European Economic Letters
ISSN 2323-5233
Vol 13, Issue 1s (2023)
http://eelet.org.uk

The Process of Blockchain Technology

Akhil Avasarala[1], Vinita Golani[2], Sandeep Kelkar[3], Bijith Marakarkandy[4]
[1,2] Student at We School, Mumbai, [3,4] Faculty at We School, Mumbai

Abstract

Blockchain technology, an emergent digital technology that in recent years has gained popularity especially in finance and banking due to the rapid increase in the Cryptocurrency values. Blockchain's distributed and decentralised nature can help businesses increase efficiency, reduce costs, improve integrity and transparency, security, and traceability. Blockchain has been most widely used in finance and banking, but other industries are now experimenting with it. This paper discusses blockchain technology, its key design features, typical consensus, and its advantages. Lastly, a brief insight is presented into open challenges and potential future advancements in the field of Blockchain.

Keywords: Blockchain, Decentralization, Distributed ledger, Consensus algorithms, Cryptocurrency, Smart contracts.

Introduction

A public ledger called blockchain stores transactions as a list of blocks. This chain expands as additional blocks are consistently added to it. User security and ledger consistency are guaranteed via distributed consensus techniques and asymmetric cryptography. Blockchains offer decentralisation, persistence, auditability, and anonymity. The advantages of blockchain can increase productivity and decrease costs. Without a bank or other middleman, blockchain can be utilised for digital assets, remittances, and online payments. Blockchain was first proposed in 2008 and put into use in 2009. It can also be used by smart contracts, public services, IoT, and security services. Blockchain cannot be changed. Transactions are sealed by the blockchain. Blockchain draws clients to reliable companies. Blockchain prevents single points of failure because it is distributed. When it comes to smart contracts, the agreement could be automatically carried out by miners.

Although there are technological obstacles, blockchain technology has the potential to revolutionise Internet systems. Scalability is a major issue. Every ten minutes, 1 MB-sized bitcoin blocks are generated. As a result, the Bitcoin network's 7 transactions per second limit prevents it from supporting high-frequency trading. Larger blocks demand more storage and propagate through the network more slowly. Centralization will happen as a huge blockchain is maintained by fewer users. Therefore, it is challenging to strike a balance between block size and security. Second, egotistical mining techniques increase miners' profits. For financial gain, miners hide blocks. Therefore, recurring branches can hinder blockchain growth. Thus, solutions are needed for these problems. Blockchain transactions can have privacy leaks even when employing public and private keys. Privacy can potentially be compromised in blockchain transactions

using public and private keys. Consensus algorithms based on proof-of-work and proof-of-stake have flaws as well.

Literature Review

Blockchain-related research has become an interdisciplinary study that is not limited to the scopes of computing, engineering, or encryption. Our study focuses on to understand the architecture of blockchain and its process. Blockchain is a multi-disciplinary technology that researchers have investigated across a variety of different fields. Specifically, case study, review, and conceptual framework have been the most popular methodologies that scholars have used to conduct blockchain-related research

Currency dominates digitalization discussions. Bitcoin is e-currency. Blockchain moves bitcoins. Government, healthcare, and e-voting use it. Transaction security is crucial now. Security makes blockchain networks popular. Authors have covered blockchain characteristics beyond security. Blockchains, like all inventions, face many challenges. Blockchain implementation issues were discussed. Authors discusses blockchain technology, its applications, and challenges. (Shweta Singh, Anjali Sharma, Dr. Prateek Jain,2018)

One application that makes advantage of Blockchain technology is Bitcoin. Bitcoin is a form of organisational convention that underpins the global web architecture and is used each time we browse the internet, much like HTTP or TCP layers. A blockchain is a ledger of sophisticated transactions that is decentralised and not significantly influenced by any one person, group, or organisation. Since the blockchain technology is organised, it is challenging to change the rules or its core functionality without the consent of the users. Blockchain is a technology that securely maintains continually evolving systems of information exchanges and records. There is no centralised position in a blockchain architecture; instead, exchange records are stored and spread throughout the organisation. Although it wasn't given a name at the time, the usage of blockchain in the digital peer-to-peer money system known as Bitcoin was announced to the world in a whitepaper in 2008. Since blockchain technology is organised, it is incredibly difficult to change the guiding principles or content without the consent of the harmed parties. (Vinay Srivastava,2020)

Blockchain acts as an unchangeable ledger that enables decentralised transaction processing. Blockchain technology still faces many obstacles, including scalability and security issues, which must be resolved. Bitcoin has been one of the most successful digital currencies, with its capital market reaching $10 billion in 2016. The blockchain, which was first proposed in 2008 and implemented in 2009, is the core technology used to build the Bitcoin network and allows transactions to occur without the involvement of a third party. All committed transactions are recorded in a list of blocks in the blockchain, which could be thought of as a public ledger. For user security and ledger consistency, asymmetric cryptography and distributed consensus algorithms have been used. It can also be utilised in other industries, such as public smart contract services, IoT reputation management, and security services. These industries benefit blockchain in a number of ways. Although blockchain technology has a lot of potential for building the next generation of Internet systems, there are a number of technical obstacles to overcome. Furthermore, it has been demonstrated that privacy leakage can occur in blockchain even if users only use their public key and

private key for transactions. Additionally, there are some significant issues with current consensus algorithms like proof of worker and proof of stake. (Zheng, Xie, Dai, Chen & Wang, 2017)

