University of Ibadan
Journal of Science and Logics in ICT Research

Comparative Analysis of Eight Different Blockchain Technology Schemes and Their Implementations

[1]✉Ugwu, J. N., [2]Hassan, J. B, [3]Akinsanya, S. E., [4]Ayogu, B. A., [5]Adubi S. S. and [6]Olagunju, M.

Department of Computer Science, Federal University, Oye-Ekiti , Nigeria
joel.ugwu@fuoye.edu.ng

Abstract

Blockchain is a digital ledger that allows a transparent links of increasing record which are connected together with the means of cryptographic algorithms. Blockchain technology has attracted more speculations in various sectors recently, due to its ability of decentralised, robust and secure data exchange amongst various application platforms. There are important key variations between each blockchain technology scheme in regards to their architecture, scalability, interoperability, security features, consensus mechanism, and application. This difference in the block chain technology scheme has brought about the need to comparatively analyse different block chain technology schemes in order to better comprehend their strengths and weaknesses, advantages and disadvantages, scope and limitations so as to be able to access and measure suitability for efficient implementation in different case scenarios. In this study, 16 different qualities are compared amongst eight of the most popular blockchain technology. It concludes with a synopsis of these technologies and suggestions for the most widely used ones.
.

Keywords: *Blockchain, distributed ledger, cryptography, decentralized transaction, consensus mechanism, hash functions, tokens*

1.0 Introduction

Blockchain refers to a digital ledger which essentially involves continuous links of increasing records referred to as blocks which are connected together with the aid of cryptography [1]. Blockchain technology has evolved as a suitable solution for decentralized, secure, robust and transparent exchange of data between different application platforms and domains. Every blockchain scheme comprises various development structures, which include key elements like interoperability, consensus mechanism, security, scalability and system architecture. The rapidly developing technology known as blockchain is not as complicated as it might first seem. It acts as the foundation of digital currencies, operating as a distributed, transparent, and decentralized ledger system. To better understand these ideas, let's imagine a situation in which a transaction fails for any reason, such insufficient funds or a problem with a third-party payment gateway. At these situations, the payment and data kept at a central location that is prone to hackers and laborious procedures. Blockchain was developed as a solution to these issues. It introduced the practice of adding blocks following each transaction, which are shared by all network users and create a distributed, decentralized network [2].

As seen in Figure 1. Blocks that are connected to each other provide the basic structure of a blockchain. A blockchain is essentially a series of sequentially linked blocks, each holding transaction details. There is no parent block for the first block, referred to as the genesis block. A block is made up of several parts, most notably the hash that is created at the time of block creation and is specific to both the block and its parent block. This hash acts as unique information that sets one block apart from another [3]. The block also includes other relevant transaction information, sender and

Ugwu, J. N., Hassan J. B., Akinsanya, S. E., Ayogu, B. A., Adubi S. S. and Olagunju, M. (2024). Comparative Analysis of Eight Different Blockchain Technology Schemes and Their Implementations, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 11 No. 1, pp. 74 – 87.

recipient details, and a timestamp that indicates the transaction's execution time.
Interoperability is essential for facilitating seamless communication and transaction exchange among diverse blockchain networks. Various interoperability approaches, including protocols like Polkadot and Cosmos, aim to overcome challenges such as data standardization and consensus interoperability [4]. These solutions foster collaboration across blockchain ecosystems, enabling interoperable asset transfer and cross-chain smart contract execution. Consensus mechanisms play a crucial role in determining how transactions are validated and added to the blockchain ledger. Common mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) offer different trade-offs in decentralization, security, and energy efficiency [5].

Emerging mechanisms such as proof of history (PoH) address scalability and environmental concerns, reflecting ongoing innovation in this area. Security is paramount in blockchain systems to ensure data integrity, confidentiality, and availability. Techniques like cryptographic hashing and digital signatures are employed to secure transactions, while auditing and bug bounty programs help identify and mitigate vulnerabilities [6]. Scalability is a significant challenge for blockchain systems, particularly those using PoW consensus [7]. Solutions like layer 2 scaling and on-chain scaling aim to improve transaction throughput and reduce latency, but scalability remains an ongoing concern. These key elements are what make most blockchain unique in their functionality.
Blockchain is decentralised which implies that there is no central authority or third party in charge of the system, transactions carried out are initiated and recorded by a group of connected computers on the network, this makes the system highly resistant to hacking and other security threats. Therefore the need for comparative analysis of different blockchain technology schemes can never be over emphasised, because it can bring to light significant knowledge of their strengths and weaknesses and also provide information that can enable future research development in this domain. Blockchain technology has emerged as a promising solution for secure, decentralised, and transparent data sharing across various application domains. However, there are significant differences between different blockchain technology schemes in terms of their architecture, consensus mechanisms, security features, scalability, interoperability, governance structures, and application domains.

