D are four transactions, all executed on the same block. Each transaction is then hashed, leaving you with:

* Hash A
* Hash B
* Hash C
* Hash D

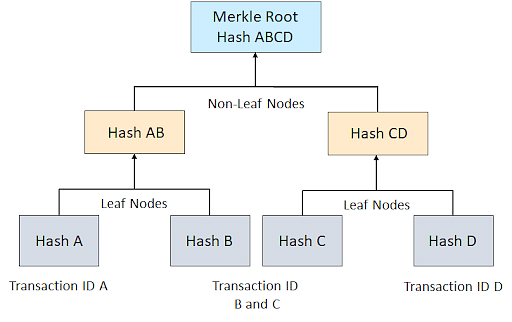
The hashes are paired together, resulting in:

* Hash AB

and

* Hash CD

And therefore, your Merkle Root is formed by combining these two hashes: Hash ABCD.



In reality, a Merkle Tree is much more complicated (especially when each transaction ID is 64 characters long). Still, this example helps you have a good overview of how the algorithms work and why they are so effective.

1. **Benefits of Merkle Tree in Blockchain**

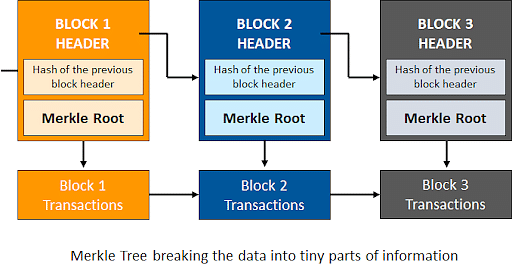
Merkle trees provide four significant advantages -

* ***Validate the data's integrity:*** It can be used to validate the data's integrity effectively.
* ***Takes little disk space:*** Compared to other data structures, the Merkle tree takes up very little disk space.
* ***Tiny information across networks:*** Merkle trees can be broken down into small pieces of data for verification.
* ***Efficient Verification:*** The data format is efficient, and verifying the data's integrity takes only a few moments.

1. **Why is it essential to Blockchain?**

Think of a blockchain without Merkle Trees to get a sense of how vital they are for blockchain technology. Let’s take Bitcoin scenario because its use of Merkle Trees is essential for the cryptocurrency.

If Bitcoin didn't include Merkle Trees, per se, every node on the network would have to retain a complete copy of every single Bitcoin transaction ever made. One can imagine how much information that would be. Any authentication request on Bitcoin would require an enormous amount of data to be transferred over the network: therefore, you'll need to validate the data on your own. To confirm that there were no modifications, a computer used for validation would need a lot of computing power to compare ledgers.



Merkle Trees are a solution to this issue. They hash records in accounting, thereby separating the proof of data from the data itself. Proving that giving tiny amounts of information across the network is all that is required for a transaction to be valid. Furthermore, it enables you to demonstrate that both ledger variations are identical in terms of nominal computer power and network bandwidth.

**Data Privacy and Blockchain**

Data Privacy is sometimes referred to as information privacy, which deals with the proper handling of sensitive data including personal data. Data privacy has regulated the manner in which personal data is collected, processed, stored to ensure proper handling of data.

Data is the most important asset in a business. We live in an era where companies find value in collecting and sharing data. The business had to meet legal responsibilities about the collection, storage, and process of personal data.

Data privacy issues and properly applying laws has increasingly contributed to the business for success. Perspective on objectivity and how they affect the applicability of various data protection and privacy laws have to be drawn. It creates a challenge to identify data controllers and data processors in various blockchain implementations. In distributed blockchain networks there is the territorial implication. A great variety of regulations can incur significant overhead costs. There should be potential restrictions when cross-border data transfer takes place. They require some centralized program to implement them. Difficult to implement in public blockchain with undefined groups. Applying criteria for processing personal data in the blockchain should be structured.

1. **Data Threat Mitigation steps**

Several risk management strategies can be developed when considering data privacy in blockchain technology:

* Use permissioned blockchain to support governance models:
  + Authorize selected number of approved participants.
  + Technical measures to reduce the amount of personal data that participants process.
  + Allocating data processing responsibly.
  + Responding to individual requests.
  + Deploying data processing agreement.
  + View differences between public and private blockchain implementation.
* Limit personal data stored in the blockchain:
  + Avoid putting personal data on a blockchain.
  + The financial system does not involve a naïve user.
  + Avoid payload for storing personal data on the blockchain.
  + Use one-time addresses to secure data in the blockchain.
  + Supply management chain to limit data on the blockchain.

1. **Blockchain Privacy Management**

From the perspective of privacy compliance blockchain technology appear to be least ambiguous. Processing data on a public blockchain may involve significant business risks.

Suggestion from technologists:

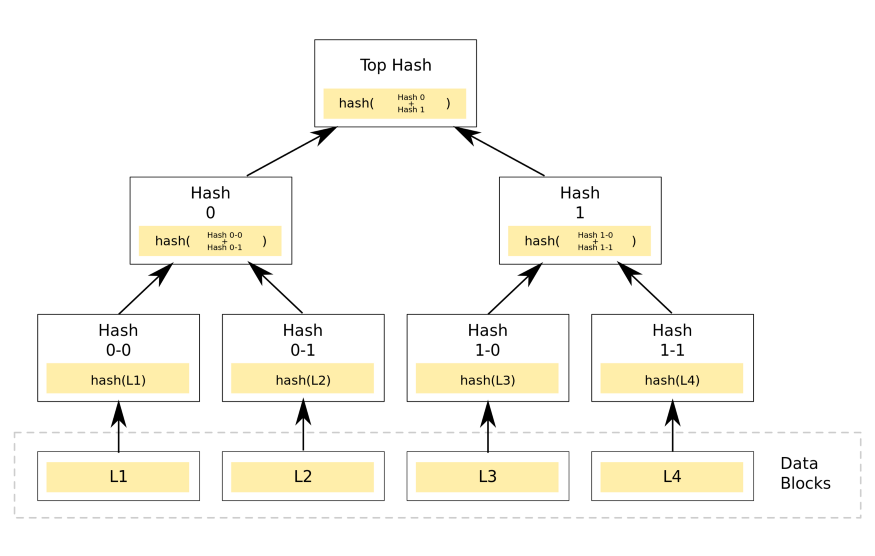
* Managing and verifying consent.
* Minimizing sharing of data between the data controller and data processor.
* Providing individuals with clear notification.

Self-governing blockchain-enabled identity and data management solutions to maintain data and privacy policy can be the potential solutions.

**Payment Verification**

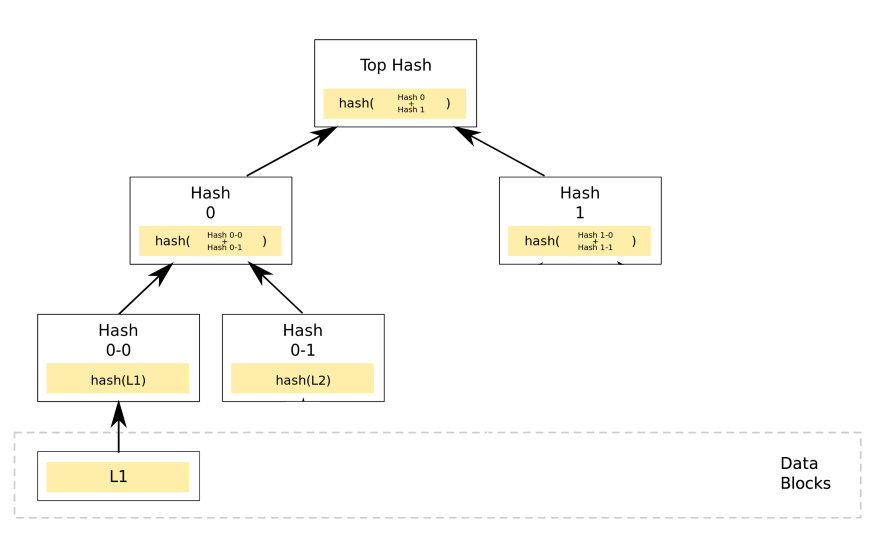
Simple Payment Verification, usually abbreviated to SPV, is a system that enables light clients (wallets running on low-end systems) to verify that a transaction has been included in Bitcoin and therefore a payment has been made.

