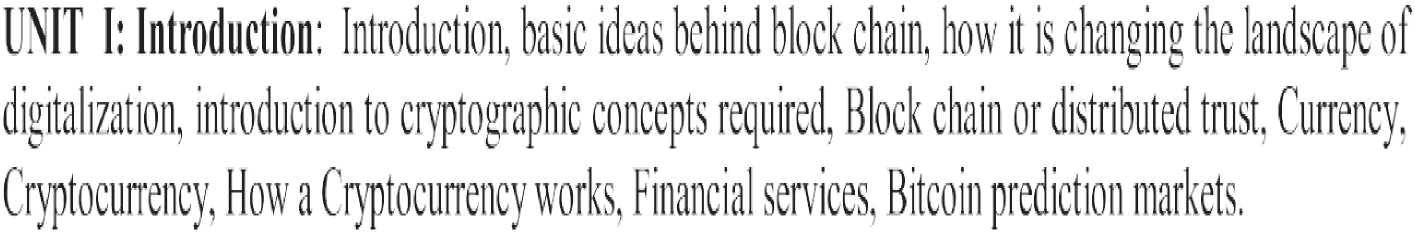
VIGNAN'S INSTITUTE OF ENGINEERING FOR WOMEN
(Approved by AICTE & Affiliated to JNTU-GV, Vizianagaram) Estd. 2008
Accredited by NBA for UG Programmes of EEE, ECE, CSE & IT
ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 Certified Institution
NAAC A+ NATIONAL ASSESSMENT AND ACCREDITATION COUNCIL

BLOCK-CHAIN TECHNOLOGIES

UNIT-1



UNIT I: Introduction: Introduction, basic ideas behind block chain, how it is changing the landscape of digitalization, introduction to cryptographic concepts required, Block chain or distributed trust, Currency, Cryptocurrency, How a Cryptocurrency works, Financial services, Bitcoin prediction markets.

Introduction:

Block-chain defined: Block-chain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a block chain network, reducing risk and cutting costs for all involved.

Why block chain is important: Business runs on information. The faster it's received and the more accurate it is the better. Block chain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members.

A block chain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

Key elements of a block chain:

Distributed ledger technology
All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

Immutable records
No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts
To speed transactions, a set of rules — called a smart contract — is stored on the block chain and executed automatically. A smart contract can define conditions for corporate bond transfers; include terms for travel insurance to be paid and much more.

How block chain works:

1. **As each transaction occurs, it is recorded as a "block" of data** those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.
2. **Each block is connected to the ones before and after it** these blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.
3. **Transactions are blocked together in an irreversible chain: a block chain** each additional block strengthens the verification of the previous block and hence the entire

block chain. This renders the block chain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

Benefits of block chain:

What needs to change: Operations often waste effort on duplicate record keeping and third-party validations. Record-keeping systems can be vulnerable to fraud and cyber-attacks. Limited transparency can slow data verification. And with the arrival of IoT, transaction volumes have exploded. All of this slows business, drains the bottom line — and means we need a better way. Enter block chain

Greater trust

With block chain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential block chain records will be shared only with network members to whom you have specifically granted access.

Greater security

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

More efficiencies

With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the block chain and executed automatically.

Types of block chain networks:

There are several ways to build a block chain network. They can be public, private, and permissioned or built by a consortium

Public block chain networks

A public block chain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of block chain.

Private block chain networks

A private block chain network, similar to a public block chain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private block chain can be run behind a corporate firewall and even be hosted on premises.

Permissioned block chain networks

Businesses who set up a private block chain will generally set up a permissioned block chain network. It is important to note that public block chain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

Consortium block chains

Multiple organizations can share the responsibilities of maintaining a block chain. These pre-selected organizations determine who may submit transactions or access the data. A consortium block chain is ideal for business when all participants need to be permissioned and have a shared responsibility for the block chain.

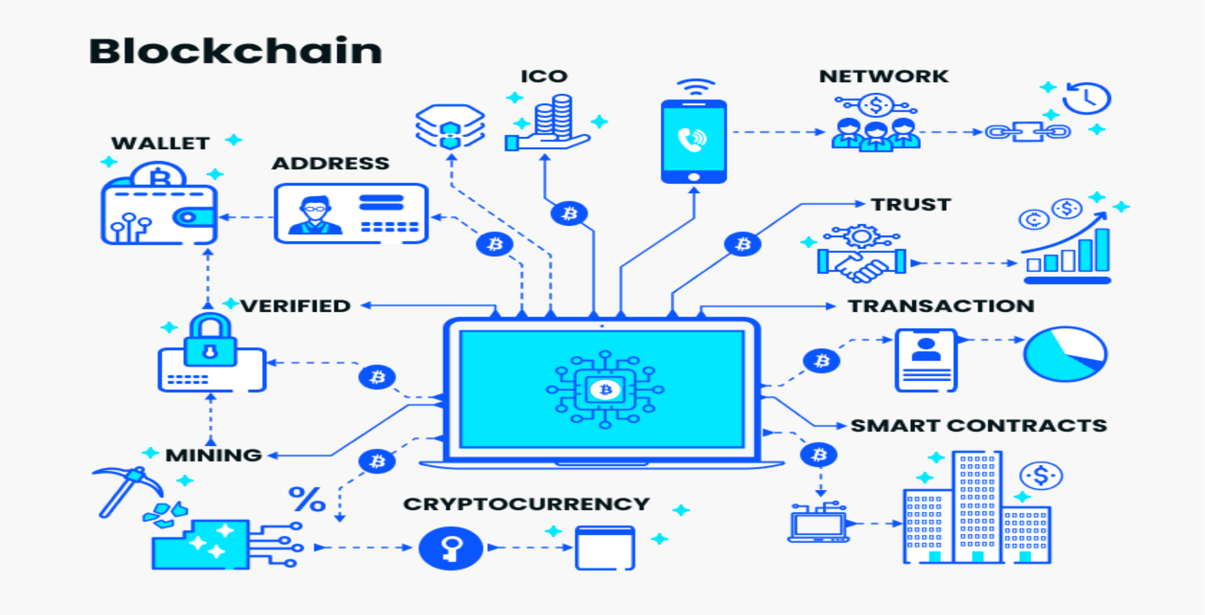
Basic Ideas behind block chain:

