Survey Report

On

Types of Blockchains and its Real-Time Use Cases

Introduction

The blockchain technology was introduced in 2008 through Bitcoin, which solved the double-spending problem without needing a trusted intermediary like a financial institution. Initially, Bitcoin's blockchain was designed for peer-to-peer currency exchange with limited programmability, supported by a scripting system called Script. However, Vitalik Buterin expanded this concept by developing Ethereum, a blockchain platform equipped with a Turing-complete programming language that allowed the creation and execution of decentralized applications (DApps) and smart contracts.

The growth of blockchain technology has led to the development of various blockchains and software stacks to support different use cases beyond digital currencies. Ethereum’s programmability has fostered innovation in areas like identity verification, digital voting, and supply chain management. Furthermore, blockchain's ability to provide transparency, immutability, and decentralization has proven beneficial for sectors requiring secure record-keeping, including property title registries and public voting systems.

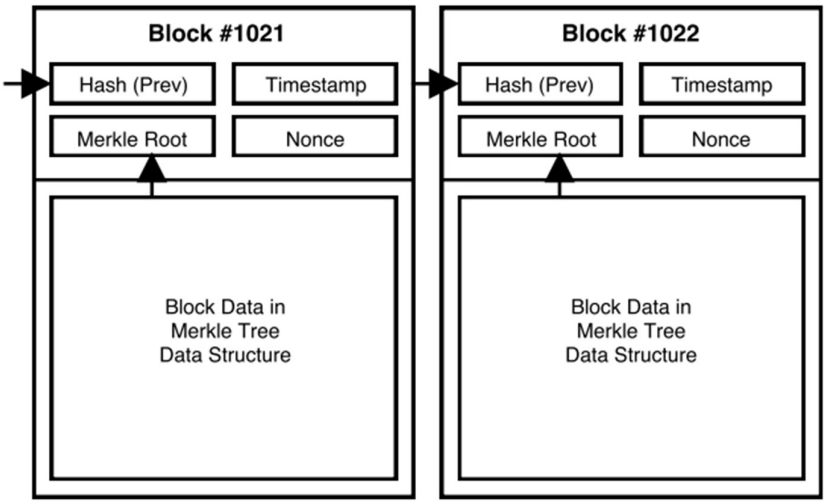
History

Blockchain technology's history dates back to the 1980s, with early ideas surrounding decentralized digital currencies and cryptographic protocols. One key innovation during this time was the Blind Signature, a cryptographic primitive introduced by David Chaum, which paved the way for secure e-cash systems. In 1990, Chaum commercialized this concept through Digicash, the first digital currency, but it ultimately failed due to its reliance on a centralized third party and its eventual bankruptcy in 1998.

Several other attempts at decentralized currencies followed, such as E-gold in 1996, which achieved a user base of 5 million but was ultimately shut down due to its association with illegal activities. Wei Dai's b-money proposal introduced the concept of decentralized consensus using computational puzzles but lacked practical implementation details.

The turning point came in 2008 with the release of the Bitcoin whitepaper by Satoshi Nakamoto, which introduced the first successful decentralized digital currency and blockchain application. This system combined public key cryptography and the proof-of-work consensus algorithm to solve the double-spending problem without a central authority. Nakamoto's breakthrough laid the foundation for the blockchain revolution, leading to subsequent innovations such as Ethereum and a wide range of blockchain-based applications

Blockchain Concept



General Structure of a Block in a Blockchain.

Blockchain is an immutable, distributed, digital ledger technology designed to record transactions securely, with its core foundation based on decentralization, cryptography, and peer-to-peer networking. The key concept of blockchain is that it enables trust in a trustless environment, where there is no need for a central authority to validate or govern transactions. Instead, the network participants themselves validate transactions through consensus mechanisms.