This is possible by using the Merkle tree to store the transactions in each block. A Merkle tree is a structure created by grouping all the transactions in pairs and hashing them together, then proceeding to hash the resulting hashes together and continuing this process till there is only one hash left, called the merkle root. This creates a tree where every node has two children, which can be used to create their parent node.



Visualization of a merkle tree, L1-L4 are Bitcoin transactions

Someone that only knows the Merkle root/top hash can verify if a transaction is part of the tree, that is, if it’s been included into a Bitcoin block. This is done by taking the nodes that are in the path that connects the Merkle root with one of the bottom transactions and bundling them together to create a proof:



A SPV proof constructed to prove that L1 is included in the block

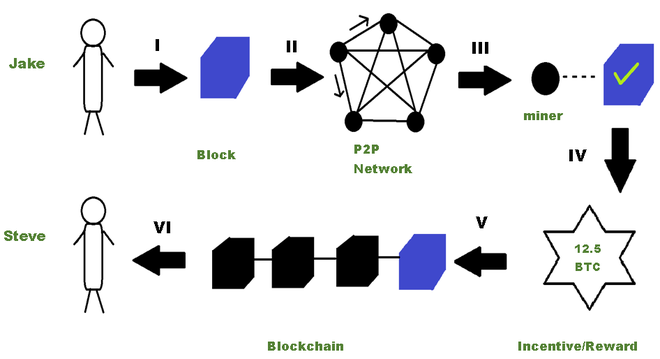
With that proof, our original user that only had access to the top hash can follow the path back to the roots in a verifiable way, he can check that Hash1 and Hash0 hashed together generate the top hash, meaning that Hash1 and Hash0 are its legitimate children, then apply this same check to Hash0–0 and Hash0–1, thus asserting that these two are also part of the original block, and, finally, check that L1 is the source of Hash0–0, proving that L1 is included in the block, therefore confirming it as an accepted Bitcoin transaction.

Running a full node requires downloading the entire blockchain, but if we use SPV proofs we only need to know the merkle root of each block in order to verify the transactions, so we only have to store 80 bytes per block, instead of the much larger size per block required for full nodes. This decrement of over 99.99% makes running the verification inside a low-resource device or a smart contract feasible.

**Resolving Conflicts and Creation of Blocks**

Bitcoin mining is the process of adding transaction records in the form of blocks to the blockchain and the nodes in the network that compete against each other to create a valid block and successfully add it to the blockchain are called miners. Since the process of creating a valid block requires a lot of processing power, there is an incentive mechanism, in which the miners are rewarded for their work via the Proof-of-Work (PoW) algorithm. The PoW algorithm is a consensus algorithm that is adopted in the blockchain network where the miners have to solve complex puzzles (which require a lot of processing power) and then they are paid in bitcoins for creating a valid block and successfully adding it to the blockchain.

The process of adding blocks (transactions) to the blockchain can be understood with the following diagram and its corresponding steps.

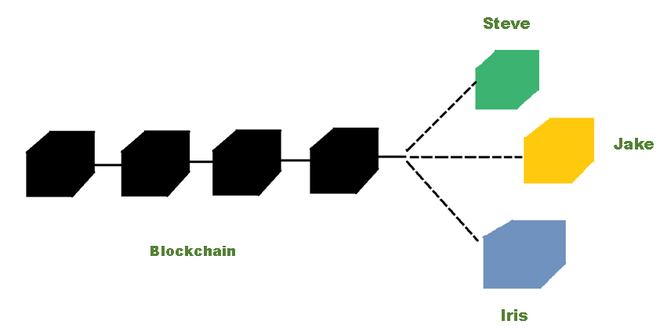


The steps involved in a Bitcoin Transaction are given below:

1. Jake initiates a transaction of say 15 BTC that needs to be transferred to Steve.
2. A block consisting of the transaction is flooded throughout the P2P network.
3. The miners validate the transaction via the proof-of-work consensus algorithm
4. An incentive is given for the miners who successfully create a valid block.
5. The new block consisting of the transaction gets added to the blockchain.
6. Steve receives the 15 BTC that was sent by Jake thereby completing the transaction.

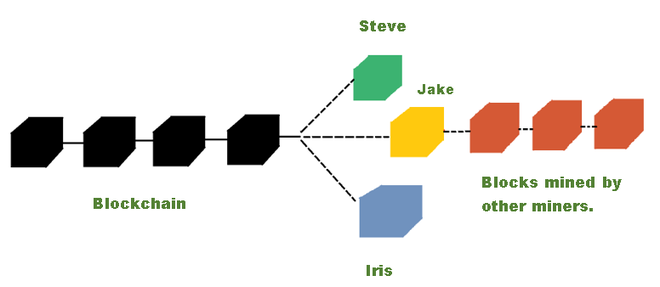
From the above-given steps, in step 5, a conflict can arise where multiple miners create blocks at the same time and try to add them to the last valid block of the blockchain. In this case which block will be appended to the blockchain?

Consider Steve, Jake and Iris are miners in the blockchain and they simultaneously create their respective blocks which are known as candidate blocks (represented in green, yellow, and blue respectively). Out of these candidate blocks, a decision has to be made to choose which of these blocks should be put in the chain.



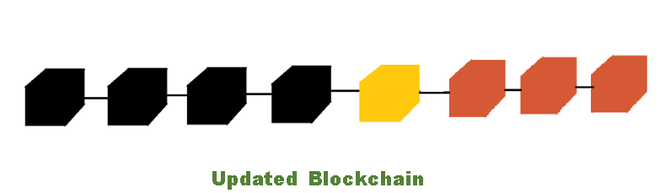
***A conflict arises when Steve, Jake, and Iris mine their block at the same time***

This conflict is resolved using **the longest chain rule** which is adopted by every node in the network to achieve consensus on the valid structure of the blockchain. To add a node in the blockchain, a miner in the network needs to have a computer with high processing power. In this case, let us say Jake’s computer has more processing power as compared to the computers of Steve and Iris. So, Jake can create a block faster than Steve and Iris. Meanwhile, other miners are trying to create other valid blocks, so these blocks are created on the block which has occurred first, and since Jake’s block was created faster than Steve’s and Iris’s, it occurs first in the chain and the miners add their blocks (given below in red ) on top of Jake’s blog (given below in yellow).