As a developing technology, blockchains undoubtedly will continue to develop due to their ability to disrupt a variety of industries and domains. The technology is anticipated to demonstrate its viability through additional proof-of-concept applications. (Niranjanamurthy, Nithya & Jagannatha, 2019)

Blockchain is a chain of linked blocks that functions as a digital ledger. In support of Bitcoin. Additionally, it includes digital wallets. Blockchains are used to record these transactions by other applications and cryptocurrencies like Bitcoin. Blockchains are decentralised databases that share all public records, transactions, and digital events with users. Validated transactions are irreversible. This technology is scalable, fault-tolerant, efficient, and reliable. The three characteristics are combined in manufacturing, government, and finance (i.e., Efficiency, Scalability and Security). Blockchain transactions are validated by multiple computers. These systems for validating blockchain transactions establish a peer-to-peer network. Before adding transactions to the blockchain, they are verified, and they stop invalid blocks from being added. In order to make the chain unbreakable and each block irreversible, a cryptographic hash can link a new block to a previous block. Blockchain enables secure transaction exchange without middlemen. IoT, Cloud, and customer relationships are all integrated. Issues in the financial and non-financial industries are resolved by distributed ledger and blockchain security. In this study, authors integrated hardware and blockchain technology to build a safe data platform. (VivekanadamB,2020)

Business models are being disrupted by digital technology, which is also influencing the world. Blockchain technology is attracting the attention of Indian industries. As applications for blockchain technology expand, industry leaders are customising it for various use cases. Blockchain technology facilitates the development of decentralised applications. This essay explains the structure and workings of the blockchain technology. The advantages and features of Blockchain are covered. Use cases and a blockchain fit assessment have not been widely used in banking transactions and about Blockchain security. (Tejal Shah, Shailak Jani, 2018)

The authors have outlined the key characteristics of blockchain technology, including how the following nine aspects primarily reflect its core technical characteristics: Decentralization, disintermediation, immutability, anonymity, smart contracts, traceability and provenance, cost reduction, transparency, and security and privacy are some of the other terms used. The three categories that make up blockchain essentially include all of the related platforms, such as consortium, private, and public blockchain systems. blockchain. Technically speaking, game theory and a reward mechanism can be used to solve some of the transaction and mining problems that blockchain still has. Distributed ledger is a common term used to describe blockchain. Its core still consists of a unique database that is organised by blocks. Blockchain technology can be used in a wide range of situations that call for thorough and reliable data processing in addition to financial application scenarios. The performance of business activities, such as data privacy and security, decentralised framework and infrastructure design, and Industrial 4.0, will be facilitated by the intellectual integration of blockchain and IoT. The main factors influencing business adoption of blockchain, from a technical perspective, are its decentralisation, smart contracts, and confidentiality. In order to increase their ability to implement blockchain, businesses should increase their resource input and

develop their technical and managerial capabilities. Blockchain's advantages in terms of capability, interoperability, scalability, and agility offer a potential framework for IS discipline research. (Zheng, Lu, 2022)

Scalability, interoperability, privacy and security, self-serving mining, quantum resilience, and a lack of governance and standardisation are just a few of the issues that the paper has illustrated as current research and business challenges to adopting the Blockchain for various applications. Despite the widespread use of Blockchain applications, numerous problems remain. By doing this, Blockchains' scalability, effectiveness, and durability will all improve. They share many characteristics with other people, and the majority of their fundamental workings have been understood for a long time. However, combining these features makes them incredibly suitable for various applications, demonstrating the keen interest from numerous industries. Blockchains are better suited to be used in more domains as their level of maturity rises. Blockchains are frequently cited as a database replacement (and even a cure-all), but this is far from the truth. As was already mentioned, many situations could be replaced by traditional databases. (Gad, Mosa, Abualigah & Abohany, 2022)

Ambitious start-ups are already working to create industry applications and refined blockchain technologies that actually add value to businesses in novel ways. The time has come to talk about how the technology can help organisations now that the bitcoin and block-chain craze is over. Blockchain's future looks promising as it moves closer to the plateau of productivity and the slope of enlightenment. Unknown combinations of technologies will open the door for intriguing new business applications as new blockchain technologies and applications continue to appear. Blockchain, a highly secure, decentralised technology, and artificial intelligence, a highly centralised technology, are already being paired for greater distribution of the data and algorithms that will shape the future development of artificial intelligence, according to entrepreneurs, venture capitalists, and academics. Since its enormous computing power could be used to defeat the cryptography on which traditional blockchains rely, quantum computing is viewed as a potential blockchain killer. However, a fully quantum blockchain (also known as a "quantum blockchain") is thought to be a potential defence against malicious attacks. (Kietzmann & Archer-Brown, 2019)

The blockchain technology is dependable and unbreakable due to its benefits, including transparency, trust, multiple copies of the transactions, and a decentralised digital ledger. Because it can simplify the majority of systems across numerous industries, blockchain technology is useful and adaptable for our world. However, because it is still in its infancy, there is little research on how to actually implement it. Due to the advantages of the Blockchain technology, a bright future free from fraud and deception is promised to us. Because the Blockchain can bring honest and reliable business, governmental, and logistical systems, the developers must invest more time in the practical application and integration of the Blockchain into the already existing systems of the major industrial directions. (Golosova & Romanovs, 2018)