1.1 Terminologies commonly used in blockchain

The following are the key terminology used in blockchain technology.

i. Blockchain: A decentralised, digital ledger that records transactions in a secure and transparent manner.
ii. Cryptography: The practice of secure communication in the presence of third parties. In blockchain technology, cryptography is used to secure and verify transaction

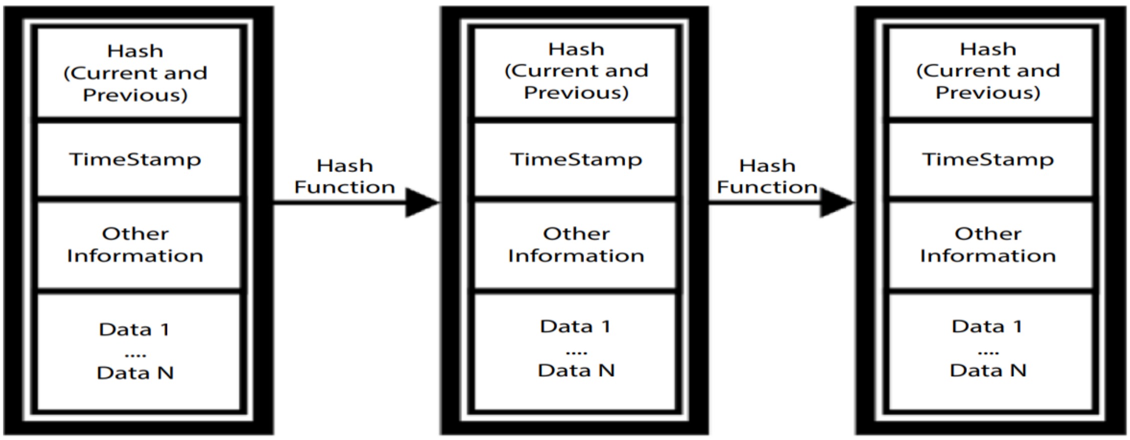

Figure 1: System Architecture of Blockchain [8].

iii. Distributed ledger: A ledger that is maintained by a network of nodes, rather than a central authority.
iv. Smart contract: Self-executing code that is stored on a blockchain and can be used to automate transactions and enforce rules.
v. Consensus mechanism: A mechanism used in blockchain technology to achieve agreement among nodes on the state of the ledger.
vi. Mining: The process of verifying and adding transactions to a blockchain through the use of computational power.
vii. Node: A device or computer that participates in a blockchain network by maintaining a copy of the ledger and verifying transactions.
viii. Fork: A split in a blockchain network that results in the creation of two separate blockchains.
ix. Token: A digital asset that is created and managed on a blockchain.
x. Hash function: A mathematical function that converts data of any size into a fixed-length output, used to secure and verify data in a blockchain network.
xi. Merkle tree: A data structure used to efficiently store and verify the integrity of large amounts of data in a blockchain.
xii. Public key/private key: A pair of keys used in cryptography to secure and verify transactions in a blockchain network. As we proceed to other aspects of blockchain technology scheme, the need to go into more details on some of the above listed terminology will be justified in the other parts of this research project.

1.2 Characteristics of blockchain technology

Now that we have talked about the fundamentals of blockchain technology scheme, let go into something a little more intriguing which is the reason why blockchain technology is gaining huge speculation in most industries and causing impacts globally. Every technology is most at times identified by their unique characteristics and features. Blockchain technology is no exemption from this, it possesses some relevant and edge cutting characteristics.

i. Decentralization: Blockchain technology operates in a decentralized manner, avoiding the need for a central authority or intermediary to validate transactions. Instead, it relies on a network of computers (nodes), which collectively maintain and validate the blockchain [9]. This decentralization aspect enhances security, censorship resistance, and trust in the system.
ii. Immutability: Once a transaction is recorded on a blockchain, it becomes nearly impossible to alter or tamper with. Each new block on the chain is linked to the previous one through cryptographic hashing algorithms, ensuring the integrity and immutability of the data [10]. This characteristic can provide transparency and provenance in various sectors, such as supply chain management and digital identity verification.
iii. Transparency: Blockchain technology enables transparency by allowing anyone to access and verify the data recorded on the blockchain. This transparency helps in building trust among participants and eliminates the need for blind trust in intermediaries [11]. Anyone can audit the blockchain, enhancing accountability and reducing fraud.
iv. Security: Blockchain technology employs various security measures to protect data integrity and prevent unauthorised access [1]. The use of cryptographic algorithms ensures that transactions and data cannot be modified without proper authorization. Additionally, the decentralised nature of blockchain makes it less vulnerable to hacking attacks, as it does not rely on a single point of failure.
v. Privacy: While blockchain offers transparency, it also provides privacy features. Confidential information can be secured through encryption techniques, ensuring that only authorised parties have access to sensitive data. Several blockchain protocols and frameworks, such as zero-knowledge proofs, have been developed to enable privacy while maintaining the benefits of transparency [12].

1.3 Different Form of Blockchain

There are three major forms of blockchain. Public blockchain, private blockchain and consortium blockchain.

a) Public Blockchain

A public blockchain allows anyone in the network to verify transactions and participate in the consensus process. Its initial purpose was to eliminate the need for a central authority in a secure asset exchange. This is achieved by creating a block of peer-to-peer transactions, with each transaction being associated with the blockchain before being recorded in the system. As a result, it can be confirmed and synchronised with every node in the network [13]. Individuals with a computer and internet connection can join as nodes and gain access to the complete history of the blockchain. The high level of redundancy in a public blockchain ensures its strong security. However, it suffers from slow processing speed and inefficiency. The significant amount of electricity required for validating each transaction is enormous and grows substantially as more nodes are added to the network [14]. In simpler terms, a public blockchain allows users to remain anonymous and keeps all transactions transparent. It may not be as fast or cheap as a private blockchain, but it is still faster and cheaper than traditional accounting systems.

b) Private Blockchain

Private blockchain refers to a specific type of blockchain technology that is restricted in access and allows for a certain level of involvement from intermediaries [15]. Unlike public blockchains, private blockchains have strict management and control over data access authority within the network. In a private blockchain, no nodes in the network are involved in the process of verifying and validating transactions. Instead, this responsibility lies solely with a designated company or organisation who initiates, verifies, and validates each transaction. This approach provides a heightened level of efficiency in the verification and validation of transactions since it eliminates the need for consensus among various network participants. However, the major drawback of private blockchains is their lack of decentralised security, which is a key feature provided by public blockchains.