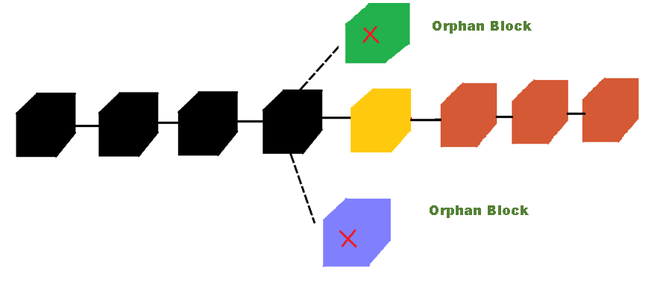
***Other miners create their block at the top of Jake’s block***

It can be seen from the above diagram that the unit with Jake’s block is the longest unit and according to the longest chain rule, the unit with the longest length must be accepted as the valid version of the blockchain. Therefore, the updated valid version of the blockchain looks like the one below:



***The updated version of the blockchain is distributed in the entire P2P network***

The blocks created by Steve and Iris are discarded and they become **orphan blocks** since they are not part of the main chain of blocks anymore.



***Orphan blocks are discarded from the blockchain***

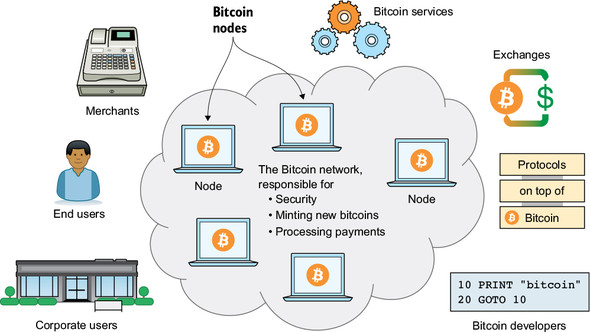
It is important to note that the transactions inside these orphan blocks are valid because someone in the network has initiated it, but cannot be included in the blockchain as they do not follow the longest chain rule. So, these transactions are sent back to the **transaction pool** (which contains those transactions that are not yet mined), where the miners can pick them from the pool and then start mining them again.

**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

1. **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.

1. **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.

1. **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.

1. **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**

1. **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

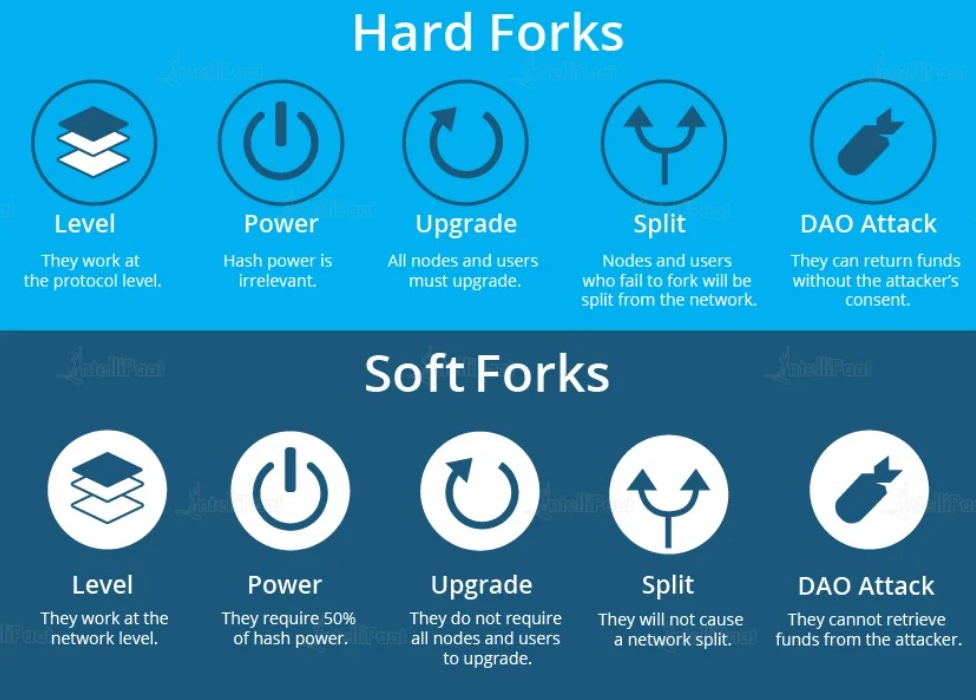
The decentralized nature of public blockchains means that the participants on the network must be able to come to an agreement as to the shared state of the blockchain. The unanimous consensus among the network nodes results in a single blockchain that contains verified data that the network asserts 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.

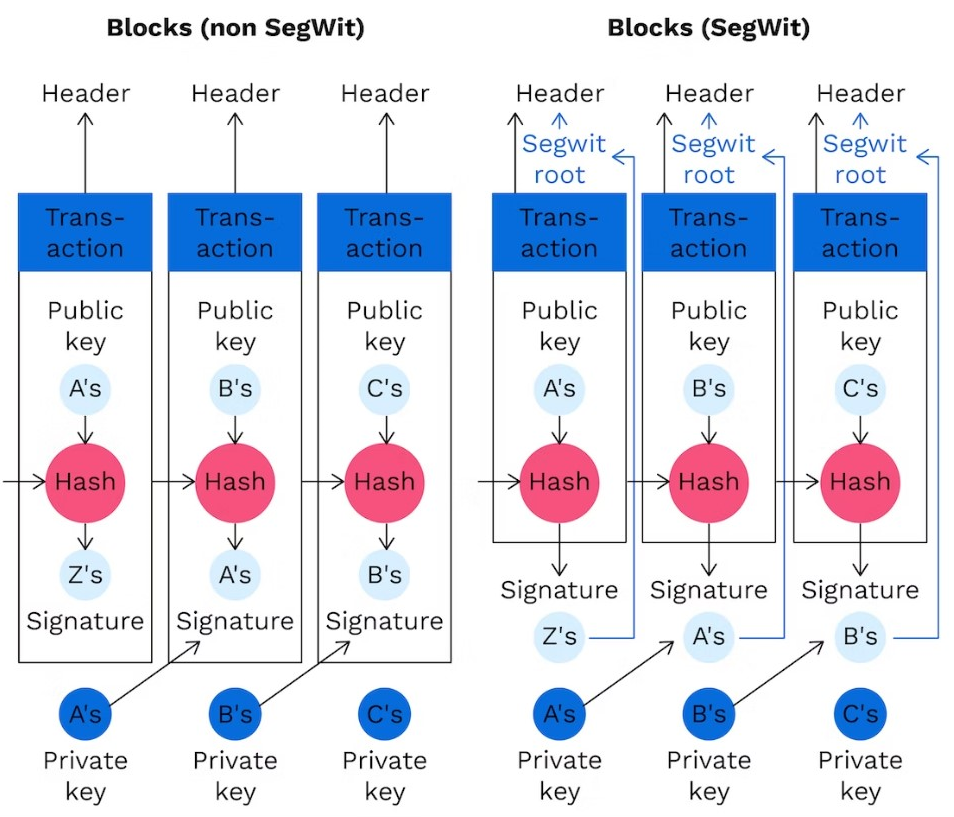
1. **SegWit**

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:

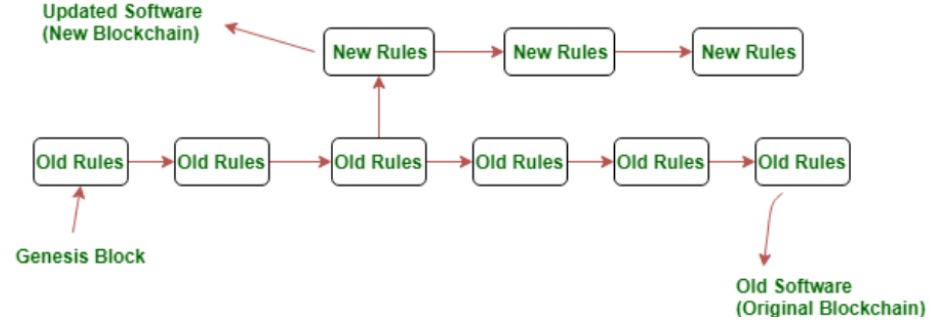
* To get a profit from the favourable market conditions like bull run on bitcoins price.
* Get more flexibility with the money.
* Fiat currency is the most common form of currency worldwide.
* Pay a bill.