Block chain technology is a decentralized digital ledger that records transactions in a secure and transparent manner. Each block in the chain contains a unique code and a record of previous transactions. Block chain technology is used to create a decentralized, secure database that multiple parties can access and update in real time.

In simple terms, block chain is a special kind of computer database that makes it easy and safe for lots of people to share information with each other. Instead of keeping all the information in one place, it stores data in blocks connected like links in a chain.

Each block chain involves a series of transactions. Note that each new structure appears on the block chain. However, a decentralized database run by various candidates is called DLT or Distributed Ledger Technology. Block chain refers to a type of DLT that records each transaction using a HASH (immutable cryptographic signature).

Where Can We Use Block chain Technology



Difference between a Block chain Ledger and a Database

Both the database and Block chain record transactions, but the database is centralized and has a single point of failure. In contrast, Block chain is decentralized and distributed across multiple nodes in the network.

Each node in the block chain network collectively participates in a consensus algorithm using Proof-of-Work.

Databases are owned by a central office, company, or government institution that controls access by granting different roles to different users. Block chain, on the other hand, is a peer-to-peer network where every node can connect to every other node. A secure cryptographic protocol like SHA-256 connects the blocks in the chain.

Understanding the Key Terminologies of Block chain Technology

Ledger

The ledger records transactions such as payment, supply chain details, medical, real estate contracts, etc.

SHA-256

SHA-256 is a cryptographic algorithm that accepts input of any length, deterministically encodes the data, and returns a hash of 256 bits or 64 characters. The SHA-256 hashing algorithm ensures that the output can never track back to the input, making it very secure.

Mining

It is the process of verifying and recording new transactions on the block chain performed by Miners, for which they have special mining software.

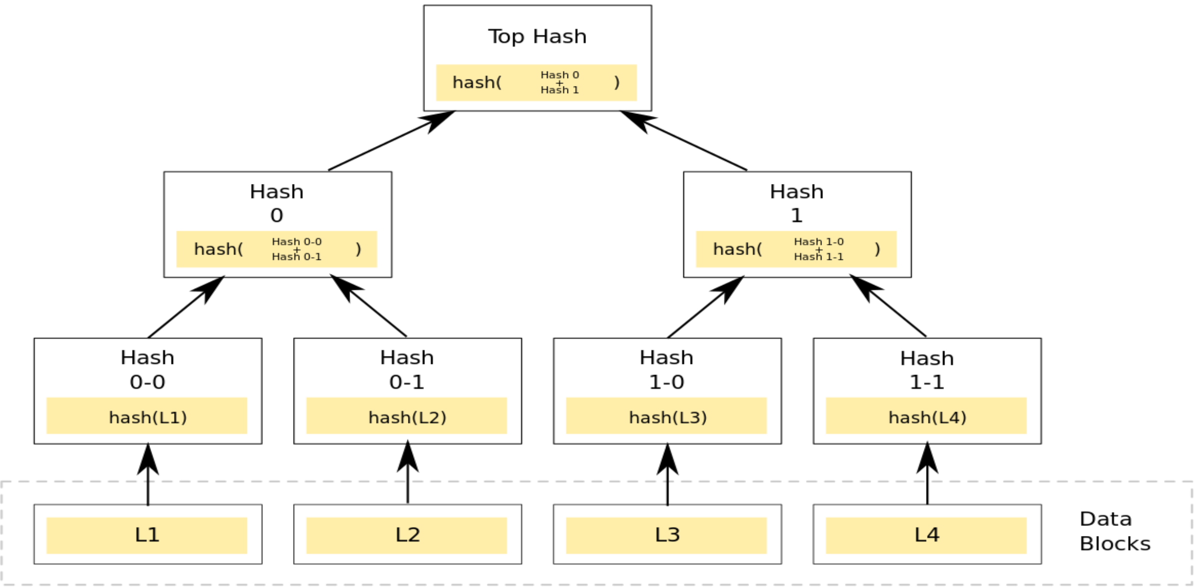
Node

A node in a block chain can be any electronic device that is part of a peer-to-peer network and maintains its copy of the block chain.

The Merkle Tree

A Merkle tree is also called a “hash binary tree,” a data structure for storing transactions in the block chain efficiently and securely.

A Merkle tree summarizes all transactions in a block by creating a digital fingerprint of the entire set of transactions. It is created by repeatedly hashing a pair of transactions from the bottom until we have only one hash, referred to as the Root Hash or Merkle Root.



How it changing the landscape of Digitization:

In this rapidly changing world a large number of businesses have been eagerly engaging in digital transformation to streamline their arduous processes and boost ROI. New trends and cutting-edge technologies have hit the business world from literally all sides and have helped them push on to the next level. It is of paramount importance for management teams to be quick on the uptake to recognize the innovation capacity that digital technology has in stock for their organizations.