Different threats that interact with the PoW and PoS protocols can attack the blockchain. Nearly none of them are attainable. The author mentions the following attacks: Attack of 51% - This occurs when two miners calculate the block's hash at the same time and produce identical results. In this scenario, the blockchain will split, giving users access to two chains that are both accepted as true. DDoS assault. Numerous requests that are similar to one another make up the attack. Protection against DDoS attacks

includes block sizes up to 1 MB, script sizes up to 10000 bytes, signature checks up to 20000, and a maximum of 20 keys for multiple signatures. (Golosova & Romanovs, 2018)

The blockchain architecture, benefits, and uses in industry were discussed by the author. The best place to start using blockchain is in a single-use, independent application where there is no need for third parties or other applications to coordinate. Considering that bitcoin already has a strong and tested architecture, introducing bitcoin as a payment system would be a simple way to implement blockchain. Blockchain implementation as a database technology for managing and maintaining digital transaction records would be another secure and efficient strategy. A new, better solution must always be implemented, which requires careful planning and execution. This is never an easy task. A good strategy would be to offer affordable, effective, and adaptable solutions without having any negative effects on the end users. The transformative applications can help public identity systems or algorithm-driven decision-making systems, and new ecosystems will be efficiently governed with their assistance. (Sarmah, 2018)

This paper examines the potential integration with building information modelling (BIM) workflow and provides a thorough overview of BCT and its applications in various fields. The main ideas behind Blockchain Technology (BCT) are the development of a digital distributed consensus, ensuring that data is decentralised among numerous nodes in the network that hold the same information, and making sure that no single node holds total control over the network. The use of such decentralised technology in any sector would necessitate increased security, enforce accountability, and could possibly speed up the transition from the current hierarchical structure to a decentralised, cooperative chain of command. It would also likely have a positive impact on culture and society by promoting trust and transparency. Distributed ledgers' stability and security are enhanced by the interconnectivity in blockchain applications that is enforced cryptographically. (Nawari & Ravindran, 2019)

Blockchain uses a decentralised consensus protocol for transaction processing and validation. It was created to do away with intermediaries, especially in the world of financial transactions. The most widely used consensus mechanisms by the current blockchain systems are PoW, PoS, PBFT, and DPoS. The selection of blockchain systems is influenced by important elements like investment capacity, privacy requirements, and objectives. For instance, financial institutions are more interested in private blockchains because they value the privacy component. Companies that share similar objectives and activities, however, are more willing to split costs and data and may choose consortium blockchains. Blockchain technology can be used in a variety of industries, including advertising and media, energy, real estate, healthcare, and many more. For blockchain to be effective and durable, it is critical to address its current limitations. (Baiod, Light & Mahanti, 2021)

Blockchain Architecture

Similar to a traditional public ledger, the blockchain is made up of a number of blocks that each contain a comprehensive list of transaction records. In Figure 1, a blockchain is used as an illustration. The parent block, which is essentially a hash value of the block that came before it and points to it, is a reference that each block contains. The genesis block of a blockchain is the very first block and has no parent block.

European Economic Letters
ISSN 2323-5233
Vol 13, Issue 1s (2023)
http://eelet.org.uk

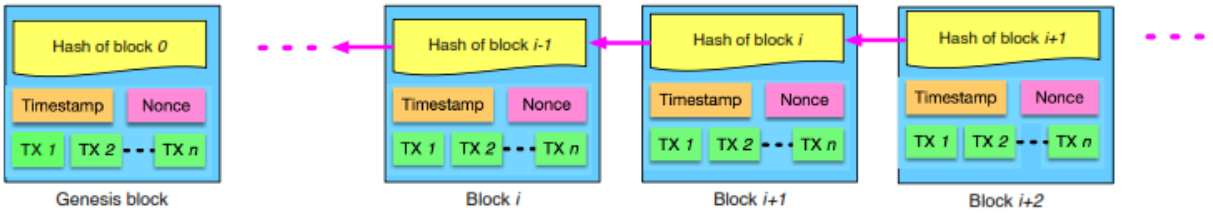

Figure 1: An example of blockchain which consists of a continuous sequence of blocks

Block:
According to Figure 2, a block is made up of the block header and the block body. The block header in particular includes:

- The block header in particular includes:
- Block version: indicates which set of block validation rules to follow.
- Parent block hash: a 256-bit hash value that points to the previous block.
- Merkle tree root hash: the sum of all the block's transactions.
- Timestamp: The present time expressed in seconds since January 1st, 1970 (UTC).
- nBits: A compact representation of the current hashing target.
- Nonce: a 4-byte field that typically begins with 0 and grows with each hash calculation.

A transaction counter and transactions make up the block body. Depending on the block size and the size of each transaction, a block can contain a maximum number of transactions.