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.

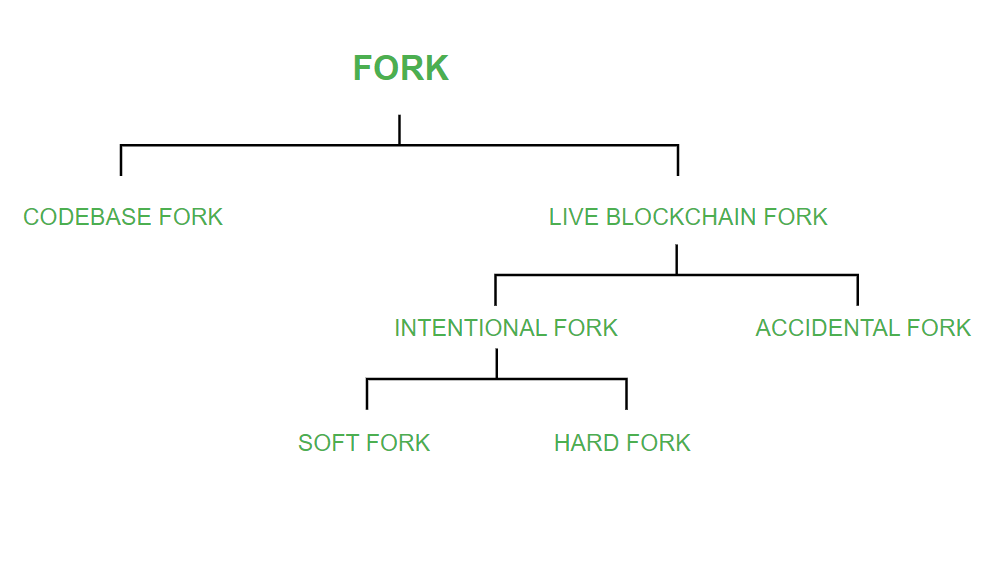
**More understanding about Forks**

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**

1. **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.

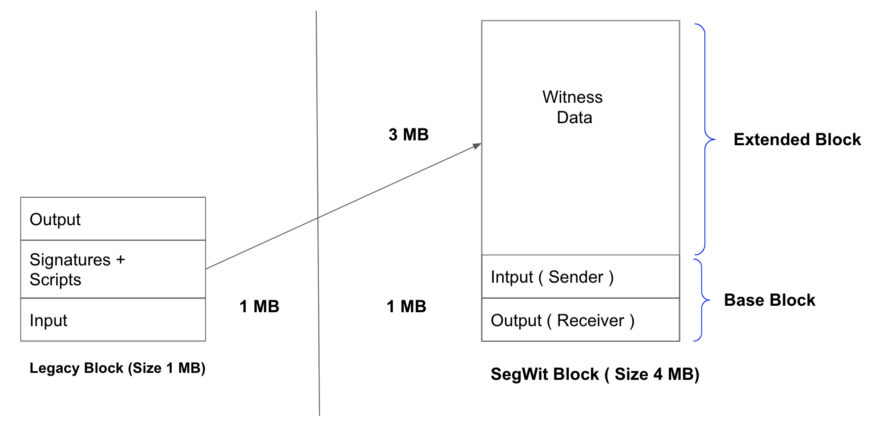
**Example:** The new Casper update in the Ethereum Blockchain in which the consensus protocol will change from a type of Proof of Work (PoS) to a type of Proof of Stake (PoS). The nodes which install the Casper update will use the new consensus protocol. Full nodes that do not choose to install the Casper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

**MODULE 5**

**Introduction to Ethereum**

Ethereum is a blockchain-based computing platform that enables developers to build and deploy decentralized applications—meaning not run by a centralized authority. You can create a decentralized application for which the participants of that particular application are the decision-making authority. Ethereum is considered by many to be the second most popular cryptocurrency, surpassed now only by Bitcoin.

**Ethereum Features**

**Ether:** This is Ethereum’s cryptocurrency.

**Smart contracts:** Ethereum allows the development and deployment of these types of contracts.

**Ethereum Virtual Machine:** Ethereum provides the underlying technology—the architecture and the software—that understands smart contracts and allows you to interact with it.

**Decentralized applications (Dapps):** A decentralized application is called a Dapp (also spelled DAPP, App, or DApp) for short. Ethereum allows you to create consolidated applications, called decentralized applications.

**Decentralized autonomous organizations (DAOs):** Ethereum allows you to create these for democratic decision-making.

These are Ethereum’s essential features. Let’s discuss each of these features in more detail.

1. **Ether**

Ether (ETH) is Ethereum’s cryptocurrency. It is the fuel that runs the network. It is used to pay for the computational resources and the transaction fees for any transaction executed on the Ethereum network. Like Bitcoins, ether is a peer-to-peer currency. Apart from being used to pay for transactions, ether is also used to buy gas, which is used to pay for the computation of any transaction made on the Ethereum network.

Also, if you want to deploy a contract on Ethereum, you will need gas, and you would have to pay for that gas in ether. So gas is the execution fee paid by a user for running a transaction in Ethereum. Ether can be utilized for building decentralized applications, building smart contracts, and making regular peer-to-peer payments.

1. **Smart Contracts**

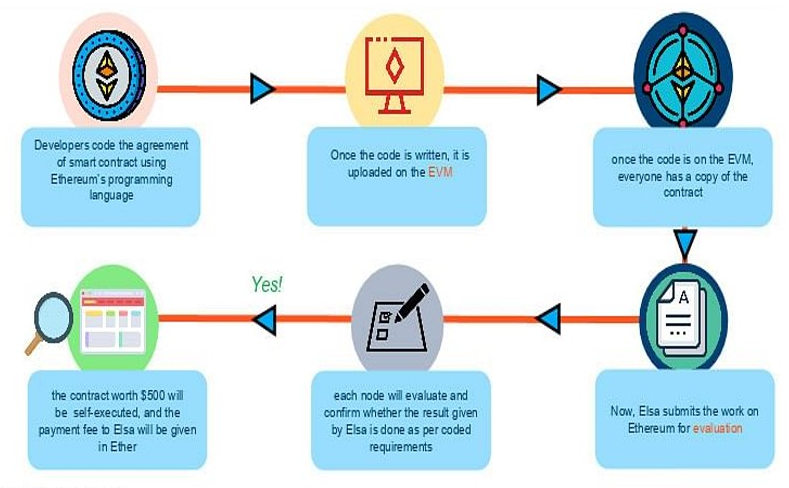
Smart Contracts are revolutionizing how traditional contracts work. A smart contract is a simple computer program that facilitates the exchange of any asset between two parties. It could be money, shares, property, or any other digital asset that you want to exchange. Anyone on the Ethereum network can create these contracts. The contract consists primarily of the terms and conditions mutually agreed on between the parties (peers).

