Cryptocurrency: The word cryptocurrency itself is a blend of two Greek words, "**crypto**," which means "to be hidden or to be kept private. The second word in the blend "**currency**" refers to the object used to transfer value from one party to the next.

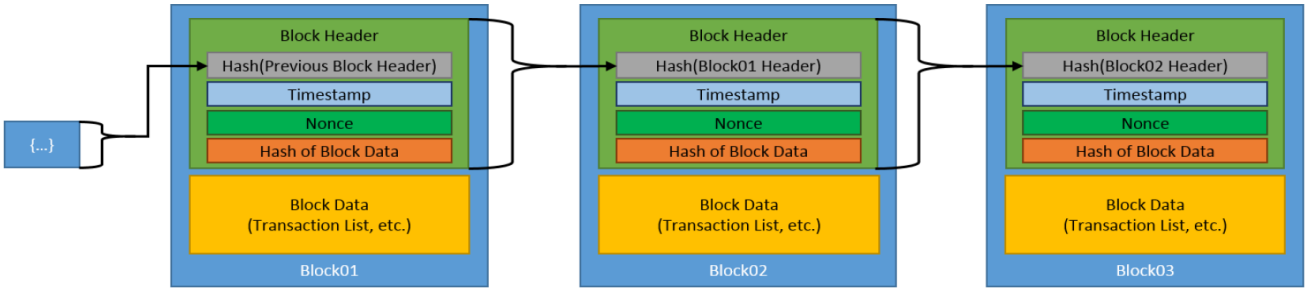
- Today, that object is money, but in the modern world of cryptocurrency, it is **digital code**. It is basically the use of a complex code to encrypt data transfers to exchange value. This is done by creating complex mathematical formulas and unique protocols designed to make the codes virtually impossible to break, counterfeit, or duplicate. These protocols then not only protect the transaction between two parties but they also conceal the identity of all those involved.
- The beauty of cryptocurrency is that it is not under the control of any governmental agency, so there is no **centralized** institution or political entity responsible for determining its value (using **blockchain technologies)**. The value, therefore, is determined primarily by its users and is based on supply and demand.
- It is used just like you would use a physical currency; you can make purchases, save it, trade it, or even invest it in the same manner. The difference is that you would never hold them in your hands; they only exist as **lines of code** maintained in a database, and just like with physical currency, you cannot change its value. If you have $20 bill in your hand, there is no way you can change that to $100 or any other value. It is what it is. However, you can always add to it, subtract from it, or save it anytime you like.
- Cryptocurrencies are the first—and therefore most developed—application of **blockchain** technologies. They create money without central banks and facilitate payments without financial institutions.

Historical Background of blockchain: The roots of blockchain technology go back much further than its current link to digital currencies. The groundwork for blockchain was laid in the early '90s by researchers **Stuart Haber** and **W. Scott Stornetta**. They developed an early prototype for a system that would securely timestamp digital documents, preventing any possibility of backdating or alteration, effectively setting the stage for later blockchain frameworks. In 1998, a computer scientist, Nick Szabo conceptualized 'bit gold', a decentralized digital currency that, although never realized, foreshadowed the structure of **Bitcoin**.

It wasn't until 2009 that blockchain found its first significant application with the creation of Bitcoin by the pseudonymous **Satoshi Nakamoto**. Bitcoin was groundbreaking; it was the first technology to prevent the issue of double spending in a digital currency without relying on any central authority, due to its transparent and immutable **ledger** system.

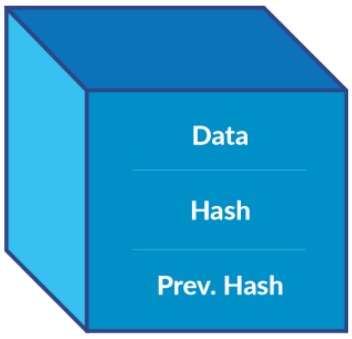
In the years following Bitcoin's debut, blockchain applications have proliferated far beyond the realm of cryptocurrency. Today, it's being used to create impenetrable voting systems (انظمة الانتخابات), enhance supply chain transparency, and even verify identities and property ownership.

Blockchain Technology: Blockchain is a collection of records linked to each other, strongly resistant to alterations, protected using cryptography with a foundation of distributed processing and persistence.



