Boom in Blockchain Technology and its Applications

Mitali Agrawal

Muskan Gehlot

Mr. Nitesh Tejra

Computer Science Department

Medi-Caps University

Abstract

The ability of blockchain technology to solve long-standing problems related to economic growth is gaining traction. Proponents of blockchain claim that it would increase trade and partnership opportunities by reducing dependence on intermediaries and the frictions that come with them. The aim of this paper is to provide a clear picture of the technology's potential and details of the technology for those who are new to this domain.

Introduction

A blockchain is a distributed software network that serves as a digital ledger as well as a mechanism for transferring assets securely without the use of a third party. Blockchain is a technology that enables the digital exchange of units of value, similar to how the internet facilitates the digital flow of information. On a blockchain network, everything from currencies to land titles to votes can be tokenized, stored, and traded.

The Bitcoin blockchain, a free, censorshipresistant, peer-to-peer electronic cash system, was the first manifestation of blockchain technology in 2009. Aside from safe value transfer, blockchain technology also offers a permanent forensic record of

transactions and a single version of the reality – a network state that is completely transparent and shown in real time for the benefit of all participants.

The digital ledger is similar to a Google spreadsheet that is exchanged across several machines in a network and stores transactional records based on actual transactions. The intriguing aspect is that everyone can view the data, but they cannot alter it.

Working of blockchain technology

Blockchain is a combination of three leading technologies:

- Cryptographic keys
- A peer-to-peer network containing a shared ledger
- A means of computing, to store the transactions and records of the network

Two keys are used in cryptography: a

private key and a public key. These keys aid in the efficient completion of transactions between two parties. These two keys are unique to each individual and are used to create a protected digital identity reference.

The most critical feature of Blockchain technology is the protected identification. This identity is known as a "digital signature" in the cryptocurrency world, and it is used to authorise and monitor transactions.

The peer-to-peer network is combined with the digital signature; a large number of people acting as authorities use the digital signature to reach a consensus on transactions and other issues. When they approve a contract, it is checked mathematically, resulting in a successful protected transaction between the two networked parties. To summarise,
Blockchain users use cryptography keys to conduct various forms of digital transactions over a peer-to-peer network.

The way Blockchain technology confirms and authorises transactions is one of its most important features. For example, if two people want to make a transaction using their private and public keys, the first person will connect the transaction details to the second person's public key. This entire set of data is compiled into a block.

A digital signature, a timestamp, and other significant, valid details are all included in the block. It's worth noting that the block doesn't include the names of the people involved in the transaction. This block is then sent to all of the network's nodes, and the transaction is completed successfully when the correct person uses his private key to align it with the block.

The Blockchain can store transactional information of assets, cars, and other items in addition to financial transactions.

Here's a use case that illustrates how Blockchain works:

1. Hash encryption Blockchain technology encrypts data with hash encryption, relying primarily on the SHA256 algorithm to do so. The SHA256 algorithm is used to submit the sender's address (public key), the receiver's address, the transaction, and his/her private key information. The encrypted data, known as hash encryption, is sent around the world and checked before being added to the Blockchain. The SHA256 algorithm makes hash encryption almost impossible to crack, making sender and receiver authentication much easier.

2. Proof of work

In a Blockchain, each block consists of 4 main headers.

• Previous Hash: This hash address refers to the block before this one.

• Transaction Details: Information on all of the transactions that may take place.

• Nonce: An arbitrary number used in cryptography to distinguish the hash address of a block.

• Block Hash Address: A hashing algorithm is used to transmit all of the above (i.e., the preceding hash, transaction data, and nonce). This produces an output with a 256-bit, 64character-long value known as the unique 'hash address.' As a result, it's referred to as the block's hash.