The smart contract’s primary feature is that once it is executed, it cannot be altered, and any transaction done on top of a smart contract is registered permanently—it is immutable. So even if you modify the smart contract in the future, the transactions correlated with the original contract will not get altered; you cannot edit them. The verification process for the smart contracts is carried out by anonymous parties in the network without the need for a centralized authority, and that’s what makes any smart contract execution on Ethereum a decentralized execution.

The transfer of any asset or currency is done in a transparent and trustworthy manner, and the identities of the two entities are secure on the Ethereum network. Once the transaction is successfully done, the accounts of the sender and receiver are updated accordingly, and in this way, it generates trust between the parties.

In conventional contract systems, you sign an agreement, then you trust and hire a third party for its execution. The problem is that in this type of process, data tampering is possible. With smart contracts, the agreement is coded in a program. A centralized authority does not verify the result; it is confirmed by the participants on the Ethereum blockchain-based network. Once a contract is executed, the transaction is registered and cannot be altered or tampered, so it removes the risk of any data manipulation or alteration.

Let’s take an example in which someone named Zack has given a contract of $500 to someone named Elsa for developing his company’s website. The developers code the agreement of the smart contract using Ethereum’s programming language. The smart contract has all the conditions (requirements) for building the website. Once the code is written, it is uploaded and deployed on the Ethereum Virtual Machine (EVM). EVM is a runtime compiler to execute a smart contract. Once the code is deployed on the EVM, every participant on the network has a copy of the contract. When Elsa submits the work on Ethereum for evaluation, each node on the Ethereum network will evaluate and confirm whether the result given by Elsa has been done as per the coding requirements. Once the result is approved and verified, the contract worth $500 will be self-executed, and the payment will be paid to Elsa in ether. Zack’s account will be automatically debited, and Elsa will be credited with $500 in ether.



1. **Ehereum Virtual Machine**

EVM is designed to operate as a runtime environment for compiling and deploying Ethereum-based smart contracts. EVM is the engine that understands the language of smart contracts, which are written in the Solidity language for Ethereum. EVM is operated in a sandbox environment—basically, you can deploy your stand-alone environment, which can act as a testing and development environment. You can then test your smart contract (use it) “n” number of times, verify it, and once you are satisfied with the performance and the functionality of the smart contract, you can deploy it on the Ethereum main network.

Any programming language in the smart contract is compiled into the bytecode, which the EVM understands. This bytecode can be read and executed using the EVM. Solidity is one of the most popular languages for writing a smart contract. Once you write your smart contract in Solidity, that contract gets converted into the bytecode and gets deployed on the EVM, thereby guaranteeing security from cyberattacks.

Suppose person A wants to pay person B 10 ethers. The transaction will be sent to the EVM using a smart contract for a fund transfer from A to B. To validate the transaction; the Ethereum network will perform the proof-of-work consensus algorithm. The miner nodes on Ethereum will validate this transaction—whether the identity of A exists or not, and if A has the requested amount to transfer. Once the transaction is confirmed, the ether will be debited from A’s wallet and will be credited to B’s wallet, and during this process, the miners will charge a fee to validate this transaction and will earn a reward. All the nodes on the Ethereum network execute smart contracts using their respective EVMs.

**Proof of Work**

Every node in the Ethereum network has:

* The entire history of all the transactions—the entire chain
* The history of the smart contract, which is the address at which the smart contract is deployed, along with the transactions associated with the smart contract
* The handle to the current state of the smart contract

The goal of the miners on the Ethereum network is to validate the blocks. For each block of a transaction, miners use their computational power and resources to get the appropriate hash value by varying the nonce. The miners will vary the nonce and pass it through a hashing algorithm—in Ethereum, it is the Ethash algorithm. This produces a hash value that should be less than the predefined target as per the proof-of-work consensus. If the hash value generated is less than the target value, then the block is considered to be verified, and the miner gets rewarded. When the proof of work is solved, the result is broadcast and shared with all the other nodes to update their ledger. If other nodes accept the hashed block as valid, then the block gets added to the Ethereum main blockchain, and as a result, the miner receives a reward, which as of today stands at three ethers. Plus, the miner gets the transaction fees that have been generated for verifying the block. All the transactions that are aggregated in the block—the cumulative transaction fees associated with all the transactions are also rewarded to the miner.

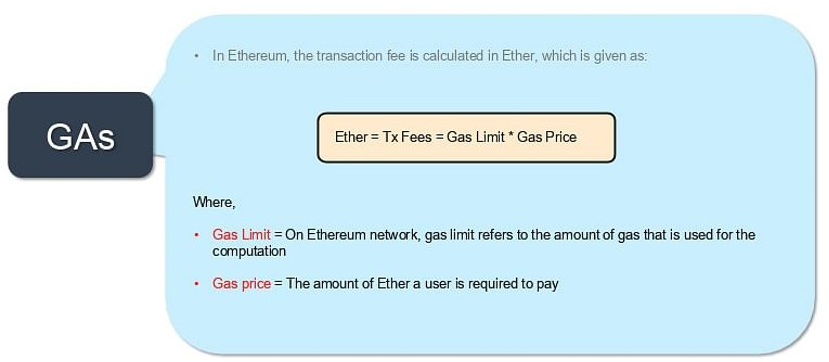
**Proof of Stake**

In Ethereum, a process called proof of stake is also under development. It is an alternative to proof of work and is meant to be a solution to minimize the use of expensive resources spent on mining using proof of work. In proof of stake, the miner—who is the validator—can validate the transactions based on the number of crypto coins he or she holds before actually starting the mining. So, based on the accumulation of crypto coins the miner has beforehand, he or she has a higher probability of mining the block. However, proof of stake is not widely used as of now compared to proof of work.

**Gas**

Just like we need fuel to run a car, we need gas to run applications on the Ethereum network. To perform any transaction within the Ethereum network, a user must make a payment, in this case paying out ethers, to get a transaction done, and the intermediary monetary value is called gas. On the Ethereum network, gas is a unit that measures the computational power required to run a smart contract or a transaction. So, if you must do a transaction that updates the blockchain, you would have to shell out gas, and that gas costs ethers.

In Ethereum, the transaction fees are calculated using a formula. For every transaction, there is gas and its correlated gas price. The transaction fees equal the amount of gas required to execute a transaction multiplied by the gas price. “Gas limit” refers to the amount of gas used for the computation and the amount of ether a user is required to pay for the gas.



For a particular transaction, if the gas limit was 21,000, the gas used by the transaction was 21,000, and the gas price was 21 Gwei, which is the lowest denomination of ether. So, 21 Gwei \* 21,000 gave the actual transaction fees: 0.000441 ethers, or about 21 cents as of today. As mentioned, the transaction fee goes to the miner, who has validated the transaction.

To understand the gas limit and price, let’s consider an example using a car. Suppose your vehicle has a mileage of 10 kilometers per litre and petrol costs $1 per litre. Under these parameters, driving a car for 50 kilometers would cost you five litres of petrol, which is worth $5. Similarly, to perform an operation or to run code on Ethereum, you need to obtain a certain amount of gas, like petrol, and the gas has a per-unit price, called gas price. If the user provides less than the amount of gas to run an operation, then the process will fail, and the user will be given the message “out of gas.” Gwei is the lowest denomination of ether used for measuring a unit of a gas price.

1. **Decentralized Applications (Dapps)**

Let’s compare decentralized applications with traditional applications. When you log in to Twitter, for example, a web application gets displayed that is rendered using HTML. The page will call an API to access your data (your information), which is centrally hosted. It’s a simple process: your front end executes the backend API, and the API goes and fetches your data from a centralized database.