Despite the fact that the decentralized ledger technology (DLT) is still in its infancy, experts claim that in the coming years it will produce a substantial impact on all businesses worldwide, regardless of their industry specifics. So, for example, we have already witnessed digital transformation in retail, supply chain, healthcare, manufacturing, eCommerce, real estate, and many other industries. It's pretty clear that blockchain will make its presence felt everywhere and we are yet to see even more elaborate enterprise blockchain solutions.

Blockchain in digital transactions

It goes without saying that fast speed is one of the most important factors in digital transformation, and blockchain, for its part, is famous for demonstrating great speeds when carrying out transactions. What is more, all processes related to keeping and transferring data in a blockchain are generally highly secure. Consequently, fully automated transactions can be adopted in a number of areas and make them more productive.

Blockchain for better connectivity

Considering the importance of digital transformation, a lot of companies globally have switched to rebuilding their communication strategies and techniques. So, for instance, the Internet of Things (IoT) is capable of connecting different devices, whereas cloud-based services allow for seamless access to data and applications. These innovations and developments provide companies with a wide range of opportunities to rebuild their production and work processes. At the same time, these constantly increasing levels of connectivity present some challenges to companies when it comes to dealing with the data. However, the advanced blockchain platforms which heavily rely on the proof-of-stake validation are capable of safely and reliably handling huge amounts of data that is being generated.

Smart contracts powered by blockchain

As of today, smart contracts are used in multiple business processes. They can not only securely store information in a blockchain but also automatically alter the data in a highly trustworthy way. Smart contracts powered by blockchain can be deployed based on the pre-defined agreements; they are generally tamper-proof, highly efficient, and most importantly transparent. They look very promising and are bound to prompt the digitalization of business processes further.

Blockchain for long-term prosperity

A large number of businesses globally may be afraid of blockchain or probably think that only high-tech businesses need to apply it. Still, it’s worth noting that in the future some or probably a majority of large companies will demand their contractors to start using blockchain too in order to achieve higher results, better productivity, and more efficient management. That is exactly why now is the most suitable time to direct your attention to blockchain and put your business on the DLT-rails.

Introduction to Cryptographic Concepts Required:

Cryptography means developing techniques or methods to prevent an outsider from accessing or understanding data from a private message. Let’s review some terms related to cryptography:

1. Encryption: Process of converting plaintext to a ciphertext (random sequence).

2. Decryption: Conversion of ciphertext to plain text; inverse of encryption

3. Cipher: This is the cryptographic algorithm that was used in encryption

Hence, cryptography basically involves sending encrypted messages across a secure channel which is then decrypted in order to obtain the real message. The sender encrypts the message using an algorithm and a specific key, which will be used by the receiver to carry out the decryption of the encrypted message.

These keys are vital to ensure that unauthorized or unwanted individuals/organizations are unable to access the message, data or transaction. Thus, these keys bring the crypto aspects to our information.