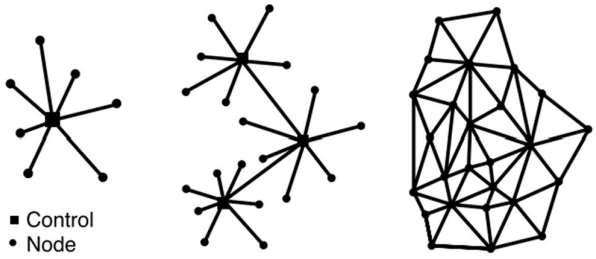
At the heart of blockchain technology is the ledger system, which originated from ancient accounting practices but evolved into a triple-entry accounting system with blockchain. Transactions are stored digitally in a way that ensures they cannot be altered once recorded, as long as the majority of nodes in the network operate honestly. This is achieved through cryptographic hash functions, which secure the data by generating unique identifiers (hashes) for each transaction or block of transactions. Any attempt to modify a block would change its hash, alerting other nodes of the discrepancy.

Blockchain operates on a peer-to-peer network, where every participant (node) holds a replica of the blockchain. The nodes communicate using a consensus

algorithm to agree on the validity of new transactions. Proof of Work (PoW), one of the earliest and most widely used consensus algorithms, involves solving computationally intensive puzzles to secure the network, ensuring that blocks are added in a fair and orderly manner.

Another critical aspect of blockchain is its decentralized nature. Unlike traditional systems where a central authority controls data, blockchain is maintained by all participating nodes, making it more resistant to attacks and ensuring transparency and security. Furthermore, smart contracts, first popularized by the Ethereum blockchain, have extended blockchain's functionality, enabling automated, programmable transactions that execute without intermediaries.

Overall, blockchain represents a revolutionary approach to securing and managing digital information, with applications far beyond its original use in cryptocurrencies



Centralised, Decentralised and Distributed Network

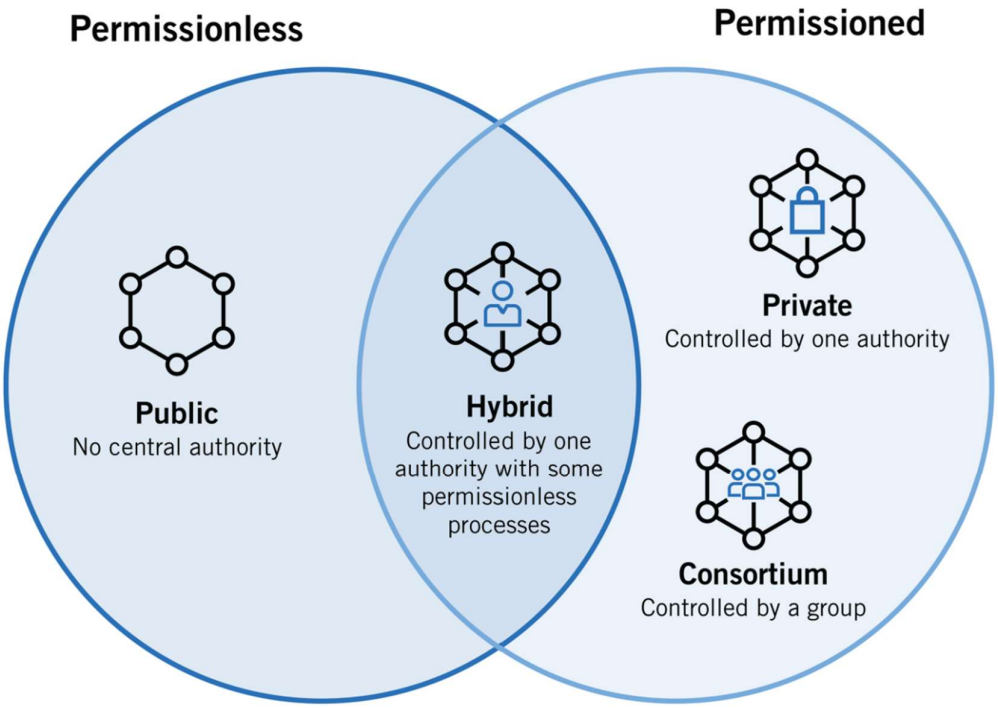
Types Of Blockchain

All types of blockchains can be characterized as permissionless, permissioned, or both. Permissionless blockchains allow any user to pseudo-anonymously join the blockchain network (that is, to become "nodes" of the network) and do not restrict the rights of the nodes on the blockchain network. Conversely, permissioned blockchains restrict access to the network to certain nodes and may also restrict the rights of those nodes on that network. The identities of the users of a permissioned blockchain are known to the other users of that permissioned blockchain.