If we transform this application into a decentralized application when you log in, the same web application gets rendered, but it calls a smart contract-based API to fetch the information from the blockchain network. So, the API is replaced by a smart contract interface, and the smart contract will bring the data from the blockchain network, which is its back end. That blockchain network is not a centralized database; it’s a decentralized network in which the participants of the network (the miners) validate (verify) all the transactions that are happening using the smart contract on the blockchain network. So, any transaction or action happening on a Twitter-type application that has now been transformed will be a decentralized transaction.

A Dapp consists of a backing code that runs on a distributed peer-to-peer network. It is a software designed to work in the Ethereum network without being controlled by a centralized system, as mentioned, and that is the primary difference: it provides direct interaction between the end-users and the decentralized application providers.

An application qualifies as a Dapp when it is open-source (its code is on Github), and it uses a public blockchain-based token to run its applications. A token acts as fuel for the decentralized application to run. Dapp allows the back end code and data to be decentralized, and that is the primary architecture of any Dapp.

1. **Decentralized Autonomous Organizations (DAOs)**

DAO is a digital organization that operates without hierarchical management; it works in a decentralized and democratic fashion. So basically, a DAO is an organization in which the decision-making is not in the hands of a centralized authority but preferably in the hands of certain designated authorities or a group or designated people as a part of an authority. It exists on a blockchain network, where it is governed by the protocols embedded in a smart contract, and thereby, DAOs rely on smart contracts for decision-making—or, we can say, decentralized voting systems—within the organization. So, before any organizational decision can be made, it must go through the voting system, which runs on a decentralized application.

People add funds through the DAO because the DAO requires funding in order to execute and make decisions. Based on that, each member is given a token that represents that person’s percentage of shares in the DAO. Those tokens are used to vote in the DAO, and the proposal status is decided based on the maximum votes. Every decision within the organization must go through this voting process.

**Real-World Applications of Ethereum**

* **Voting Systems**

As we’ve seen with DAO, voting systems are adopting Ethereum. The results of polls are publicly available, ensuring a transparent and fair democratic process by eliminating voting malpractices.

* **Banking Systems**

Ethereum is getting adopted widely in banking systems because with Ethereum’s decentralized system; it is challenging for hackers to gain unauthorized access. It also allows payments on an Ethereum-based network, so banks are also using Ethereum as a channel to make remittances and payments.

* **Shipping**

Deploying Ethereum in shipping helps with the tracking of cargo and prevents goods from being misplaced or counterfeited. Ethereum provides the provenance and tracking framework for any asset required in a typical supply chain.

* **Agreements**

With Ethereum smart contracts, agreements can be maintained and executed without any alteration. So in an industry that has fragmented participants, is subject to disputes, and requires digital contracts to be present, Ethereum can be used as a technology for developing smart contracts and for digitally recording the agreements and the transactions based on them.

**Advantages and Disadvantages of Ehereum**

Here are the advantages of Ethereum enjoyed by the enterprises:

* Decentralization:

The decentralized design of Ethereum effectively distributes knowledge and trust among network members, removing the need for a central body to run the system and mediate transactions.

* Rapid deployment:

Instead of building a blockchain implementation from scratch, organizations can quickly create and administer private blockchain networks using an all-in-one SaaS platform like Hyperledger Besu.

* Permissioned network:

There are many open-source protocol layers that allow enterprises to build on public or private Ethereum networks, guaranteeing that their solution meets all regulatory and security standards.

* Network size:

The Ethereum mainnet demonstrates that a network with hundreds of nodes and millions of users can function. Most business blockchain competitors run networks with less than ten nodes and have no precedent for a large and successful network. For corporate collaborations that are bound to outgrow a few nodes, network scale is important.

* Private transactions:

In Ethereum, businesses may obtain privacy granularity by joining private partnerships with private transaction layers. Private information is encrypted and only shared with those who need to know.

* Scalability and performance:

Consortium networks created on Ethereum may outperform the public mainnet and grow up to hundreds of transactions per second or more depending on network setup, thanks to Proof of Authority consensus and bespoke block time and gas limits. Ethereum will be able to boost its throughput in the near future because of protocol-level solutions like sharding and off-chain, as well as layer 2 scaling solutions like Plasma and state channels.

* Finality:

The consensus method of a blockchain ensures that the transaction record is tamper-proof and canonical. For different enterprise network instances, Ethereum offers customizable consensus mechanisms such as RAFT and IBFT, ensuring immediate transaction finality and reducing the required infrastructure that the Proof of Work algorithm requires.

* Tokenization:

Any item that has been registered in a digital format can be tokenized on Ethereum. Organizations may fractionalize formerly monolithic assets (real estate), broaden their product line (provably rare art), and open new incentive models by tokenizing assets (crowdsourced data management).

* Interoperability and open source:

On Ethereum, consortiums are not bound by a single vendor's IT environment. Customers of Amazon Web Services, for example, can use Kaleido's Blockchain Business Cloud to run private networks. The Ethereum ecosystem, like the Java community, encourages contributions to the codebase through Ethereum Improvement Proposals (EIPs).

* Standards:

The ecosystem is kept from being fragmented through protocols for token design (ERC20), human-readable names (ENS), decentralized storage (Swarm), and decentralized communications (Whisper). The Client Specification 1.0 of the Corporate Ethereum Alliance outlines the architectural components for compatible enterprise blockchain implementations.

Ethereum has some disadvantages as well:

* Uses a Complicated Programming Language:

While Ethereum is Turing complete and uses a programming language similar to C++, Python, and Java, learning Solidity, the native language of Ethereum, may be challenging. One of the most significant concerns is the scarcity of beginner-friendly classes.

* Issues with Scaling:

Unlike Bitcoin, which has a singular purpose, Ethereum has a ledger, a platform for smart contracts, and so on, all of which may lead to errors, malfunctions, and hacks.

* Ethereum Investing Can Be Risky:

Ethereum investing, like any other cryptocurrency, can be risky. Cryptocurrencies are very volatile, resulting in significant gains as well as significant losses. The price of Ether has changed significantly in the past, which might be a significant disadvantage for certain investors, particularly beginners. In addition, Ethereum's fees change, which is inconvenient.

**Ethereum Vs. Bitcoin**

The Bitcoin vs. Ethereum argument has been garnering more attention these days. Bitcoin has become a very popular and well-known cryptocurrency around the world. It also has the highest market cap among all the cryptocurrencies available right now. In a way, it’s the current world champion when it comes to cryptocurrencies. On the other side is Ethereum. Ethereum did not have the revolutionary effect that Bitcoin did, but its creator learned from Bitcoin and produced more functionalities based on the concepts of Bitcoin. It is the second-most-valuable cryptocurrency on the market.

* **History**

Bitcoin was the first cryptocurrency to be created; as mentioned, it was released in 2009 by Satoshi Nakamoto. It is not known if this is a person or group of people, or if the person or people are alive or dead. Ethereum, as noted above, was released in 2015 by a researcher and programmer named Vitalik Buterin. He used the concepts of blockchain and Bitcoin and improved upon the platform, providing a lot more functionality. Buterin created the Ethereum platform for distributed applications and smart contracts.

* **Concepts**

Bitcoin enables peer-to-peer transactions. It acts as a replacement for fiat currencies but doesn’t have all the problems associated with fiat currencies. You don’t have to pay high transaction fees, and you also don’t have a centralized authority that regulates how bitcoins work. Ethereum enables peer-to-peer transactions as well, but it also provides a platform for creating and building smart contracts and distributed applications. A smart contract allows users to exchange just about anything of value: shares, money, real estate, and so on.