3. Mining

Mining is the method of adding transactional data to the current digital/public ledger in Blockchain technology. Though it is most commonly associated with Bitcoin, the term is often applied to other Blockchain technologies. Mining entails creating a difficult-to-forge hash of a block transaction, ensuring the security of the entire Blockchain without the need for a central system authority.[1]

Components of blockchain

It is important to understand the logical elements of a blockchain ecosystem and what each component does in order to understand how blockchain technology differs from its application to cryptocurrencies. The following are the four (4) key components of every blockchain ecosystem:

1. a node application
2. a shared ledger
3. a consensus algorithm
4. a virtual machine

Node Application

Each device with an Internet connection must instal and run a computer application unique to the environment in which it wishes to participate. In the case of the Bitcoin ecosystem, each device must have the Bitcoin wallet application installed.

Participation in certain blockchain projects, such as Bankchain, is limited and involves special permissions. Only banks are allowed to run the node application on Bankchain. The Bitcoin ecosystem, on the other hand, allows everyone to download and instal the node application and thereby participate in it.

Regardless of one's qualifications, having a node application allows one to participate in the blockchain ecosystem.[6]

Shared Ledger

This is a necessary element. The distributed ledger is a data system within the node application that is maintained. You can access the ledger contents for that ecosystem once the node programme is up and running.

You are free to run as many node applications as you want, and they can all participate in their respective blockchain ecosystems. It's important to remember that regardless of how many ecosystems you participate in, each ecosystem will have only one shared ledger.

Consensus Algorithm

This is just a natural part of the ecosystem. The consensus algorithm is part of the node application and provides the "rules of the game" for how the ecosystem can arrive at a single ledger view. Depending on the optimal characteristics of the ecosystem, various ecosystems have different strategies for achieving consensus.

Virtual Machine

Any participant in the ecosystem runs the virtual machine, which is the final logical aspect implemented as part of the node application.

A virtual machine is a representation of a machine generated by a computer programme and controlled by language instructions. It's a software abstraction kept inside a machine.

Classification of blockchain

The permission model, which decides who can maintain a blockchain network, can be classified.

Blockchain technology is a framework that allows users in a peer-to-peer network to share data. Based on different principles, such as authentication and access control mechanisms, the blockchain may be classified as a private blockchain, public blockchain, or hybrid blockchain.

Private/permissioned

Permissioned blockchain networks are those in which users who publish blocks must first be approved by a third party. It is possible to limit read access and who can issue transactions since the blockchain is maintained by only approved users. Permissioned blockchain networks may either allow anyone to read the blockchain or only allow approved individuals to read it. Open source or closed source applications may be used to create and manage permissioned blockchain networks.

Organizations that need tighter control and protection of their blockchain can use permissioned blockchain networks. Permissioned blockchain networks can also be used by organisations who want

to collaborate but don't trust each other fully. Public/permissionless

There are no restrictions on participants joining the blockchain network in a permission-less or public blockchain, and they can participate in transaction validation as well as mining. Each peer in a public blockchain network has full permissions to participate in the transaction validation and block ledger maintenance processes. One of the most well-known examples of public blockchains is the Bitcoin cryptocurrency. It's intended for large networks with a large number of anonymous peers. Since all peers are involved in the project, the public blockchain has high computations to validate blocks in the network.

Hybrid

A consortium blockchain combines private and public blockchains; the blockchain's protocols are controlled by a group of entities or participants to ensure transaction validation. Instead of making anyone participating in the process or having only one person determine the validation process, the consortium blockchain enables a group of individuals or organisations to validate blocks. Consortium blockchain systems, such as Hyperledger Burrow, are an example.

Finally, the permission-less blockchain necessitates large computations in order to add new blocks to the network. As a result, it is unsuitable for IoT devices with limited resources. As a result of their low latency and high transaction volume, private and consortium blockchains are better suited for IoT.[2]

Main characteristics

Decentralization, traceability, and tamper proofing are all possible features of blockchain technology. These features will benefit a variety of IoT applications, including smart vehicles, smart cities, and healthcare systems, by allowing for safe data sharing without the involvement of third parties, as well as traceability and accountability.

Decentralization: Unlike centralization, which allows only the network administrator to conduct the authorization and validation procedures, blockchain's decentralised nature allows all users of the blockchain network to participate in the process of validating transactions.