Block: A Block is a collection of data and a unique alphanumeric value generated using the data called **Hash**. It also contains the Hash of the **previous** Block.

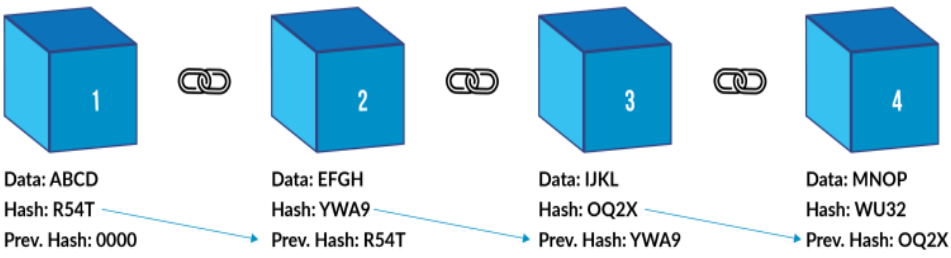
Data: The data inside a Block is dependent on the application, and it could be anything based on the use case.



Hash: It's a code generated based on the data in the Block. It is always unique, even though the data could still be the same.

Previous Hash: It's the Hash code of the previous Block. This is how a chain of blocks is created in a blockchain. Each block contains a hash of the previous block to make it a chain of blocks. This 'previous hash' helps to navigate the entire chain and makes it hard to tamper with data of any block.

The first block in the blockchain won't have a previous hash populated, and it's called a **Genesis** block.

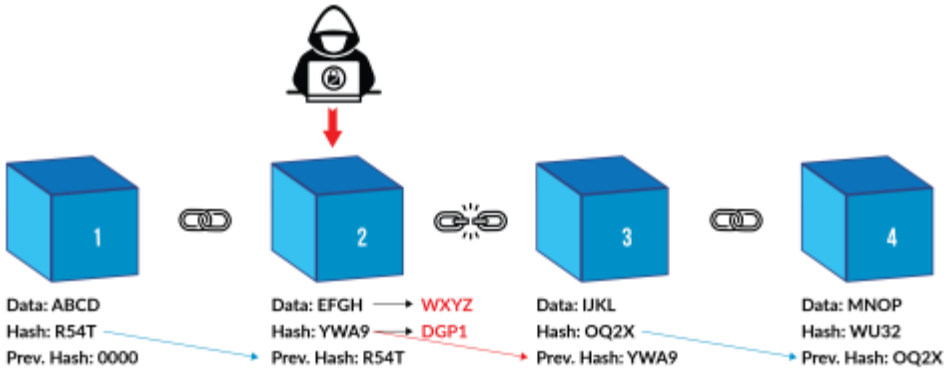


Immutable of Blockchain: Once a block is written, it's immutable, meaning it cannot be altered. If any malicious actor alters a block, its hash changes which is already recorded in the next chained block.

For instance, if a malicious actor tries to make a change to the data on block #2, its corresponding hash value needs to be regenerated. If a hash value is regenerated for block #2, the previous hash in block #3 gets delinked, hence breaking the chain.

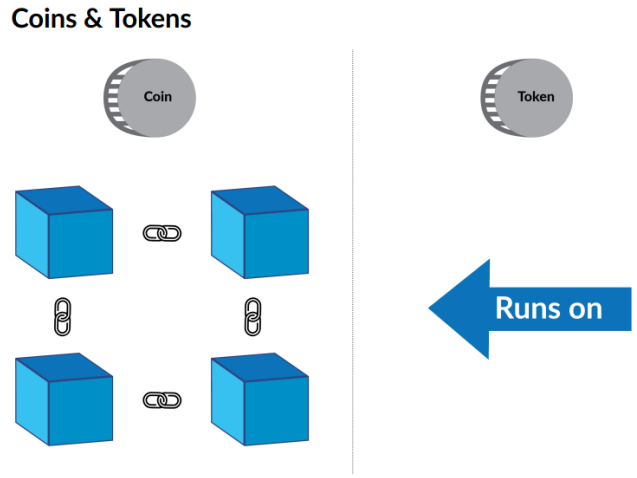
So theoretically, if someone changes a block, the entire chain must be changed, which requires heavy processing power.