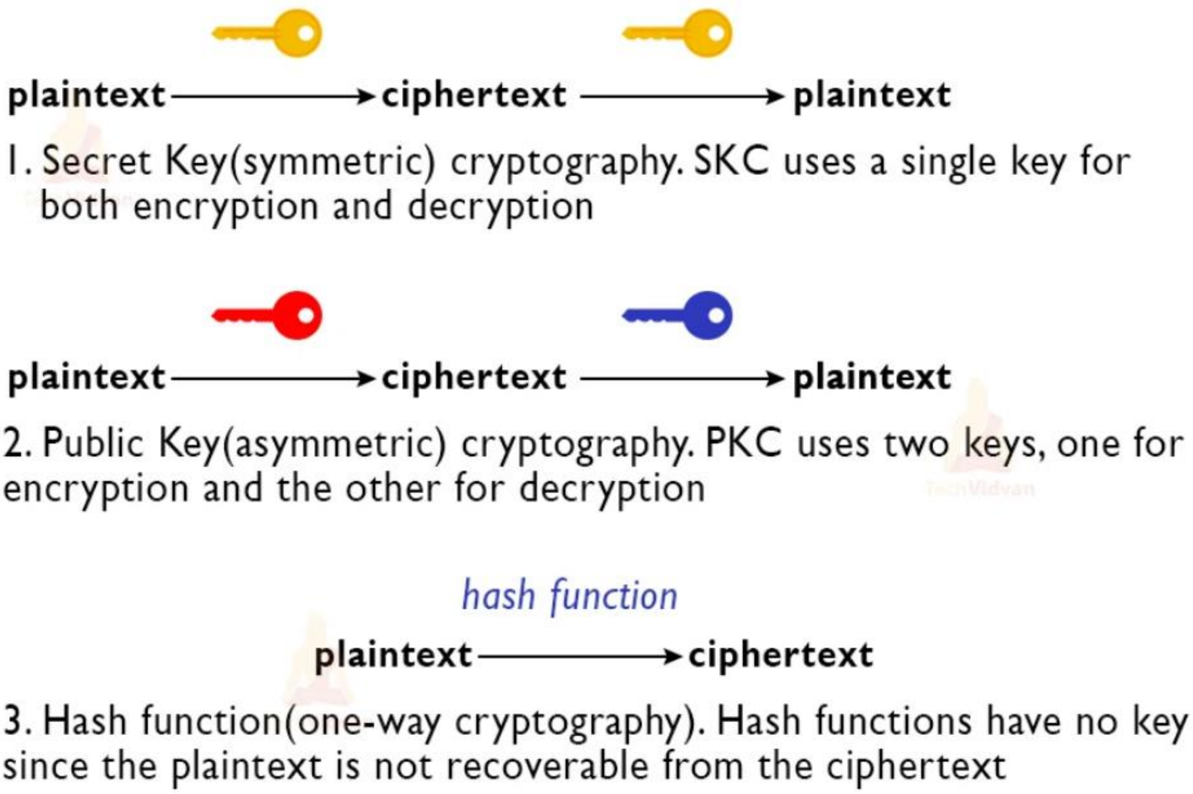
Types of Cryptography in Blockchain

Over the years, cryptography has been of utmost importance to secure important documents through the course of history. Hence, we have a number of types of cryptography that vary according to algorithms used, like:

1. Symmetric Key / Secret-Key Cryptography: Popular encryption method that involves a single key used in both encryption and decryption.

2. Asymmetric Key / Public Key Cryptography: This method involves a pair of keys, public key (for encryption) and private key (for decryption). Both the keys are generated using the same algorithm.

3. Hash Functions: This is a different kind of method that does not involve any key. Cipher is used to generate a hash value of a fixed length from the plaintext. It is highly secure.



1. Secret Key(symmetric) cryptography. SKC uses a single key for both encryption and decryption

2. Public Key(asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption

3. Hash function(one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext

Cryptography in Blockchain

Blockchain technology employs both hash function and asymmetric key cryptography. Asymmetric key cryptography is also used in blockchain. Here, the private key is produced by a random number and the public key is calculated by an irreversible algorithm.

The 2-key authentication system makes it more secure and resistant to attacks. Blockchain uses this method for Digital Signatures. These provide integrity to the data transfer process, and are proof that the data has not been altered, hence often termed as digital fingerprints too because of their uniqueness. Hash functions are used to allow all participants to view the blockchains. The SHA-256 hashing algorithm is the most preferred for this purpose.

Role of cryptography in blockchain

Hash functions and asymmetric keys allow secure data transfer and storage in a blockchain. In fact, hashing allows data storage in a way that it is impossible to generate the input even if output is known. Hence reverse engineering is impossible. The technology is deterministic, thus a particular input will always give the same output and a slight change in the input will drastically alter the output.

SHA 256

This is a hashing algorithm where SHA stands for Secure Hash Algorithm.

Hashing is the process of scrambling raw information to the extent that it cannot be reproduced to its original form. The process takes the plaintext and passes it through a function that performs mathematical operations to convert it to ciphertext. This function is called the hash function, and the output is called the hash value/digest. SHA256 refers to the fact that the hash digest at the end of this algorithm will always be of 256 bits.

Characteristics of hash functions

1. Deterministic: Slight change in the data drastically changes the output

2. Unique output: Each input value has a unique output, but any input will have the same output.

3. Irreversible: The input cannot be generated even if we had access to the output and hash function, hence no reverse engineering

4. Fast Computation: Very quick encryption.

Hence, hash functions are used to link blocks to one another and maintain data integrity inside a block. If data inside a single block is altered or tampered, the chain will break and the blockchain will become invalid.

Benefits of a cryptographic hash to a blockchain

1. Prevents unauthorized modifications

2. A slight change in the input will drastically alter the output

3. Verification of transactions

4. Access to proof of ownership of specific information without revealing the information.

Understanding Digital Signatures in blockchain

Digital signature basically refers to a mathematical approach for creating digital codes which are used to verify if a digital message (or documents) is valid or not. Digital signatures can be considered as proof for the authentication and non-repudiation of the blockchain. They address the requirements of data integrity, immutability and authentication. Effectiveness of blockchain cryptography and these digital signatures depends on symmetric and asymmetric key encryption.

BLOCKCHAIN OR DISTRIBUTED TRUST

The blockchain enables the construction of a vast ledger that is distributed as far and as wide as desired, visible to everyone, updated in accordance with a transactional principle similarly distributed and guaranteed by a community, without the need for a trusted third party as a central authority.

The blockchain makes five promises:

1. Distributed trust.

2. A system of transactions.

3. Guaranteed by an extended community

4. No trusted third parties.

5. The capacity to operate complex protocols.

The blockchain is a genuine innovation: twenty years ago, it was by no means obvious that one day it would be possible for one technology to honour even the first four promises. Having said that, it is very much the combination of the five promises that defines the block chain’s scope of application. If we needed a solution capable of fulfilling only one or two of these promises, other cheaper and more efficient methods would exist

The fifth promise is crucial, as it lends the blockchain its capacity for disruption: the ability to handle complex protocols (money transfers, banking, validation, and so on) in an automated way, with much lower transaction costs compared with systems that require human input, above all in the form of a trusted third party. In other words, the blockchain not only transports information, but also algorithms, and it does so with the same guarantee of trust as applies to the information itself. Already, the reader can begin to imagine the consequences that this could have regarding the automation of a whole range of processes currently carried out by human beings – notarised certificates.

CURRENCY, CRYPTOCURRENCY

Digital Currency – is the digital format of fiat currency that you carry around in your wallet or withdraw from an ATM. It’s the same currency that is backed by an authority, the Reserve

Bank of India in case of Indian currency, and can be exchanged for actual currency if and when it is scheduled to be launched in 2023.