In public blockchains, security is achieved through multiple nodes participating in the verification process and reaching a consensus, which enhances the immutability and trustworthiness of the system. In contrast, private blockchains depend on a central entity or entities, which introduces a single point of failure and potential vulnerabilities in the system. Contrarily, private blockchains offer the advantage of allowing companies to tailor access rights to specific individuals and grant a greater level of privacy compared to public blockchains [14].

This makes private blockchains suitable for businesses following a traditional governance model. By adopting privately-run blockchains, organisations can modernise and adapt to the demands of the 21st century. Furthermore, private blockchains are more likely to gain acceptance from government entities and private sector companies due to their ability to maintain a central authority and provide a more secure, efficient, and faster technology.

c) *Consortium Blockchain*

A consortium blockchain is a type of blockchain that combines elements of both public and private blockchains, resulting in a partially decentralised network [16]. Within this network, data or transaction details can be either open source or private, and the node in the network has the authority to choose beforehand. It is important to understand the distinction between a consortium blockchain and a fully private blockchain. A consortium blockchain is a type of blockchain where a predetermined set of nodes or entities (such as board members or a council of elders) are responsible for verifying and validating transactions or blocks. Unlike public blockchains, where anyone with an internet connection can participate in the verification process, consortium blockchains limit the control to a specific group.

The advantage of using a consortium blockchain is that it combines the benefits associated with private blockchains, such as efficiency and transactional privacy. However, unlike a private blockchain that is controlled by a single company or organisation, a consortium blockchain allows multiple entities to participate in the management, ensuring a more distributed and decentralised approach [17]. By operating under the management of a group of entities, a consortium blockchain allows for collaboration and partnership among organisations. This creates endless possibilities for different organisations to work together, sharing information and resources securely through the blockchain platform. consortium blockchain offers the advantages of private blockchains in terms of efficiency and privacy, while also promoting collaboration and partnership among a group of entities. It ensures a distributed approach to verification and validation, providing a secure platform for organisational partnerships.

1.4 Consensus Algorithm of blockchain

The consensus algorithm of a blockchain is a crucial mechanism that facilitates the coordination and agreement among participating nodes within the network. This algorithm is responsible for determining the order and validating the transactions recorded on the blockchain. By achieving consensus, blockchain networks ensure the integrity, trustworthiness, and security of the distributed ledger system [18]. The importance of the consensus algorithm lies in its ability to create a shared agreement on the state of the blockchain. This agreement is fundamental to prevent any malicious actions or fraudulent activities from corrupting the system.

Without consensus, there would be no way to ensure that all nodes in the network have a consistent understanding of the blockchain's history. In turn, this would undermine the trust and reliability that makes blockchain technology unique. The consensus algorithm is an integral component of blockchain technology. Its role is to enable participating nodes to reach a unified agreement on the order and validity of transactions. By doing so, consensus algorithms safeguard the integrity and security of the blockchain, making it a reliable and transparent platform. The diverse range of consensus algorithms available provides blockchain platforms with options that best suit their specific requirements, striking a balance between security, efficiency, scalability, and decentralisation.

Below are some popular consensus mechanisms that have been implemented in blockchain:

i. Proof of work: Proof of work is a consensus algorithm utilised in various blockchain systems. It functions by necessitating the completion of computationally demanding tasks. This approach ensures that participants within the network must exert sufficient effort to validate and record transactions on the blockchain. Simultaneously, multiple nodes within the network engage in a race to accomplish these computationally intensive operations swiftly. The process is efficiently structured to ensure that the participant who has accomplished the task provides evidence to other network members, allowing them to validate the legitimacy of their contributions In the system this mechanism, participants, known as miners, compete to solve complex mathematical puzzles in order, For instance, [19] discussed the potential vulnerabilities of PoW. PoW is a widely used consensus mechanism, however, it has led to environmental concerns due to its high energy consumption [20].
ii. Proof of stake: Unlike Proof of Work (PoW), where participants engage in a competition utilising their computational power to be chosen for writing data onto the blockchain and subsequently receive rewards, Proof of Stake (PoS) is a consensus algorithm that determines the selection of a computer to author a new block on the blockchain based on the amount of stake accumulated by a network participant [21]. This stake essentially represents a quantity of cryptocurrency coins that are held and invested within the network, unable to be accessed or traded. Peercoin was the pioneer in implementing this strategy, giving participants with substantial coin holdings an upper hand compared to their counterparts. To carry out this process, the participants need to provide information regarding their

possession of coins and the duration of time they have held them.

Participants must stake a greater amount of coins than the potential reward for adding a transaction to the blockchain. If any fraudulent transactions are identified, the network seizes all the coins being staked by the participant attempting the attack. One advantage of this approach is its reduced reliance on hardware, making it more environmentally friendly compared to PoW. Nonetheless, computing power is still necessary to generate blocks, although it is significantly less than what is required for PoW [22]. Some studies have highlighted the advantages of PoS over PoW, such as lower energy consumption [23] and enhanced security [24].

2. Related Works

Mittal *et. al.* [8] explore the comparison analysis of several blockchain systems, they looked at the advantages and disadvantages of five top choices in 21 different categories. Their purpose is to give a thorough grasp of the unique features of each platform and to provide advice on selecting the best blockchain platform for a given set of requirements and objectives.

Faqir-Rhazoui *et. al.* [25] compare various platforms designed for decentralized autonomous organizations (DAOs) on the Ethereum blockchain. Their research entails analyzing and evaluating various platforms, providing insightful information about their features, capacities, and efficacy in the context of decentralized governance frameworks.

Ali *et. al.* [26] presents a comparative study focusing on the utilization, benefits, challenges, and functionalities of blockchain technology. Through their research, they investigate and compare various aspects of blockchain adoption, providing insights into its advantages, difficulties, and operational capabilities.

Yadav and Singh [27] compare consensus methods in the context of blockchain technology. Their research compares and contrasts the various consensus mechanisms used in blockchain systems, and it is presented in the framework of the RACCCS 2019 conference. Through their study, they hope to shed light on the advantages, disadvantages, and performance traits of these algorithms, improving knowledge of their applicability for different blockchain uses.

Al-Breiki *et. al.* [28] provide an extensive analysis with an emphasis on reliable blockchain oracles. Their research comprises a detailed analysis and comparison of different blockchain oracle solutions. They also highlight challenges for open research in this area. By raising knowledge and understanding of blockchain oracle technology, their effort hopes to facilitate the creation of more dependable and secure decentralized networks.

Alahmadi *et. al.* [29] conduct a comparative analysis that highlighted how blockchain technology can be used to support digital transformation in the ports and shipping sector. Their research compares and analyzes several blockchain solutions in this situation in an effort to shed light on the advantages and disadvantages of each. In the end, the study advances the digitalization of the shipping industry by illuminating how blockchain might be used to improve port and shipping operations' efficiency, security, and transparency.

Khrais [30] compares blockchain and IOTA technologies, in the research presented at the Fourth International Conference on I-SMAC. The study explores the unique qualities, capabilities, and uses of IOTA and blockchain technology. By comparing them, the study hopes to shed light on their advantages, disadvantages, and applicability for different use cases in the IoT, social, mobile, analytics, and cloud computing areas.

Fan *et. al.* [31] offer a methodical examination that centers on the assessment of blockchain system performance. Their investigation comprises a thorough analysis of the different blockchain systems, approaches, and performance indicators. Their goal is to shed light on areas that require improvement and offer a comprehensive grasp of the variables affecting blockchain performance. Researchers and practitioners interested in learning more about the performance traits of blockchain systems will find this survey to be a useful resource.

Li, and He [32] compare and contrast Bitcoin, Ethereum, and Libra. In this study, several features of these three well-known cryptocurrencies are compared and examined, including their use cases, security, scalability, consensus processes, and underlying technology. In order to improve awareness of each cryptocurrency's functions and possible uses in the field of digital finance and beyond, the study attempts to shed light on the unique qualities, advantages, and disadvantages of each one through its examination. The paper examined only three blockchain techniques and their implementations which are not sufficient since there exist a wider range of different blockchain techniques and their implementations.

3.0 Blockchain Technologies

The analysis presented in this chapter is based on extensive research, reviewing academic papers, technical documents, whitepapers of different blockchain technologies. A systematic approach is adopted to ensure thorough examination of each technology, considering both quantitative and qualitative factors. The research approach is observational research which involves observing and analysing existing phenomena without intervening or manipulating variables. In the context of this research different types of blockchains technology based on their existing characteristics, features, and performances would be compared and analysed. This typically involves collecting and analysing data from various sources, such as whitepapers, technical documentation, real-world implementations, and user experiences.

3.1Blockchain Scheme based on evolution:

a) Sovrin

Sovrin, launched in 2016, was developed by the Sovrin Foundation, a non-profit organization. It was created with the vision of providing an open-source, global public utility for self-sovereign identity. Sovrin's goal is to enable individuals to have control over their personal data and identities in a secure and decentralized manner. Security is a core focus for Sovrin [33]. To ensure the protection of user data, Sovrin employs cryptographic algorithms, decentralized identifiers (DIDs), zero-knowledge proofs, and selective disclosure mechanisms. These security measures not only safeguard user data but also enable secure sharing of verifiable credentials, enhancing privacy and control for individuals. In terms of consensus mechanism, Sovrin utilizes a modified federated Byzantine Agreement (BFT) consensus mechanism. This mechanism combines the advantages of the Practical Byzantine Fault Tolerance (PBFT) and the Ripple consensus protocols. By leveraging this consensus mechanism, Sovrin ensures the accuracy, reliability, and security of the identity information stored within its network.

Scalability is an important consideration for Sovrin. To address large-scale identity management requirements, Sovrin implements pluggable consensus mechanisms. This approach allows for potential enhancements in scalability as future advancements in consensus protocols become available. By focusing on scalability, Sovrin strives to meet the increasing demands of its user base while maintaining a secure and efficient identity management system [34]. Sovrin places a strong emphasis on interoperability by adhering to open standards and protocols such as the World Wide Web Consortium (W3C) and Decentralized Identifiers (DIDs). By conforming to these standards, Sovrin ensures seamless integration with various identity systems and platforms, allowing for effective interoperability and enabling individuals to utilize their self- sovereign identities across different domains.

b) *Ripple*

Ripple, originally established in 2004 as a RipplePay platform, underwent rebranding as Riple Labs in 2012 to concentrate on the development of decentralized financial systems. Its security is upheld through the employment of the Ripple Protocol Consensus Algorithm (RPCA), which ensures the network's protection [35]. This algorithm relies on trusted validators within the network to validate transactions and establish consensus. Additionally, Ripple employs a distributed agreement protocol, incorporating a consensus mechanism based on the concept of Byzantine fault tolerance.

c) *Ethereum*

It is an open-source, publicly accessible distribution system based on blockchain technology that aims to bring the concept of a global computer to life. This platform makes a variety of digital contracts and financial transactions easier. Operating on a decentralized blockchain, it provides unique features including cryptocurrency integration, smart property management, Decentralized Autonomous Organizations (DAOs), and smart contracts. Clients are required in order to use the Ethereum Blockchain and its features, including smart contracts. Some clients are made by the community of programmers, but the majority are built by the Ethereum Foundation. Ethereum functions as a Decentralized Autonomous Organization (DAO), which means that its whole existence is based on the blockchain and is regulated by its protocol. Programming languages used to create Ethereum smart contracts include Serpent, Solidity, and LLL. Ethereum's proof-of-work mining algorithm, the Ethash Algorithm, is well-known for its memory-intensive consensus process [36]

d) MediLedger

MediLedger, founded in 2017 by Pfizer, Genentech, and AmerisourceBergen, emerged with the intention of tackling issues in the pharmaceutical supply chain. The company recognized the prevalence of counterfeit drugs and recognized the need for more efficient processes. To address these challenges, they developed a blockchain-based platform. One of the key aspects of MediLedger's platform is its focus on security. The company achieves this by implementing a private blockchain network that restricts access to authorized participants. This ensures that only trusted individuals can interact with the system. Additionally, the platform utilizes cryptographic algorithms to validate transactions, ensuring data integrity and preventing unauthorized [37].

e) Hyperledger

Hyperledger is an open-source, multi-project platform that can be downloaded by anybody. It is managed by the Linux Foundation and promotes cooperation in the field of blockchain technology amongst various industries[31]. Hyperledger was founded in December 2015 by a group of technical specialists from different industries with the main goal of making blockchain technology more user-friendly. Later, in May 2016, Brian Behlendorf was named the project's executive director. People can design custom blockchains with Hyperledger software, and many businesses have embraced Hyperledger to improve their operations. Contributions from people all over the world are welcome to help Hyperledger grow as a platform and product.

There was a gap in addressing business-to-business (B2B) transactions, in contrast to platforms like Bitcoin or Ethereum, which largely specialized to business-to-customer (B2C) interactions. Confidentiality is important in B2B situations, and not every transaction should be made public. This is similar to private business transactions that take place between two organizations without the involvement of a third party [38]. Developers designed Hyperledger as a software solution that allows the construction of customized blockchain services based on particular demands and requirements, acknowledging the distinctiveness of organizations. In recent years, Hyperledger has drawn a wide range of participants from industries such as supply chain management, technology, and finance, providing a range of approaches to tackle the unique problems associated with business-to-business transactions. Although Hyperledger doesn't come with a cryptocurrency by default, users can build one if needed, unlike some other platforms. It also includes chain code-coded smart contracts. Golang and Java are the two main programming languages utilized in the open-source Hyperledger project.

f) R3 Corda

After its April 2016 launch, Corda became an open-source platform in November of that same year. Over 800 technologists and business executives attended CordaCon, R3's flagship conference, which took place in September 2017 to learn about the most recent Corda applications and noteworthy advancements in blockchain technology [39]. Afterwards, Corda 1 which prioritized API stability was launched in October 2017. Later in 2017, Corda 2 was released in response to this. Wire stability was achieved with Corda 3, and with over 1,800 commits, Corda 4 was released. The open-source blockchain platform Corda is designed with the banking industry in mind [40].

Despite using distributed ledger technology, it differs from conventional blockchains. The main goal of Corda is to reduce costs associated with middlemen in order to expedite business transactions. It only focuses on financial transactions and leverages smart contracts to enable direct, private transactions. Corda functions as a private platform that lets companies and individuals carry out transactions in private. It permits parties to exchange only the information that is required, avoiding the need to broadcast details over the network. Owing to the billions of industrial transactions that take place every day, Corda provides many versions to enable smooth information sharing between concurrent apps on the same network. Interestingly, Corda does not have its own money and is not restricted to any particular consensus algorithm. As of right now, 300 members of the global ecosystem operate the 300 Corda nodes that make up the publicly available Corda network [41].

g) Stellar

Stellar was founded in 2014 by Jed McCaleb and Joyce Kim, and the Stellar Development Foundation looks after it as a non-profit [42]. The open-source Stellar payment protocol makes it possible to transfer different currencies with ease. Historically, money transfers between nations with different currencies have required money to be converted via intermediaries, which has led to high transaction costs and decreased security. Sending money to the US, for example, requires changing Indian Rupees to US Dollars through a number of intermediaries, which comes with a high cost and security risk. In order to tackle these obstacles, Stellar was presented. It seeks to simplify financial transactions by offering a single network that is accessible to all parties and lower transaction fees, which usually total between 9 and 10% of the transferred value. Stellar boasts several noteworthy features.