With today's ever-growing capacity of processing power, it could theoretically still be possible to change the entire chain. To avoid that, any change to the block must go through something called the **Consensus** model.



Consensus:

A block can be added to the chain by a technique called the Consensus model. The processing nodes which are distributed across, must reach a consensus before adding a new block to the chain by solving a complex problem presented to them.



Blockchain networks run on thousands of computers, and to motivate people to run them, an incentive is needed. This incentive is the cryptocurrency in the form of **Coin** or **Token**.

Coin: Uses its own blockchain network to keep track of all the data, operates independently of any other platform.

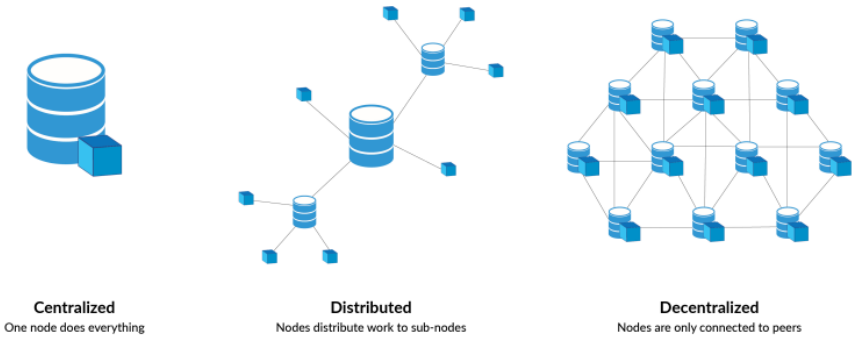
Token: Uses other Blockchain's network and infrastructure and does not worry about how it's validated on the network. The Token just runs on other Blockchain's network.

Public Key/ Private Key: Cryptocurrencies are built upon Public-Key Cryptography (PKC), a cryptographic system that uses pairs of keys – public keys, which are publicly known and essential for identification, and private keys, kept secret and used for authentication and encryption.

Public Key: A public key allows you to receive cryptocurrency transactions. It's a cryptographic code that's paired with a private key. While anyone can send transactions to the public key, you need the private key to "unlock" it and prove that you are the owner of the cryptocurrency received in the transaction.

Private Key: A private key gives you the ability to prove ownership or spend the funds associated with your public address. While you can generate a public key with a private key, doing the opposite is practically impossible because of the one-way "trap-door" function. You can have any number of public keys connected to a private key.

Decentralized: Blockchain takes decentralization to an all-new level. Anything which has been centralized and managed by a central body is being re-imagined with Blockchain networks. No single person, body, or entity owns any of the networks. Instead, everyone who is part of the network owns it – whether it is infrastructure, processing, persistence, changes to the network, or even decision making.



Bitcoin cryptocurrency: The first such blockchain based cryptocurrency was Bitcoin. Within the Bitcoin blockchain, information representing electronic cash is attached to a digital address. Bitcoin users can digitally sign and transfer rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions.

The Bitcoin blockchain is stored, maintained, and collaboratively managed by a distributed group of participants. This, along with certain cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions).

The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted **third** party.

- It also enabled the issuance of new cryptocurrency in a defined manner to those users who manage to publish new blocks and maintain copies of the ledger; such users are called **miners** in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain.

- In Bitcoin, the blockchain enabled users to be pseudonymous. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible. This has effectively enabled Bitcoin to offer pseudo-anonymity because accounts can be created without any identification or authorization process.

Since Bitcoin was pseudonymous, it was essential to have mechanisms to create trust in an environment where users could not be easily identified. Without trusted intermediaries, the needed trust within a blockchain network is enabled by four key characteristics of blockchain technology, described below:

• **Ledger** – the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.

• **Secure** – blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.

• **Shared** – the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.

Distributed – the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.

- For blockchain networks that allow anyone to anonymously create accounts and participate (called **permissionless** blockchain networks), these capabilities deliver a level of trust amongst parties with no prior knowledge of one another; this trust

can enable individuals and organizations to transact directly, which may result in transactions being delivered faster and at lower costs.

- For a blockchain network that more tightly controls access (called **permissioned** blockchain networks), where some trust may be present among users, these capabilities help to bolster that trust.