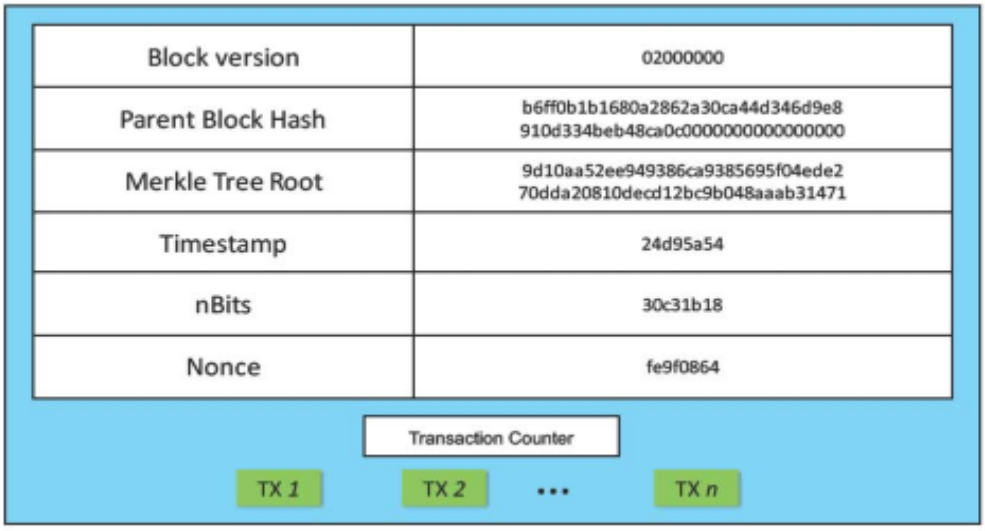

Figure 2: Block structure

A transaction counter and transactions make up the block body. Depending on the block size and the size of each transaction, a block can contain a maximum number of transactions. Blockchain verifies the

authenticity of transactions using an asymmetric cryptography mechanism. In an unreliable setting, an asymmetric cryptographic digital signature is used. Next, we give a quick example of a digital signature.

Digital signature:

Each user is in possession of a set of private and public keys. The transactions are signed using the private key. Public keys that are accessible to everyone in the network are used to access the distributed, digitally signed transactions. An illustration of a digital signature used in blockchain is shown in Figure 3. The signing phase and the verification phase are the two stages of a typical digital signature. Alice first creates a hash value derived from the transaction when she wants to sign it. She then uses her private key to encrypt this hash value before sending Bob, another user, the encrypted hash along with the original data. By comparing the decrypted hash value with the hash value obtained from the received data using the same hash function as Alice's, Bob can confirm the received transaction. The elliptic curve digital signature algorithm is one of the common digital signature algorithms used in blockchains.

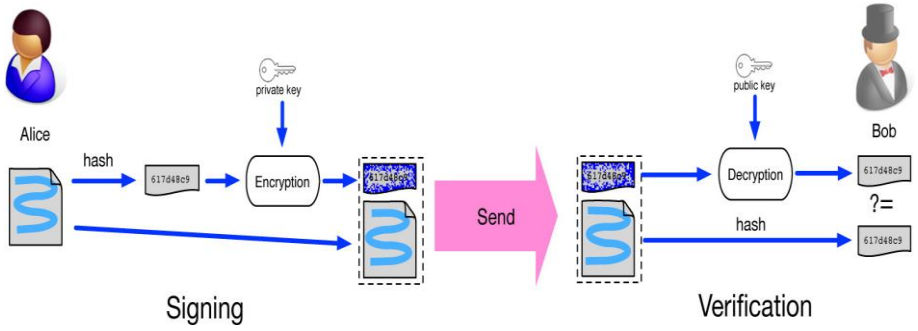

Figure 3: Digital signature used in blockchain

Key characteristics of blockchain:

In summary, blockchain has following key characteristics.

Decentralization: Traditional centralised transaction systems experience cost and performance bottlenecks at the central servers because each transaction must be verified by the central trusted agency (such as the central bank). However, a transaction in the blockchain network can be made between any two peers (P2P) without requiring authentication from a centralised body. Blockchain technology has the potential to significantly reduce server costs and performance bottlenecks at the central server (including development and operation costs).

Persistency: Because every transaction on the network must be verified and recorded in blocks that are scattered across the entire network, it is virtually impossible to tamper with them. Other nodes would also verify and validate each broadcasted block's transactions. Any falsification could therefore be quickly identified.

Anonymity: With a generated address, each user can communicate with the blockchain network. A user could also create numerous addresses to protect their identity. There is no longer a single entity in charge

of protecting user privacy. With the help of this mechanism, the transactions recorded in the blockchain are kept somewhat private. Be aware that due to an inherent constraint, blockchain cannot guarantee perfect privacy preservation.

Auditability: Users can easily verify and trace the history of records by gaining access to any distributed network node because every transaction on the blockchain is verified and recorded with a timestamp. Each transaction on the Bitcoin blockchain could be iteratively linked to transactions that came before it. It enhances the data stored in the blockchain's transparency and traceability.

Taxonomy of blockchain systems:

Current blockchain systems can be roughly categorized into three types: public blockchain, private blockchain and consortium blockchain.