Traceability: It is simple to audit since all participants in the blockchain have copies of the ledger's transactions. As a result, the blockchain network's actors will verify data exchange (transaction) for a specific blockchain address. A timestamp is allocated to each record stored in a blockchain, ensuring transaction traceability. The blockchain provides a kind of pseudo anonymity in addition to maintaining user privacy.

Tamper-proof: Via shared consensus mechanisms, all peers in the P2P network authorise and verify new joining blocks in the blockchain. As a result, the blockchain is immutable; for example, if an attacker were to alter any record in the blockchain, he or she would need to accommodate the majority of the network's users, and would otherwise be easily identified.

Transparency: All actors in public blockchain systems (such as Bitcoin and Ethereum) have the same access privileges, allowing them to take part in the process of validating and documenting new transactions in the blockchain. As a result, all players in the blockchain network will be able to see the data registered in the ledger.

Models

What Is A Blockchain Business Model? A business model is a term that refers to a company's plan or strategy for generating profit through the selling of a product or service. It details a company's strategies to create and sell a product or service. Each organisation will develop business models that are tailored to their specific needs. The blockchain business model is decentralised, enables peer-to-peer transactions, and aids in the creation of a trustworthy network. Tokens are used in blockchain-based business models to generate revenue.

Need for A Blockchain Business Model Businesses and end-users benefit from blockchain business models. Investors, not entrepreneurs, must be the target of a successful business model. As a result, business ventures would concentrate on utility rather

than valuation. Employees and end-users alike would profit from blockchain business ideas that work at both the macro and micro levels.

Traditional Business Model A conventional business model involves the provision of goods or services in exchange for a benefit. Consumers pay the prescribed price for the good or service. This rate is calculated using information about the salaries and other costs incurred by the company when delivering the product or service. They use a centralised model, which varies depending on the market.

Best blockchain Models

• Blockchain As A Service (BaaS)
It is the most widely used company strategy. It entails creating a platform for companies to control their blockchain systems. Companies would be able to experiment, analyse, and perform research in this ecosystem. Since it eliminates the need for hardware, BaaS helps businesses to concentrate on their development cycle. Bitcoin and Ethereum can be used as a service as well.

• Token Economy- Utility Token Business Model
The cumulative satisfaction derived from the consumption of products or services is referred to as utility. The utility token model is based on the use of tokens to drive business functionality. They make use of utility tokens to power the network and make network operations easier. Businesses keep a portion of the utility tokens and give the remainder to the network. When the value of utility tokens fluctuates, they benefit.

• Blockchain-Based Software Products
Businesses must buy a blockchain solution and incorporate it into their infrastructure in order to implement blockchain faster. This will aid in the creation of blockchain companies that develop solutions and then market them to larger corporations. Demonstrating blockchain technology to businesses can be highly lucrative because, in addition to receiving a fair payment up front, they would not be required to provide post-implementation support.

• P2P Blockchain Business Model This is a peer-to-peer business model. This allows end-users to communicate directly with one another. This business model can be monetized through a variety of methods, including BaaS, tokens, and transaction fees. These serve as a storage and sharing site for data.

• Blockchain Professional Services Leading expert software companies offer these services to entrepreneurs and other businesses to help them get started with blockchain. For example, if a company needs someone to create a custom business project for them, they can employ companies like IBM, Deloitte, or others to do so. Rather than investing in hardware, software, or team building, it entails directly engaging the services of blockchain development firms. This competition also includes smaller players.

Applications and uses

Cloud Storage: A decentralised framework for storing files in the cloud is provided by blockchain. In nature, it's similar to the Inter Planetary File System (IPFS), except that instead of a client-server web, it uses a distributed web system to share and store files. Instead of requesting a central server, each website will function as a node that has direct P2P file transfers with other nodes.

Cryptocurrency: The foundation of cryptocurrency systems like Bitcoin is blockchain technology. Cryptocurrency is a digital currency that is encrypted and can be used as a medium of trade in transactions by everyone. The blockchain network is used for such transactions. The records related to the generation and transaction of cryptocurrency between two nodes are permanently stored in the blocks of a blockchain. Cryptocurrency wallets are now accessible, allowing you to submit and receive cryptocurrencies as well as trade them for other currencies.