At a high level, blockchain technology utilizes well-known computer science mechanisms and cryptographic primitives (**cryptographic hash functions**, **digital signatures**, **asymmetric-key cryptography**) mixed with record keeping concepts (such as append only ledgers).

Cryptographic Hash Functions: An important component of blockchain technology is the use of cryptographic hash functions for many operations. Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, text, or image). A specific cryptographic hash function used in many blockchain implementations is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256).

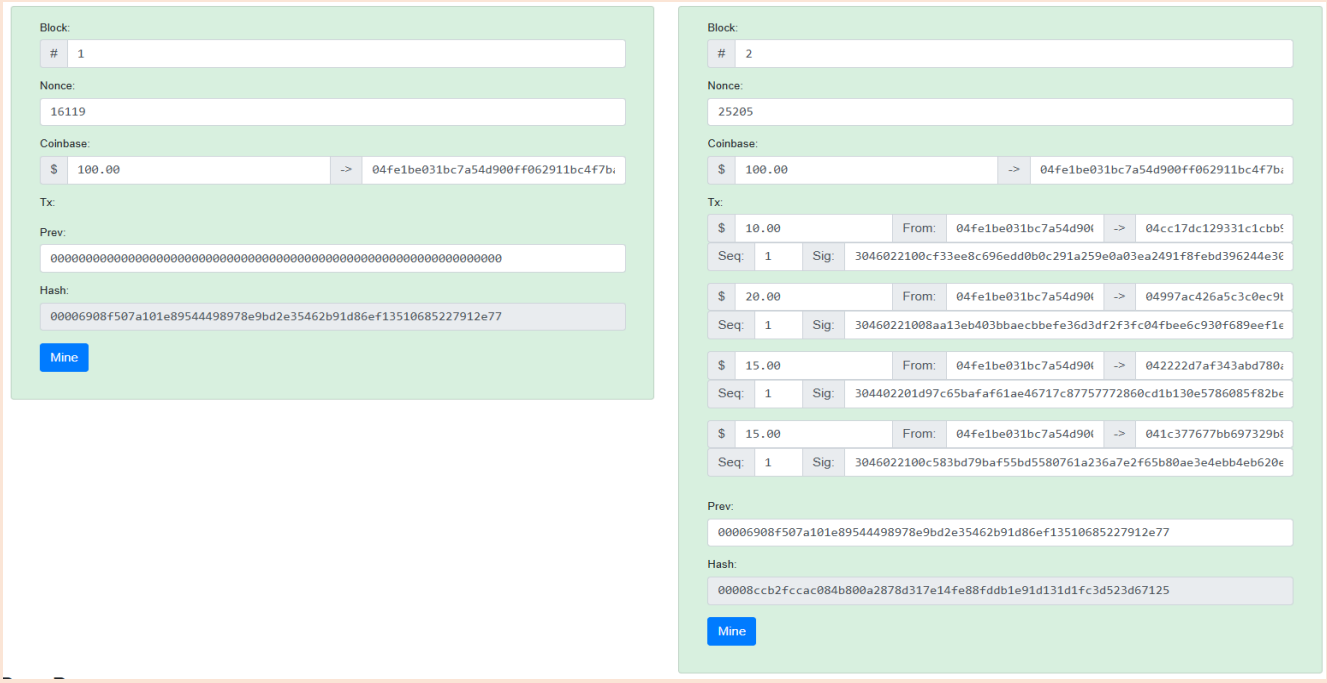
Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