* **Mining**

In Bitcoin, miners can validate transactions with the method known as proof of work. This is the same case for Ethereum. With proof of work, miners around the world try to solve a complicated mathematical puzzle to be the first one to add a block to the blockchain. Ethereum, however, is working on moving to a different form of transaction validation known as proof of stake. With proof of stake, a person can mine or validate transactions in a block based on how many coins he owns. The more coins a person holds, the more mining power he will have. In Bitcoin, every time a miner adds a block to the blockchain, he is rewarded with 6.25 bitcoins, a rate set in November 2021. In Etherium a miner, or validator, receives a value of 3 ether every time a block is added to the blockchain, and the reward will never be halved.

* **Fees**

The transaction fees in Bitcoin are entirely optional. You can pay the miner more money to have him pay special attention to your transaction; however, the transaction will go through even if you don’t pay a fee. On the other hand, you must provide some amount of ether for your transaction to be successful on Ethereum. The ether you offer will get converted into a unit called gas. This gas drives the computation that allows your transaction to be added to the blockchain.

* **Time**

As for the average amount of time it takes to add a block to the blockchain, in Bitcoin it takes 10 minutes. In Ethereum, it takes only about 12 to 15 seconds.

* **Hashing Algorithms**

Hashing algorithms are how these systems can maintain their privacy and ensure security. Bitcoin uses a hashing algorithm known as SHA-256. Ethereum uses a cryptographic algorithm called Ethash.

* **By the numbers**

Bitcoin has over 18 million bitcoins currently in existence, and Ethereum has 118 million ether. Now even though Ethereum has easily crossed the 100 million mark, the market capitalization for Bitcoin is $781 billion, whereas for Ethereum it’s only $368 billion. So even though Ethereum has more coins on the market, it isn’t at the level of Bitcoin.

The number of Bitcoin transactions that take place in a day currently hovers around 260,000; for Ethereum, it’s about 1.2 million. As for the number of blocks that have been mined, for Bitcoin, it’s over 718,000, and for Ethereum it’s about 13 million. This has a lot to do with the fact that it takes a lot less time for a block to be added to Ethereum than to Bitcoin.

The current block size is 1,268 kilobytes for Bitcoin and 94 kilobytes for Ethereum. And while the market value of Bitcoin is significantly higher than that of any form of digital currency on the market right now, it is closely followed by Ethereum, which hopes to take over one day.

The answer to the question of which cryptocurrency is better in the choice between Bitcoin vs. Ethereum, it depends entirely on requirements. While Bitcoin works better as a peer-to-peer transaction system, Ethereum works well when you need to create and build distributed applications and smart contracts.

**Introduction to Smart Contracts**

Smart contracts are a type of digital agreement based on blockchain technology and are executed to form a legal contract between two parties involved. Smart contracts have been in the market even before the advent of blockchain technology. However, recent developments in the blockchain have paved the way to an increasingly secure form of smart contracts. These are now gradually being adopted in the market. Smart Contracts are one of the most promising applications based on blockchain technology.

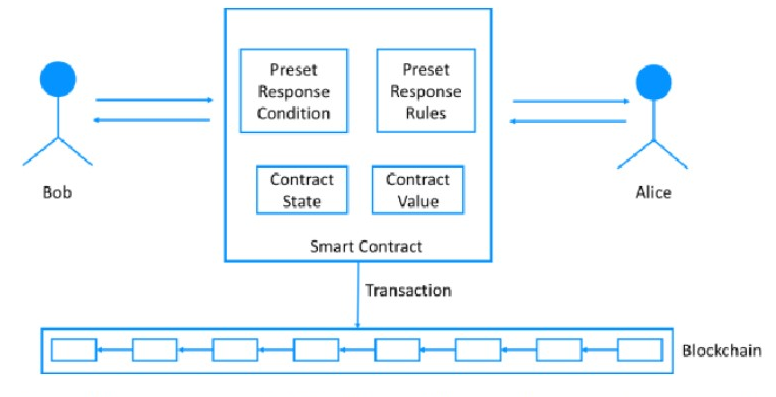
1. **What are Smart Contracts?**

Smart contracts are a set of conditions written in the form of code that meet the agreed criteria between two involved parties. The code that resides on the blockchain is distributed and highly secure. This piece of code, when executed, gets registered in the form of a blockchain transaction while ensuring the terms of the agreement are met. This execution of smart contracts on the blockchain is immutable and irreversible. Hence, any smart contract execution is tracked from beginning to end of the transaction cycle between the two parties involved. It can be tracked chronologically in a transparent manner.

1. **Why did the need to introduce smart contracts arise?**

With the ever-advancing digital era, smart contracts have gained popularity for preparing and executing agreements. These can be implemented among any two parties residing anywhere across the globe. It is easy to implement, transparent, accessible, and free of distance and geographical constraints.

For instance, an organization based out of India can get into an agreement with a client from Europe without having to physically travel and sign a legal agreement. Once both parties reach a consensus on the terms and conditions of the agreement, a smart contract is designed using the ‘if…then…else’ – statements with the help of a code. It is implemented over blockchain and registered as a blockchain transaction while minimizing frictions involved in a legal process.



**The flow of a Smart Contract execution**

Smart contracts can be used for many different domains, as explained below:

**Real estate transactions**

Any real estate transaction in buying, selling, renting, or listing a property for rent/sale can be executed using multiple contracts hosted on a blockchain.

**Cryptocurrency investments**

To invest in Cryptocurrency, there are multiple platforms in the market like CoinDCX, CoinBase, UnoCoin, etc.

Other popular use – cases are in the domains of Credit Lending, Medical Records preservation, and access and Identity verification and management.

1. **Features of Smart Contracts**

**Secure –** Smart contracts are a piece of code designed to minimize human error and issues. They are highly secure as they reside on the blockchain distributed across multiple systems and are immutable.

**Scalable –** Smart contracts are easy, efficient, offer greater execution speed, and promise higher accuracy.

**Easy to implement and track –** Once a smart contract is written in code on blockchain technology, it can be easily executed with the click and consent of both parties. Since it is registered as a transactional record in the blockchain, it is also easy to track.

**Reduce Friction –** Smart contracts reduce friction incidents involving intermediaries, geographical constraints, fees of execution, and commission.

**Transparent –** data, agreement terms, and execution history can be shared transparently with all involved parties.

**Encourages Savings in terms of time, energy and finances –** Smart contracts are executed when certain conditions decided by the participating parties are met and do not need an intermediary to solicit the agreement. This significantly reduces the time spent in the implementation of the contract. Moreover, they are a cost-effective proposition as they save on the cost of legal intervention.

1. **Use of Smart Contracts in Day-to-day Business Deals and Projects**

Smart contracts can be widely used by businesses across domains like healthcare, e-commerce, real estate, decentralized finance, and more. They are developed on the Ethereum blockchain using the Solidity programming language, an open-source blockchain where community help is available. Smart contracts are used in many day-to-day business processes, including legal agreements, timeline bindings, and business terms between two parties.

Let’s discuss this with the help of two examples:

* Suppose you are a cosmetics vendor who wants to list and sell your products on an online e-commerce platform. As a cosmetics vendor wanting to sell your products on an e-commerce platform, you must first register on their portal and list yourself as a retailer. Post registration, you will be required to sign an agreement with details of the listed products, a revenue sharing agreement based upon the sales, and other contract terms. This form of agreement can be developed on the Ethereum blockchain with the help of Solidity, a programming language. The execution will be much faster once both parties agree on the terms of the agreement.
* Imagine you are a mediator who deals in rental properties and sales in a specific area in Bengaluru. If you deal with property and real estate rentals and purchases in Bengaluru, Smart Contracts are immensely beneficial.
* Smart Contract for the Sale of the Real Estate Property: The terms of the deal would

involve –

* The cost of the property
* Ownership transfer
* Purchase agreement
* Number of parking
* Maintenance charges
* Society formation details along with other information

A smart contract listing the above agreement terms is developed and executed, making the deals faster and more robust. Moreover, it is highly secure as the transaction records are immutable and stored as a Blockchain transaction.

* Smart contract for renting a Real estate property: For rental agreements, smart contracts are designed in a standard format listing the following:
* Details of the Broker, owners, and tenant
* Lease period
* Lock-in period
* Date of rent transfer every month as per the rent cycle
* Terms of hand-over at the end of the rent tenure

Suppose a standard smart contract format is designed using solidity on the Ethereum blockchain and exposed as an API. In that case, brokers can feed in the required details and execute the rent agreement without any third party.

**Law and Regulations**

Given the unique nature of smart contracts and the ways they differ from traditional paper agreements, there are concerns surrounding their enforceability. In general, smart contracts are enforceable as long as they follow the basic rules of contractual agreements. These include the following.

**a. Offer, Acceptance, Consideration**

As with any agreement, there must be an offer, an acceptance of that offer and consideration.

• Offer: One or both parties offer the terms of the agreement.

• Acceptance: Both parties accept the terms as offered (often after some negotiation).

• Consideration: There is something of value being offered to each party.

If any of these components are lacking, it is not a legally enforceable contract.

**b. Legally Permissible Terms**

In general, you cannot use a contract to bind parties to terms that are illegal to enforce. For instance, asking parties to waive certain rights that cannot be legally waived will likely nullify that section of the agreement. This may present a special challenge for smart contracts since making sure such terms are severable from the rest of the agreement—which cannot be edited once executed—may be more difficult than it would be with a paper contract.

**c. Legal To Sign Electronically**

Finally, smart contracts need to be legally eligible for electronic signatures. Some types of agreements cannot be signed electronically, including wills and other estate documents; court orders; product recall notices involving health and safety; documents required to accompany hazardous substances being transported; notices of cancellation of utility services; and eviction notices. Most transactions involving smart contracts won’t involve any of these categories, but it’s still worth remembering what can and can’t be signed electronically.

**Legal Challenges of Smart Contracts**

Smart contracts execute automatically, and once they’re set in place, they cannot be modified. These facts create some interesting challenges, particularly in the event of disputes or unenforceability.

* **Automatic Enforcement:** If it turns out that the terms of a smart contract are not legal to enforce, it creates a more difficult situation than one would have with a traditional paper contract. Once the contract is programmed and agreed upon, it will execute automatically, which may lead to some difficulty in remedying any unlawful enforcement.
* **Modifying the Contract:** Making modifications to the contract can also be a challenge, at least once it’s set into motion. Once a smart contract is in force, it cannot be modified. This means if any changes are desired, the entire contract needs to be canceled and redrawn. For this reason, maintaining a backup copy of the code is recommended.
* **Handling Disputes:** Due to the difficulty of adjusting a smart contract once it’s in place, it’s important for each party to be absolutely clear on the terms from the outset. The agreement needs to be treated as if it’s going to be permanent from the very beginning, so great care should be taken to make sure it doesn’t lead to disputes. If a dispute does occur, both the contract’s permanence and automatic execution could pose a barrier to enacting changes.

**Case Studies**

Now you understand how smart contracts work, let’s look at some smart contract examples from the real world.

**Clinical trials**

Data sharing between institutions is vital to effective clinical trials. With the support of smart contracts, professionals can seamlessly share data across the industry. Blockchain technology can also help with the authentication of the data to ensure it is accurate. This is a gamechanger for those trying to launch wide-reaching clinical trials. Smart contracts have many uses in the healthcare industry.

**Music industry**

Emerging music artists depend on streaming income as they get started in the industry. Smart contract applications can make royalty payments easier. For instance, these contracts can include which percentage of the royalty income goes to the record label and the artist. These payments can happen instantly, which is a major win for all parties involved. Tune.fm, for example, is a tokenized music economy that helps artists get paid directly for every second streamed using JAM tokens. Artists can mint NFTs for exclusive content and sell them directly to fans for JAM tokens.

**Supply chain management**

As self-enforcing contracts, smart contracts can operate autonomously without the need for any intermediaries or third parties. If you designed a smart contract for an end-to-end supply chain, this would require no daily management or auditing. Any deliveries received outside the schedule could trigger pre-agreed escalation measures to ensure a smooth operation.

Datahash, formerly Entrust, is Australia’s first full-service agricultural supply chain platform. It is working to thwart the $3 billion-a-year market in fraudulent wine. The platform relies on Hedera Consensus Service to trace its data in a trusted way.

**Property ownership**

You can use smart contract technology to offer fractional ownership of real estate. Rather than one person owning a property, you can segment ownership so people can buy tokens of the property. When someone owns a token, they co-own a percentage of the property. This makes it easy for anyone to jump on the property market and make micro-investments.

**Mortgages**

The mortgage industry needs a massive overhaul. It’s currently bloated with costly third parties and time-consuming processes. Smart contracts can ensure that lenders and loan seekers agree to clear terms and conditions, such as proof-of-funds and payment planning. This emerging technology can validate mortgage transactions without the need for any lawyers or other third parties.

**Retail**

Smart contracts can help to streamline administrative processes that are often a burden to brick-and-mortar retailers. Retailers can create smart contracts to enable fast payments to contractors. Another possibility: Digitize payroll administration and track it in real-time. Retailers also can place unique blockchain identifiers on inventory units to create visibility across supply chains.

In this sector, Dropp enables micropayments for small value transactions in both cryptocurrency and dollars. Merchants save money and grow their business, and consumers get convenient access to products and services.

**Digital identity**

From reputational data to digital assets, you can store components on a smart contract to form a digital identity. When smart contracts are connected to various online services, the counterparties can learn about the individuals without revealing their identities. Smart contracts could contain credit scores that lenders can use to measure potential risk.

For example, MyEarth ID is a decentralized Identity Management System that allows users to control their digital identity data and securely verify it with third parties.

**Recording financial data**

Smart contracts can help to facilitate accurate and transparent data collection. When it comes to recording financial data, smart contracts can radically reduce costs for auditing and ensure compliance. These smart contracts can execute set financial rules without the need for any intervention. This can streamline administrative workflows and save accountants time.

At another intersection of smart contracts and finance, AllianceBlock is building a protocol to bridge decentralized finance (DeFi) and traditional financial services (TradFi). AllianceBlock's AllianceBridge is a validator network leveraging the Hedera Consensus Service.

**Voting in elections**

Smart contracts could create a secure environment for voting, reducing the risk of potential voter manipulation. Each vote using a smart contract is ledger-protected. Due to the encryption, these are incredibly hard to decode. Smart contracts could also increase voter turnout. With an online system powered by smart contracts, there is no need to travel to a polling station.

**Insurance sector**

The insurance world is full of disputes. With this in mind, smart contracts have an important role to play in automating policies and services in the insurance industry. This can help to reduce insurer costs and result in lower premiums. With automated claims payment processes powered by smart contract technology, policy-holders can get paid faster than through current manual processes.