Cryptocurrency – is not backed by a central figure but derives its purchasing power from its community of users. Technically, they are pieces of code created by ‘mining’ that are managed through a digital ledger called as blockchain to ensure transparency at each stage of its journey. Although coins like Bitcoin and Ethereum have many uses when it comes to NFTs and the upcoming metaverse, they cannot be utilised outside of blockchain as these are digital assets that can be traded but not used as a legal tender in India.

HOW A CRYPTOCURRENCY WORKS

Cryptocurrency is decentralized digital money that is based on blockchain technology and secured by cryptography. To understand cryptocurrency, one needs to first understand three terminologies – blockchain, decentralization, and cryptography.

In simple words, blockchain in the context of cryptocurrency is a digital ledger whose access is distributed among authorized users. This ledger records transaction related to a range of assets, like money, house, or even intellectual property.

The access is shared between its users and any information shared is transparent, immediate, and “immutable”. Immutable means anything that blockchain records is there for good and cannot be modified or tampered with – even by an administrator.

How Does Cryptocurrency Work?

Cryptocurrencies are not controlled by the government or central regulatory authorities. As a concept, cryptocurrency works outside of the banking system using different brands or types of coins – Bitcoin being the major player.

1. Mining

Cryptocurrencies (which are completely digital) are generated through a process called “mining”. This is a complex process. Basically, miners are required to solve certain mathematical puzzles over specially equipped computer systems to be rewarded with bitcoins in exchange.

In an ideal world, it would take a person just 10 minutes to mine one bitcoin, but in reality, the process takes an estimated 30 days.

2. Buying, selling, and storing

Users today can buy cryptocurrencies from central exchanges, brokers, and individual currency owners or sell it to them. Exchanges or platforms like Coinbase are the easiest ways to buy or sell cryptocurrencies.

Once bought, cryptocurrencies can be stored in digital wallets. Digital wallets can be “hot” or “cold”. Hot means the wallet is connected to the internet, which makes it easy to transact, but vulnerable to thefts and frauds. Cold storage, on the other hand, is safer but makes it harder to transact.

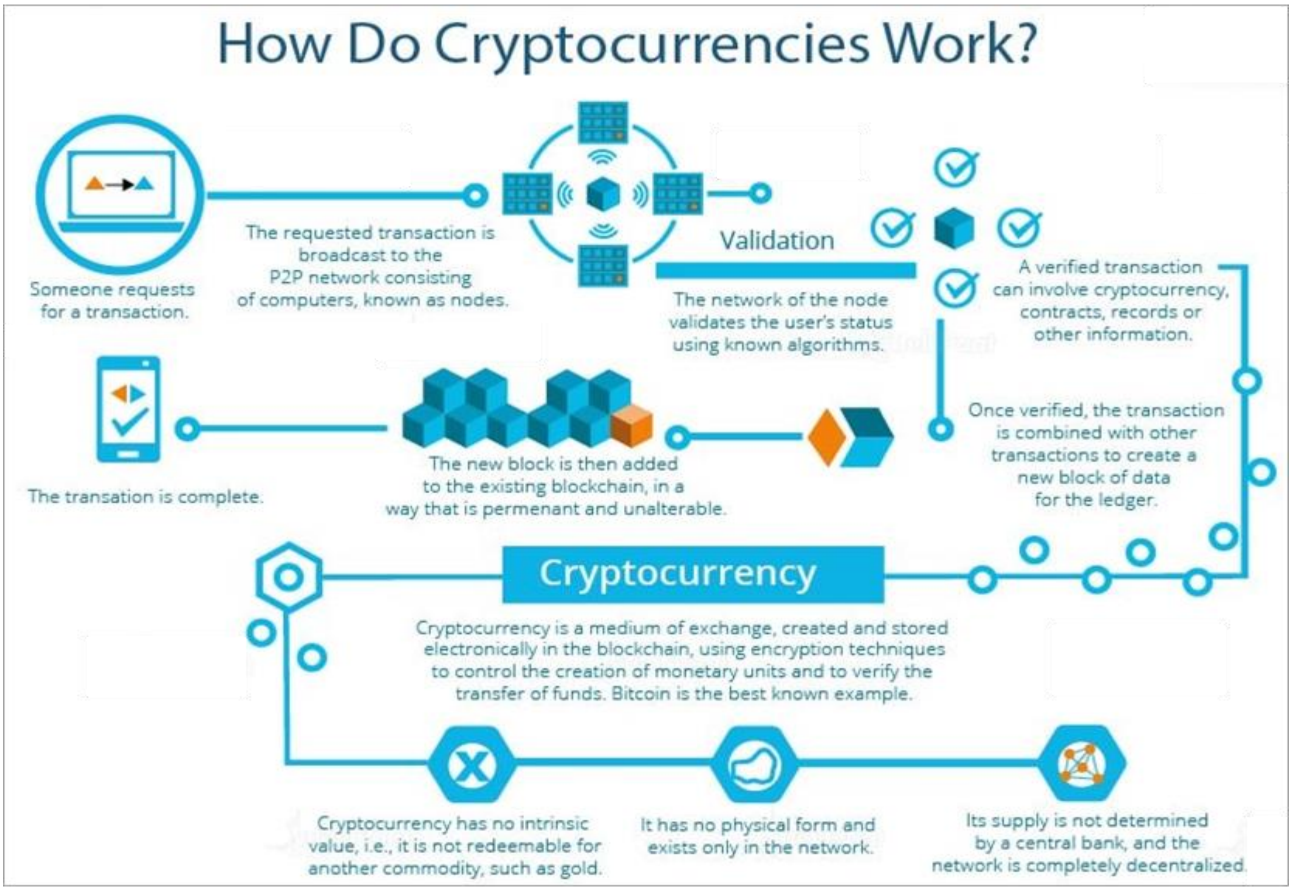
3. Transacting or investing

Cryptocurrencies like Bitcoins can be easily transferred from one digital wallet to another, using only a smartphone. Once you own them, your choices are to:

