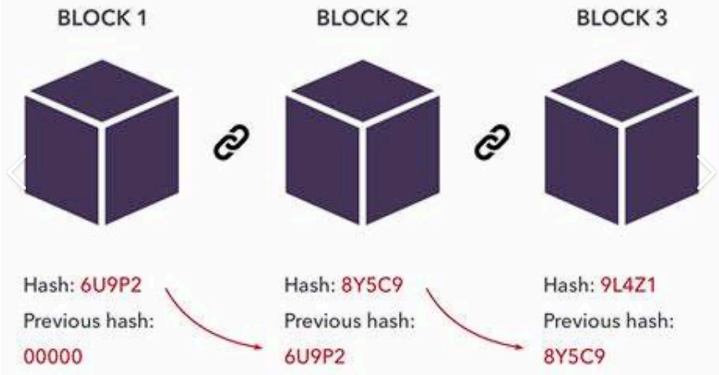
Introduction to Blockchain Technology

What is blockchain?

A method for introducing a secure and decentralized record of enormous transactions. It's a **digital ledger** that is distributed across a network of computers, ensuring that **no single entity** has control over the entire history of transactions via a few processes. There are **decentralization**, **distributed ledger**, **cryptography**, etc neither single entity from failures. Each **"BLOCK"** in the blockchain **contains** a **number of transactions**, and every time a transaction **occurs** on the blockchain, the record of the transaction is **added** subsequently to every **participant's ledger**.



Unique aspect of blockchain is achieved through **cryptographic techniques**, ensuring that a transaction is **recorded** in a **block**, it cannot be **altered retroactively** without **altering** all **subsequent blocks**, the unique characteristics makes blockchain **valuable** for the system that requires an immutable and transparent record of transactions.

Origin

First outlined in 1991 by Stuart Haver and W.Scott Stornetta, two researchers who wanted to implement a system where **document timestamps** could not be tampered with. Invention of **Bitcoin**, a **digital currency**, by an individual under pseudonym **Satoshi Nakamoto** in 2008, entitled "Bitcoin: A Peer-to-Peer Electronic Cash System," to create a **decentralized currency** free from central authority or government control.

"Bitcoin: A Peer-to-Peer Electronic Cash System" by **Satoshi Nakamoto**:
A purely p2p version of electronic cash would allow online transactions/payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending, therefore, a solution proposed to double-spending using a p2p network. The network timestamps transactions by **hashing** them into an **ongoing chain** of

hash-based proof-of-work, forming a record that **cannot be changed** without **redoing** the proof-of-work. The **longest chain** not only serves as **proof of** the sequence of **events witnessed**, but proof that it came from the largest pool of the **CPU** or the **power** of a machine. As long as the majority of CPU power is controlled by **nodes** that are not cooperating to attack the network, they will generate the **longest chain** and outpace attackers. The network itself requires minimal structure. **Messages** are **broadcast** on a best effort basis, and **nodes** can **leave** and **rejoin** the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

"Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money" by **Nathaniel Popper**
The author introduces us to the **central characters** who played pivotal roles in **Bitcoin's development**. From an **Argentinian millionaire** to a **Chinese entrepreneur**, and even the elusive creator of Bitcoin, Satoshi Nakamoto. **"Digital Gold"** explores the notion of a new currency maintained by users' computers worldwide which is a concept that has both fascinated. Bitcoin has grown into a technology worth billions of dollars, with followers who view it as a groundbreaking idea to the creation of the Internet. **Believers** from **Beijing to Buenos Aires** envision a **financial system free** from **traditional banks** and **government control**, and **Bitcoin** has the potential to **decentralize** some of society's fundamental institutions.

Blockchain Process

1. Someone requests a **transactions.**
2. The **requested transaction** is **broadcast** to a **Peer-to-Peer** network consisting of computers known as **nodes.**
3. The P2P network of nodes **validated** the transaction and the user's status using known **algorithms**.
4. Once **verified**, the transaction is **combined** with other transactions to create a **new** block of data for the **ledger.**

5. The **new block** is then **added** to the **existing blockchain** in a way that is **permanent** and **unalterable.**
6. The transaction is completed.

Blockchain Characteristics

1. Data Immutability
   Ensures that once data (**transactions**) is **recorded** on the blockchain, it becomes **tamper-resistant** and virtually **impossible to alter**. The cryptographic nature of blockchain and the **interlinking** of blocks **through hashes** create a secure and unchangeable history of transactions.

2. Decentralization
   There is **no central authority** or i**ntermediary controlling** the blockchain network. Instead, it operates on a **distributed network of nodes** where **each node** has its own **copy** of the entire blockchain. This **eliminates** the **need for intermediaries**, like banks or government control entities, **fostering a peer-to-peer environment.**

3. Transparency
   Ensures transparency by making all **transactions visible** to every participant in the network. Once a **transaction is added** to the blockchain, it becomes a **permanent** and **auditable record** that anyone on the network can **inspect/withdraw**.

4. Trust
   The **immutable recording** of transactions in a **distributed ledger** ensures that the data is reliable and **cannot be manipulated**. Verification and validation processes, often achieved through **consensus mechanisms** like Proof of Work or Proof of Stake, further enhance trust by **requiring agreement** among **network participants** before a **transaction is** considered **valid**.

   In summary, data immutability ensures the security and permanence of recorded transactions, decentralization eliminates the need for intermediaries, transparency provides visibility into the transaction history, and trust is established through a combination of immutable recording, verification processes, and consensus mechanisms. Together, these characteristics make blockchain a robust and trustworthy technology for various applications, including cryptocurrencies like Bitcoin.