Firstly, it operates as a multi-currency network, allowing any currency, asset, or token to be issued directly within its framework. Transactions within the Stellar network are confirmed in less than 5 seconds, and the associated transaction fees are minimal, with only a cent charged for every 10,000 transactions. Participants in the Stellar platform have the flexibility to select trusted network members from a pool of available participants. Notably, Stellar's processing capability is significantly high, enabling it to handle thousands of transactions per second. The native cryptocurrency of the Stellar network is Lumens (XLM), which serves as the medium for real-time value transfer within the network and acts as a bridge currency between digital-fiat assets issued by Anchors. Additionally, the Stellar Decentralized Ledger serves as a versatile database capable of storing various types of data, including account balances, payments, and offers to buy and sell assets. These offers collectively form a global order book known as the Decentralized Exchange (DEX) [43].

h) Multichain

People from a wide range of businesses have demonstrated a strong interest in blockchain technology and its possible uses. Apart from the diverse range of open-source blockchain platforms, there exists an additional category referred to as multi-chain platforms. Multi-chain platforms were first introduced in 2015 to serve companies that need private financial transactions that are not available to third parties [44]. An API and command-line interface are provided by multichain technology to enable the creation of private blockchains. Multi-chain systems are becoming more and more popular as a result of their applicability for data-centric applications. All users within the blockchain ecosystem have access to the blockchain ledger, which guarantees total transaction stability and control. On the other hand, in a multichain network, several users create their own blockchain networks, and transactions that take place within these networks are not visible to other users unless they are specifically authorized to do so. For example, although Bitcoin runs on a single blockchain network, in less than a year, over ten distinct applications have been created on multichain platforms, with solutions in the pharmaceutical industry garnering significant attention [45].

The purpose of multichain technology is to guarantee the safe custody and transfer of digital assets. In multichain blockchains, the Proof of Work consensus technique is used for mining; however, its application within a network is voluntary. To mine multichain blocks in a private multichain network, nodes or miners need to have legitimate authority. As a result, when compared to other platforms, transaction costs in multichain technology are significantly cheaper [46]. Nodes interact and communicate with one another during the handshaking process in a multichain network, much like when two people shake hands physically. The blockchain's nodes use lists of permissions and IP addresses to identify one another. This allows nodes to communicate with each other through message sending; in the event that the procedure is not successful, the peer-to-peer connection is broken.

4.0 Comparative Analysis of the Blockchain Technologies

Table 1 shows a comprehensive comparison of the eight different types of blockchain schemes with their different characteristics

Table 1: Comparative Analysis of The Blockchain Technology

Technology	**Sovrin**	Ripple	**Ethereum**	**MediLedger**	**Hyperledger**	**R3 Corda**	**Stellar**	**Multichain**
Operation Mode	Public	Private	Public	Private	Consortium	Private	Private	Private
Year of Starting	2016	2012	2015	2017	2015	2014	2014	2015
Aim	Sovrin's aim is to create a decentralized and self-sovereign identity environment.	Ripple seeks to tackle the inefficiencies and expensive nature inherent in conventional payment systems.	Ethereum's main goal is to offer a decentrelized framework where smart contracts and decentrelized applications (DApps) can be developed and launched	MediLedger's core objective is to transform the pharmaceutical supply chain through the utilization of blockchain technology.	Hyperledger provides a platform for enterprises to develop their own permissioned blockchain networks.	The main goal of R3 Corda is to furnish a decentralized platform customized for enterprises across diverse sectors, facilitateing the creation and implementtation of distributed ledger applications.	Stellar's main objective is to enable swift, economical, and secure cross-border payments and asset transfers, with a specific focus on serving individuals, businesses, and finance-	Crafted to ensure the secure transfer and custody of digital assets.

							al institu-tions in developing economies.	
Gover-nance	Stewards	Stakeholders and internal leadership team	Ethereum Develop-ers	Medildger leadership team	Linux Foundation	R3	Development Team	Open Source
Curre-ncy	Sovrin does not possess a crypto-curren-cy unique to its platfo-rm.	XRP	Ether(ETH)	MediLedger does not possess a proprietary digital currency of its own.	Hyperledger lacks its proprietary digital currency.	No Proprietary digital currency	Lumens (XLM)	Native Currency
Conse-nsus	network of validat-or nodes operated by stewards	Ripple Protocol Consensus Algorithm	Proof-of-work to Proof-of Stake	Permissioned Blockchain Model	PBFT (Practical Byzantine Fault tolerance)	Notary Nodes	FBA (Federated byzantine agreement)	Proof of Work
Smart Contr-acts	No	No	Yes	Yes	Yes	Yes	No	Smart Filter
Langu-age used for develop-pment	Python	XRP Ledger	GoLang + Python	Java/ Python	GoLang + Java	Kotlin + Java	Metron	C++/Java Script
Secon-dary Storage	Rocks DB	Rocks DB	Rocks DB	Rocks DB	Rocks DB	H2Database	Rocks DB	LevelDB
Hash functi-on	SHA-256	Hash function of	Keccak256	SHA-256	SHA3 SHAKE256	SHA-256	SHA-256	SHA-256
Statef-ul/Stateless	Stateful	Stateful	Stateful	Stateful	Stateful	Stateful	Stateful	Stateless
Purp-ose	B2C (Busin-ess to Customer)/B2B (Business to Business)	B2B	B2B/B2C	B2B	B2B	B2B	B2B	B2B
Trans-action per	100	1500	15-30	2000+	20,000+	15-1678	3,000+	500-1000

second								
API Access Avail-ability	Yes	Yes	Yes	No	No	Yes	Yes	Yes
SDK Avail-ability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalab-ility	Yes	Yes	No	Yes	Yes	Yes	Yes	yes
Trust Model	Trusted	Semi-trusted	Untrusted	Trusted	Semi-trusted	Trusted	Semi-trusted	Trusted

5.0 CONCLUSION

In conclusion, the comparative analysis of different blockchain technology schemes illuminates the multifaceted nature of this revolutionary technology. Blockchain offers a plethora of advantages that have the potential to transform various industries. Its core strengths lie in decentralization, immutability, and transparency. By removing the need for intermediaries and central authorities, blockchain technologies enable trustless transactions and data integrity while reducing costs and enhancing efficiency. Moreover, the security features of blockchain, such as cryptographic hashing and consensus mechanisms, provide robust protection against tampering and unauthorized access. This is especially valuable in environments where data security and integrity are of paramount importance. Additionally, the potential for smart contracts and decentralized applications (DApps) opens up new avenues for automation and innovation. However, alongside its benefits, blockchain technology also presents a set of challenges. Scalability remains a significant concern, as existing blockchain platforms encounter limitations in processing a high volume of transactions quickly and cost-effectively.

These eight technologies are evaluated based on a number of key features to help developers choose the best one. This comparison highlights the advantages and disadvantages of each platform and acts as a competitive assessment. Developers can evaluate various platforms by consulting the provided table. For example, Stellar lacks native smart contract functionality and instead uses transactions to create smart contracts, whereas Ethereum is seen as an untrusted platform unfit for commercial use. Stellar and R3 Corda show themselves to be incredibly scalable systems. Due to its durability and simplicity, Ethereum stands out as the basic platform overall, providing the framework for other platforms with additional functionalities. Many people are still ignorant of the special advantages that blockchain offers, like immutability, tamper-proofing, reliability, and better security. It will be interesting to see how these technologies continue to develop and innovate as they add new features on a regular basis.

References

[1] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: research and applications*, *3*(2), 100067.

[2] Mohammed, A. H., Abdulateef, A. A., & Abdulateef, I. A. (2021, June). Hyperledger, Ethereum and blockchain technology: a short overview. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-6). IEEE.

[3] Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, *13*(2), 1-15.

[4] Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, *54*(8), 1-41.

[5] Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE access*, *9*, 43620-43652.

[6] Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access*, *10*, 122679-122695.

[7] Yang, D., Long, C., Xu, H., & Peng, S. (2020, March). A review on scalability of

blockchain. In *Proceedings of the 2020 the 2nd International Conference on Blockchain Technology* (pp. 1-6).

[8] Mittal, N., Pal, S., Joshi, A., Sharma, A., Tayal, S., & Sharma, Y. (2021). Comparative analysis of various platforms of blockchain. *Smart and Sustainable Intelligent Systems*, 323-340.

[9] Merrell, I. (2022). Blockchain for decentralised rural development and governance. *Blockchain: Research and Applications*, *3*(3), 100086.

[10] Imteaj, A., Amini, M. H., Pardalos, P. M., Imteaj, A., Hadi Amini, M., & Pardalos, P. M. (2021). Introduction to Blockchain technology. *Foundations of Blockchain: Theory and Applications*, 3-13.

[11] Xu, P., Lee, J., Barth, J. R., & Richey, R. G. (2021). Blockchain as supply chain technology: considering transparency and security. *International Journal of Physical Distribution & Logistics Management*, *51*(3), 305-324.

[12] Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, *20*(24), 7171.

[13] Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, *182*, 103035.

[14] Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., ... & Chen, S. (2020). Public and private blockchain in construction business process and information integration. *Automation in construction*, *118*, 103276.

[15] Jo, M., Hu, K., Yu, R., Sun, L., Conti, M., & Du, Q. (2020). Private blockchain in industrial IoT. *IEEE Network*, *34*(5), 76-77.

[16] Liang, W., Yang, Y., Yang, C., Hu, Y., Xie, S., Li, K. C., & Cao, J. (2022). PDPChain: A consortium blockchain-based privacy protection scheme for personal data. *IEEE Transactions on Reliability*.

[17] Singh, S., Kumar, A., & Kathuria, M. (2022). Understanding the public, private and consortium consensus algorithms in blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, *3*(3), 269-288.

[18] Yusoff, J., Mohamad, Z., & Anuar, M. (2022). A review: Consensus algorithms on blockchain. *Journal of Computer and Communications*, *10*(09), 37-50.

[19] Gürcan, Ö. (2022). Proof of work is a stigmergic consensus algorithm: Unlocking its potential. *IEEE Robotics & Automation Magazine*, *29*(2), 21-32.