a) Use them to buy goods or services

b) Trade in them

c) Exchange them for cash


How Do Cryptocurrencies Work?
Someone requests for a transaction.
The requested transaction is broadcast to the P2P network consisting of computers, known as nodes.
Validation
The network of the node validates the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permenant and unalterable.
The transation is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Cryptocurrency has no intrinsic value, i.e., it is not redeemable for another commodity, such as gold.
It has no physical form and exists only in the network.
Its supply is not determined by a central bank, and the network is completely decentralized.

Bitcoin As The First Cryptocurrency

History of Bitcoin

Bitcoin was initiated by a person or a group using a pseudonym or name Satoshi Nakamoto in 2008, as a digital currency or Internet money that is free of manipulation by central authorities or governments. Bitcoin.org was registered as a domain name on 18 August 2008.

Then, Satoshi Nakamoto, later that year, posted on a cryptographic mailing list, a link to the Bitcoin white paper Bitcoin: A Peer-to-Peer Electronic Cash System. The paper discussed a peer-to-peer system that would be used for electronic transactions without relying on human trust.

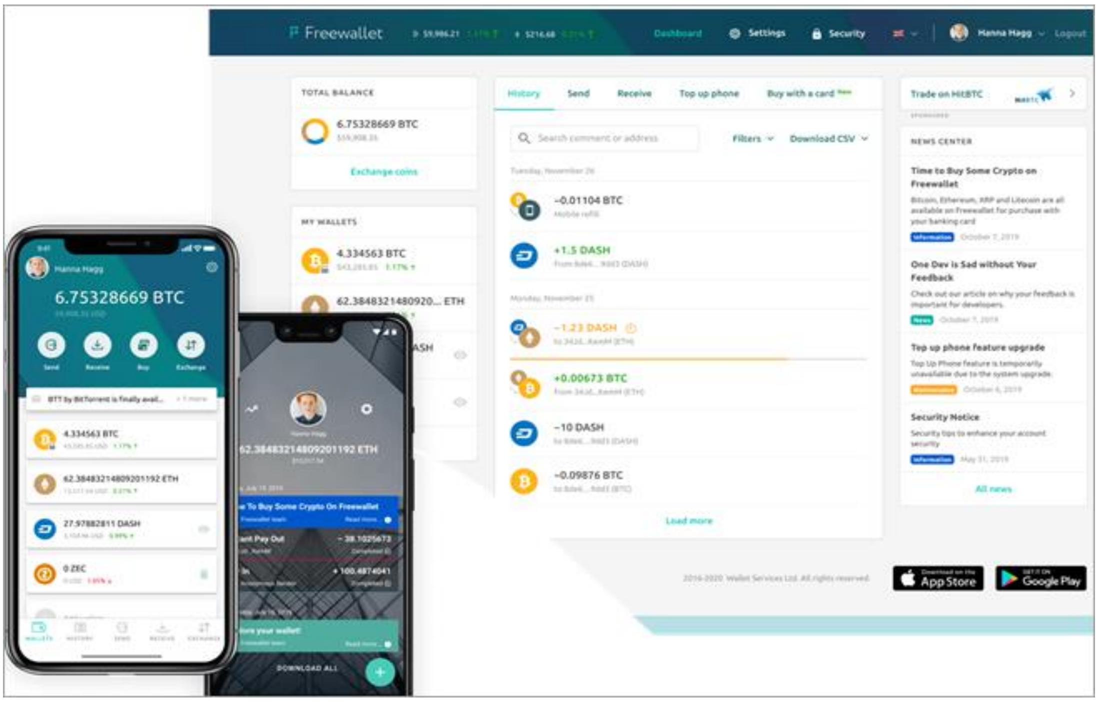
The Bitcoin network then came into operation on 3 January 2009 with Satoshi Nakamoto mining the genesis block number 0. The Coinbase of the block carried the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This referred to the headline published on the same date by The Times and also referred to the instability of central-bank-issued reserve currencies.

- The first Bitcoin client was released on 9 January 2009 and hosted by SourceForge. Hal Finney, a programmer who downloaded the software the same day, used the software to receive 10 Bitcoins from Satoshi Nakamoto. This marked the world's first Bitcoin transaction.
- Before Bitcoin, David Chaum, and Stefan Brands had developed issuer-based e-cash protocols. Adam Back also developed the Hashcash scheme for spam control based on Proof of Work. Wei Dai had created b – money, a Bitcoin predecessor before Bitcoin, and which was the first proposal for distributed digital scarcity-based cryptocurrencies.
- Nick Szabo whose bit gold was a direct precursor of Bitcoin architecture, although it was never implemented. The proposal investigated the use of Byzantine fault-tolerant protocol to store and transfer Proof of Work solutions. Hal Finney had also developed reusable proof of work system.
- Wei Dai and Nick Szabo became huge supporters of Bitcoin.
- Individuals negotiated the value of the first Bitcoins via the Bitcoin Forum. Some of the first notable transactions of Bitcoin included a purchase of pizza from Papa John's on which 10, 000 BTC were spent.