- Consensus determination: Every node on a public blockchain could participate in the consensus procedure. And in consortium blockchain, only a chosen group of nodes are in charge of validating the block. Regarding private chain, it is entirely under the control of one organisation, which could choose the final consensus.
- Read Permission: While read permission is dependent on a private blockchain or consortium blockchain, transactions in a public blockchain are visible to everyone. Whether the stored information is public or restricted could be decided by the consortium or the organisation.
- Immutability: Since each node in the distributed network stores a different transaction, it is virtually impossible to alter the public blockchain. The consortium blockchain or private blockchain, however, could be reversed or tampered with if the majority of the consortium or the dominant organisation wants to.
- Efficiency: As there are many nodes in the public blockchain network, it takes a long time for blocks and transactions to spread. If network security were taken into account, public blockchain restrictions would be much more stringent. As a result, there is low transaction throughput and high latency. Private blockchain and consortium blockchain may be more effective with fewer validators.
- Centralised: Public blockchains are decentralised, consortium blockchains are partially centralised, and private blockchains are fully centralised as they are controlled by a single group. This is the main distinction between the three types of blockchains.
- Consensus process: The public blockchain's consensus process is open to participation from anyone in the world. Both consortium blockchain and private blockchain are permissioned, unlike public blockchain. To participate in the consensus process in a consortium or private blockchain, one node must be certified.

Table 1: Difference Between Public , Private, and Consortium Blockchain

Property	*Public blockchain*	*Consortium blockchain*	*Private blockchain*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

Public blockchain can draw a lot of users because it is accessible to everyone. Furthermore, communities are very active. Every day, new public blockchains are created. The consortium blockchain has a wide range of potential business applications.

Consensus Algorithms

It can be difficult to come to a consensus in a distributed environment. The distributed nature of the blockchain network presents another difficulty. Blockchain does not have a central node to guarantee that distributed nodes' ledgers are identical to one another. To guarantee that ledgers across various nodes are consistent, some protocols are required. Next, we outline a number of popular strategies for achieving consensus in the blockchain.

Approaches to consensus:

PoW (Proof of work) is a consensus strategy used in the Bitcoin network.
In order to authenticate POW, a challenging computational process is needed. In POW, each node in the network computes a hash value of the block header, which is constantly changing. According to the consensus, the calculated value must be less than or equal to a specific given value. To reach the target in the decentralised network, all participants must continuously calculate the hash value using various nonces. All other nodes must mutually verify the accuracy of the value after one node obtains the pertinent value. Then, in the event of fraud, the transactions in the new block would be verified. Then, a new block is added to the blockchain to represent the authenticated result, which was determined from the collection of transactions used for the calculations. The POW procedure is known as mining, and the nodes that calculate the hashes are known as miners. An incentive mechanism (such as giving the miner a small portion of Bitcoins) is also suggested because calculating the authentication is a time-consuming process.

When several nodes locate the appropriate nonce almost simultaneously in a decentralised network, valid blocks may be generated simultaneously. As a result, branches like those in Figure 4, may develop. It is unlikely that the following block will be generated simultaneously by two conflicting forks. A chain is deemed to be authentic in POW protocol if it keeps getting longer. Consider Figure 4 once more. Think about two forks produced by blocks B11 and G11 being validated simultaneously. The newly created block

is added to one of the forks as the miners work on both of them. The miners working on fork G11-G12 will switch to block B12 when a new block (let's say B12) is added to block B11. Since it is no longer increased, Block G12 in the fork G11-G12 becomes an orphan block. In most cases, it becomes nearly impossible to reverse the blockchain and alter the transactions once a certain number of new blocks have been added to it. When approximately six blocks are generated on the Bitcoin blockchain, the relevant blockchain is regarded as the genuine one (e.g., the chain of blocks B11, B12, B13, B14, B15 and B16 in Figure 4). Block interval is influenced by various parameter settings. Ethereum blocks are created every 17 seconds, whereas Bitcoin blocks are created every 10 minutes on average.

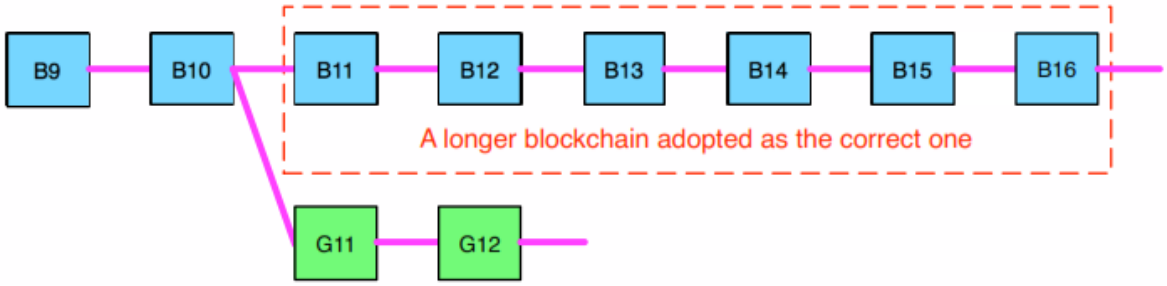

Figure 4: A blockchain branching scenario (the longer branch would be admitted as the main chain while the shorter one would be deserted)

Proof of stake (PoS) is an energy-saving alternative to POW. Users of POS are required to show ownership of the amount of currency instead of being required to find a nonce in an infinite space because it is thought that users who have more currencies would be less likely to attack the network. The selection process based on account balance is quite unfair because the network will always be dominated by the richest individual. The stake size is therefore combined with a number of solutions to determine which one will be used to forge the next block. Blackcoin in particular, uses randomization to foretell the next generator. It employs a formula that searches for the lowest hash value in conjunction with the stake amount.