History and Evolution of Blockchain

1. Early foundations (1990s)
   Researchers Stuart Haber and W. Scott Stornetta **proposed** a cryptographically secure chain of blocks to **timestamp digital documents**, preventing **backdating** or **tampering**.

2. The Bitcoin Revolution (2008-2009)
   True birth of blockchain, Satoshi Nakamoto, marked the true genesis of blockchain. Born in the aftermath of the global financial crisis, Nakamoto aimed to establish a **decentralized monetary** system free from **central control**. **Bitcoin**, the first use of blockchain, introduced a revolutionary method for **securing** and **validating transactions** through a **distributed ledger**. The operational launch of the Bitcoin (currency exchange only) blockchain in January 2009, with the mining of the "Genesis Block," represented the practical realization of blockchain technology's potential.

   Native currency: Bitcoin

3. Beyond Bitcoin (2010-2017)
   The potential of blockchain began to be recognized beyond just **powering cryptocurrencies**. Developers and entrepreneurs started exploring other uses of blockchain for creating **decentralized applications (DApps)** beyond currency transactions.

4. **Ethereum** (2015) [**20k to 100k transactions/sec**]
   One of the significant developments was the introduction of Ethereum in 2015 by Vitalik Buterin, Gavin Wood and Jeffrey Wilcke. Ethereum expanded upon Bitcoin's capabilities, introducing currency exchange and the amalgamation of **smart contracts** with the terms of the **agreement** directly **written into code**, enabling **more complex** and **automated interactions** on the **blockchain**. Ethereum marked the shift from blockchain as a financial tool to a multi-functional platform and can be used for all kinds of blockchain applications.

   Smart Contracts (Short Definition)
   Provide the capability of "**code execution**" for embedding business login on Blockchain. **Self-enforcing agreements** (Only enforced by the parties to it; no external party interference) embedded in computer code. Allow the performance of credible transactions without third parties. Broader applications for blockchain technology.

   Native Currency: Ether

5. Hyperledger Fabric (2017) **[20k translation/sec]**
   Modular blockchain framework that serves as a foundation for developing blockchain-based products, solutions, and applications within private enterprises such as

banks, financial institutions, and supply chain networks, can utilize Hyperledger Fabric to build secure and efficient blockchain solutions.

From the perspective of **Architecture**, Hyperledger Fabric provides a modular architecture that allows **interchangeable** components. These components include **consensus mechanisms** and **membership services**. It enables a **plug-and-play** environment, making it **flexible** for various use cases. **Fabric** is designed to meet **diverse industry needs**, suits for a wide range of applications. To ensure privacy, **Fabric** offers a unique approach to **consensus** that balances **scalable performance** with privacy. It ensures robustness, customization, and scalability for **distributed ledger applications**.

6. Maturation and Diversification (2018-Present)
   Various new blockchain platforms have **emerged**, each with specific focuses like improved scalability, security, or interoperability. Major industries, including finance, healthcare, supply chain, and even governments, have begun adopting blockchain for its **transparency, security**, and efficiency. The technology's evolution has also **sparked debates** and **research** in **areas** like **scalability** (e.g., **Bitcoin's Lightning Network**), **sustainability** (concerns over **energy consumption** in **Proof of Work** models), and **regulatory acceptance**.

The need for web3 and how it is different from web2

Web1 (frontend)
First iteration of the internet was primarily a collection of static websites or the “Read-only Web”, serving as a digital information repository and served with limited interactivity. During the phase, users only passively consume the information displayed on websites, lacking interaction of the dynamic and interactive features. Typically, web1 were informational and presented in a one-way communication format, and the overall web experience was largely static and read only with minimal user engagement or participation.

Web2 (Centralized)
The internet known as social web or “Read-Write Web”, is characterized by interactive experiences, social media, and user-generated content. The internet transformed into a dynamic platform where users could actively contribute, share and collaborate from blogging. Besides, Web2 supports key components such as modern frontend backend technologies, cloud computing and databases. Emphasize engagement and interconnected online experiences. However, Web2 centralized the control of data and platforms in the hands of a few major companies leading to concerns over privacy, data ownership and monopolistic practices.

Web3

Web3 focus shifts to decentralization, increase privacy, a more secure and transparent internet infrastructure, openness and greater user empowerment. Web3 is built upon the backbone of blockchain technology, which allow for decentralized and p2p interactions without the need for intermediaries. Web3 will be anywhere, accessible from any device and can be accessed anytime by anyone. The goal is to reduce reliance on centralized authorities, enhance user control over personal data. Where individuals have greater ownership and control over their digital identities and assets.

Web2	Web3
Dominated by centralized services like Google, FB, Amazon, where user data is controlled by these entities	Decentralized networks, offering a platform where data is distributed access a network, mitigating the risks of centralized control and data breaches from failures.
Data ownership and privacy. Surrender their data to the service provider.	Emphasize user sovereignty over personal data. Ensure that individuals maintain ownership and control over their own data.
Many web2 applications	Characterized by open protocols and standards, enabling different services and applications to interact more. Foster a more interconnected and interoperable web ecosystem.
Not possible for tokenization	Incorporates concepts like cryptocurrencies and non-fungible token (NFTs) allwing for the creation, ownership and trading digital assets. The tokenization introduces new economic models and opportunities for users to directly benefit from the value they create online

Digital assets NFTs
Decentralized Autonomous Organization (DAO)
Metaverse

Key concepts: blocks, transactions, decentralized networks

Concept:

- Transaction are broadcast to the network
- Transaction are collected in blocks
- Blocks are chained together
- All nodes maintain the same ledger
- Distributed ledger replaces databases

Blockchain vs traditional databases