(i) Downloading a wallet and generating an address

To send, sell, or buy Bitcoin, a wallet address is required. Generating a wallet address is not difficult. Most wallets, on downloading, allow generating a wallet address automatically.

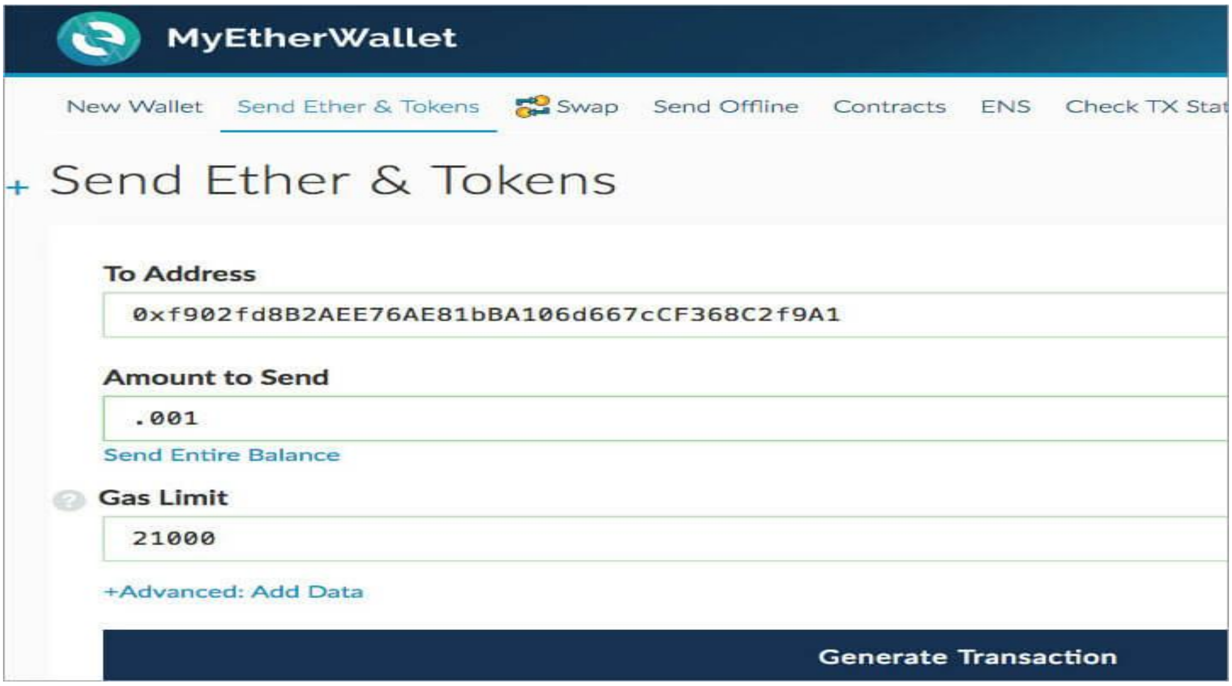
A user can then share this wallet address with other users who want to send or sell crypto. These wallets also allow the user to download and save a private key or seed word that can restore it if deleted wrongfully or when a password is lost.



(ii) **Sending and receiving**

A Bitcoin wallet allows a user to send, store, and receive Bitcoins, but technically stores private and public keys. The private and public key secures cryptocurrencies through cryptography encryption.

1) During the send transaction, the user will assign crypto to the receiver's public key which is associated with the receiver's wallet address that the sender is using.



To Address

0xf902fd8B2AEE76AE81bBA106d667cCF368C2f9A1

Amount to Send

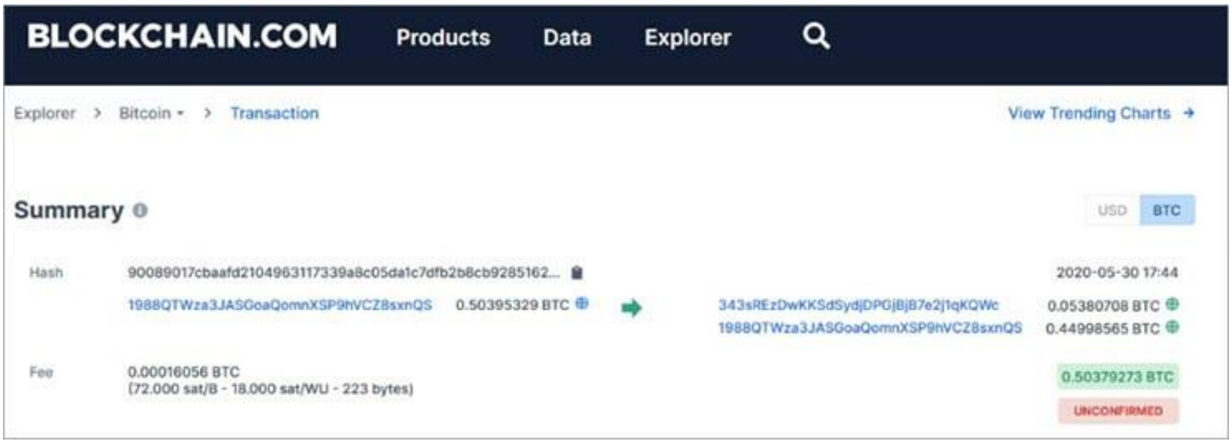
.001

Gas Limit

21000

The receiver then uses its private key to claim ownership by authenticating their wallet and decrypting data related to the corresponding public key where the crypto was assigned. The transaction received can be seen on the wallet's history of transactions or blockchain explorers such as Blockchain.