Practical byzantine fault tolerance (PBFT), A primary would be chosen in every round in accordance with certain regulations. Additionally, it is in charge of directing the transaction. Three phases could be used to describe the entire process: pre-plan, prepare, and commit. A node would move on to the next phase in each phase if it received votes from more than 2/3 of all nodes. Therefore, for PBFT to work, every node must be known to the network. In PBFT, there is no hashing process. While SCP allows participants to select which group of other participants to believe, PBFT requires each node to query other nodes.

Delegated proof of stake (DPOS) Similar to POS, miners are given preference to create blocks based on their stake. POS and DPOS are fundamentally different from one another because POS is a direct democracy and DPOS is a representative democracy. A block is created and validated by delegates chosen by stakeholders. Block validation would require a lot fewer nodes, which would speed up block confirmation and transaction confirmation. In the interim, network parameters like block size and block intervals could be adjusted. Additionally, since the delegates could be easily removed by a vote, users do not need to worry about the dishonest delegates.

Ripple is a consensus algorithm that makes use of subnetworks that are collectively trusted within a larger network. Nodes in the network are split into two groups: servers that take part in the consensus process and clients that only transfer money. While each Ripple server has a Unique Node List (UNL) to query, PBFT nodes must query each node in the network. The server values UNL highly. The server would consult the UNL nodes to decide whether to add a transaction to the ledger. The transaction would be recorded in the ledger if the percentage of received agreements reached 80%. If there are fewer than 20% of faulty nodes in UNL, the ledger for that node will continue to be accurate.

C. Advances on consensus algorithms

Effective consensus algorithms promote convenience, safety, and efficiency. Numerous efforts have recently been made to enhance blockchain's consensus algorithms. New consensus algorithms are being developed with the goal of resolving some specific blockchain issues. Peer Census' main goal is to separate block creation from transaction confirmation in order to significantly speed up consensus. Additionally, Kraft suggested a new consensus technique to guarantee that a block is generated at a reasonably constant rate. High block generation rates are known to jeopardise Bitcoin's security. To address this issue, the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule is suggested. GHOST weights the branches so that miners can select the best one to follow rather than the longest branch scheme. There is a new consensus algorithm for peer-to-peer blockchain systems in which whoever offers noninteractive retrievability proofs for previous state snapshots is accepted to generate the block. Instead of storing entire blocks, miners only need to keep old block headers in such a protocol.

Applications of blockchain

There are diverse of applications of blockchain technology. In this section, we summarise several typical applications of blockchain.

Payments:

Blockchain initially existed as a peer-to-peer electronic cash system when Nakamoto unveiled the bitcoin. As a successful method of sending money across borders and receiving remittances at a lower transaction cost than the traditional financial system and with a significantly faster settlement speed, the bitcoin payment system has grown in popularity. Currently, hundreds of trillions of dollars are transferred globally through an antiquated financial system with high costs and slow payments. Public blockchain-based cryptocurrency systems, like Bitcoin and Ethereum, remove the need for trusted intermediaries to verify and settle transactions by enabling anyone in the world to send, receive, and transfer money.

Financial Clearance and Settlements:

Without a clearinghouse, businesses and institutions can use blockchain to record, validate, and process financial settlements. Blockchain can speed up clearing processes that involve modifying debts to approve payments. Compared to existing systems like SWIFT, blockchain can enable direct settlement of transactions and maintain track of those transactions more efficiently.

Finance for Trade:

There are many problems with traditional trade finance, including loaded paper, more mistakes, and a slow method of processing transactions between counterparties. The world of trade finance can benefit greatly

from blockchain, which can eliminate paperwork, automate transactions and payments, lower fraud, reduce costs, track and trace shipments, and give everyone involved access to the same data.

Accounting Application:
For the accounting industry, blockchain technology has great potential. Self-auditing and immutable records can result in significant reductions in the difficulty and complexity of audits, as well as a significant change in how much time and effort are needed to verify a company's financial statements. Blockchain offers an innovative new way to track, process, verify, and store financial transactions and information that has the potential to fundamentally alter the accounting industry and the business ecosystem.

Insurance:
BCT can be used by insurance companies to automate insurance claims, eligibility checks, and privilege execution. By significantly reducing the workload of insurance agents who are tasked with manually reviewing and cross-referencing insurance claims with factual data, this would be advantageous in terms of cost savings. Clients would also gain because efficient payouts would be guaranteed through quick transactions.

Business:
Instead of the time-consuming sequential verification process, implementing BCT can speed up business transactions by obtaining multiple approvals at once with the least amount of supervision needed. Blockchain technology is anticipated to improve accountability and transparency in supply chain networks. BCT can be used effectively in logistics, identifying fake goods, reducing paper load processing, facilitating origin tracking, enabling direct transactions between buyers and sellers without the use of middlemen, and enhancing intra-organizational procedures.

Government Sectors:
BCT has many potentials uses in the public sector, including facilitating transparency with non-profit organizations and managing medical records, voting and identification, land registration and property monitoring, transportation, disaster management, and real estate monitoring.

Academia:
By addressing the issues of vulnerability, security, and privacy in any learning environment, BCT application can provide a secure system for storing educational data records about students and teachers.

Healthcare:
With numerous applications in fields like public healthcare management, longitudinal healthcare records, automated health claims settlement, online patient access, sharing patients' medical data, user-oriented medical research, drug counterfeiting, clinical trial, and precision medicine, BCT has tremendous potential to advance the healthcare industry.

