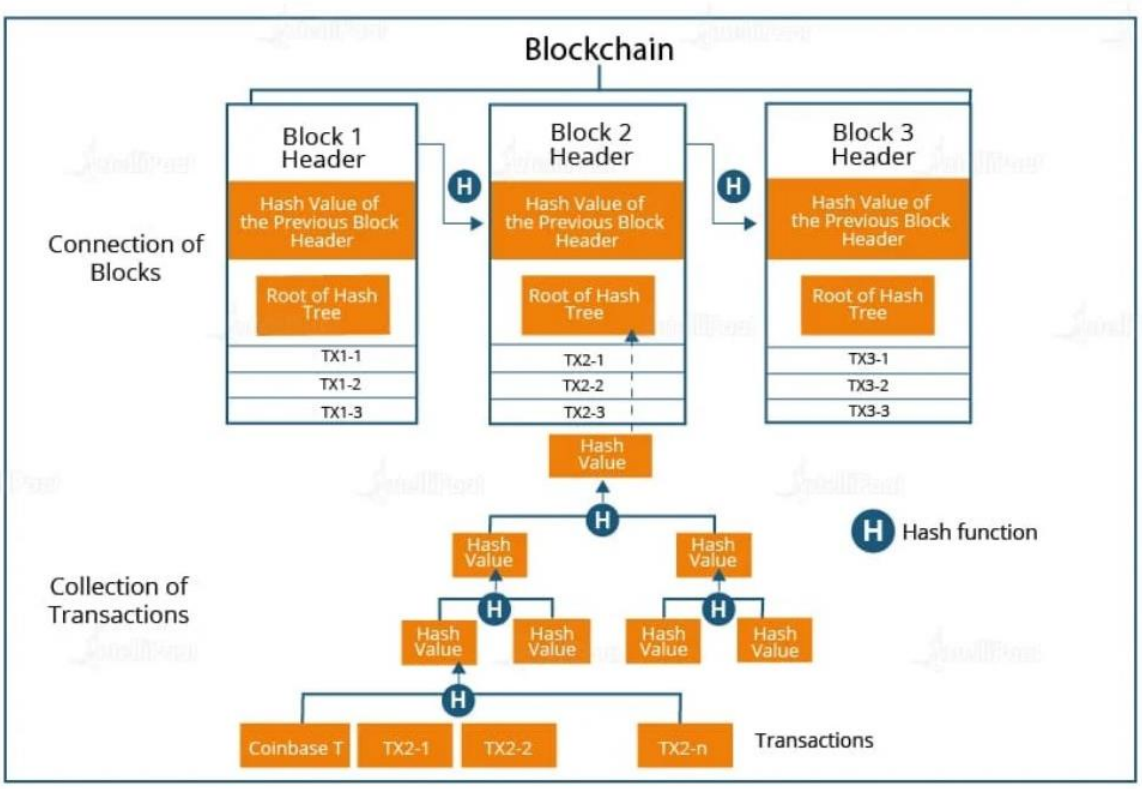
MODULE 2

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.



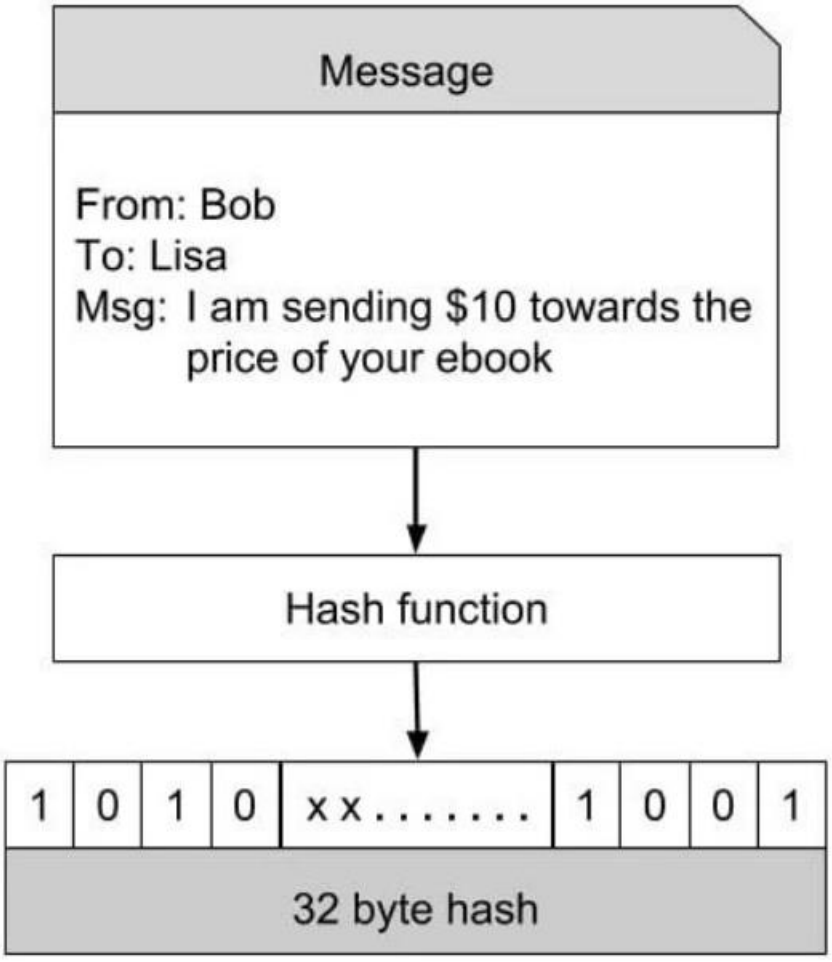
Main aspects of architecture include the blockchain platform, nodes, transactions that makeup blocks, security implementations, and the process of adding new blocks to the chain. The blockchain architecture is undoubtedly complex, but once you get a hold of it you will get acquainted with the same.

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.

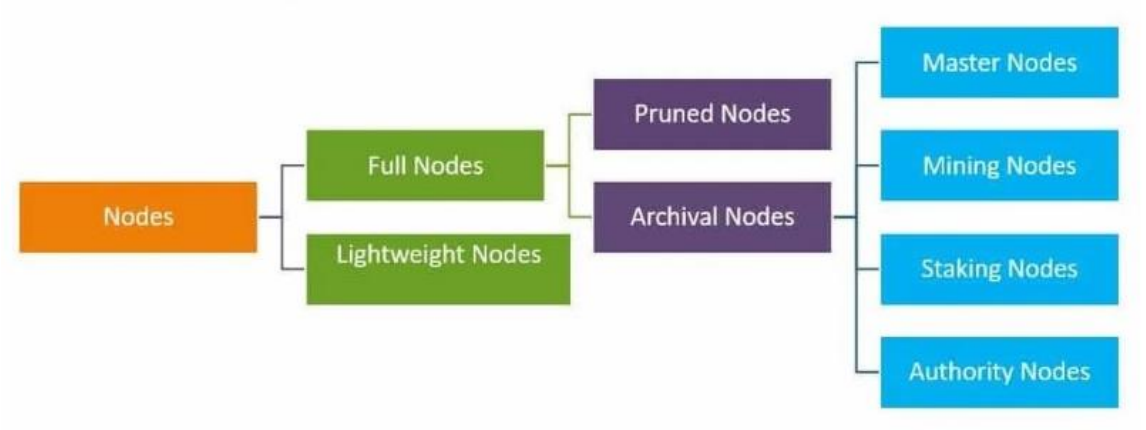


Bob, while placing an order with Lisa, creates a message which is like the one shown above. This message is hashed through a hash function that produces a 32 byte hash code. The beauty of the hash is that for all practical purposes it can be considered unique for the contents of the message. If the message 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.

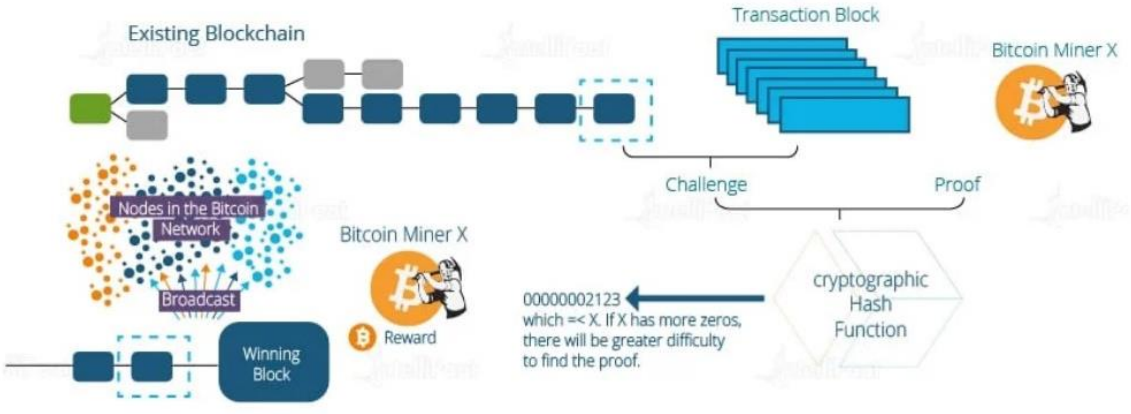
Blockchain Consensus

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 implements 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.

i. 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.

ii. 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.

iii. 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.

iv. 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

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.