The below image is an example of a Blockchain explorer showing a completed transaction. Senders and receivers can use explorers to confirm that amount has been sent and received.



Summary

Hash 90089017cbaafd2104963117339a8c05da1c7dfb2b8cb9285162... 2020-05-30 17:44

1988QTWza3JASGoaQomnXSP9hVCZ8sxnQS 0.50395329 BTC → 343sREzDwKKSdSydjDPGjBjB7e2j1qKQWc 0.05380708 BTC
1988QTWza3JASGoaQomnXSP9hVCZ8sxnQS 0.44998565 BTC

Fee 0.00016056 BTC
(72.000 sat/B - 18.000 sat/WU - 223 bytes)

0.50379273 BTC
UNCONFIRMED

Both the private key and the public key used to authenticate the transaction are cryptographically associated with the wallet address.

Another aspect of cryptocurrency working is the creation of a digital signature. The digital signature works in the same way that a signature on a document proves the validity and authenticity of the source.

#3) Hence, a cryptocurrency cannot be copied. The user who sends a transaction uses their private key to create this digital signature, and thus creates mathematical proof that the crypto was sent from his wallet. It also prevents copying of the transaction or crypto.

(iii) Mining and confirmation of the transaction

Once the sender broadcasts the transaction to the blockchain network, the nodes, through the mining process confirm the transaction meets the criteria pre-coded on the blockchain.

The nodes confirm that the transaction is coming from a verifiable source, and other details, for instance, that the user has enough spendable balance. The nodes then mine the transaction by adding it to the block and then to the previous blocks on the blockchain.

The user will then receive the Bitcoins on their wallet through the address they have provided to the sender. The receiver can only spend the Bitcoins by authenticating with their private key, which confirms that he/she is the actual owner of the wallet where the Bitcoins were sent.

(iv) Records and transaction tracking

The Bitcoin wallet then allows tracking of all the transactions relating to the private keys generated on it. It allows transparency of transactions with all the history visible publicly.

Plus these data are immutable or the storage is permanent on the blockchain. Any user can trace the status of the transactions, whether confirmed, rejected, or pending.

Secondly, the blockchain public ledger allows Bitcoin to calculate wallet balances and spendable balances. In a nutshell, most the cryptocurrencies work in a similar way to Bitcoin.

CRYPTOCURRENCY IN FINANCIAL SERVICES

Access to and use of financial services, known as financial inclusion, is crucial for economic growth and development. Unfortunately, a large portion of the population, particularly in developing nations, still lacks access to basic banking services. The World Bank estimates that 1.4 billion adults worldwide are without access to these services, which limits economic opportunities and perpetuates poverty.

Beyond providing access to traditional banking services, cryptocurrency can also offer a range of other financial services. For example, cross-border payments can be made more efficient using cryptocurrency, making it an attractive option for migrant workers sending money to their families. Furthermore, it enables access to alternative financial services, such as loans, savings and insurance, without the need for intermediaries, making it more cost-effective for those who use it.

Cryptocurrency can also help improve financial transparency and reduce corruption by creating a decentralized and transparent ledger, which can help to increase trust in financial systems globally. The use of smart contracts can help automate the execution of financial agreements and reduce the need for intermediaries.

BITCOIN PREDICTION MARKETS

What are prediction markets?

Prediction markets are marketplaces where people trade on the outcomes of future events. Market prices can indicate what the marketplace believes the probability of the event is. For example, “who will win in a sporting event?” For this sporting event there will be two tokens, one for each team. If the price of token A is higher than token B, it means that the market believes team A has a higher chance of winning.

How prediction markets work

Most prediction markets are a binary option market (e.g., “yes” or “no), where the two options will expire at the price of 0% or 100%. Before expiry, the two assets trade between 0% and 100%, which indicates what the marketplace thinks the odds are. Let’s return to our sporting event example. If the market price of token A is US$0.30 and the price of token B is US$0.70, then the market believes the likelihood of team B winning is approximately 70%.

What are the uses of prediction markets?

Prediction markets can be seen as an extension of derivatives markets. Derivatives, such as futures and options, are used to predict the future price of assets such as oil, gold, stocks, and bitcoin. Prediction markets do the same for events.

Prediction markets might also be a public good. They have proven to be relatively accurate at predicting future events. Companies such as Google have begun to use prediction markets. Financial institutions pay attention to prediction markets on things like Central Bank rate hikes. News organizations and society at large pay attention to prediction markets on political elections.

Prediction markets are still a young industry. It seems likely that their predictive power will only increase as a more and varied group of people participate.

Centralized or decentralized prediction markets

Most prediction markets exist within the legacy finance and web2 framework. There are many centralized prediction markets regulated by government organizations like the SEC. These centralized markets have several problems that impact their predictive power.

The most important problem with these centralized markets is that they have low limits on how much each person can bet. This limits the predictive power of prediction markets, because even if a person has very strong conviction about an outcome and the means to back it up, they are capped at limits well under $1,000. This is especially true when someone believes that the likelihood of an event is very mispriced. They, and like minded people, will be unable to capitalize on the market mispricing, and the prediction market will grossly misrepresent the probabilities.

Decentralized crypto prediction markets solve these problems. They do not limit people’s ability to fully express their conviction on an outcome. There are decentralized projects that do no have jurisdictional or KYC requirements. Finally, as is the case when comparing any DeFi protocol to its legacy market counterparts, fees are much lower.