Applications in Real Estate:
Due to the large number of parties involved, including brokers, government property databases, title companies, escrow companies, inspectors, appraisers, and notaries public, real estate transactions are

complicated, opaque, and expensive. Blockchain in real estate creates reliable and effective workflows, improving visibility and transparency at every stage and ultimately making investments safer for everyone.

Challenges

Despite the enormous potential of blockchain, it faces many obstacles that prevent it from being widely used. Here are some significant obstacles and recent developments that we list.

A. Scalability

The blockchain grows in size as more transactions are made every day. Each node must keep a record of every transaction in order to validate it on the blockchain and determine whether the source of the current transaction has been spent or not. Additionally, the Bitcoin blockchain can only process about 7 transactions per second due to the original restriction on block size and the time interval used to generate a new block, which does not meet the requirement of processing millions of transactions per second. Since the capacity of blocks is so low, many small transactions could experience delays because miners favor those with high transaction fees.

B. Privacy Breach

The public key and private key of a blockchain can aid in some privacy protection. Without disclosing their real identities, users carry out transactions using their private and public keys. However, because all transaction values and balances for each public key are made public, blockchain cannot guarantee transactional privacy. In order to strengthen blockchain anonymity, a variety of strategies have been proposed. These strategies can be loosely classified into two categories:

For users, Blockchain employs pseudonymous addresses. It is still possible to connect addresses to user real identities because numerous users routinely deal with the same address. Money is moved via a service known as mixing from numerous input addresses to various output addresses in order to maintain anonymity. As an illustration, user Alice wants to send money to Bob at address B. Alice and Bob's relationship might be made clear if she makes a direct transaction using input address A and output address B. Therefore, Alice could transfer money to Carol, a dependable middleman. With multiple inputs (c1, c2, c3, etc.) and multiple outputs (d1, d2, B, d3, etc.), Carol then transfers money to Bob. The output addresses also include Bob's address B. Therefore, it becomes more difficult to establish Alice and Bob's relationship. The middleman, however, might be dishonest and deliberately divulge Alice and Bob's personal data. Additionally, Carol might transfer Alice's funds to her own address rather than Bob's.

C. Anonymous:

The zero-knowledge proof is employed in the Zerocoin protocol. While validating those coins are on a list of acceptable coins, miners are not required to validate a transaction with a digital signature. To prevent

transaction graph analyses, the origin of payments is separated from transactions. But it still makes the destination and value of payments clear.

D. Selfish Mining:
Blockchain is vulnerable to attacks from selfish, complicit miners. There is a demonstration on how the network is weak even if only a small portion of the hashing power is used for fraud. Selfish miners keep their mined blocks without broadcasting them, and the public is only made aware of the private branch if certain conditions are met. All miners would accept the private branch because it is longer than the current public chain. Prior to the private blockchain publication, ethical miners waste their time and energy on a pointless branch, while self-interested miners mine their own private chain without interference. Thus, egotistical miners typically earn more money.

Future directions

Blockchain evaluation:
Testing and standardisation phases for blockchains could be separated into two stages. All criteria must be created and approved during the standardisation phase. When a blockchain is created, it can be tested against the predetermined standards to determine whether it really functions as well as its creators claim. Regarding the testing phase, various criteria need to be used when conducting blockchain testing. For instance, a user in charge of an online retail business is concerned with the blockchain, so it is necessary to test the capacity for a blockchain block, the average time it takes from the time a user sends a transaction until it is packed into the blockchain, and other factors.

Halt the centralization tendency:
Blockchain is intended to be an independent system. There is a tendency for miners to become concentrated in the mining pool. The top 5 mining pools collectively own more than 51% of the Bitcoin network's overall hash rate. Since the blockchain is not meant to be a centralized. To address this issue, research can be conducted in this area.

Analytics for big data:
Blockchain technology and big data may complement one other. Data management and data analytics are the broad areas into which the combination has been separated in this case. In terms of data management, as blockchain is secure and decentralised, it might be utilised to store important data. Blockchain might also ensure the data's originality. For instance, if patient health data is stored on a blockchain, it cannot be changed and is challenging to steal. When it comes to data analysis, big data analytics may be applied to blockchain transactions.

Future applications of blockchain:
Although the financial industry is now where blockchains are most frequently employed, new applications are constantly being developed for other industries. To enhance their systems, traditional industries might think about integrating blockchain technology. Reputations of users may be stored on a blockchain. Blockchain could increase efficiency in the developing industry at the same time.

Due to market, cultural, and geographic restrictions, businesses access and adapt information resources extremely differently, which leads to unequal opportunities and unfair competition. An organization's ability to access information resources and solve IT-related problems will be greatly improved by blockchain's dispersed network and rapid interoperability. Future research can be done based on the theory of technical innovation, resource endowment, and informatization to examine blockchain-related information concerns and service modes of blockchain economy.

Hype Cycle of Blockchain:

Below is the Gartner's hype cycle of block chain technology 2022. Consumer apps like NFT games and commerce are driving innovation as enterprises gradually begin to realize business value. Enterprise applications like aircraft maintenance, food safety use tokenized real-world assets and smart contracts to manage them.