Permissionless blockchains tend to be more secure than permissioned blockchains, because there are many nodes to validate transactions, and it would be difficult for bad actors to collude on the network. However, permissionless blockchains also tend to have long transaction processing times due to the large number of nodes and the large size of the transactions. On the other hand, permissioned blockchains tend to be more efficient. Because access to the

network is restricted, there are fewer nodes on the blockchain, resulting in less processing time per transaction.

Like so many things, pros come with cons, and the reduced processing time in permissioned blockchains is no exception: the centralization of permissioned blockchains to some central authority (be it a government, a company, a trade group, or some other entity or group that is granting the permission to nodes and creating the restrictions of the blockchain) makes it a less secure system that is more prone to traditional hacking vulnerabilities. The fewer nodes there are on a blockchain, the easier it is for bad actors to collude, so private blockchain administrators must ensure nodes adding and verifying blocks are highly trusted.



1. Public Blockchains :

Public blockchains are permissionless in nature, allow anyone to join, and are completely decentralized. Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data. To date, public blockchains are primarily used for exchanging and mining cryptocurrency. You may have heard of popular public blockchains such as Bitcoin, Ethereum, and Litecoin. On these public blockchains, the nodes “mine” for cryptocurrency by creating blocks for the transactions requested on the network by solving cryptographic equations. In

return for this hard work, the miner nodes earn a small amount of cryptocurrency. The miners essentially act as new era bank tellers that formulate a transaction and receive (or “mine”) a fee for their efforts.

2. Private (or Managed) Blockchains :

Private blockchains, which may also be referred to as managed blockchains, are permissioned blockchains controlled by a single organization. In a private blockchain, the central authority determines who can be a node. The central authority also does not necessarily grant each node with equal rights toperform functions. Private blockchains are only partially decentralized because public access to these blockchains is restricted. Some examples of private blockchains are the business-to-business virtual currency exchange network Ripple and Hyperledger, an umbrella project of open-source blockchain applications.

Both private and public blockchains have drawbacks - public blockchains tend to have longer validation times for new data than private blockchains, and private blockchains are more vulnerable to fraud and bad actors. To address these drawbacks, consortium and hybrid blockchains were developed.

3. Consortium Blockchains :

Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain. Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security. However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk (which we will examine in an upcoming article). Further, some members of supply chains may not have the needed technology nor the infrastructure to implement blockchain tools, and those that do may decide the upfront costs are too steep a price to pay to digitize their data and connect to other members of the supply chain. A popular set of consortium blockchain solutions for the financial services industry and beyond has been developed by the enterprise software firm R3.

In the supply chain sector, CargoSmart has developed the Global Shipping Business Network Consortium, a not-for-profit blockchain consortium which aims to digitalize the shipping industry and allow maritime industry operators to work more collaboratively.

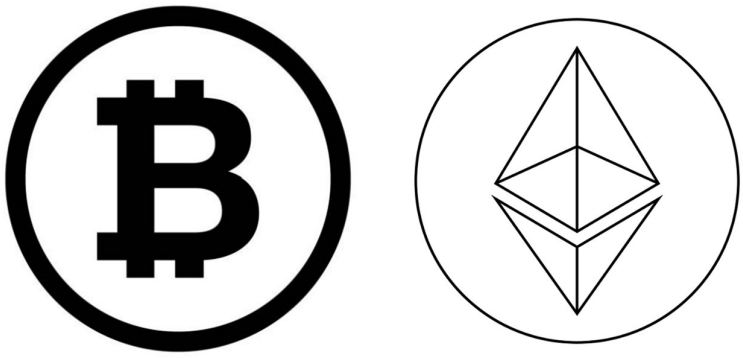
4. Hybrid blockchains:

Hybrid blockchains are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations. An example of a hybrid blockchain is IBM Food Trust, which was developed to improve efficiency throughout the whole food supply chain.