[20] Wendl, M., Doan, M. H., & Sassen, R. (2023). The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management*, *326*, 116530.

[21] Ge, L., Wang, J., & Zhang, G. (2022). Survey of consensus algorithms for proof of stake in blockchain. *Security and Communication Networks*, *2022*, 1-13.

[22] Syed, M., & Ul Abadin, Z. (2022, July). A Pattern for Proof of Stake Consensus Algorithm in Blockchain. In *Proceedings of the 27th European Conference on Pattern Languages of Programs* (pp. 1-5).

[23] Gundaboina, L., Badotra, S., & Tanwar, S. (2022, March). Reducing resource and energy consumption in cryptocurrency mining by using both proof-of-stake algorithm and renewable energy. In *2022 International Mobile and Embedded Technology Conference (MECON)* (pp. 605-610). IEEE.

[24] Bala, K., & Kaur, P. D. (2022). A novel game theory based reliable proof-of-stake consensus mechanism for blockchain. *Transactions on Emerging Telecommunications Technologies*, *33*(9), e4525.

[25] Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. *Journal of Internet Services and Applications*, *12*, 1-20.

[26] Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access*, *9*, 12730-12749.

[27] Yadav, A. K., & Singh, K. (2020). Comparative analysis of consensus algorithms of blockchain technology. In *Ambient Communications and Computer Systems: RACCCS 2019* (pp. 205-218). Springer Singapore.

[28] Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE access*, *8*, 85675-85685.

[29] Alahmadi, D. H., Baothman, F. A., Alrajhi, M. M., Alshahrani, F. S., & Albalawi, H. Z. (2022). Comparative analysis of blockchain technology to support digital transformation in ports and shipping. *Journal of Intelligent Systems*, *31*(1), 55-69.

[30] Khrais, L. T. (2020, October). Comparison study of blockchain technology and IOTA technology. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 42-47). IEEE.

[31] Fan, C., Ghaemi, S., Khazaei, H., & Musilek, P. (2020). Performance evaluation of blockchain systems: A systematic survey. *IEEE Access*, *8*, 126927-126950.

[32] Li, W., & He, M. (2020, October). Comparative analysis of bitcoin, ethereum, and libra. In *2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)* (pp. 545-550). IEEE.

[33] Nassr Eddine, B., Ouaddah, A., & Mezrioui, A. (2022, May). Blockchain-Based Self Sovereign Identity Systems: High-Level Processing and a Challenges-Based Comparative Analysis. In *International Conference on Advanced Intelligent Systems for Sustainable Development* (pp. 489-500). Cham: Springer Nature Switzerland.

[34] Shobanadevi, A., Tharewal, S., Soni, M., Kumar, D. D., Khan, I. R., & Kumar, P. (2022). Novel identity management system using smart blockchain technology. *International Journal of System Assurance Engineering and Management*, *13*(Suppl 1), 496-505.

[35] Islam, M. R., Rashid, M. M., Rahman, M. A., & Mohamad, M. H. S. B. (2022). Analysis of blockchain-based Ripple and SWIFT. *Asian Journal of Electrical and Electronic Engineering*, *2*(1), 1-8.

[36] Thai, Q. T., Ko, N., Byun, S. H., & Kim, S. M. (2022). Design and implementation of NDN-based Ethereum blockchain. *Journal of Network and Computer Applications*, *200*, 103329

[37] Kumar, M. (2022). Blockchain Technology–A Algorithm for Drug Serialization. *Universal Journal of Pharmacy and Pharmacology*, 61-67

[38] Melo, C., Oliveira, F., Dantas, J., Araujo, J., Pereira, P., Maciel, R., & Maciel, P. (2022). Performance and availability evaluation of the blockchain platform hyperledger fabric. *The Journal of Supercomputing*, *78*(10), 12505-12527

[39] Ramadoss, R. (2022). Blockchain technology: An overview. *IEEE Potentials*, *41*(6), 6-12.

[40] Panda, S. K., Daliyet, S. P., Lokre, S. S., & Naman, V. (2022). Distributed ledger technology in the construction industry using corda. *The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm*, 15-41.

[41] Kumari, K. A., Sangeetha, S., Rajeevan, V., Dharshini, M. D., & Haritha, T. (2022, December). Trade Management System Using R3 Corda Blockchain. In *International Conference on Intelligent Systems Design and Applications* (pp. 257-275). Cham: Springer Nature Switzerland.

[42] Shamsi, K., Shayegan, M. J., Uddin, M., & Chen, C. L. (2022). A Fair Method for Distributing Collective Assets in the Stellar Blockchain Financial Network. *Sustainability*, *14*(9), 5311.

[43] Bhatnagar, M., & Thankachan, D. (2022). Improving the Scalability of Blockchain Powered IoT Networks Using Improved Fuzzy Stellar Consensus Protocol. *Computer Science, Technology and Applications*, 79.

[44] Ismail, S., Reza, H., Zadeh, H. K., & Vasefi, F. (2023, March). A Blockchain-based IoT Security Solution Using Multichain. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1105-1111). IEEE.

[45] Umran, S. M., Lu, S., Abduljabbar, Z. A., & Nyangaresi, V. O. (2023). Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. *Internet of Things*, *24*, 100969.

[46] Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., & Han, W. (2022). An overview on cross-chain: Mechanism, platforms, challenges and advances. *Computer Networks*, *218*, 109378.