Healthcare: We can safely store information about patients and medications in a database using block-chaining. Doctors can access patient information and histories to help assess a situation at a specific point in time to ensure adequate care. Drug counterfeiting in the medical supply chain may also be monitored and dealt with by organisations. This is due to the fact that they can store supply chain data in the blockchain as permanent blocks.

Smart Contracts: When two parties sign an agreement or make a deal, it is best that the parties sign a paper-based contract (which specifies all of the deal's terms and conditions). However, there is a possibility of fraud and tampering with this way of doing business and signing contracts. The smart contract concept was created using blockchain as the foundation technology. Once developed, they are digital, self-executing contracts that are registered and stored in a blockchain. A smart contract is a computer programme that contains all of the terms and conditions of a contract between two parties and executes itself after all of the conditions have been met. This provides a 100 percent assurance and eliminates the possibility of fraud in the transaction.

Elections: Another fascinating fact about blockchain is that we can vote online using a blockchain system as the backbone, which ensures record protection and confidentiality. People can vote online instead of going to a polling station, and the votes would be securely recorded on a blockchain. Hacking into the system and tampering with the votes cast is virtually impossible. As a result, blockchain technology is ideal for online voting, as it will significantly increase the number of people who vote.

Digital Identity Management: The chances of fraud have increased dramatically as a result of the digital revolution. Cybercrime and digital fraud are becoming increasingly common. This is due to people's digital identities being easily hackable, which hackers can use to commit fraud and theft. Blockchain is the best option for ensuring the protection of people's digital identities. As a universal online directory, having ids, passwords, and authorized documents stored on blocks in a blockchain. There can be no fraud because the blockchain system requires every user's identity to be verified. If the credentials do not match the blockchain network's records, one cannot access the online ledger. A blockchain framework thus eliminates the possibility of hacking.

Supply Chain Audits: In supply chain audits, block-chaining often aids in ensuring the authenticity of a product. Manufacturers can store product information on a blockchain, and customers can check the records on the blockchain to verify the product's authenticity.
Internet of Things: The use of blockchain and smart contracts in the implementation and operation of IoT systems may be beneficial. A smart contract may store apps, sensors, and other important information that ensure the electronic device and network operate properly. [4]

Positive aspects of blockchain

Here are some major advantages of the blockchain technology that makes it so unique and popular.

•Immutable data: A data record or information that has been stored or inserted as a block in the blockchain cannot be changed. The data in the blockchain is immutable, which means that no one can alter it and it will remain in the blockchain indefinitely.

•Digital freedom and decentralization: The blockchain network as a whole is decentralised because it gives each user their own digital independence. There is no single authority in charge of the network's other users. In terms of operation, each node is self-contained.

•Anonymity and privacy: The blockchain network employ stringent security measures to ensure that transactions are carried out safely. Users that use blockchain to store cryptocurrencies such as Bitcoin can do so anonymously (without revealing their true identities), ensuring their privacy and security.

•Security: Cryptography is the blockchain's protection tool, which guarantees that hackers cannot alter or tamper with the data records stored in the blocks. Since all blocks in the blockchain are

connected by encrypted hash functions, it is impossible to commit fraud or carry out illegal transactions on the blockchain network.

•No intermediaries: Since the blockchain network is point-to-point, transactions take place directly between two nodes without the need for a middleman. An intermediary is not needed to facilitate transactions between two parties.

•Transparency: To all those that are a member of the network, the digital distributed ledger system offers a great deal of accountability. A network's nodes each have their own copy of the ledger and the ability to validate transactions. As a result, no one should conceal their personal information or purchases from other consumers, ensuring fair trade.

•Consensus-based: The blockchain principle is based entirely on consensus, which means that for any transaction that occurs between two nodes in a blockchain, a request for clarification is sent to all other nodes. A transaction is entered into the memory pool to create a new block after it has been checked by all nodes. Several of these checked transactions are stored in the memory pool.

Limitations of blockchain

- Power Use

  In comparison to other technologies, the Blockchain consumes a lot of energy. One of the reasons for this consumption is that every time a new node is created, it interacts with every other node at the same time.