Real-Time Application of Blockchain

1. Money Transfer

Blockchain allows fast, secure, and low-cost money transfers by eliminating intermediaries like banks. Cryptocurrencies like Bitcoin and Ethereum enable peer-to-peer transactions that are verified through a decentralized network of nodes. This reduces transaction fees and ensures transparency and security. Blockchain-based transfers are particularly advantageous for cross-border payments, where traditional systems are often slow and expensive.



2. Smart Contracts

Smart contracts are self-executing contracts with terms coded directly into the blockchain. They automatically execute and enforce agreements when predefined conditions are met, eliminating the need for intermediaries such as lawyers or notaries. Ethereum, the leading blockchain for smart contracts, allows developers to build decentralized applications (DApps) that rely on these contracts, streamlining processes like insurance claims, financial transactions, and legal agreements.

3. Internet of Things (IoT)

Blockchain enhances IoT by providing a secure and decentralized framework for data exchange between devices. Each IoT device can record its transactions or

activities on a blockchain, ensuring that the data is tamper-proof and transparent. This is particularly useful in industries like supply chain management, where IoT devices monitor goods, and blockchain ensures data integrity, improving traceability and automation.

4. Personal Identity Security

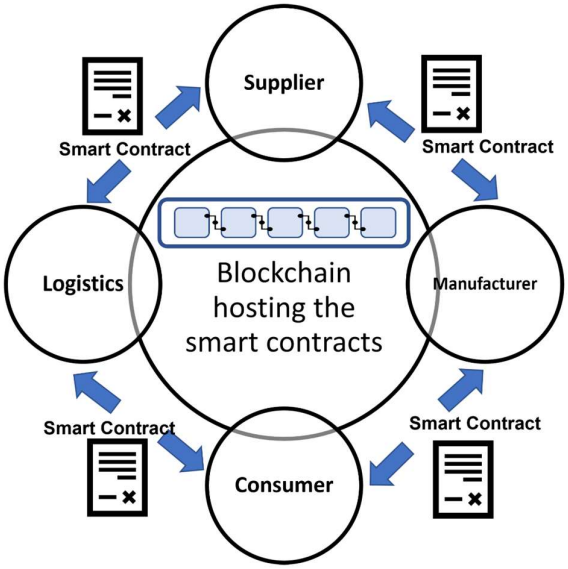
Blockchain enables secure and tamper-resistant digital identity systems. Users can store personal identity information on a blockchain, giving them control over their data. Blockchain-based identity solutions eliminate the need for centralized authorities, reducing the risk of data breaches. Individuals can share only necessary information with third parties, safeguarding privacy and ensuring data security.

5. Healthcare

In healthcare, blockchain secures and decentralizes patient records, making them accessible only to authorized individuals. Medical data is stored in an immutable and encrypted format, ensuring privacy while allowing for secure sharing between hospitals, labs, and patients. This improves patient outcomes by providing a more efficient system for managing medical records, verifying prescriptions, and ensuring accurate diagnosis.

6. Logistics

Blockchain is used in logistics to track goods in real-time across the supply chain. Each transaction or movement of goods is recorded on a blockchain, providing an immutable history of the product's journey from origin to destination. This improves transparency, reduces fraud, and helps companies verify the authenticity and condition of products, enhancing trust among participants in the supply chain.



7. Non-Fungible Tokens (NFTs)

NFTs are unique digital assets stored on a blockchain, primarily used to represent ownership of digital art, music, and other digital collectibles. Since each NFT is recorded on the blockchain, ownership can be verified, and the asset's provenance is transparent. This has revolutionized the art world, allowing creators to sell their work directly to buyers while securing their intellectual property rights.

8. Government

Blockchain can improve government services by ensuring transparency and efficiency in areas like voting, land registries, and public records management. It enables secure and tamper-proof systems for recording and verifying government data. For instance, blockchain-based voting systems allow for secure, verifiable elections with increased trust and reduced fraud risks.

9. Media

Blockchain addresses issues of copyright infringement and unfair distribution of revenue in the media industry. By recording ownership and licensing agreements on a blockchain, content creators can receive fair compensation for their work. Blockchain also ensures that digital content like music, films, and articles is distributed according to pre-set terms, providing transparency and reducing piracy.