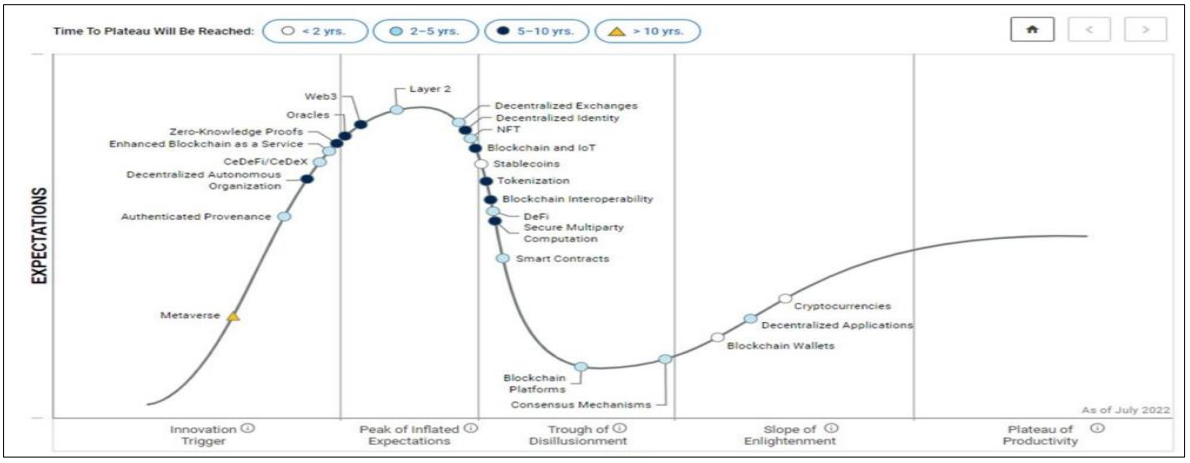

Figure 5: Hype Cycle of Blockchain

Key adoption drivers - outlined include:

- The expected adoption of central bank digital currencies (CBDCs) is a major factor in the adoption of distributed ledger technologies (DLTs) for the movement of money in payment networks, banking, and social networks.
- Applications for decentralised finance (DeFi) offer significantly higher financial rewards than conventional finance. Hedge funds and other centralised businesses already benefit from this.
- Asset tokenization, including the phenomenal growth of NFTs and DeFi tokens, as well as the prospect of future tokens connected to real assets.
- Alternatives to Ethereum chain transactions are available on blockchains like Binance, Cardano, and Solana.
- Blockchain interoperability has made enormous strides, with DeFi applications already utilising gateways and abstraction middleware.

- Blockchain's transition to more energy-efficient consensus techniques like proof of stake from the proof-of-work (POW) consensus method, which is still used for Bitcoin (PoS). This pattern is being driven by Ethereum's ongoing upgrades.

Conclusion

Because of its decentralised infrastructure and peer-to-peer nature, blockchain is a technology that has a bright future. Through its design features, the blockchain has shown its potential to simplify complicated procedures like transaction verification, reconciliation and settlement, and dispute resolution. We have provided an overview of blockchain process in this paper. We begin by providing a summary of the blockchain's architecture and important features. The common consensus algorithms used are covered. Additionally, blockchain can revolutionise traditional business due to its essential features like distribution, anonymity, immutability, and audibility. Since the role of intermediaries was intended to be eliminated, particularly in the context of financial transactions, blockchain. Blockchain, has numerous uses that go far beyond Bitcoin. We are all aware of how powerful blockchain technology can be in solving issues. But we are also beginning to notice some of the problems that blockchain is facing, particularly in terms of scalability, security, and regulation. For blockchain to be effective and durable, it is critical to address its current limitations.

Acknowledgement

The work described in this paper was supported by our institute Welingkar Institute of Management Development and Research, Mumbai for giving us this opportunity. We would also like to express our special thanks of gratitude to our mentor Prof. Sandeep Kelkar for providing his valuable guidance.

References

[1] Singh, S., Sharma, A., & Jain, P. (2018). A Detailed Study of Blockchain: Changing the World. International Journal of Applied Engineering Research, 13(14), 11532-11539.
[2] Srivastava, V. A Survey on Blockchain Technology & Future Scope.
[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.
[4] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22(6), 14743-14757.
[5] Vivekanadam, B. (2020). Analysis of recent trend and applications in block chain technology. Journal of ISMAC, 2(04), 200-206.
[6] Shah, T., & Jani, S. (2018). Applications of blockchain technology in banking & finance. Parul CUniversity, Vadodara, India.
[7] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.
[8] Zheng, X. R., & Lu, Y. (2022). Blockchain technology–recent research and future trend. Enterprise Information Systems, 16(12), 1939895.

[9] Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging trends in blockchain technology and applications: A review and outlook. Journal of King Saud University-Computer and Information Sciences.

[10] Kietzmann, J., & Archer-Brown, C. (2019). From hype to reality: Blockchain grows up. Business Horizons.

[11] Golosova, J., & Romanovs, A. (2018, October). Overview of the blockchain technology cases. In 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) (pp. 1-6). IEEE.

[12] Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE) (pp. 1-6). IEEE.

[13] Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2), 23-29.

[14] Nawari, N. O., & Ravindran, S. (2019). Blockchain technology and BIM process: review and potential applications. J. Inf. Technol. Constr., 24(12), 209-238.

[15] Baiod, W., Light, J., & Mahanti, A. (2021). Blockchain technology and its applications across multiple domains: a survey. Journal of International Technology and Information Management, 29(4), 78-119.