- Cost

  According to reports, the average cost of a Bitcoin transaction is $75$160, with the majority of this cost being covered by energy use. There are very few chances that technological advancements will be able to solve this issue. The storage problem, on the other hand, could be covered by the energy problems, which cannot be resolved.

- Uncertain regulatory status

  The central government has developed and controls modern money in every part of the world. Bitcoin's acceptance by existing

financial institutions becomes a stumbling block.[5]

Comparison of various blockchain platforms

Ethereum

Ethereum is a decentralised, open-source blockchain that allows users to create smart contracts. The platform's native cryptocurrency is Ether. It is the second largest cryptocurrency by market capitalization, after Bitcoin. The Ethereum blockchain is the most widely used.[7] **Hyperledger Fabric**

Hyperledger Fabric is designed to serve as a foundation for building modular applications and solutions. Plug-and-play modules, such as consensus and membership services, are possible with Hyperledger Fabric. Its modular and adaptable architecture caters to a wide variety of industry applications. It takes a novel approach to consensus that allows for scalability while maintaining privacy.

Ripple Net

Ripple Net makes running a high-performance payments company simpler than it's ever been.

Financial institutions will grow into new markets around the world and even remove pre-funding by leveraging the power of XRP via Ripple Net's On-Demand Liquidity service, which uses the most advanced blockchain technology for global payments.

We're working with our customers to create a more equitable financial system that provides quality financial services to more people and SMEs.

Stellar

Stellar is a distributed ledger technology-based payment protocol. It enables cross border transactions between any two currencies in a matter of seconds. It resembles other blockchain-based cryptocurrencies in several respects.

Stellar blockchain, according to their website, is a "platform that links banks, payment systems, and people" with the aim of "moving money easily, efficiently, and at almost no cost." [7]

models are among the most serious issues in digital advertising. Since the technology would only enable the right businesses to thrive, blockchain can provide solutions to these issues. It would reduce the number of bad actors in the supply chain, lowering the risk of fraud and other problems.[3]

• **Blockchain in cybersecurity:** The Blockchain Technology's ground-breaking cryptography feature will aid in the encryption and verification of data. As a result, the data is less likely to be hacked or changed without permission.

The following is a comparison of some blockchain systems used by businesses to develop blockchain-based applications.

	Ethereum	Hyperledger Fabric	Ripple Net	Stellar
Industry Focus	Cross-industry	Cross-industry	Financial services	Financial Services
Ledger Type	Permissionless	Permissioned	Permissioned	Both public and private
Consensus Algorithm	Proof of Work	Pluggable Framework	Probabilistic Voting	Stellar Consensus Protocol
Smart Contract	Yes	Yes	No	Yes
Governance	Ethereum Developers	Linux Foundation	Ripple Labs	Stellar Development Foundation

Table 1

Scope of blockchain in future

- **Blockchain in digital advertising:** In today's world, challenges such as domain fraud, bot traffic, lack of accountability, and long payment

- **Blockchain in Forecasting:** The Blockchain technology is set to change the entire science, consultancy, review, and forecasting approach. Online platforms are used to build the majority of global distributed prediction markets.[3]

- **Blockchain in cloud storage:** Since data on a centralised server is vulnerable to hacking, data loss, and human error, Blockchain's distributed/decentralised protection feature can

make cloud storage more secure and resilient against hacking.

- • **Healthcare Sector:** In India, the healthcare sector is one of the most data-poor. Many hours are spent compiling patient information that should be spent on delivering medical care to those who are in desperate need.

References

1. www.shiksha.com/itsoftware/articl es
2. https://dataflair.training/blogs
3. https://blockchain.ieee.org/p u blications/ieee-talksblockchain/137-ieee-talksblockchain-overview-of-theblockchain-ecosystem
4. https://www.simplilearn.co m/ tutorials/blockchain-tutorial
5. https://www.geeksforgeeks. or blockchain technology introduction
6. https://medium.com/@neoca pita
7. https://www.leewayhertz.co m /blockchain-platforms-for top-blockchain-companies/