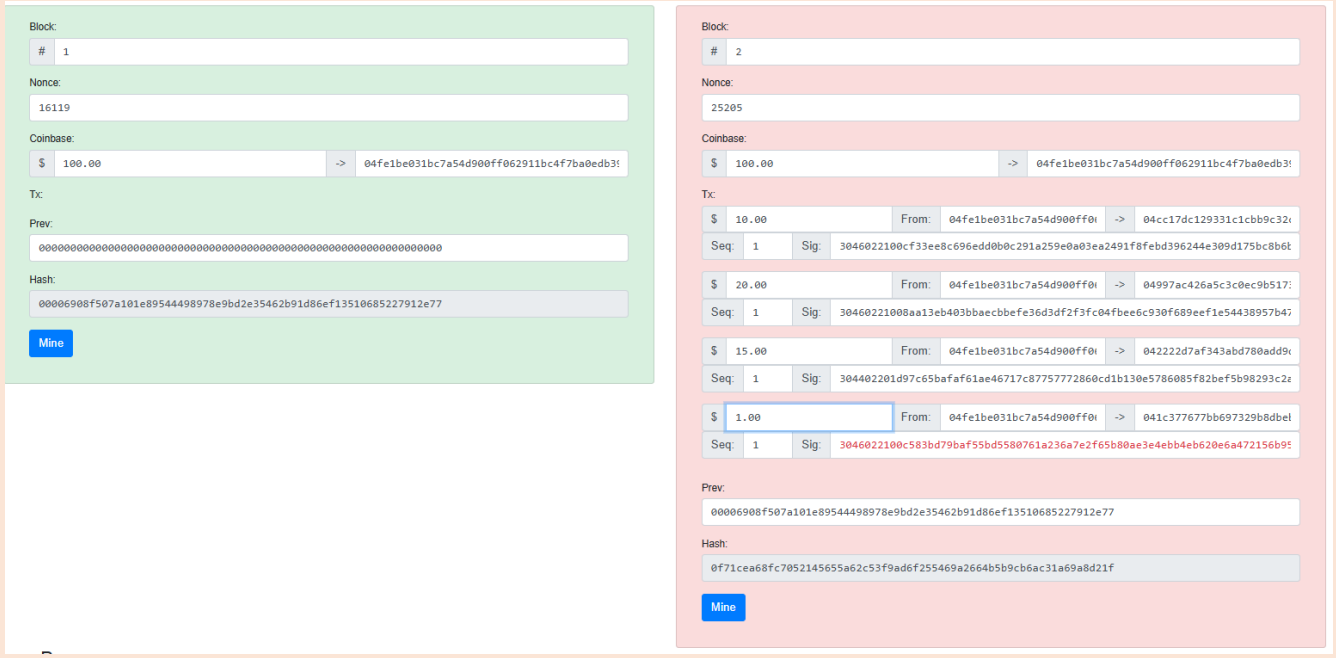
Cryptographic Nonce: A cryptographic nonce is an arbitrary number that is only used once. A cryptographic nonce can be combined with data to produce different hash digests per nonce:

$$hash\,(data\ +\ nonce)\ =\ digest$$

Only changing the nonce value provides a mechanism for obtaining different digest values while keeping the same data.

Example of blockchain:





<u>The total number of Bitcoins</u>: The total number of Bitcoins issued is not expected to reach 21 million. That's because the Bitcoin network uses bit-shift operators—arithmetic operators that round some decimal points down to the closest smallest integer.

This rounding down may occur when the block reward for producing a new Bitcoin block is divided in half, and the new reward amount is calculated. That reward can be expressed in satoshis, with one satoshi equaling **0.00000001** Bitcoins. Because a satoshi is the smallest unit of measurement in the Bitcoin network, it cannot be split in half.

Illustration showing Bitcoin mining rewards and halving events from 2009 to 2024 highlighting diminishing new coin issuance over time

With the number of new Bitcoins issued per block decreasing by half approximately every four years, the final Bitcoin (realistically, the final satoshi) is not expected to be generated until 2140 (it might be earlier). The number of new Bitcoins minted per block was 50 when Bitcoin was first established and has since decreased to 3.125 as of 2024—the next halving to 1.5625 is expected sometime in 2028.

Sample Use Cases

Voting: Voting with Blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using Blockchain in this way would make votes nearly impossible to tamper with. The Blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election.

Property Records: In the present day, the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index. This process is not just costly and time-consuming, it is also prone to human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain can eliminate the need to scan documents and track physical files in a local recording office. If property ownership is stored and verified on the Blockchain, owners can trust that their deed is accurate and permanently recorded.

Supply Chain: As in the IBM Food Trust example, suppliers can use Blockchain to record the origins of their purchased materials. This would allow companies to verify the authenticity of not only their products but also common labels such as "Organic," "Local," and "Fair Trade."

Healthcare Records: Healthcare providers can leverage Blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the Blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the Blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy.