A Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations

Farhat Anwar[1], Burhan Ul Islam Khan[2]*, Miss Laiha Mat Kiah[3], Nor Aniza Abdullah[4], Khang Wen Goh[5]*
Dept. of ECE, Kulliyyah of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia[1, 2]
Dept. of Comp. Sys. & Tech., Faculty of CS & IT, Universiti Malaya, Kuala Lumpur, Malaysia[3, 4]
Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia[5]

***Abstract*—Blockchain technology is based on the idea of a distributed, consensus ledger, which it employs to create a secure, immutable data storage and management system. It is a publicly accessible and collectively managed ledger enabling unprecedented levels of trust and transparency between business and individual collaborations. It has both robust cryptographic security and a transparent design. The immutability feature of blockchain data has the potential to transform numerous industries. People have begun to view blockchain as a revolutionary technology capable of identifying "The Best Possible Solution" in various real-world scenarios. This paper provides a comprehensive insight into blockchains, fostering an objectual understanding of this cutting-edge technology by focusing on the theoretical fundamentals, operating principles, evolution, architecture, taxonomy, and diverse application-based manifestations. It investigates the need for decentralisation, smart contracts, permissioned and permissionless consensus mechanisms, and numerous blockchain development frameworks, tools, and platforms. Furthermore, the paper presents a novel compendium of existing and emerging blockchain technologies by examining the most recent advancements and challenges in blockchain-enabled solutions for a variety of application domains. This survey bridges multiple domains and blockchain technology, discussing how embracing blockchain technology is reshaping society's most important sectors. Finally, the paper delves into potential future blockchain ecosystems providing a clear picture of open research challenges and opportunities for academics, researchers, and companies with a strong fundamental and technical grounding.**

***Keywords*—Blockchain; blockchain applications; consensus algorithms; distributed ledger; smart contract**

I. Introduction

According to the National Institute of Standards and Technology (NIST), blockchains are "tamper-evident and tamper-resistant digital ledgers executed in a distributed form, i.e., without a single repository, and usually without a central authority," i.e., a government, bank, or company. In their most basic form, blockchain technologies provide a platform for the secure movement of data involved in any transaction, including contracts and financial transactions [1]. Cryptography is at the core of blockchain technology, ensuring that the data being exchanged has not been tampered with and gives integrity and authenticity. The transactions involved in blockchain are just a transfer of assets, and the assets are essentially data, which may represent financial information, healthcare information, or even company information [2]. Blockchain is a buzzword that will likely be heard more in the future. Bitcoin and blockchain are gaining technical insight and becoming the chosen technology for implementing a wide range of commercial solutions in the current technological age. Most businesses worldwide are considering using blockchain technology, and even the government is laying the groundwork for the future. In general, individuals may become perplexed by the terms bitcoin and blockchain. Bitcoin is a digital cryptocurrency that may be used to make online payments without relying on a third party. In contrast, blockchain is the platform and structure that ensures every transaction is visible and unchangeable [3].

Blockchain is a public distributed ledger accessible to everyone, and anyone can become a member of this network. Bitcoin is considered the first step in developing blockchain technology [4]. Satoshi Nakamoto, the creator of bitcoin, originally announced the cryptocurrency in 2008 [2]. Satoshi Nakamoto was an unknown individual or group of individuals who began working on the bitcoin concept in 2007 under the name Satoshi Nakamoto. On the 18th of August, they registered the domain name bitcoin.org. Soon after, on the 31st of October, they issued a whitepaper detailing bitcoin, the transaction procedures, Proof-of-Work (PoW), and other aspects of the cryptocurrency. On the 9th of November, 2008, the sourceforge.net website registered the first bitcoin project. At 18:15:05 GMT on the 3rd of January, 2009, the Genesis Block (also known as block 0) was established. Blockchain is not only about tokens and coins. Blockchain is more than bitcoin [5]. The information on a blockchain is stored in blocks, which are bits of data that have been cryptographically encrypted [6]. To build a chain, each consecutive block must contain information about the previous block. As a result, the word blockchain was coined. Cryptographic hash functions and public key cryptography are used to ensure the anonymity of the blockchain [7]. It also aids in the achievement of transparency. New transactions are added to the current information based on the miners' agreement in the network. As a result of existing economic processes such as PoW, Proof-of-Stake (PoS), and others [8], the rules for validating

*Corresponding Author.

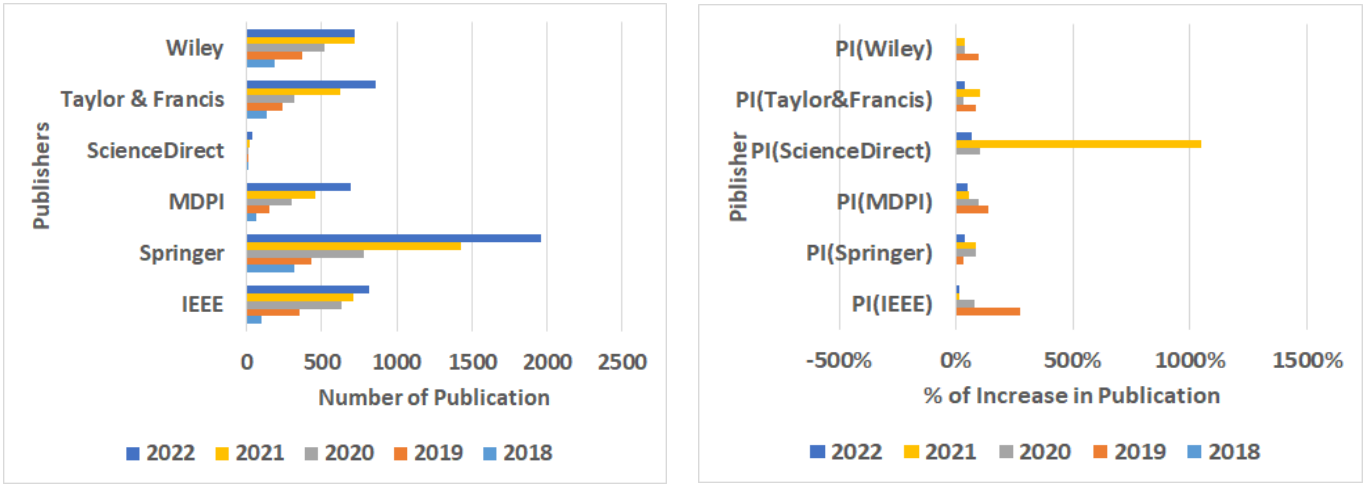
This research has been supported by the Ministry of Higher Education Malaysia through its Fundamental Research Grant Scheme under Grant ID FRGS/1/2019/ICT05/UM/01/1.

transactions are codified in the form of algorithms applied by miners who are also paid with a native coin.

Moreover, because the ledger operates on a distributed network, all nodes participating in the network receive a duplicate of the original information [9]. Depending on the scenario, every node in the network serves as a client and a server. Blockchain technology is available in many forms as it has undoubtedly advanced over the last decade. There are several types of blockchain technologies, each with its purpose and set of difficulties. The two most frequent types are public and private, widely utilized by bitcoin networks and private businesses. Also gaining popularity are hybrid blockchains. Besides ensuring the secure movement of currency, the technology creates a permanent historical record of all transactions and a single version of events. This condition is entirely transparent and shown in real-time for the convenience of all participants. However, blockchain technology, irrespective of the type of blockchain protocol implemented, will significantly impact the transformation of centuries-old business practices, the establishment of greater levels of legitimacy in government, and the creation of new avenues of economic opportunity for common citizens. Fig. 1 gives a brief overview of blockchain technology.

The primary objective of this manuscript is to provide an overview of the many blockchain-related technologies and developments currently in progress. For this purpose, the proposed scheme is based on the desk research methodology considering all the major implementations from the most reputable publishers (such as IEEE, ScienceDirect, MDPI, etc.). Overall, 223 manuscripts were read and evaluated, but only 144 were chosen to be included in this paper. This review only considers papers that primarily discuss implementation strategy and results. As shown in Fig. 2, leading academic publishers like Wiley, Taylor & Francis, ScienceDirect, MDPI, Springer, and IEEE have all published increasing numbers of articles about blockchain technology in the last five years. The outcome shows a spontaneous increase in publication in the last three years.

Fig. 1. Overview of Blockchain Technology.



(a) (b)

Fig. 2. Research Publication Trends Towards Blockchain Technology. (a) Total Publication (2018-2022); (b) % of Increase (PI) in Publication (2018-2022).

A. Organization of the Study

This study is organized as follows: Section I briefs about the significance of using blockchain in current times with a brief on its usage and formation in the industry. Section II discusses the history of blockchain with respect to multiple generations and the essential characteristic of its evolution. It also presents a clear idea about the crucial blockchain features required for confirming the proper functioning of blockchain technologies irrespective of any application. Further, this section discusses three essential types of blockchain: public, private, and hybrid forms, with compact information about its features and associated issues. This section also illustrates all the reported research attempts and highlights their advantages and limitations. Section III reviews existing architectures and components of blockchain along with its working. This section also highlights scientific developments in consensus algorithms. Further, it also presents the rationale behind migrating to SHA-3 encryption and a compact-and-illustrative discussion of approaches of consensus approach in the blockchain. The blockchain framework and platform are illustrated with respect to its advantages and shortcomings in Section IV. Section V examines emerging blockchain applications concerning their utilization and prominent issues. Section VI highlights some of the study's essential findings that offer a contributory inference from the viewpoint of analyzing the strengths and weaknesses of existing approaches in the blockchain. It also presents a briefing about the novelty of the proposed review with some existing notable reviews. A thorough examination of the challenges and unsolved research problems linked to blockchain security is included in Section VII. Further, the characteristic of a unified blockchain and its associated concerns are highlighted. Section VIII discusses the open research questions from the literature review that should be pursued in the future, and Section IX provides conclusions. References are listed at the end.

II. History, Features and Types of Blockchain

A. History of Blockchain: A Brief Overview of Three Generations

Blockchain technology began as an infrastructure for the bitcoin cryptocurrency and has since evolved into a true game-changer. Unfortunately, in addition to regularly providing new possibilities and applications, this technology has also attracted its fair share of hype and fraud. As a result, many entrepreneurs and engineers remain confused about the actual economic implications of blockchain technology. They are still unsure about its impact on businesses and whether or not they should invest in its development in the first place. Albeit, going over a few data shown in Fig. 3 shows the actual state of the technology and how the world responds to the most essential yet cliche topic of all: how to the technology. This will help better understand blockchain technology's impact on the global economy.

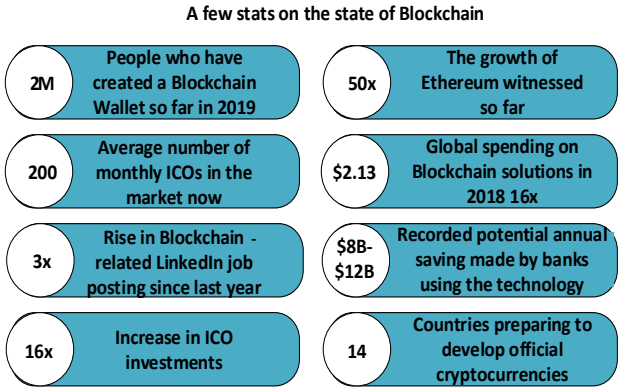


Fig. 3. A Few Statistics Illustrating the Current Development of Blockchain Technology [8].

1) Blockchain 1.0: Blockchain's first generation was intended to improve the traditional monetary system. During this time, bitcoin and other cryptocurrencies were introduced, most of which were written in C++ and followed the PoW consensus paradigm. Although blockchain-based cryptocurrencies improved transactional experience, developers discovered that the technology has far-reaching applications beyond cryptocurrencies. This became the impetus for the creation of the second generation.

2) Blockchain 2.0: As bitcoins remained a hot topic in the market, Ethereum and intelligent contracts became famous in the second blockchain generation. As a result, Ethereum's developers began addressing the coin as a cryptocurrency and platform for delivering a scalable experience and developing decentralized applications, DAPPs. They have also started to investigate the concept of smart contracts, which may be used to make agreements more secure, automated, and practical [7].

3) Blockchain 3.0: In theory, the third generation of blockchain 3.0 is the generation that showcases the most effective blockchain-based solutions currently available. As a result of this generation's focus on the economic and market implications of blockchain technology, several issues related to the creation of blockchain solutions, such as the inability to conduct cross-chain transactions, have been successfully addressed [8]. Furthermore, when it comes to developing blockchain applications, professional blockchain software developers have taken cognizance of the opportunity to use a variety of consensus algorithms other than PoW. Additional concepts such as DLT (Decentralized Ledger Technology), Information for Operational and Tactical Analysis (IOTA), and Currency of the Internet (COTI) have been developed in this generation. They have emerged as the best explanation for how blockchain will transform the world.

4) Blockchain 4.0: Business leaders are lining up to adopt blockchain technology and make it the focal point of their technological solutions. Blockchain 4.0 delivers ideas and solutions for industries that make it functional for the demands of modern business. Automation, integration of execution frameworks, and enterprise resource planning are the focal points of industry 4.0. Blockchain contributes to this modern industrial revolution by giving an increased level of privacy and security insurance to participants in it. Data collecting, asset management, supply chain management, healthcare, and financial transactions are just a few sectors where blockchain has proven beneficial. This means that blockchain 4.0 is improving the suitability of blockchain 3.0 for use in real-world business applications.

Blockchain technology is continually evolving and improving in terms of efficiency and reliability [10][11]. Blockchain technology is, thus, continually evolving and improving in terms of efficiency and reliability. There are various recent advancements towards the utilization of the blockchain-based technology. One such field is to ensure the participation of vehicles in a smart grid environment [12]. One of the critical problems in a smart grid environment is an intruder's theft of user information. Another point of vulnerability in the smart grid is the usage of central nodes for storing and sharing data. There are more malicious activities and vulnerabilities towards such a centralized storage system.

Over time, cryptography's relevance has started to increase in blockchain deployments. The primary role of cryptography in the blockchain is to protect data consistency and user privacy through symmetric or asymmetric encryption [13]. Aside from that, the adoption of digital signatures in the blockchain is more noticeable, which facilitates signing up the data block with transactional records. To date, multiple cryptographic-based approaches have been applied to secure blockchain technology [14]. The main reasons why cryptographic techniques are used in the blockchain are their ability to encrypt data, their inability to change, their ability to be scaled up, and their failure to be disputed [14].

The work carried out by Li et al. [15] used a signature-based blockchain protocol to resist key leakage attacks. The authors have used a puncturable signature scheme where an adaptive signing is carried out based on the bloom filter and Diffie-Hellman structure. Another signature-based scheme was introduced by Shahid et al. [16], where hashing is used for performing one-time signatures. The outcome offers a significantly reduced size of signatures and keys. Cai et al. [17] have constructed a protocol for quantum blind signatures and a blockchain smart contract system. Zhang and Lee [18] have presented a blockchain-based security system using group signatures to authenticate the blocks. The model is claimed to resist multiple attacks related to consensus algorithm vulnerabilities. Xiao et al. [19] have used a multi-signature approach to secure the blockchain platform. The model is claimed to maximize the efficiency of transactions. Existing schemes have also introduced secret-sharing methods to strengthen blockchain operations' security features. Private key distribution protocols that rely on secret sharing have been developed to secure financial applications, as demonstrated by the work of Xiong et al. [20]. Zheng et al. [21] have used generative adversarial networks to develop a unique secret-sharing scheme to mitigate the lost key issue and reduce the communication efficiency using blockchain. Kim et al. [22] have developed a distributed blockchain operation using a local secret-sharing scheme to enhance the cost of communication and storage. Yin et al. [23] have used a unique cryptographic deployment where a decentralized attribute key is used for encryption. A script interpreter is used for implementing ciphering processes to ensure the secret sharing of private data. Lyu et al. [24] have used a combined regulation scheme using threshold secret sharing over blockchain miners and regulatory authority. Further steganography-based blockchain schemes are also noted to be implemented in the existing system. According to this process, the embedding capacity of the host data is initially computed, followed by hiding the secret information and then formulating a blockchain network. The work by Mohsin et al. [25] used Particle Swarm Optimization for carrying out the image steganography process over a blockchain. Sarkar et al. [26] have developed a decentralized network of steganography blockchains. The secret shared key is used for further encrypting the stego-image. The outcome of the study is known to offer a higher payload. The work carried out by Giron et al. [27] has investigated steganographic structures over blockchains using Least Significant Bits over bitcoin. However, the adoption of cryptographic techniques is also associated with various limitations, as follows:

- Expensive Nature: Various studies, for example [27]-[29], have used sophisticated forms of public key encryption, which not only necessitate higher maintenance costs for key infrastructure management but also result in delays.
- Attack-Specific Solution: Most cryptographic-based approaches are highly effective at identifying and stopping predefined attacks [29]-[31], but they have received little attention regarding new evolving threats or dynamic attacks.
- Challenges in Accessibility: In the event of a network attack, data or services may be difficult to access due to the use of digital signatures or potential encryption in a critical time frame.

B. Blockchain Features

Blockchain technology has the following critical characteristics:

1) Security: Due to the usage of asymmetric cryptography, blockchain systems are intrinsically safe. Asymmetric cryptography consists of a series of public keys visible to everyone and private keys only visible to the system's owner. Using these keys, you can confirm that you own the transaction and cannot be tampered with [32]-[34]. The decentralized structure of blockchain systems, which utilize peer-to-peer (P2P) consensus processes, removes single points of failure for data compared to centrally kept data and

hence is substantially more susceptible to being compromised [34].

2) Disintermediation / Decentralization: Decentralization gives users data control and reduces the need for strong central authorities, making the system more equitable and secure. The blockchain system is more reliable and robust because each distributed node is mainly autonomous and has equal obligations and rights. If one distributed node fails, the entire network is not affected [33]. The blockchain's distributed information eliminates data loss or destruction due to reliance on a centralized place and eliminates misuse of information. Decentralized transaction execution and validation reduce intermediary costs and improve performance at central servers [33].

3) Transparency: The blockchain ledger allows anybody to see the history and specifics of each transaction. This amount of transparency is unheard of in massive financial systems. This kind of openness is achieved using a blockchain network with numerous validating peer nodes and no central authority [35]. Aside from the economic suitability of large corporations, the transparency feature has found application in healthcare and clinical trial data disclosure. Individual patients can utilize blockchain technology to readily examine their claims, medical history, transactions, and past-due payments. Researchers, doctors, and patients have long kept clinical trial data secret, causing a lack of trust in findings [36]. The transparency of blockchain has been found to assist supply chain management malpractices and product history obscurity [36]. Transparency may also help ensure fair elections and increase voter confidence [29].

4) Autonomy: Trust is established between the parties in most transactions, ensuring mutual commitment. Trust is no longer an issue with blockchain technology. The blockchain can work as a P2P system without a responsible third party. Participating nodes on the blockchain system using advanced distributed consensus algorithms [33] to handle the owner confirmation problem in transaction processes while maintaining system integrity. These blockchain transactions are executed without the intervention of a third party due to failsafe consensus mechanisms [36].

5) Immutability: It is also referred to as unforgeability, untameability, immutability, and persistency. Immutability indicates that it cannot be changed or interfered with once data is added [34]. To prevent tampering, data blocks in a blockchain structure are timestamped and encrypted with a hash algorithm [33][36]. However, immutability poses its own difficulties and obstacles for blockchain technology, and some are now questioning its benefits [37].

6) Traceability: Transparency is the capacity to track data's origin, destination, and update sequence between nodes. While data traceability is required to ensure data integrity and trust, it also improves data governance, compliance with legislation, and understanding of the impact of change [37]. Data traceability is supported by blockchain technology due to the time stamping of data updates and additions.

7) Anonymity: Blockchain's anonymity protects privacy against unlawful entry or surveillance. To maintain anonymity, transactions must be authorized without revealing personally identifiable information about the parties involved. The data is shared between nodes utilizing a trust-based method. Thus, node information is not disclosed or validated, and the data transfer is anonymous [38]. Users can communicate with produced blockchain addresses to hide their real identities. However, due to the public and distributed nature of the blockchain, total privacy cannot be guaranteed.

8) Democratized: P2P voting allows all nodes in a blockchain system to make choices democratically. Decentralized nodes employ consensus processes to enable particular nodes to introduce additional blocks to an existing blockchain, ensuring the bitcoin is correctly recorded to the shared data ledger, and its duplicates are perfectly synchronized. Nodes can accept blocks by extending them and reject incorrect blocks by not extending them [39].

9) Integrity: Blockchains are designed to resist data modification. Data integrity ensures data accuracy and consistency throughout its life cycle [35]. To do this, the blockchain network uses decentralized, immutable shared ledgers. Once a data block is approved to be included in a blockchain, it cannot be modified or amended. As a result, data reliability and integrity are essentially guaranteed [33].

10)Programmability: A standard application programming interface, API, allows users to design apps using blockchain technology. Smart contracts and decentralized apps can be created using the flexible scriptwriting framework. A programming interface for network administration is provided by the node software-defined networking (SDN) controllers [32]. Users, data query layers, infrastructure layers, and existing database layers are all data structuring provenance proposed by authors [40]. All blockchain systems provide a scripting language [41]. Authors in [32] recommend a user-friendly API. Ethereum, Tron, and Cardano are examples of programmable blockchains.

11)Fault tolerance: Blockchain is designed to be redundant and inefficient to enable excellent fault tolerance and immutability [42]. The P2P architecture of the network allows each node to act as both a client and a server, giving the network an extremely high error margin for node failures and network transit issues [42]. Blockchain is supposed to be Byzantine Fault-Tolerant, meaning that even if some nodes are down or functioning incorrectly, the network will still reach a consensus.

12)Automatic: Using specialized consensus protocols, all nodes in the system may validate and transact data automatically. Blockchain is managed and confirmed without manual involvement by a protocol [41].

C. Types of Blockchain

Blockchain can be divided into public and private categories: A public blockchain is a permissionless distributed ledger. Anyone with an internet connection must sign up on a blockchain platform to join the network. As it is primarily

used for cryptocurrency mining and trading, a public blockchain user or node can access past and present data, validate transactions, and mine cryptocurrencies. The most common public blockchain is bitcoin and Litecoin. A private blockchain is typically utilized within an organization or industry where only a small number of individuals are allowed to participate in a blockchain network instead of a public blockchain. Both public and private blockchains are further divided into permissioned and permissionless blockchains. Table I compare and contrast the permissions of various blockchain types:

Another form of blockchain is called a hybrid blockchain which integrates private and public blockchains. Users can control who has access to the blockchain data. Encrypted data can be made public while the remainder of the blockchain remains secret. Due to the flexibility of the hybrid system, users can quickly join a private and public blockchain. An example is the Dragonchain. The similarities and differences between different types of blockchains are illustrated in Table II.

Currently, various scientific research contributions are made toward the above-mentioned different forms of blockchain. Table III highlights the frequently encountered problems being addressed by notable researchers using multiple blockchains.

TABLE I. PERMISSIONS OF VARIOUS BLOCKCHAINS

Public and Permissioned	**Public and Permissionless**	**Private and Permissioned**	**Private and Permissionless**
Restricted and open	Transparent and open	Restricted (hybrid methodology)	Read transparent but restricted
Read restricted and write all	Read all and write all	Read restricted and write restricted	Read all and write restricted
All can connect and transact, but read and audit is limited to permissioned users only	All can connect, transact, audit, and read	No one is allowed to connect, transact, audit, and read	All can connect, none is allowed to transact, and all can audit and read
Full write equity	Strictly democratic owing to total equity	Restricted	Full read equity
Example: Ethereum	Examples: Litecoin, Ethereum, and bitcoin	Example: Corda, Hyperledger Fabric, and R3	Example: Hyperledger Fabric

TABLE II. PERMISSIONS PERSPECTIVE OF SIMILARITIES AND DIFFERENCES OF BLOCKCHAINS

	Public	**Private**	**Hybrid**	**Consortium**
Membership	Unidentified Permissionless Can be malicious	Identified Permissioned Trustworthy	A mixture of Permissionless and Permissioned Identified Trustworthy	Permissioned Identified Trustworthy
Consensus Methodologies	PoW, PoS, Proof-of-Authority, Proof-of-Elapsed time, etc.	Voting or multi-party consensus Algorithm	Private Sidechains Consensus Mechanisms	Multi-party consensus algorithm or voting
Speed of Transaction	Time-consuming	Faster and lighter	Faster and lighter	Lighter and faster
Consumption of Energy	Huge energy consumption	Small energy consumption	Small energy consumption	Small energy consumption
Data in Blockchain	No finality 51% attack	Enable finality	Enable finality	Enable finality
Network	Decentralization	Partial decentralization	Partial decentralization	Partial decentralization (Hybrid between Private and blockchain)
Description	Anyone can write and read on the network, irrespective of its location. Data is validated by each network member ("node").	Permission to write and read data onto the blockchain is controlled by a "highly trusted" organization - the blockchain owner.	Controlled Permission on Read and Write.	Permissions to validate, write and read on the blockchain are regulated by some predetermined nodes, which might not be the same for every blockchain entity.
Benefits	- Secure - Transparent	- Efficient - Private	- Access control - Better performance - Scalability	- Efficient - Private
Challenges	- Inefficient -Performance -Scalability -Security	- Controlling (power is confined to one organization only) - Challenging to align several organizations to use a single blockchain - Trust - Auditability	- Difficult to align many organizations (Especially Competitors) & Set Consensus rules to join the blockchain as board members & share their data.	
Use Case	Cryptocurrency Document validation	Supply chain Asset Ownership	Medical Records Real Estate	Banking Research Supply chain

TABLE III. EXISTING RESEARCH CONTRIBUTION FROM VARIOUS TYPES OF BLOCKCHAIN

	Authors	Problems	Methodology	Advantage	Limitation
Public Blockchain	Lee et al., 2019 [43]	Immutability	Hashing, sidechains	Higher scalability in design	Model not benchmarked
	Guo et al., 2019 [44]	Storage optimization	Redundant Residual Number System	Highly fault-tolerant	No comparative analysis
	Baza et al., 2021 [45]	Security in ride-sharing applications, fair payment	Analytical modeling based on trust, reputation	Ensures privacy preservation	Lacks comparative analysis, no extensive analysis towards security
	Asheralieva and Niyato, 2021 [46]	Resource management	Stochastic Stackelberg game, deep learning	Effective convergence performance	Success depends on a singular environment
	Mohammadzadeh et al., 2021 [47]	Invoice factoring	Smart contract management, Diffie-Hellman Key exchange	Highly simplified implementation scheme	Involves extensive time for signature verification
	Cai et al., 2021 [48]	Data privacy in crowdsensing	Open service system, private blockchain, SHA-256	Offers better verifiability, trust, and robustness	Assumption depends on the discretion of the client and could narrow down to the centralized crowd
	Bai et al., 2022 [49]	Participation of public	Consensus algorithm	Address scalability issues	Couldn't resist other forms of attacks apart from Denial of Service (DoS)
Private blockchain	Wu and Tsai, 2019 [50]	Securing agriculture network	Dark web technology	Effective privacy preservation	Resistive against only Distributed Denial of Service (DDoS) attack
	Hou et al., 2021 [51]	Data tampering in Internet of Things (IoT)	Secure consensus network	Better latency performance	Demands predefined information of the incoming malicious transaction
	Toyoda et al., 2020 [52]	Bottleneck analysis of private blockchain	Analytical framework on Ethereum	Better throughput performance	Doesn't exhibit extensive analysis with comparison
	Xu et al., 2021 [53]	Privacy on data sharing	Publishing protocol using histogram	Ensure data anonymity	Highly complete encryption scheme for large network
	Huang et al., 2020 [54]	Consensus problem	Analytical approach using the probability of network splitting, time out period of election, and rate of packet loss	Optimizes consensus algorithm	No comparison with the existing consensus-based approach
	Chattaraj et al., 2022 [55]	Access control in Software-Defined Network	Access control using a certificate, attribute-based encryption	Applicable for next-generation network	Not resistive against dynamic attackers
	Baucas et al., 2021 [56]	Monitoring of smart homes	Trilateration using the received signal strength indicator	Highly reduced execution time	Not benchmarked
	Shah et al., 2021 [57]	Resource optimization in a power grid	Heuristic approach	Reduced computational time	Demands extensive resources to process
Hybrid blockchain	Kim et al., 2022 [58]	Interoperability in heterogeneous hybrid blockchain	Analyzing multiple blockchain architecture	Identified tradeoffs in existing blockchains	Study applicable to a specific form of blockchain
	Liu et al., 2020 [59]	Energy management	Stackelberg game, blockchain	Optimal energy scheduling	Utility allocation is based on limited constraints
	Akkaoui et al., 2020 [60]	Data exchange in healthcare	Blockchain and edge computing	Significant reduction in execution time	No comparative analysis to prove its effectiveness
	Polge et al., 2021 [61]	Extensibility of blockchain operation	Emphasizing upper layers with real network infrastructure	Enhanced rate of propagation	Complex deployment cost, specific to the bitcoin application
	Zhu et al., 2020 [62]	Leveraging Crowdsensing operation	Blockchain and crowdsensing, dual consensus protocol	Extensive privacy protection	Cannot resist dynamic attacks
	Subramanian et al., 2021 [63]	Supply chain in pharmacy	Cryptocurrency, mobile application	Offers reliable suggestions for critical illness	Not assessed for a large number of operations
	Fan et al., 2021 [64]	Privacy in IoT	Federated learning, reverse auction	Offers better computational efficiency	Not assessed for a large number of operations
	Zhang et al., 2021 [65]	Controllable decentralization	Unique account scheme, an unspent transaction output	Enhance transaction processing	Higher maintenance cost
	Subramanian and Thamppy, 2021 [66]	Tracking automobiles	Ethereum blockchain, Truffle platform, Astute contract	Transaction transparency	Not assessed for a large number of operations
	Cui et al., 2020 [67]	Authentication in sensor network	Local and public chain, mutual authentication	Better security performance	Doesn't address resource demands

From the above table, it is noted that various significant research work is being evolved to improvise the performance and address multiple problems on different taxonomies of blockchain. Irrespective of various methodologies being adopted, it is observed that almost all the existing approaches toward different types of blockchains are witnessed with limiting factors. The most prominent limiting factor is narrowed implementation scope, where the system model's performance is not practically or mathematically proven for its efficiency over a large-scale deployment environment. Apart from this, the lack of benchmarking is another questionable factor towards reliable implementation over ground reality.

III. Blockchain Architecture

Blockchain is a decentralized database organized in a linked list of blocks, as shown in Fig. 4. Block: A block is a set of valid transactions [68]. In a blockchain system, each node can initiate an exchange of information and broadcast it to all other nodes in the network. The network nodes use past transactions to validate the transaction, and after the transaction is validated, it is added to the current blockchain. The number of transactions is aggregated and inserted into the blockchain block depending on the time window. "A block may include more than 500 transactions on average," according to bitcoin, "and the average block size is roughly 1 MB, an upper bound proposed by Satoshi Nakamoto in 2010" [69]. The type of blockchain used determines the type of data recorded within a block. In the case of bitcoin, a block comprises sender information, receiver information, and the number of bitcoins to be transmitted. The Genesis Block, often known as block 0, is the foundation for all subsequent blocks in a blockchain. In the chain of blocks, each new block is linked to the previous block by a connecting link, as shown in Fig. 4.

As illustrated in Fig. 5, each block has a header and a body. The block header (Fig. 5) contains metadata about the block, such as the previous block's hash, the nonce, the Merkle tree root, and the date.

- Previous block hash: Every block in the blockchain derives from the block before it in the inheritance chain, as shown in Fig. 6. The blockchain system is tamper-proof by using past blocks' hash to generate the new ones' hash.
- Mining statistics used in the block construction: The technique must be complex enough to prevent tampering with the blockchain.
- Bitcoin Mining: Using the previous block hash value, the transaction root hash value T, and the nonce value $nonce$ obtained by solving the consensus method, the current block hash value is calculated using (1).

$$H_k = Hash(H_k - 1|T|\ |nonce|) \quad (1)$$

- Merkle Tree Root: A Merkle tree structure organizes the transactions. The Merkle tree's root is a verification of all transactions. The Merkle root illustrated in Fig. 7 is utilized to build the block hash.

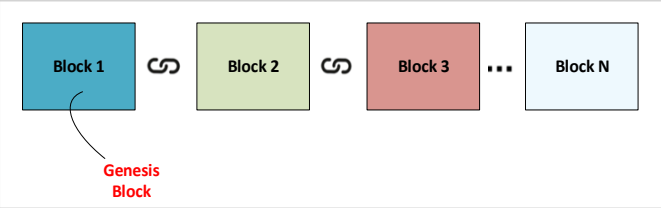


Fig. 4. Blockchain: a Chain of Linked Data Blocks.

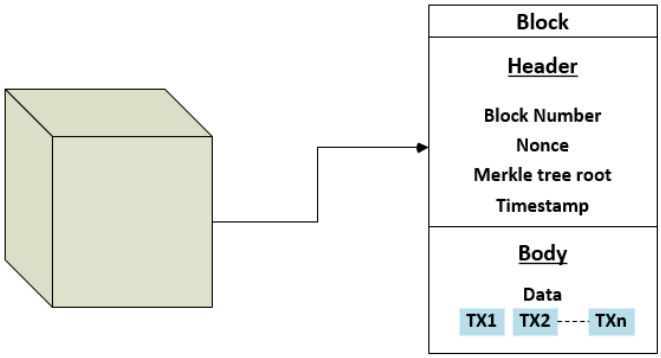


Fig. 5. Structure of a Block.

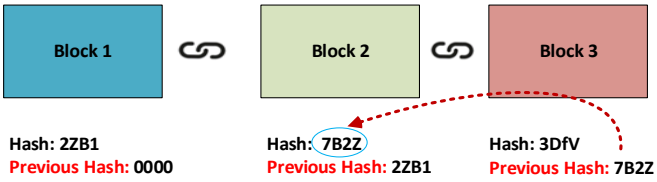


Fig. 6. Blocks Linked by Reference to the Previous Block Header Hash.

Blocks are linked together in a "chain," as depicted in Fig. 8, by incorporating the previous block header hash. This preserves the chain's integrity because modifying one last block will necessitate updating every subsequent block.

Blockchain technology is based on three fundamental principles: transparency, authenticity, and auditing. Its transparent and encrypted chain design allows everyone to witness the information flow between numerous blocks with all the details. It is like a well-connected distributed network. At the start of every new transaction, every computer database competes with all other databases to produce a new block with the necessary features. The database that successfully solves the mathematical coding and creates the block wins. This block is audited and authenticated by the other blocks. After all the blocks confirm the transaction, the data is encrypted but transparently stored in the database. Auditing and authentication processes are automatically initiated and run in the background for every block. Blocks are connected in an appropriate linear, chronological sequence, with every block holding a hash of the previous block. The transition history is still available in other blocks even if the initial original traction block is removed or hacked. As illustrated in Fig. 8 and Fig. 9, the blockchain architecture comprises six significant components integrated into the many layers of the blockchain.

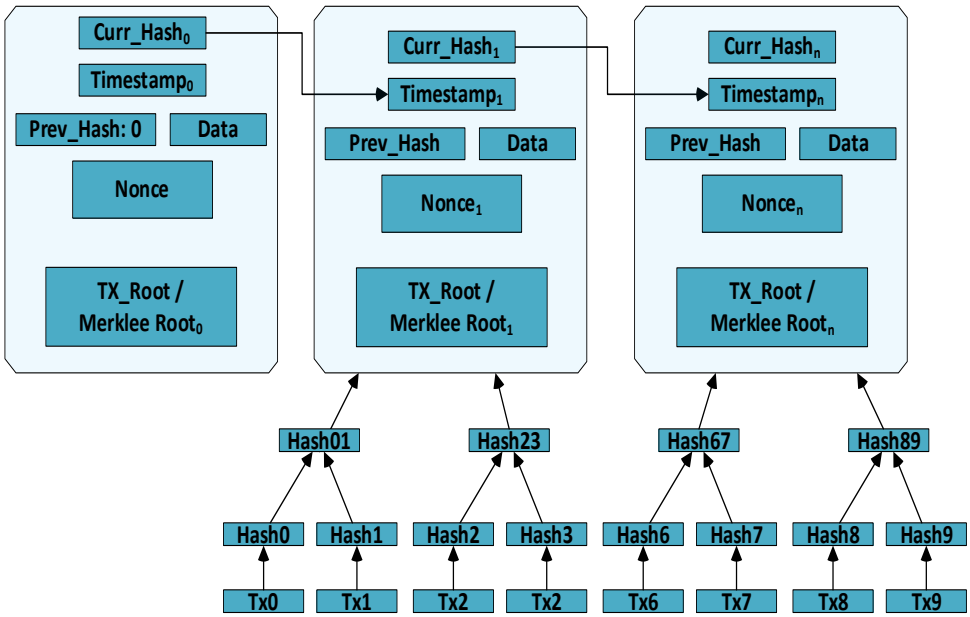


Fig. 7. A Merkle Tree Example (Binary Hash Tree).

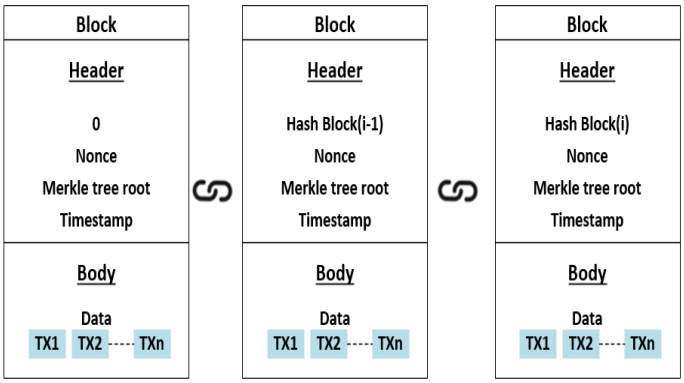


Fig. 8. The Architecture of a Data Chain in a Blockchain Network.

1) Data layer: This layer comprises the chained data blocks and the techniques that go with them, like hash algorithms (e.g., SHA256 [75]), timestamp technologies, asymmetric encryption (e.g., Elliptic Curve Digital Signature Algorithm (ECDSA) [76]), and Merkle trees [77]. Each node employs various strategies to encapsulate transactions and received code in new blocks, including the hash function and Merkle tree. Each block is given a timestamp showing when it was created. After that, this new block will join the chain by connecting to the original block [70].

2) Network layer: The network or the P2P layer handles inter-node communication. It handles block propagation discovery and transactions. Also known as propagation, nodes cannot discover each other and synchronize without this P2P layer.

3) Consensus layer: This layer contains several consensus techniques (such as Proof-of-Stake (PoS) and PoW [76]) for maintaining data consistency and fault tolerance in distributed networks.

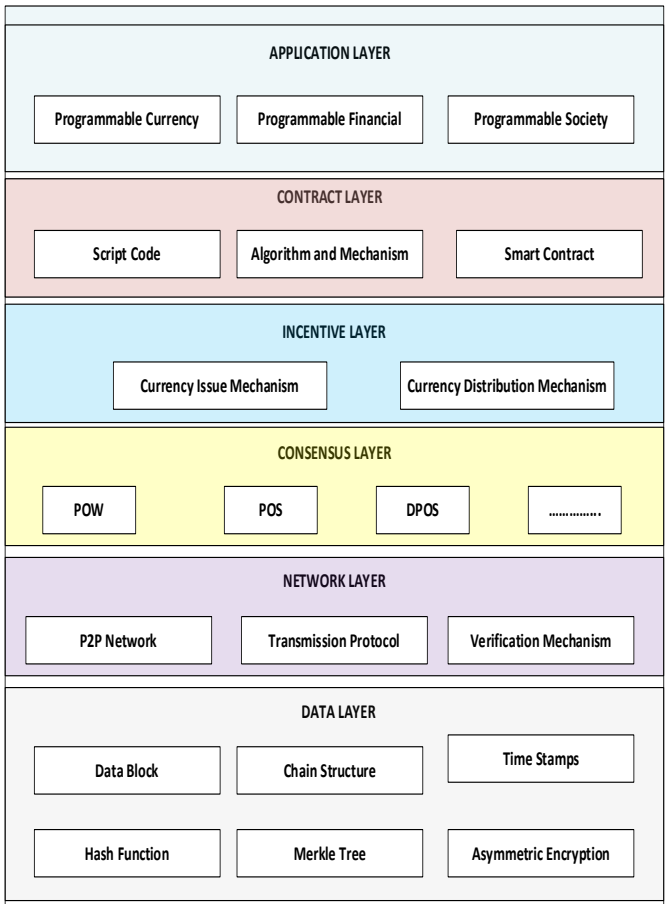


Fig. 9. Blockchain Layered Architecture.

4) Incentive layer: With this layer, the blockchain's security verification can be strengthened by offering specific incentives to nodes cooperating in security verification. This layer incorporates economic rewards into the blockchain, the

currency distribution system, and the currency issue mechanism to ensure that individuals who help generate the next block receive a possible benefit [70]. Miners (the creators of new blocks) are rewarded with incentives (some coins) to encourage the network to continue working on data verification and ensuring the chain's security [71].

5) Contract layer: In this layer, there are a variety of scripts and algorithms, as well as smart contracts, which are self-executing code that is saved and secured by the blockchain.

6) Application layer: This layer consists of potential applications, scenarios, and use cases [70], among other things.

A. Components of Blockchain

A blockchain comprises many different components, each serving a specific purpose in its creation. These components are [72]:

1) Ledger: A blockchain ledger is a distributed, immutable record of its history used for decentralized data storage.

2) Peer network: A P2P network is a distributed network architecture that allows participants to share resources. The participants make their resources (such as storage capacity, processing power, link capacity, printers, etc.) accessible to other participants at their leisure. Each peer (participant node) in such a network performs the functions of both (server and client).

3) Membership services: Some blockchain types require prior authorization to participate. Indeed, membership services on the blockchain are responsible for authorizing, authenticating, and managing users' identities.

4) Smart contract: It is a self-executing contract in which the agreement's terms are encoded in lines of code that both parties can read and comprehend. Put another way. It is the digital equivalent of a traditional paper contract. Nick Szabo, an American computer scientist and digital currency researcher, suggested smart contracts in 1994. The smart agreement is executed over a blockchain network, duplicating its code throughout the network's machines. This makes it possible to be secure and transparent and facilitate contractual obligations.

5) Wallet: Stores key pairs and users' credentials to initiate and sign digital transactions.

6) Events: Refers to notifications of blockchain updates and activities; examples of events include adding a new block to the blockchain, alerts from smart contracts on the blockchain that enable such contracts, and the creation and propagation of a transaction made across the peer network.

7) Systems management: Blockchain is a constantly growing system that must evolve to suit its participants' needs. Indeed, systems administration provides the capability to update, monitor, and build blockchain components to suit users' needs.

B. Consensus Algorithms

A consensus technique is used in the blockchain network to reach a consensus on the status of the distributed ledger [73]. With no central authority, all network participants should collaborate to make the best choice for the network. In a context where strangers do not have faith in one another, achieving consensus among participating nodes was perhaps the most significant development that opened the way for blockchain and resulted in a set of methods to reach an agreement among participating nodes. Consensus mechanisms are communication protocols that allow robots or humans to operate together decentralized. Fig. 10 depicts our classification of the blockchain consensus model, developed after surveying the literature. As shown in Fig. 10, consensus models may be divided into nine broad groups with some different varieties based on subtle changes in how they operate.

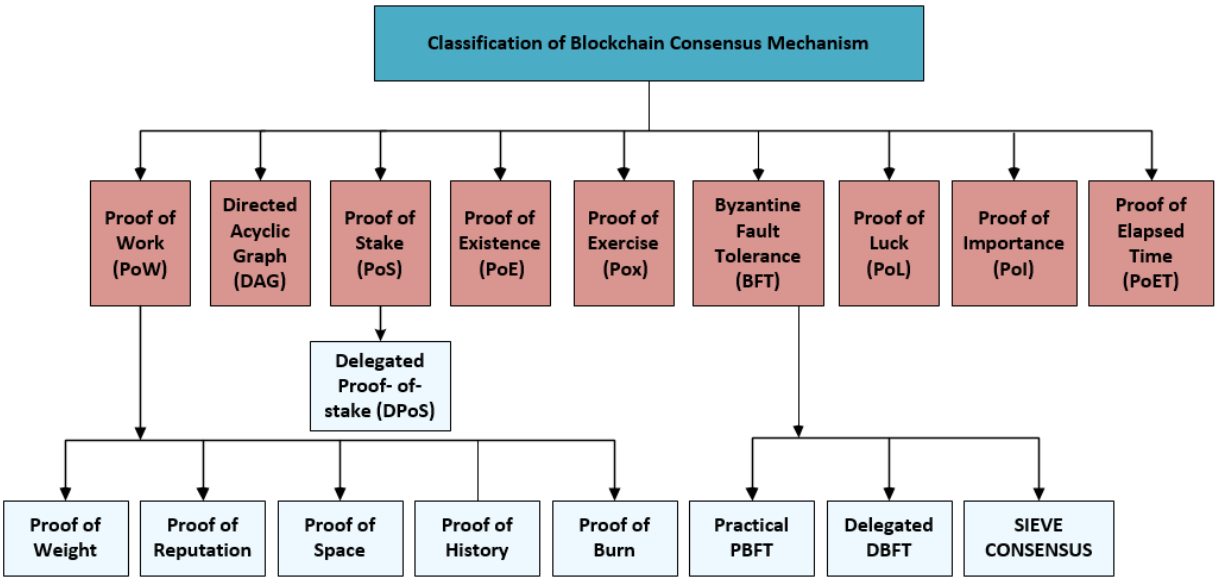


Fig. 10. Blockchain Consensus Algorithms.

TABLE IV. COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS

Consensus Algorithm	Chief Characteristic	Fault Tolerance	Scalability	Power Consumption
Proof-of-Work (PoW)	Power of computation	Poor	High	Enormous
Directed Acyclic Graph (DAG)	Consensus for IoT blockchain	NA	Very high	High
Proof-of-Stake (PoS)	Stake in terms of the number of coins	Less than 51 per cent stake	High	Poor
Proof-of-Existence (PoE)	Use the timestamp of the transaction to validate document existence	NA	Unknown	Unknown
Proof-of-eXercise (PoX)	Miner shall solve a matrix-based problem	NA	Unknown	Fractional energy saving
Delegated Proof-of-Stake (DPoS)	Voting to choose the witness node	Less than 51 per cent of validators	High	Poor
Proof-of-Elapsed Time (PoET)	Lottery based election	Yes		Massive
Byzantine Fault Tolerance (BFT)	Reach consensus despite the failure of some nodes to respond	33 per cent of nodes are Faulty	Poor	Poor
Delegated Byzantine Fault Tolerance (DBFT)	Reach a consensus with Untrustworthy participants	Less than 33 per cent of replicas	Low	Medium
Proof-of-Importance	Estimate importance counts coins that have been in an account for a fixed period	Unidentified	Moderate	Low energy saving
Proof-of-Luck	Cumulative luck value	NA	It does not scale well	Reduced power of computation

Table IV compares consensus algorithms based on essential criteria such as consensus model prominence, scalability, and fault tolerance.

1) Proof-of-Work: PoW is widely considered the blockchain's fundamental consensus model. PoW is built on the idea of competing for computational power to create new blocks in the blockchain. This approach requires a miner to compute and output a value. The winning value is lower than the value set by the network. PoW through the nodes is used to deal with forking (i.e., two nodes provide the winning value). The research community has developed various PoW techniques [73], such as:

a) Proof-of-Weight: Based on algorithm consensus, Proof-of-Weight consensus adds "weight" to the essential principle of PoW. These weights are proportionate to the values generated by the nodes in the network. The goal is to avoid "double-spending," where a consumer can use the same digital token twice by adding relative weight.

b) Proof-of-Reputation: A node's reputation is built by participating in transactions and holding assets. Blockchain validates a new block created by the highest reputation node. This technique prevents nodes from a reputation for prior misbehavior and adds to the blockchain's security.

c) Proof-of-Space: It is a PoW where a node requesting service must allocate more disc space than usual. This data is given to the verifier node to prove that enough space is allocated for a service request.

d) Proof-of-History: This consensus approach demands nodes to offer evidence of history. It establishes a historical record to prove an event that happened at a particular time. This is an alternative to trusting the transaction's timestamp.

e) Proof-of-Burn: This consensus method relies on burning coins to mine the next blockchain block and sending bitcoin to an unrecoverable address. Nodes burn more coins to increase lottery odds. Compared to PoW, Direct Acyclic Graph (DAG) is advocated as a viable blockchain consensus method for the IoT blockchain framework (IOTA). Scalability is an advantage of DAG since data is uploaded to the blockchain in parallel. It adds a block to the ledger as the previous transaction is processed. DAG also combats "double-spending" using powerful algorithms.

2) Proof-of-Stack: This method avoids the need for expensive mining equipment. A PoS node can execute mining or block validating based on its stake [74]. PoS recommend buying cryptocurrencies to increase block formation chances.

a) Delegated Proof-of-Stack (DPoS): It is a PoS variant where participants are encouraged to vote for the witness node, which will generate a block in the blockchain and serve as a witness [94]. The witness node is paid for producing blocks but is barred from future voting if it cannot create blocks.

3) Proof-of-Existence (POE): It is a system for authenticating the presence of documents at a specific time. Without releasing the data itself, data ownership information might be revealed. This POE paradigm helps show the existence of intellectual property documents such as patents.

4) Proof-of-Exercise (PoX): It offers a Proof-of-Exercise alternative to the PoW [95]. An exercise in PoX is a matrix based on a real-world scientific issue. It works on matrices created by system employees. Ribonucleic acid (RNA) and Deoxyribonucleic acid (DNA) sequencing and data comparison are excellent examples of matrix problem-solving.

5) Byzantine Fault Tolerance (BFT): System failure due to Byzantine fault in blockchain requires consensus [73]. Even if some nodes fail to reply, the network should reach an agreement and maintain data consistency. The distribution system makes it difficult.

a) Practical Byzantine Fault Tolerance (PBFT): Authors in [87] suggest PBFT in their work. Authors in [75] offer the first state-machine replication mechanism for asynchronous networks - a distributed file system with BFT.

b) Delegate Byzantine Fault Tolerance (DBFT): The DBFT described in the NEO whitepaper is a variation of the traditional BFT [76]. NEO blockchain's core library is currently utilizing this technology. According to them, a novel mathematical model may be used to test consensus behavior when combined with a discrete model. When compared to other algorithms, this method is more capable of coping with participants who are not trustworthy.

c) Sieve consensus: Sieve is a form of PBFT consensus for non-deterministic chain code execution [77]. Replicates can create non-deterministic chain code output. The sieve can assess the output if a small number of replicas show minimal divergence.

6) Proof-of-Luck (PoL): A new consensus approach reduces the necessary processing power and increases transaction throughput [78]. This algorithm is based on Trusted Execution Environment (TEE). PollRound and PollMine are the primary functions where each block is given a luck value between 0 and 1. The total of all luck values included within each blockchain block is combined to provide a cumulative luck value. A miner will choose to join the luckiest chain.

7) Proof-of-Importance (PoI): New Economy Movement (NEM/ XEM) uses this algorithm. This system assigns a rating to accounts based on the number of vested and unvested coins. PoI measures "importance" by how long a node's coins have been in their account. Every day, 10% of the current unvested sum becomes vested. It also depends on the account's position within the network and the number of coins vested.

8) Proof-of-Elapsed Time (PoET): For each block, a new leader is chosen by a lottery system under this consensus option. TEE is used to ensure the integrity of the electoral process. The basic steps in choosing a leader are as follows:

- It runs on miner and validator nodes.
- The validator node with the least wait time wins the election as a leader node.

The fundamental disadvantage of this consensus technique is that it requires specialized hardware [74]. A good consensus algorithm is efficient, safe, and easy to implement. Recently, efforts have been made to improve the consensus algorithms used in blockchain technology. New consensus mechanisms are being developed to solve some challenges associated with the technology. The central concept of PeerCensus [79] is to isolate block generation from transaction confirmation to boost the consensus speed dramatically. An improved consensus algorithm for ensuring blocks is produced orderly and predictable has been suggested by authors in [80]. Bitcoin's security is known to be compromised by fast block production. The Greedy Heaviest Observed Subtree (GHOST) chain selection rule [81] was devised to address this. It weighs the branches so that miners can choose the best one. Authors in [82] proposed a consensus protocol that rewards non-interactive retrievability evidence for P2P blockchain networks. Miners save storage space by storing old block headers instead of complete blocks.

IV. Blockchain Framework and Platform

A blockchain framework is a software system that facilitates the deployment and creation of blockchain applications. The blockchain frameworks provide infrastructure and libraries for application development. Nodes and the software they run make up the network infrastructure. The node can be physical, virtual, or containerized. Blockchain identity management is controlled by software that provides capabilities and features such as transaction data, user identification, and the consensus mechanism for blockchain. A smart contract application is composed of code that operates within its architecture. The client application communicates with the infrastructure. The latter serves as an external interface to the application. Developing applications outside the blockchain network should be possible with a good blockchain platform. As long as the program works on a small network, it should work on a more extensive infrastructure [83]. Before developing the software, there is no need to set up the network infrastructure. Choosing an enterprise blockchain framework is difficult because no single framework has all the functionalities. As demonstrated in Fig. 11, the primary blockchain framework challenges are storage, processing power, and scalability.

Fig. 11. Blockchain Computational Complexity.

Stakeholders must be highly cautious before, during, and after using blockchain in the enterprise. Many factors must be addressed while selecting a blockchain framework. Table V shows some of the selection criteria for blockchain frameworks.

TABLE V. Standards of Selection for Blockchain Frameworks

Criterion	Explanation
License	Features and kind of license (paid or free)
Activity	Framework upgradability support
Support model	Framework support, popularity, longevity
Roadmap	Framework roadmap and vision
Reliable backing	Corporate or open-source community
Ease of use	Intuitive and widely adopted

This section describes the most popular blockchain frameworks and platforms and is as under:

1) Bitcoin - (programming language: C++): It is the world's first and most popular cryptocurrency. Someone or a group using the pseudonym Satoshi Nakamoto established it in 2009. Cryptocurrencies like Ethereum, Litecoin, Dash, and

bitcoin cash are the blockchain's descendants. Bitcoin is a P2P electronic payment system that does not require a central clearing agency. Cryptocurrency users execute transactions by sending electronic instructions that specify who should be credited and debited and where the change should be deposited (if any). The pros and cons of bitcoin are depicted in Table VI.

TABLE VI. ADVANTAGES AND DRAWBACKS OF BITCOIN

Advantages	Drawbacks
Payment flexibility	Volatility and risk
Security and control	The size of the blockchain is about 242.2 GB
High capitalization	Time-consuming (7 transactions per second)
Minimal commission fee	Complete lack of fully-fledged smart contracts
Large-scale trading	Lack of understanding and awareness

2) Ethereum – (programming language: Go, Solidity): Ethereum is a framework with an open code for developing and launching almost any decentralized online services for a blockchain (DApps), whose work is based on smart contracts. Ethereum is a cryptocurrency that is built on the Ethereum blockchain. Vitalik Buterin made an offer in 2013 that was accepted. There are four chief components in Ethereum:

- Instead of designing different frameworks for each application or language, EVM allows all of them to be used on one blockchain. This helps create DApps in lotteries, for example.
- Smart Contracts are computer algorithms for trading gold, cryptocurrency, and other assets without a third party. If the smart contract's code's criteria are met, it executes automatically.
- DApps use smart contracts for market predictions, digital signatures, and asset transfer assurances. Most existing DApps utilize Ethereum.
- Network performance is improved via a collection of programming solutions. Ethereum now leverages Merkle trees to improve transaction hashing and scalability [108].

The pros and cons of Ethereum are depicted in Table VII.

TABLE VII. ADVANTAGES AND DRAWBACKS OF ETHEREUM

Advantages	Drawbacks
Capitalizes on blockchain	Slow transaction processing
With a $9.7 billion market worth, it's backed by huge names such as JPMorgan Chase, Amazon, Microsoft, IBM, etc.	Centralization - The Data Access Object (DAO) attack emphasized the importance of developers' word over community votes
Daily traffic	PoS update
A powerful team	The downside of being the first mover
Reliable	Scams in the marketplace

3) Tezos - (programming language: OCaml): It is an innovative contract platform created in 2014. In Leased Proof-of-Stake (LPoS), a participant makes a new block, which thirty-two other participants accept. Tezos has certain unique features that set it apart from other platforms:

- Formal verification of smart contract code.
- It is possible to upgrade the network without branching (fork).

The pros and cons of Tezos are depicted in Table VIII.

TABLE VIII. ADVANTAGES AND DRAWBACKS OF TEZOS

Advantages	Drawbacks
Community Governance (The protocol rewards its community for conducting needed or desired improvements)	In-Fighting (After its successful ICO, Tezos experienced a lot of conflict between the Tezos Foundation and the Breitmans' company in the US)
Supportive Community	Token Issuance Delays
Formal Verification	Lawsuits

4) Hyperledger (Sawtooth, Fabric, Burrow, Indy, Iroha, Cello): It is not a coin, a blockchain, or a firm, but a complex project of the Linux Foundation (Fabric, Sawtooth, and Burrow). It is a kind of open-source platform for developing enterprise blockchain applications which began in 2015. The pros and cons of Hyperledger are depicted in Table IX.

TABLE IX. ADVANTAGES AND DRAWBACKS OF HYPERLEDGER

Advantages	Drawbacks
Modularity in architecture	Intricate fabric architecture
Performance optimization	A shortage of verified use cases
Hybrid model	Fault tolerance in the network
Membership with permission	A lack of expertise among programmers
Query capability resembling SQL	

5) Hedera Hashgraph: The platform is still in the early stages of development. Histogram consensus is used by the Hedera PoS open network to ensure maximum security (ABFT) while consuming little bandwidth. The pros and cons of the Hedera Hashgraph are depicted in Table X.

TABLE X. ADVANTAGES AND DRAWBACKS OF HEDERA HASHGRAPH

Advantages	Drawbacks
Highly secure	Not open-sourced but patented
Faster: Transactions being processed in parallel	There are only 19 governors, which brings decentralization into question
The platform supports the same object-orient programmed language, Solidity, which is used for smart contracts	Lack of proven use cases

6) Ripple - (programming language: C++): Its unique feature is the absence of blockchain. Instead, it "runs a network of independent checking nodes." People, banks, organizations, and states can check nodes. A distributional

registry is created every second, and XRP is the cryptocurrency token. The pros and cons of Ripple are depicted in Table XI.

TABLE XI. ADVANTAGES AND DRAWBACKS OF RIPPLE

Advantages	Drawbacks
Transactions with XRP are quick and inexpensive	The consensus protocol appears to be potentially less secure
The use of Ripple's payment network has already begun in financial institutions	Numerous Ripple's financial partners exclusively use RippleNet, not the company's XRP cryptocurrency
Small company owners and consumers can utilize XRP to conduct safe money transactions	Ripple has sparked controversy due to its private ownership and the Securities and Exchange Commission (SEC) lawsuit
Currency transfers on a global scale are possible	Purchasing XRP is challenging in the United States

7) Quorum - (programming language: Java): It is an Ethereum fork that maximizes transaction and contract anonymity in banking and related fields. JP Morgan created it to solve critical financial issues with smart contracts and distributional registries. It facilitates institutional volume deals and can restrict access to transaction history while maintaining system openness. When it comes to transaction verification and controlling communication between nodes, they rely on the BFT and Raft transaction algorithms to keep operations private. This solution's flaw is centralization. The pros and cons of Quorum are depicted in Table XII.

TABLE XII. ADVANTAGES AND DRAWBACKS OF QUORUM

Advantages	Drawbacks
Exceptional performance	Framework features are only partially utilized
Consensus mechanisms based on voting	Message overheads
Privacy of transactions and contracts has been improved	Multiple "chosen" nodes confirm transactions.
Blockchain with permission	Anonymit.
	Block size restrictions

8) Corda - (programming language: Kotlin): This is a private distribution platform using Java Virtual Machine (JVM) based smart contract. Corda was created by R3 (R3CEV LLC) to record, monitor, and synchronize financial agreements. For this, a new consensus mechanism was developed, which checks and signs contracts using notarial nodes. Nodes confirming valid interest in the transaction's assets can access the data. The pros and cons of Corda are depicted in Table XIII.

TABLE XIII. ADVANTAGES AND DRAWBACKS OF CORDA

Advantages	Drawbacks
The ability to reach a consensus on individual agreements and contracts	Using oracles (humans) to verify information and papers decreases their credibility
Restricted access	Financial sector-specific
Based on the R3 industry standard	Only financial sector users

9) Electro-Optical System (EOS) - (programming language: C++): EOS is a platform for decentralized applications; Platform rights are shared according to interest. Buying 20% of EOS blockchain firm tokens gives you 20% of the project's revenues, property, copyright, and reputation. The pros and cons of EOS are depicted in Table XIV.

TABLE XIV. ADVANTAGES AND DRAWBACKS OF EOS

Advantages	Drawbacks
Throughput is 1200 transactions per second	There isn't even a Graphical User Interface (GUI) wallet for this project, which is still in development
New crowdfunding model	Crowdfunding conditions might frighten DApp developers
The delegate PoS consensus algorithm has a high scalability potential	The EOS team is slow to report to investors
DApps toolbox for developers	Cryptocurrency is the most criticized

10)Stellar Smart Contracts (SSC) - (programming language: JavaScript, Python, Golang, PHP): The smart contracts used are not Ethereum smart contracts. It is a transactional turing, not a thorough one. SSC can be written in any Stellar language. The pros and cons of SSC are depicted in Table XV.

TABLE XV. ADVANTAGES AND DRAWBACKS OF SSC

Advantages	Drawbacks
Fast Transaction Speed	Less Literature
Multi-currency Support	Smart Contracts issues
Extremely Low Transaction Fees	

11)iOlite - (programming language: iOlite): To create smart contracts using natural language, iOlite provides an easy-to-use engine that understands natural language and compiles smart contract code. Regarding people who do not want to spend time learning, iOlite is a great option - it creates smart contracts. The pros and cons of iOlite are depicted in Table XVI.

TABLE XVI. ADVANTAGES AND DRAWBACKS OF IOLITE

Advantages	Drawbacks
No battery life restrictions or need to recharge	iOlite Vaporizer is more significant than other portable models
iOlite makes it very convenient for use on the go	The vaporizer can become too hot during long vaping sessions
A vaporizer is very compact	Vapor is less dense than other portables
Stylish design that comes in many colors	It does not diminish the effectiveness of the vaporizer
The vapor produced by the model has a fresh taste	

12)Neblio: Incorporating blockchain into existing businesses is the goal of Neblio, which has an easy-to-use API in eight popular programming languages. Neblio's primary

goal is to help established enterprises use blockchain. The Neblio blockchain technology should be accessible to developers. The pros and cons of Neblio are depicted in Table XVII.

TABLE XVII. ADVANTAGES AND DRAWBACKS OF NEBLIO

Advantages	Drawbacks
Easy-to-use	Use of private keys, which are questionable at times
Single token protocol for unique tokens	Immutable Data storage means there is no going back
Secured from third-party intervention	
Users can code in eight different programming languages	

13)Lisk - (programming language: JavaScript): This flexible blockchain technology creates a simple user interface and platform for everyone to use. Lisk begins each app on its independent side chain, the development of which can be complex. The pros and cons of Lisk are depicted in Table XVIII.

TABLE XVIII. ADVANTAGES AND DRAWBACKS OF LISK

Advantages	Drawbacks
Lisk is a decentralized DApp development platform that makes the creation of apps easy and readily accessible	Lisk is in direct competition with the leading smart contract and DApp platform in the world, Ethereum
Lisk makes use of advanced Software development kit (SDK) technology, allowing developers to produce DApps and separate blockchain	
Lisk and the process involved with creating DApps make the entire platform truly decentralized and independent	

14)Dragonchain - (programming language: Java, Python, Node, C#, Go): Disney created Dragonchain in 2014. After a year of development, the firm released the first open-source code in 2016. DragonChain provides clients with "ecosystems" without central servers. The platform's multilayer security architecture aims to carve a unique position in the cryptocurrency market. The pros and cons of Dragonchain are depicted in Table XIX.

TABLE XIX. ADVANTAGES AND DRAWBACKS OF DRAGONCHAIN

Advantages	Drawbacks
Regulated platform	Poor market performance
Great functionality	
Ease of Use	

15)NEO - (programming language: Python, JavaScript, Java, C#, Go): It is an open-source platform that uses the consensus technique DBFT (DBFT) and smart contracts and cross-platform capabilities. Smart Contracts can access external resources through Oracle's built-in component. The pros and cons of NEO are depicted in Table XX.

TABLE XX. ADVANTAGES AND DRAWBACKS OF NEO

Advantages	Drawbacks
Energy-Efficient Consensus Mechanism	Unpopularity among Westerners
Ease of Developers	To compete with Ethereum, NEO has to outperform it in every way
NEO can handle around 1000 transactions per second	

16)IOTA: IOTA is a platform designed specifically for the IoT. It is a global network of connected devices. In terms of construction, IOTA is dissimilar to Ethereum, bitcoin, and other famous blockchains because it lacks the traditional linear structure of blockchain. Such a structure limits network scalability, so IOTA uses Tangle instead. A user must confirm two other users' transactions to gain confirmation for a transaction. The pros and cons of IOTA are depicted in Table XXI.

TABLE XXI. ADVANTAGES AND DRAWBACKS OF IOTA

Advantages	Drawbacks
Micro-payments	Ternary logic
Lightweight	IoT-specific framework functions
Scalable	The code has cryptic regions
Quantum-secure	No smart contract support

17)Cosmos SDK/Tendermint - (programming language: Golang): A modular execution stack at the system's heart lets apps mix and match components as needed. All modules are also sandboxed for increased application security. Consensus algorithms include PoS and BFT. The pros and cons of Cosmos SDK/Tendermint are depicted in Table XXII.

TABLE XXII. ADVANTAGES AND DRAWBACKS OF COSMOS SDK/TENDERMINT

Advantages	Drawbacks
Fully open-source project	Delegated staking freezes ATOM while validators work
Cosmos protocol allows separate blockchains to connect effortlessly	Staked ATOM are locked in a minimum of 3-weeks
ATOM can be staked to receive interest	
The interoperability does not compromise the security that Cosmos offers	
Cosmos is a community governance system that uses keys to identify users	

18)Waves: It is a Russian platform for ICO, crowdfunding, exchanges, and payment gateways. It is a software platform that includes many useful utilities and tools for developers. Users pay for the apps with the Waves tokens. The pros and cons of Waves are depicted in Table XXIII.

TABLE XXIII. ADVANTAGES AND DRAWBACKS OF WAVES

Advantages	Drawbacks
Perfect for crowdsourcing	Unclear legal status
Fair transfers	Support issue
Scalable, fast, and low-cost	Performance issue
Extremely easily accessible	Exchange is not yet mature

19)NEM (XEM): This cryptocurrency may be used to build trade, philanthropic, and banking applications. The Proof-of-Importance (PoI) consensus generation approach distinguishes this framework from others. PoI grants block development privileges to participants with the best reputation to ensure system integrity. The pros and cons of NEM are depicted in Table XXIV.

TABLE XXIV. ADVANTAGES AND DRAWBACKS OF NEM

Advantages	Drawbacks
Less energy usage	Low NEM consumer
Good capacity	Weak debut
Low commission	PoI centralized
Anti-counterfeiting	Fewer pieces of literature

20)OpenChain - (programming language: C#): It is a general ownership register that anyone may use. It may be modeled to work with virtually any use case. This application leverages partitioned consensus. There is no miner, and transactions are free and quick. Smart Contracts are autonomous actors that receive and send transactions based on business logic. The amount of privacy is adjustable from transparent to private. It suits enterprises that want to manage and issue digital assets reliably, securely, and scalable.

21)Multichain - (programming language: C++): It is a private P2P network that uses enhanced blockchain technology for financial operations. The pros and cons of Multichain are depicted in Table XXV.

TABLE XXV. ADVANTAGES AND DRAWBACKS OF MULTICHAIN

Advantages	Drawbacks
Flexible asset metadata	No smart contracts support
Permitted follow-up issue	Since they are 100% centralized, Private blockchains are beneficial as sandboxes, but not for production as they are meant only for a specific task
Multi-asset atomic payments	
Multi-way atomic asset swaps	
Multi-signature security and escrow	
Easy to setup and configure	

22)Monax - (programming language: Go): It is an open-source framework enabling business ecosystem developers to create, send, and release blockchain-based applications. The pros and cons of Monax are depicted in Table XXVI.

TABLE XXVI. ADVANTAGES AND DRAWBACKS OF MONAX

Advantages	Drawbacks
Only Monax's contract management platform can notarize electronic signatures on the blockchain	Legal Issues
Simple integration	User acceptance
Simple, smart, and Secure	
A database of digital contracts to track your commitments in real-time	

23)NodesPlus – (programming language: C++): This Russian project uses a programmed consensus to guard against server-side assaults and assure block authenticity. It also features built-in web applications for data, safes, and software protection. The framework includes a built-in smart contract system based on JavaScript and multi-currency wallets and payments. The pros and cons of Nodesplus are depicted in Table XXVII.

TABLE XXVII. ADVANTAGES AND DRAWBACKS OF NODESPLUS

Advantages	Drawbacks
When authorized nodes have access to certain transactions, the nodes Plus software platform allows you to deploy data clustering technologies	Updates and patches
Provides the strictly irreversible transaction required by government organizations, thus equating electronic data with paper documents	User acceptance

24)Blockchain Service Network (BSN) - (programming language: DAML): The China State Data Center created the BSN, unveiled in October 2019 as a blockchain platform for individuals and small businesses. It provides its developers with tools to construct blockchain applications in major business networks to assist the digital economy and smart city efforts. The pros and cons of BSN are depicted in Table XXVIII.

TABLE XXVIII. ADVANTAGES AND DRAWBACKS OF BSN

Advantages	Drawbacks
Reduced development, deployment, and operation costs	However, faith in Chinese technology has been eroding over the last year, with many countries opposing China's dominance of the 5G rollout
Access to blockchain apps made simpler	User privacy issues; Currently, the BSN Dev Alliance has no control over user activity
Access modes are flexible	
Expanding rapidly	

25)Exonum - (programming language: Rust): It is a blockchain platform developed by the Bitfury Group specifically for enterprise projects. The source code for Exonum and its application programming interfaces (APIs) are available for anybody to view. Besides providing access to the whole codebase, Exonum also provides blockchain administration tools. The pros and cons of Exonum are depicted in Table XXIX.

TABLE XXIX. ADVANTAGES AND DRAWBACKS OF EXONUM

Advantages	Drawbacks
Developed in Rust which is among the most secure programming languages, with extensive predictable resource utilization and execution safety	Networking improvements needed
Restrict data visibility in blockchain, protecting user privacy without sacrificing security	This is a difficult time to use the network. So, even if they aren't supposed to, third parties can obtain access to blockchain data
Provides auditability	

26)Masterchain: It is a nationwide Russian blockchain network launched in 2016. It uses the Ethereum blockchain network as its foundation, but it is created with respect to Russian encryption requirements, user identification procedures, and secure scalability, among other things. The pros and cons of Masterchain are depicted in Table XXX.

TABLE XXX. ADVANTAGES AND DRAWBACKS OF MASTERCHAIN

Advantages	Drawbacks
Enables "prompt confirmation of data actuality" to a transacting customer	Closed network, Controlled by the security monitor
Instant communication	Less decentralized than blockchain

V. EMERGING APPLICATIONS OF BLOCKCHAIN

Blockchain has been suggested to be used in many applications and cases following the successful application of technology in bitcoin because of its distinguishing characteristics. The following section provides a high-level summary of each domain, shown in Fig. 12.

A. Financial Applications

Blockchain technology is now being applied in several financial sectors, including prediction markets, asset settlement, economic transactions, and business services [113]. Blockchain is expected to be essential to the global economy's long-term growth, providing benefits to the current financial system, consumers, and society [42]. The adoption of blockchain technology in financial services can provide various benefits that can help alter the financial industry. As Klynveld Peat Marwick Goerdele (KPMG) reported, blockchain technology may minimize errors by up to 95%, enhance efficiency by 40%, and cut capital expenditure by up to 75% [84]. Blockchain technology in finance is a revolutionary idea that might transform the financial services industry. Here are a few examples of blockchain financial services applications that are gaining popularity in the industry:

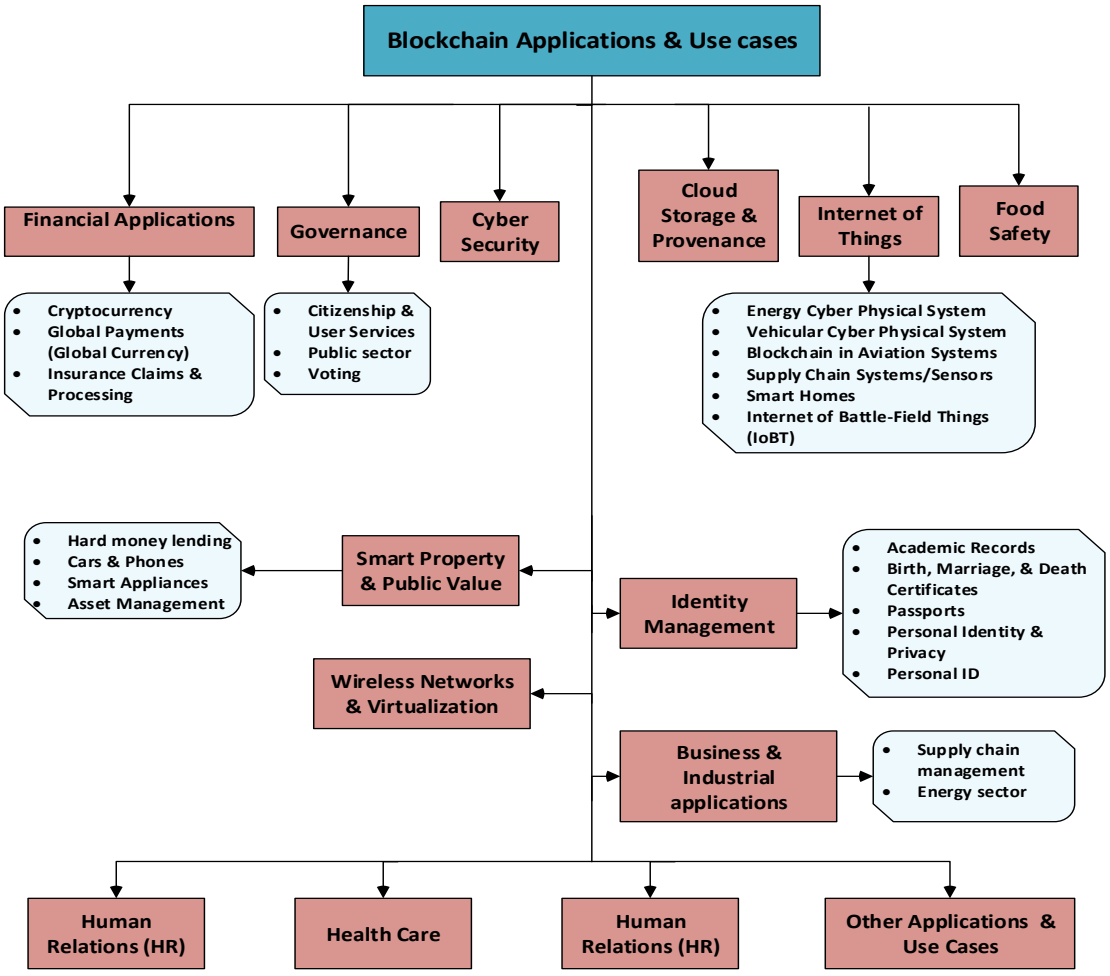


Fig. 12. Blockchain Applications.

1) Cryptocurrency: The earliest application of blockchain technology was to record digital currency transactions, and it remains the most popular usage to date. Bitcoin was the first widely adopted cryptocurrency [85]. Since then, the numerous versions of blockchain technologies have resulted in a wide range of cryptocurrencies and blockchain applications in markets and economics. Hundreds of cryptocurrencies are presently trading, according to 2017 worldwide cryptocurrency benchmarking research [86]. While many of these cryptocurrencies are labeled as "altcoins" and are essentially copies of bitcoin or other coins with different parameter settings, a small proportion of the various offerings have made significant progress.

2) Global payments (global currency): Numerous intermediates are engaged in verifying transactions, making international payments more complicated and time-consuming to complete. The entire process has the potential to be error-prone and expensive. In large part, these problems arise because financial transactions have been centralized; entities like banks and other financial institutions prescribe methods while also being accountable for verifying the transactions. Blockchain technology, which introduces a decentralized public ledger and a robust verification technique to validate transactions, minimizes the complications associated with these transactions. Global payments are made more verifiable, immutable, secure, and faster when made through this peer-to-peer network. It is currently being used by various remittance firms [87], like Abra and Bitspark, to provide remittance services using blockchain technology.

3) Insurance claims and processing: Numerous false claims have plagued the insurance industry. Thus, to efficiently handle an insurance claim, it is vital to have up-to-date data and policies associated with each claim, which is challenging with conventional methods. Blockchain technology allows for a speedy and secure approach. Similarly, because several participants or miners must consent to each transaction's legality, any false transactions or claims may be easily identified and destroyed. This ensures that the insurers receive the compensation as fast and efficiently as possible.

The open-end issues in this regard are as follows: Irrespective of some of the notable designs in recent times [88], there are still open-ended problems in applying blockchain to financial applications. Adopting blockchain in financial applications renders mainly bitcoin usage using different forms of cryptocurrencies without any dependencies on the centralized authorization. The advantage of such a scheme is highly reduced transaction fees and risks; however, deploying a secure blockchain architecture over a heterogeneous and integrated form of financial transactions is not free from the potential risk of attacks.

B. Governance

In the government sector, the usage of blockchain technology has been demonstrated in work [89]. The authors highlight better service quality, accessibility, and transparency. Blockchain technology is immune to internet attacks; transactions are public and cannot be changed or deleted once posted, making all data transactions open, safe, and secure. According to the authors [90][91], blockchain technology is suitable for the government since it is secure, P2P, decentralized, and accessible to anyone. Some of the use cases are Citizenship and User Services [92], Public Sector [93] [94] and voting.

The open-end issues in this regard are as follows: A closer look into the applications of governance using bitcoin, as mentioned above, reveals a higher dependency on consensus from the validating nodes and the users over the network. This is challenging to confirm as a regular network is usually populated by various unknown attackers and variable traffic. While using blockchain on such an application, it is challenging to conform to the robust model to promote voter participation based on common interests. Apart from this, the usage of bitcoin still doesn't witness any universally accepted governance model.

C. Internet of Things

The number of devices with internet access continues to rise annually. Connecting numerous devices together results in the Internet of Things. The IoT will revolutionise people's lives by making smart homes a reality. While having more and more of your devices online sounds like it would make life easier, the truth is that you run a significant risk of experiencing privacy and security breaches. When there are millions of interconnected devices, it is crucial to protect data and ensure accountability. The IoT could be secured by blockchain. Some of the use cases are Energy Cyber-Physical Systems [95], Vehicular Cyber-Physical Systems [96], unmanned aerial vehicle (UAV) [97], blockchain in Aviation Systems [98], Supply Chain Systems/Sensors: [99], Smart Homes [100], Internet of Battlefield Things (IoBT) [101].

The open-end issues in this regard are as follows: With its autonomous and decentralized capabilities, blockchain technology has the potential to resolve the privacy concerns surrounding the IoT by addressing the gaps and requirements of existing solutions. However, when used in an IoT setting, they still have some problems [102]. The primary issue is that if blockchain is used to improve IoT's scalability, it could eventually lead to centralization. When dealing with IoT networks, which typically have limited computational resources, the second issue is the need for ample processing time and power to carry out ciphering. The third issue is related to the storage concern brought on by the ledger's ever-increasing size, which necessitates storing all crucial data within the node. Finally, it is challenging to demonstrate the applicability of the current research work due to potential impending factors such as compliance and legal issues in various settings.

D. Cybersecurity

Blockchain technology also has potential applications in the realm of cybersecurity. When harmful data is shared among participants/organizations using blockchain, cyberattacks can be avoided in the future [103]. Because competitors could use it unilaterally if it contains identifying information, companies and governments are hesitant to discuss cyberattacks and threat intelligence. But with

blockchain and a private and public key pair, data can be sent anonymously (such as bitcoin [104]). This alleviates concerns about disseminating sensitive company or government data to potential competitors. Here are some unanswered questions: Blockchain has been touted for its purported security benefits, but if implemented incorrectly, it could expose significant vulnerabilities in the cyber security infrastructure. As a result, the blockchain is open to attacks that could slow down the formation of new chains, steal users' private keys, reverse transactions, and more. In addition, security researchers have been focusing on DoS attacks rather than developing a foolproof solution to prevent Sybil attacks, blockchain endpoint threats, routing attacks, or phishing.

E. Cloud Storage and Provenance

Blockchain can store and share metadata that documents the history of actions and creation, particularly data or file access. Data management is crucial for forensics and accountability [105]. For example, when users view and edit collaborative documents like Google Docs, the modifications are kept in the blockchain. The blockchain saves all revisions and changes made. Again, using blockchain and provenance, cloud storage, and processing can ensure accountability and integrity. Similarly, several people can easily track, modify, and alter data in the cloud for accountability and integrity. The open-end issues are as follows: Storage and provenance in the cloud by blockchain is not a simplified task. It involves a more significant deal of complexity. There is a dependency on adopting a highly sophisticated mathematical model in blockchain that can perform secure processing and transferring of data to the cloud storage system. Consequently, this viewpoint has a more significant imbalance between computational efficiency and security effectiveness.

F. Healthcare and Food Safety

Healthcare will likely be one of the most aggressive industries to adopt or drive blockchain technology. Blockchain, the future supply chain business paradigm, can be applied to the healthcare value chain. Everything from medical records to payments to processing and analytics will be automated, benefiting all stakeholders, from patients and consumers to administrators, providers, and healthcare organizations. Using blockchain in healthcare will help achieve [3]:

- Interoperability: A single format will be used to store and share data.
- Decentralized data storage: A single technology to handle all patient data.
- Power to patients: Patients who wish to be data owners will be able to choose with whom their health records are shared.

Over 0.6 billion (equal to one in every ten people) people worldwide become unwell every year due to eating contaminated food [106], making it one of the most pressing challenges to address. Every day, approximately 1167 individuals perish [106]. Due to the transparency provided by blockchain technology, users may receive information about food, such as its composition, origins, expiry dates, and so on, in seconds to help avoid food fraud. For food safety, food customers will have greater control over their information, which will be accurate and transparent.

G. Smart Property and Public Value

Blockchain technology may be utilized to maintain track of all actions and property records for any entity or property, including but not limited to: land, house, stocks, autos, and other investments. The information included in the blockchain is distributed to all parties interested or involved, and it can be used to make contracts and verify them. The lost data can be quickly recovered by copying it from the network [107]. Some use cases are hard money lending, cars and phones, smart appliances, and asset management. The efficiency and cost of conducting business are increased by removing the requirement for an intermediary to validate the transactions.

H. Wireless Networks and Virtualization

Wireless networks and virtualization are two topics that have been discussed recently. The increasing expansion of IoT and cyber-physical system (CPS) applications is putting a strain on wireless networks, and several approaches have been investigated to increase network capacity and coverage [108]. By preventing double-spending, in which multiple parties sublease the same wireless resource [109], blockchain can help network service providers like Mobile Virtual Network Operators (MVNOs) reliably maintain control over their users' quality of experience [110]. The open issues in deploying blockchain in wireless networks are mainly associated with data security.

I. Identity Management

This subsection discusses many identity management applications and their supposed effects on blockchain technology. Some of the essential use cases are Academic Records [111], Birth, Marriage, And Death Certificates [112], Passports [113], and Personal Identity and Privacy [114].

The open-end issues in this regard are as follows: Irrespective of essential studies towards identity management by blockchain, there are still open-ended issues to confirm the claimed identity's uniqueness and legitimacy. Apart from this, it is also challenging to verify the legitimacy of the owner at the same time. A specific form of threat is called synthetic identity proofing, where the social identification information of one individual is combined with different identity information (e.g., address, date of birth, etc.) from another person to generate a new form of a counterfeited identity. Unfortunately, blockchain cannot mitigate such problems as its prime task is to maintain a record being a ledger and not to perform identity verification.

J. Business and Industrial Applications

Blockchain can significantly improve, optimize, and automate commercial operations [115]. It is becoming increasingly common to see IoT and blockchain-powered e-business concepts in process today. In [170], the authors propose a business model in which transactions between devices are handled using smart contracts operating within a decentralized system based on a blockchain network. Many businesses could benefit from blockchain-based solutions that

act as distributed Business Process Management systems. The blockchain could store each business process instance, and smart contracts could handle the workflow routing, automating and streamlining intra-organizational activities while lowering costs and increasing efficiency [116]. Supply chain management [3] and Energy Sector [117] are essential use cases. Blockchain is considered a decarbonization facilitator, allowing the energy sector to shift toward more decentralized energy sources [118].

The open-end issues in this regard are as follows: Despite some promising efforts, widespread implementation of blockchain technology in the energy and supply industries has yet to overcome significant obstacles. The primary concern in applying blockchain in supply chain management is determining the degree of usage of blockchain and offering higher data quality. Further, providing a secure access protocol for a legitimate user is another significant problem in using blockchain for supply chains. From the energy sector's perspective, blockchain adoption still couldn't solve problems related to power consumption and scalability.

K. Financial Human Relations (HR)

Human resources departments identify and hire the best candidates for the best jobs, train and educate them to help the company achieve its goals, and maintain a safe and pleasant workplace where employees can be creative and productive. While blockchain's immediate disruption in the capital markets is well-known, its role in transforming HR processes and the workforce is even more fascinating and significant. Companies worldwide have recognized the great promise of blockchain technology to improve human resources and recruitment operations [3][5]. Recruitment, background checks, employee data protection, and smart contracts are just a few critical use cases for blockchain in HR.

L. Other Applications and Use Cases

Blockchain technology can be used without a trusted third party or P2P transaction system for transparency, decentralization, immutability, integrity, privacy, and security. On the other hand, the technology has some restrictions, such as the significant delay produced by the consensus mechanism when many blocks are involved [3].

VI. Essential Findings of the Study

Some of the essential findings of the study are as follows:

- A more excellent way to build a highly transparent trust can be done via public blockchain, however, it lacks an efficient control system. Furthermore, its increased price volatility makes it unsuitable for financial products. Most existing schemes are in the nascent stage of development with narrowed implementation scope over the practical ground and less benchmarked models for a public blockchain.
- A better form of control can be established by adopting existing private blockchain-based schemes making them highly reliable and secure. However, its growth is limited owing to inferior incentives. In addition, the costs associated with its management and administration are pretty complex. Existing schemes of private blockchain offers better data security, but still, they suffer from higher coverage of security options.
- Although hybrid blockchain offers beneficial features for public and private blockchains, it's not affordable compared to a public blockchain. Conventional research work on hybrid blockchain is witnessed to provide a balance between security and data transmission; however, they were not testified over larger scale of network in existing scheme.
- Majority of the existing study towards blockchain technology was found to emphasize the consensus layer for improving its functionalities. However, it should be noted that the consensus layer plays a core role in authenticating transactions and incorporating decentralization and encryption. However, there is no report of a robust model where all the above three entities have been securely protected from intrusion over the consensus layer. Further, less emphasis towards the network layer and incentive layer in existing approaches is also witnessed, which could lead to the continuation of further intrusive activities.
- Although more significant research is being carried out towards improving consensus algorithms in blockchain, but these approaches suffer from low performance and weak scalability (PoW). They also have minimal fault tolerance (PBFT) and lower decentralization (DPoS) with a complex implementation process (PoS).
- Various existing review works are being carried out to exhibit the progressive work in blockchain technology. The work carried out by authors in [119] gave some essential information about the challenges and solutions of blockchain over IoT systems. However, the work is specific towards agriculture-based applications, whereas the presented review work encompasses all the internal approaches to make any application more resilient and secure. Similar environment-specific-based review work using blockchain was also carried out in [32] which draws potential conclusive remarks about the challenges of blockchain in IoT. In contrast, the presented review work focusses on discussing the strengths and weaknesses of different types of utilization and methods of blockchain over its different taxonomies. The notable review work carried out towards smart grid systems by authors in [120] and [121] furnishes some of the transforming techniques towards decentralization scheme; however, it lacks essential discussion of limitations and research gap, which is encompassed in the presented review work. The best notable review work was witnessed in manuscript framed by authors in [122] that contains almost all the potential strengths and weaknesses of a higher number of research-based schemes in blockchains. The proposed work further contributes towards upgrading this information by focusing more on the overall compact picture of blockchain, referring to all the significant works of literature published to date.

VII. Open Challenges

Despite the rapid growth and research interest in blockchain technology, obstacles and concerns must be addressed before they can be widely adopted. Here, Fig. 13 illustrates a few blockchain concerns and challenges:

1) Privacy: It is necessary to safeguard the user's identity, location, and data from unauthorized users. The authentication of users entails using a private key to sign documents and the identification or verification of those documents utilizing the hash values compared to the public key. Based on all transactions shared between peers, anonymity cannot be guaranteed. The sharing of transactions makes it straightforward for other parties to investigate such activities and establish the genuine identities of the users involved in the transactions. While the decentralized consensus is built based on past transaction data that has been made publicly available, random users and their associated transaction data may also be made publicly available. In a similar vein, the location may be jeopardized. So, the question of confidentiality and privacy protection becomes a specific challenge.

2) Scalability: The distributed blockchain ledger includes several fields, such as events, users, and so forth. Users generate transactions, which are then appended to the blockchain as a block by a miner, forming a blockchain. This is a moderately challenging operation to do. As the application generates a significant number of transactions and related data, and as the communication infrastructure between nodes develops in size, the network's total performance will suffer. Though there are currently numerous blockchain protocols, research and development are still ongoing to create newer protocols that will address the difficulties in the technology. As a result, one of the most challenging tasks is ensuring that different protocols work together. More recent frameworks cannot scale after reaching a particular block and system size limit. As a result, the larger the blockchain, the longer it takes for the procedure to complete. Given this rapid growth in size and volume of data, scalability has emerged as a problem that must be addressed immediately.

3) Interoperability/Integration: Interoperability and integration - are important since blockchain technology is not a stand-alone application; instead, these applications are typically coordinated with diverse applications within and outside businesses. Blockchain will continue introducing new functionality to strengthen its capabilities and expand action plans. The integration of blockchain technology with current applications might be a difficult task. Specifically, interoperability and security issues are posing a significant barrier. Another concern is the numerous operating environments and platforms that may be required to interoperate to work on blockchain-based apps. Various developers may have produced old and new apps and hybrid applications utilizing multiple development processes, programming languages, and environments. As a result, the integration technique turns out to be a significant amount of work that becomes increasingly difficult over time. Some work is underway to develop viable integration models that integrate blockchain technology into various industrial applications. Despite this, there is still work to find and establish increasingly practical and flawless solutions.

4) Standards: Because cryptocurrencies are involved, valid conclusions can impact blockchain applications immediately. As a result, it is a critical issue that cannot be ignored. Numerous nations have developed rules for regulating the use of cryptocurrencies. Still, these regulations are currently inaccessible to transactions involving these currencies in the real world due to black marketing. As a result, constructing a fully legal blockchain remains a pipe dream. Regulators like the General Data Protection Regulation (GDPR) safeguard users' data. However, the technology is not capable of complying with all applicable legislation. As a result, the information the user provides may raise concerns about security, accuracy, and privacy.

5) Software testing: Compared to standard software testing methodologies, applications produced using blockchain technology must be examined for special features. Verification and validation of smart contracts must be implemented, as well. Testing the individual components and the overall software engineering process is necessary. One of the unique issues is the testing of blockchain applications. Smart contracts provide the capability of trustworthy oracles that can be readily integrated into applications while verifying the validity of these external entities [3]. Smart contracts are becoming increasingly popular.

6) Consensus algorithms: A wide range of consensus algorithms is available, each with advantages and disadvantages [123]. Attacks such as the 51 per cent attack are feasible due to this. A new consensus approach must be adopted to meet the application's needs. Different algorithms have different types of loopholes based on the features that have been changed to distinguish them from one another. Working towards a consensus algorithm requires consideration of scalability, tolerance, performance, complexity, and energy usage. New organizations that provide innovative blockchain solutions for various enterprises and business domains are emerging. A few of these solutions have already been implemented in apps, whereas others are still in the development stage, with further research being conducted to improve them [3]. It is critical to improving the application's adaptability, usability, scalability, security, dependability, and effectiveness. This can be accomplished through a variety of methods. As already noted, it is crucial to consider the numerous challenges in developing solutions to make blockchain more helpful and easier to integrate into organizational applications.

Fig. 13. Blockchain Challenges and Issues.

7) Performance issues: Blockchain systems have performance issues, like throughput bottleneck, storage constraints, and transaction latency authors in [124]. Bitcoin transactions are generally validated in an hour, which is acceptable but insufficient [9]. Blockchain-based solutions are efficient and effective when evaluated using empirical evaluation methods like experimental analysis and benchmarking [125].

8) Security: As blockchain apps become increasingly interconnected with the internet, they are subject to cyberattacks like scanning, sniffing, Sybil attacks, endpoint attacks, and DoS attacks. Blockchain miners and users control their entire system, unlike traditional methods where an external organization contains the end user. So, phishing can take the user's private keys. One example is the MtGox attack. In 2014, a bitcoin deal in Tokyo, Japan, lost $600 million. Another example is a $55 million loss versus Ether digital currencies. It is also known as a >50% attack [126]. Without adequate security measures against such attacks, all apps suffer. The idea of blockchain and its usage models is compelling. However, issues like many platforms, open access, impending developments, using open systems, and others may compromise the system's security. Existing security mechanisms help, but additional research is needed to develop more effective security models for blockchain. Attacks on key management and authentication of users and data are common.

a) Key management: A client's private key is an unrecoverable private key. However, since no central entity handles the blockchain and can track down and restore the changed data, stealing the attacker's private key is risky. Establishing reliable critical management systems in the blockchain is thus another considerable difficulty.

b) Authentication: Blockchain ensures the authenticity of a ledger and other sensitive data stored in blocks in a decentralized manner [210] by encrypting the data. To create, survey, or modify data in the blockchain, a user must first utilize a private key connected with a public key. These credentials are tied to an address in a wallet. Users can digitally sign transactions using such software keys and check their authenticity. The Elliptical Curve Digital Signature Algorithm (ECDSA) is the most often used Digital Signature Algorithm. There is still a need for a lot of studies to authenticate the information and the user. There is also the risk of a compromised wallet to be considered. Its ability to confirm identity and identity paperwork has made it a studied issue.

9) Smart contract management: Developing, deploying, and interacting with a blockchain among various members and stakeholders is a highly tough task [127]. Indeed, no matter what form of blockchain is used (public, private, or consortium), severe challenges such as management, administrative services, and smart contract debugging arise. A few of the smart contract-related concerns are as follows:

a) Privacy preservation: When building a smart contract, it is challenging to consider privacy concerns. Given the inclusion of bytecode analysis tools, the agreement faces the risk of being insecure [7][8].

b) Re-entrancy: The DAO assault extensively used re-entrance to achieve success. It impacts the execution of functions, says A and B; in most cases, A is the first to execute, followed by B. However, in this circumstance, B executes first, followed by A. Consequently, the situation deteriorates, resulting in a loss. A function is, for example, the "withdraw" function, which retrieves cryptocurrency from a record by giving cryptocurrency to a user and then "updating" the account balance. If the value of the currencies is less, the "update" should occur before the "withdraw".

c) Call to the unknown: Some Solidity functions can call the callee's fallback function when the callee's signature does not match any available users in a Solidity contract. When an attacker executes the malicious fallback function identified in their contract, they can use the call, transmit, or delegate call function to send the Ether to an address that does not exist [128]. Unlike other attacks on Ethereum, this one posed a high risk.

d) Exception syndrome: Incorrect handling of exceptions causes a syndrome that must be dealt with and a loss of currency. These occur due to an unintentional halt in the execution, and the gas quantity is deducted [128]. If an interruption happens, how to deal with it becomes a serious concern.

e) Gas exception: When a transaction is given, the "gas" is a measure of Ether used to cover the transaction's cost. If an exchange runs out of gas while being executed, it will be rescheduled; nevertheless, the sender will be obligated to pay the miner the total amount of available gas [128].

f) Programming smart contracts: Because smart contracts are immutable, security is one of the most challenging hurdles to overcome while programming them. If Ether is taken from users, it will be impossible to recover it. The other issue is data integrity and uniqueness, which are required for blockchain-based systems to be reliable and trustworthy. The economy is also a key source of concern. This is the cost of creating, executing, and deploying smart contracts, also known as the gas cost in Ethereum [128]. A single programming error will harm the economy as a whole.

10)Immutability hindrance: The immutability attribute of blockchain may make it challenging to employ the technology in some applications. For example, when used in healthcare area, the immutability feature may make it more challenging to comply with privacy rules, establishing an individual's right to have their health data erased and rendered inaccessible to third parties [129]. This is a delicate subject, and the use of technology in healthcare cannot proceed without first addressing this legal requirement [129].

11)Awareness and adoption: One of blockchain's most critical challenges is the lack of understanding and adoption. For example, many individuals are unfamiliar with how it operates. The technology's future development depends on how many parties use it, which is still an open subject.

a) Lack of expertise knowledge: A blockchain project's implementation and management are challenging tasks. The firm must have extensive expertise in the subject matter to complete the process. They must engage a large number of professionals in the blockchain sector, which creates difficulty, and as a result, it is considered one of the blockchain's downsides, according to some. Additionally, businesses must train their employees on using the technology by ensuring that the management team knows the intricacies and outcomes of running a blockchain-powered organization. They will be able to grasp client requirements and assist them in transforming their business operations to use blockchain. Not to mention that if you locate its developers and specialists, they will be more challenging to come by and more expensive than regular developers due to the demand and supply ratios. Table XXXI summarises key traits, literature references, and concerns.

TABLE XXXI. CHARACTERISTICS OF A UNIFIED BLOCKCHAIN AND RELATED CONCERNS

	Mapped Literary Jargons	**Related Concerns**
Decentralization	Decentralization [33], [35], [128]	Complex security management Significant resource requirements Resource inefficiency Out-of-date and long chains are pruned out Poor performance and latency issues Scalability Inefficient use of energy
Transparency	Transparency [33], [35], [128] Openness [131] Auditability [32]	Privacy concerns Opposite of anonymity
Autonomy	Anonymity [130] Trust-Free [133] Trustlessness [131]	Few large firms rely on computing power to make decisions
Security	Security [32], [131], [18]	Various attacks
Immutability	Immutability [32], [35], [130][133] Unforgeable [128] Persistency [130] Untamperability [131]	Irreversible smart contract bugs Difficulty applying smart contracts patches Obstacles in some applications, like patient privacy in healthcare
Anonymity	Anonymity [22][131], [128] Pseudonymity [133] Transactional Privacy [32]	Lack of transparency about real transaction participants
Democratized	Democratized [33] Synchronized through Consensus [35] Collective Maintainability [131]	Low performance owing to an excessive number of decision nodes Few large firms use computational power to make decisions
Integrity	Integrity [21] Data Reliability & Integrity [32][133] Reliable Database [131]	Various types of attacks
Programmability	Programmability [23]-[132], [133] Open Source [130] Blockchain -Based Control [35] Openness [128]	Poor user interface
Fault Tolerance	Fault Tolerance [32]	Data duplication at several nodes necessitates substantial storage Synchronization Overhead
Automatic	Automatic [133] Independence [128]	Irreversible smart contract bugs Difficulty updating smart contracts Computer software is susceptible to hacking and attacks

VIII. FUTURE RESEARCH OPPORTUNITIES

Blockchain technology can completely transform the way businesses and payments are conducted worldwide without the need for trusted intermediaries or consideration of geographical limits. As a result, many parts of the blockchain will continue to be popular study areas, including consensus methods and managed services in terms of efficiency. The following section discusses some of the most important discoveries and future directions.

- Blockchain technology must address many existing challenges to become a cornerstone technology for various domains in the future. As a starting point, it should be scalable and overcome the restrictions of high latency, low throughput, and increasing storage requirements. The research community should work around the challenge of efficiently updating smart contracts with minimal overhead. Finally, the blockchain community must handle the enormous energy consumption of many nodes taking part in the consensus process, which could become a primary climate concern.
- To assist enterprise blockchain, Intel and Microsoft have already joined forces [134]. According to the alliance, the success of its enterprise will be determined by how well it addresses concerns such as performance, confidentiality, and governance [135]. Anomaly detection frameworks (ADFs) should fundamentally incorporate support for these issues if they are to be widely accepted across a wide range of business areas. The combined capabilities of blockchain and artificial intelligence offer enormous potential for developing applications in various fields. For example, the trust in blockchain technology and the decision-making capabilities of artificial intelligence in healthcare and driverless vehicles will be an excellent fit for special applications [136]. Therefore, it will be necessary for future ADFs to include intrinsic support for these types of functionalities.
- There will be two significant hurdles in the future for promoting blockchain security. The first is to strike a balance between an individual's privacy, security, and accountability, which is made feasible primarily

through Distributed Ledger Technology. On the other hand, it is necessary to cope with the privacy and security problems arising from the IoT. These issues include legal challenges, interoperability, developmental concerns, rights concerns, regulatory concerns, a lack of standards, and issues related to the emerging IoT economy, among other things.

- It is noted that blockchain is intended to operate as a decentralized system. Meanwhile, there is a growing trend toward miners being centralized within the mining pool. To date, 51 percent of the total hash power on the bitcoin blockchain is controlled by the top five mining pools combine [135][136]. Aside from that, the selfish mining method [137] shows that pools with more than 25 percent of the overall processing capacity might generate more money than their fair share of the revenue. The selfish pool's total power might fast approach 51 percent of the full power available. A solution should be given since the blockchain is not built for a few companies.

- Blockchain's economic benefits have been thoroughly researched [3][8]. Individual businesses must comprehend how the technology affects their organizational structure, method of operation, and management approach. The market must assess whether blockchain can address market failures caused by information asymmetry and improve market efficiency and societal welfare. However, more incredible research is required to understand how it affects business and market efficiency.

- Research on throughput, latency, size and bandwidth, hard forks, versioning, and many forks is also required. This is a significant research gap that will require further research. Understandably, given the tiny size of current blockchain applications, they are not the most exciting research areas for now. Currently, bitcoin, the most popular solution, has a much lower transaction volume than VISA. It is necessary to perform additional studies on scalability in the future when blockchain solutions are utilized by tens of millions of users and transaction volumes skyrocket.

- The other research gap is usability. This study found publications that explored usability from the user's perspective, but not the developer's, as the work [138] suggests. For example, the bitcoin API is still challenging to use. This has to be researched and improved as it could lead to more bitcoin applications and solutions. Future research will likely focus on bitcoin, other cryptocurrencies, and viable blockchain uses. This study identified some research on smart contracts, licensing, IoT, and smart properties in a blockchain setting. These studies will have a considerable impact in the future and may even be more exciting than cryptocurrencies. For example, using a decentralized environment to share a virtual property might alter how corporations sell their items. Considering this, it can be confidently posited that further adoption of this technology by industry and academics will result in the significant new research.

- Improving blockchain's Interoperability and Compatibility with Existing Health Information Technology (HIT) infrastructure: Companies must know how to connect their HIT blockchain to other blockchains or non-blockchain platforms. Interoperability and data standards should be explored besides ascertaining effective integration governance mechanisms. Researchers should look at cross-authentication (for interoperable blockchains), oracles (which send external data to the blockchain for on-chain use), and application programming interfaces (APIs) (for incompatible blockchains). Many open standards exist for connecting proprietary systems to blockchain HIT, but the feasibility of using them to connect proprietary systems to blockchain HIT is still unknown [139]. Diverse stakeholders in blockchain silos cause complexity and interoperability issues that should be investigated. Security and privacy concerns require knowledge of blockchain interoperability's legal and regulatory consequences.

- HIT researchers are growing in awareness of the technological constraints of blockchain data storage and are exploring alternate techniques to comply with GDPR. Keeping addresses, hash values, and timestamps on the blockchain while storing Protected Health Information (PHI) off-chain in the cloud or on hospital servers is advised [140]. Data storage splitting can reduce system performance. On-chain and off-chain data storage should be optimized in future studies.

- The sharing economy is frequently defined as the P2P exchange of goods and services. In the future, the new sharing economy may include enterprise sharing. As a result, interconnecting blockchains may become a trend. These interfaces will let commercial operations connect identity authentication, Soft Computing and Measurements (SCM), and payment processes. They will also enable real-time data sharing and collaboration between businesses and industries.

- The vast amount of data stored in blockchain makes it possible to do Blockchain-based big data analytics. Other forms of ample data storage (for example, tensor computing) could also be improved to efficiently store and process blockchain data to save space, make it more accessible, and provide other benefits.

- Many blockchain consensus algorithms seek to replace PoW due to its massive energy waste. These new native protocols may introduce additional security risks or be impossible to deploy in reality [141]. The blockchain consensus mechanisms present a research opportunity. Future investigations are needed to seek more robust and more secure protocols than PoW while consuming less energy besides ensuring that the proper protocol is utilized in suitable applications [142].

- The threat of quantum computers to blockchain security necessitates efficient and well-proven post-quantum digital signature systems and other relevant investigations. The affordability of quantum computers is desirable, but systems like blockchain must be protected from quantum computers. Apart from ECDSA, RSA, and Digital Signature Algorithm (DSA), alternative cryptographic methods (post-quantum cryptos) are not impacted by quantum computers. Asymmetric key cryptography (Merkle signature system) and hash-based cryptography (McEliece public key system) both have such systems (e.g., AES). These include lattice-based (e.g., NTRU public key cryptosystem) and multivariate quadratic public key methods. Research is still needed to improve post-quantum cryptosystems' usability (key size), efficiency, and confidence against quantum computer threats [143]. More research is needed on quantum channels and effective post-quantum consensus techniques [144].
- Blockchain-based Decentralization Finance, sometimes known as 'DeFi,' is a new field based on blockchain technology. It is a unique, experimental type of finance, not relying on central authority or intermediaries such as exchanges or banks. DeFi is an umbrella term for many decentralized financial services and applications based on the technology. It has numerous potential study possibilities because it is new compared to the other blockchain research subjects stated above. A surge in interest in DeFi research in the coming years is anticipated.
- The interoperability of blockchain should also be investigated. Many blockchain platforms may interoperate to improve security, usability, and efficiency. Blockchain may also be used to supplement existing systems. Many businesses want to implement it but do not want to abandon their present systems. The optimal strategy to integrate the blockchain with an organization's existing systems must be researched. It is also essential to consider how different blockchain systems might work together for mutual gain.

IX. Conclusion

Blockchain technology is becoming increasingly popular for conducting decentralized transactions and data management without the involvement of an intermediary. Open and decentralized, the blockchain keeps track of all transactions between all parties involved in a form that can be independently verified. Since 2008, there has been a rise in interest in bitcoin and blockchain. However, it was just the beginning then, with no frequency of research papers. The data presented in the proposed paper (with respect to the percentage of increase in research publications in blockchain technology) now shows increasing attention towards evolving with more secure blockchain technology, witnessed only in the last three years. One of the prime reasons could be the adoption of blockchain as a new alternative for securing digital copyright data, supply chain management, the financial sector, etc. As a result of its inherent decentralization, persistence, anonymity, and auditability, the technology has drawn considerable interest from both the business and academic communities. A growing number of corporations and governments worldwide using blockchain technology to enhance their services' efficiency, scalability, and security. A complete description of blockchain technology was provided in this manuscript. At the outset, it introduced blockchain technology and its key features, including its architecture. After that, some of the most common consensus algorithms in the blockchain were discussed. Different aspects of these protocols were compared and evaluated. The study covers the basics of blockchain and some more interesting new applications and uses cases. For example, blockchain technology can have a revolutionary effect on the financial sector, e-Government, and Business Process Management (BPM) besides entertainment, healthcare, insurance, law firms, the Internet of Things, trading platforms, etc. However, there are just a few examples of the technology used with these systems. As a result, this technology is unlikely to replace existing systems or applications anytime soon wholly. Nonetheless, blockchain technology may undoubtedly be used in conjunction with existing systems and may even result in the construction of new techniques in the years ahead. For this reason, additional research into the technology is needed, as it is still in the experimental stage and numerous technical and legal challenges need to be overcome. This work serves as a helpful beginning point for future research issues related to the development of blockchain applications. It will be of use to practitioners and researchers alike in their efforts. Even though there are numerous ongoing active research projects in this field, this technology is still in its infancy; as a result, future study avenues have been identified, with an emphasis on in-depth research.

Acknowledgment

The authors express their personal appreciation for the effort of Prof. Dr. Roohie Naaz Mir, Ms. Bisma Rasool Pampori and Ms. Gousia Nissar in proofreading, editing, and formatting the paper.

References

[1] B. Thuraisingham, “Blockchain technologies and their applications in data science and cyber security,” in *2020 3rd International Conference on Smart BlockChain (SmartBlock)*, Zhengzhou, China, 2020, pp. 1–4.

[2] C. Pike, “Blockchain technology and competition policy - issues paper by the Secretariat,” *SSRN Electron. J*, 2018.

[3] F. Casino, T. Dasaklis, and C. Patsakis, “A systematic literature review of Blockchain-based applications: current status, classification and open issues,” *Telematics and Inform*, vol. 36, pp. 55–81, 2019.

[4] H. Sheth and J. Dattani, “Overview of Blockchain technology,” *Asian J. Convergence in Technol*, vol. 5, no. 1, pp. 1–4, 2019.

[5] M. Crosby, P. N. Pattanayak, S. Verma, and V. Kalyanaraman, *BlockChain Technology: Beyond Bitcoin. Appl. Innov*, no. 02, pp. 6–19, 2019.

[6] D. Vujicic, D. Jagodic, and S. Randic, “Blockchain technology, Bitcoin and Ethereum: A brief overview,” in *17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2018, pp. 1–6.

[7] R. Zhang, R. Xue, and L. Liu, “Security and privacy on Blockchain,” *ACM Comput. Surveys*, vol. 52, no. 3, pp. 1–34, 2019.

[8] Chirag, C. Impact of Blockchain on the Economy | Appinventiv. Available online: https://appinventiv.com/blog/real-impact-of-blockchain-technology-on-economy/. (accessed on 12 August 2022).

[9] S. Bragadeesh and A. Umamakeswari, "Role of Blockchain in the Internet-of-Things (IoT)," *Int. J. of Eng. & Technol*, vol. 7, no. 9, pp. 109–112, 2018.

[10] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[11] L. Lamport, "The part-time Parliament," *ACM Trans. Comput. Syst*, vol. 16, no. 2, pp. 133–169, 1998.

[12] G. Pareek and B. Purushothama, "Blockchain-based decentralised access control scheme for dynamic hierarchies,". *Int. J. Inf. Comput. Secur.*, vol. 16, no. 3-4, pp. 324-354, 2021.

[13] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the application of cryptography on the blockchain," *J. Phys.: Conf. Ser.*, vol. 1168, no. 3, pp. 1-8, 2019.

[14] K. Nelaturu, H. Du, and D. Le, "A review of blockchain in Fintech: Taxonomy, challenges, and future directions," *Cryptography*, vol. *6, no. 2*, p. 18, 2022.

[15] X. Li, J. Xu, X. Fan, Y. Wang, and Z. Zhang, "Puncturable signatures and applications in proof-of-stake blockchain protocols," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3872-3885, 2020.

[16] F. Shahid, I. Ahmad, M. Imran, and M. Shoaib, "Novel One Time Signatures (NOTS): A compact post-quantum digital signature scheme," *IEEE Access*, vol. 8, pp. 15895-15906, 2020.

[17] Z. Cai, J. Qu, P. Liu, and J. Yu, "A blockchain smart contract based on light-weighted quantum blind signature," *IEEE Access*, vol. 7, pp. 138657-138668, 2019.

[18] S. Zhang and J. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4557-4565, 2020.

[19] Y. Xiao, P. Zhang, and Y. Liu, "Secure and efficient multi-signature schemes for fabric: An enterprise blockchain platform," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1782-1794, 2021.

[20] F. Xiong, R. Xiao, W. Ren, R. Zheng, and J. Jiang, "A key protection scheme based on secret sharing for blockchain-based construction supply chain system," *IEEE Access*, vol. 7, pp. 126773-126786, 2019.

[21] W. Zheng, K. Wang, and F. Wang, "GAN-based key secret-sharing scheme in blockchain," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 393-404, 2020.

[22] Y. Kim, R. Raman, Y. Kim, L. Varshney, and N. Shanbhag, "Efficient local secret sharing for distributed blockchain systems," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 282-285, 2019.

[23] H. Yin *et al.*, "Attribute-based private data sharing with script-driven programmable ciphertext and decentralized key management in blockchain Internet of Things," *IEEE Internet of Things J.*, vol. 9, no. 13, pp. 10625-10639, 2022.

[24] Q. Lyu *et al.*, "JRS: A joint regulating scheme for secretly shared content based on blockchain," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2957-2971, 2022.

[25] A. Mohsin *et al.*, "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture," *Multimed. Tools. Appl.*, vol. 80, no. 9, pp. 14137-14161, 2021.

[26] P. Sarkar, S. Ghoshal, and M. Sarkar, "Stego-chain: A framework to mine encoded stego-block in a decentralized network," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5349-5365, 2022.

[27] A. Giron, J. Martina, and R. Custódio, "Steganographic analysis of blockchains," *Sensors*, vol. 21, no. 12, p. 4078, 2021.

[28] J. Shi, X. Zeng, and R. Han, "A blockchain-based decentralized public key infrastructure for information-centric networks," *Information*, vol. 13, no. 5, p. 264, 2022.

[29] F. Hashim, K. Shuaib, and F. Sallabi, "Connected blockchain federations for sharing electronic health records," *Cryptography*, vol. 6, no. 3, p. 47, 2022.

[30] X. Boyen, U. Herath, M. McKague, and D. Stebila, "Associative blockchain for decentralized PKI transparency. *Cryptography*, vol. 5, no. 2, p. 14, 2021.

[31] R. Longo, C. Mascia, A. Meneghetti, G. Santilli, and G. Tognolini, "Adaptable cryptographic primitives in blockchains via smart contracts," *Cryptography*, vol. 6, no. 3, p. 32, 2022.

[32] B. Cambou, B. *et al.*, "Securing additive manufacturing with blockchains and distributed physically unclonable functions," *Cryptography*, vol. 4, no. 2, p. 17, 2020.

[33] M. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet Of Things: Research issues and challenges," *IEEE Internet of Things J*, vol. 6, no. 2, pp. 2188–2204, 2019.

[34] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of Blockchain," in *10th International Conference on Communication Software and Networks (ICCSN)*, Chengdu, China, 2018, pp. 562–566.

[35] J. Xie, H. Tang, T. Huang, F. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of Blockchain technology applied to smart cities: research issues and challenges," *IEEE Commun. Surveys Tuts*, vol. 21, no. 3, pp. 2794–2830, 2019.

[36] R. Yang, F. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated Blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts*, vol. 21, no. 2, pp. 1508–1532, 2019.

[37] G. Irving and J. Holden, How Blockchain-Timestamped Protocols Could Improve The Trustworthiness Of Medical Science. *F1000Research* 2016, *5*, 222, 2016.

[38] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," *IEEE Trans. on Emerging Topics in Comput*, vol. 9, no. 4, pp. 1972–1986, 2021.

[39] "New kid on the Blockchain". *New Scientist*, vol. 225, no. 3009, pp. 7–7, 2015.

[40] "How is blockchain verifiable by public and yet anonymous?", *Quora*, 2022. [Online]. Available: https://www.quora.com/How-is-Blockchain-verifiable-by-public-and-yet-anonymous. [Accessed: 22- Jul- 2022].

[41] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of Blockchain systems," *Future Gener. Comput. Syst*, vol. 107, pp. 841–853, 2020.

[42] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag*, vol. 7, no. 2, pp. 18–21, 2018.

[43] N. Y. Lee, J. Yang, M. M. H. Onik, C. S. Kim, and Modifiable, "Public Blockchains using truncated hashing and sidechains," *IEEE Access*, vol. 7, pp. 173571–173582, 2019.

[44] Z. Guo, Z. Gao, H. Mei, M. Zhao, and J. Yang, "Design and optimization for storage mechanism of the public Blockchain based on redundant residual number system," *IEEE Access*, vol. 7, pp. 98546– 98554, 2019.

[45] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, M. Abdallah, and B-Ride, "Ride sharing with privacy-preservation, trust and fair payment atop public Blockchain," *IEEE Trans. Netw. Sci. Eng*, vol. 8, no. 2, pp. 1214–1229, 2021.

[46] A. Asheralieva and D. Niyato, "Learning-based mobile edge computing resource management to support public Blockchain networks," *IEEE Trans. Mob. Comput*, vol. 20, no. 3, pp. 1092–1109, 2021.

[47] N. Mohammadzadeh, S. D. Nogoorani, and J. L. Muñoz-Tapia, "Invoice factoring registration based on a public Blockchain," *IEEE Access*, vol. 9, pp. 24221–24233, 2021.

[48] C. Cai, Y. Zheng, Y. Du, Z. Qin, and C. Wang, "Towards private, robust, and verifiable crowdsensing systems via public Blockchains," *IEEE Trans. Dependable Secure Comput*, vol. 18, no. 4, pp. 1893–1907, 2021.

[49] Y. Bai, Q. Hu, S. H Seo, K. Kang, and J. J. Lee, "Public participation consortium Blockchain for smart city governance," *IEEE Internet of Things J*, vol. 9, no. 3, pp. 2094–2108, 2022.

[50] H. T. Wu and C. W. Tsai, "An intelligent agriculture network security system based on private blockchains," *J. Commun. Netw*, vol. 21, no. 5, pp. 503–508, 2019.

[51] L. Hou, X. Xu, K. Zheng, and X. Wang, "An intelligent transaction migration scheme for RAFT-based private Blockchain in Internet of Things applications," *IEEE Commun. Letters*, vol. 25, no. 8, pp. 2753–2757, 2021.

[52] K. Toyoda, K. Machi, Y. Ohtake, and A. N. Zhang, "Function-level bottleneck analysis of private Proof-of-Authority Ethereum blockchain," *IEEE Access*, vol. 8, pp. 141611–141621, 2020.

[53] L. Xu, T. Bao, and L. Zhu, "Blockchain empowered differentially private and auditable data publishing in industrial IoT," *IEEE Trans. Industr. Inform*, vol. 17, no. 11, pp. 7659–7668, 2021.

[54] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private Blockchains," *IEEE Trans. Syst. Man Cybern. Syst*, vol. 50, no. 1, pp. 172–181, 2020.

[55] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for Software-Defined Networks using private Blockchain," *IEEE Internet of Things J*, vol. 9, no. 2, pp. 1542–1559, 2022.

[56] M. J. Baucas, S. A. Gadsden, and P. Spachos, "IoT-based smart home device monitor using private Blockchain technology and localization," *IEEE Netw. Letters*, vol. 3, no. 2, pp. 52–55, 2021.

[57] C. Shah, J. King, and R. W. Wies, "Distributed ADMM using private Blockchain for power flow optimization in distribution network with coupled and mixed-integer constraints," *IEEE Access*, vol. 9, pp. 46560–46572, 2021.

[58] H. M. Kim, H. Turesson, M. Laskowski, and A. F. Bahreini, "Permissionless and permissioned, technology-focused and business needs-driven: Understanding the hybrid opportunity in Blockchain through a case study of Insolar," *IEEE Trans. Eng. Manag*, vol. 69, no. 3, pp. 776–791, 2022.

[59] N. Liu, L. Tan, L. Zhou, and Q. Chen, "Multi-party energy management of energy hub: A hybrid approach with Stackelberg Game and Blockchain," *J. Mod. Power Syst. Clean Energy*, vol. 8, no. 5, pp. 919–928, 2020.

[60] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge Blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[61] J. Polge, S. Ghatpande, S. Kubler, J. Robert, and Y. L. Traon, "BlockPerf: A hybrid Blockchain emulator/simulator framework," *IEEE Access*, vol. 9, pp. 107858–107872, 2021.

[62] S. Zhu, Z. Cai, H. Hu, Y. Li, W. Li, and Zkcrowd, "A hybrid Blockchain-based crowdsourcing platform," *IEEE Trans. Industr. Inform*, vol. 16, no. 6, pp. 4196–4205, 2019.

[63] G. Subramanian, A. S. Thampy, N. V. Ugwuoke, and B. Ramnani, "Crypto Pharmacy - digital medicine: A mobile application integrated with hybrid Blockchain to tackle the issues in pharma supply chain," *IEEE Open J. Comput. Soc*, vol. 2, pp. 26–37, 2021.

[64] S. Fan, H. Zhang, Y. Zeng, and W. Cai, "Hybrid Blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet of Things J*, vol. 8, no. 4, pp. 2252–2264, 2021.

[65] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, and X. Zhang, "A hybrid model for central bank digital currency based on Blockchain," *IEEE Access*, vol. 9, pp. 53589–53601, 2021.

[66] G. Subramanian and A. S. Thampy, "Implementation of hybrid Blockchain in a pre-owned electric vehicle supply chain," *IEEE Access*, vol. 9, pp. 82435–82454, 2021.

[67] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Serv. Comput*, vol. 13, no. 2, pp. 241–251, 2020.

[68] S. Kumari and S. Farheen, "Blockchain based data security for financial transaction system," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2020, pp. 829–833.

[69] B. Mohanta, D. Jena, S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," *Internet of Things*, vol. 8, pp. 1–30, 2019.

[70] M. Salimitari, M. Chatterjee, and Y. Fallah, "A survey on consensus methods in Blockchain for resource-constrained IoT networks," *Internet of Things*, vol. 11, pp. 1–23, 2020.

[71] D. Romano and G. Schmid, "Beyond Bitcoin: A critical look at Blockchain-based systems," *Cryptography*, vol. 1, no. 2, pp. 1–31, 2017.

[72] N. Shi, Architectures and Frameworks for Developing and Applying Blockchain Technology, United States of America: IGI Global, 2019.

[73] S. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of Blockchain consensus algorithms performance evaluation criteria," *Expert Syst. with Appl*, vol. 154, pp. 1–39, 2020.

[74] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure Proof-of-Stake Blockchain protocol," in *Annual Interna- tional Cryptology Conference*, 2018, pp. 357–388.

[75] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, LA, USA, 1999.

[76] D. Larimer, *DPOS Consensus Algorithm-The Missing White Paper*, Steemit, New York, USA, White Paper, 2018.

[77] A. Baliga, "Understanding Blockchain consensus models," *Persistent*, vol. 2017, no. 4, pp. 1–16, 2017.

[78] "Neo Smart Economy", *Neo.org*. [Online]. Available: https://neo.org/. [Accessed: 25- Jun- 2022].

[79] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in *Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN)*, Singapore, 2016, pp. 1–10.

[80] D. Kraft, "Difficulty control for Blockchain-based consensus systems," *Peer-to-Peer Netw. and Appl.*, vol. 9, no. 2, pp. 397–413, 2015.

[81] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's transaction processing," *Fast Money Grows on Trees, Not Chains. IACR Cryptology ePrint Archive*, vol. 2013, pp. 1–31, 2013.

[82] A. Chepurnoy, M. Larangeira, and A. Ojiganov, 2016. [Online]. Available: https://arxiv.org/pdf/1603.07926.pdf.

[83] P. Raj, A. K. Dubey, A. Kumar, and P. S. Rathore, *Blockchain, Artificial Intelligence, and the Internet of Things*, 1st ed., Cham, Switzerland: Springer, 2021.

[84] "Blockchain breaks new ground on climate risk and performance," KPMG. [Online]. Available: https://home.kpmg/xx/en/home/insights/2021/03/blockchain-breaks-new-ground-on-climate-risk-and-performance.html. [Accessed: 19-Mar-2022].

[85] G. Hileman and M. Rauchs, "Global cryptocurrency benchmarking study," *SSRN Electronic J*, pp. 8–113, 2017.

[86] "11 Money Transfer Companies Using Blockchain Technology", [Online]. Available: https://gomedici.com/11-money-transfer-companies-using-blockchain-technology-2/. [Accessed: 10- Jun- 2022].

[87] H. Kim and M. Laskowski, "Towards an ontology-driven Blockchain design for supply chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.

[88] W. Dai, Y. Lv, K. K. R. Choo, Z. Liu, D. Zou, and H. Jin, "CRSA: A cryptocurrency recovery scheme based on hidden assistance relationships," *IEEE Trans. Inf. Forensics Secur*, vol. 16, pp. 4291–4305, 2021.

[89] A. Johnson, "Everledger Is Using Blockchain To Combat Fraud, Starting With Diamonds", *Futurism*, 2015. [Online]. Available: https://futurism.com/everledger-is-using-blockchain-to-combat-fraud-starting-with-diamonds. [Accessed: 25- Jul- 2022].

[90] J. Lee, "Bidaas: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[91] W. Reijers, F. O'brolcháin, and P. Haynes, "Governance in Blockchain technologies & social contract theories," *Ledger*, vol. 1, pp. 134–151, 2016.

[92] B. Leiding and A. Norta, "Mapping requirements specifications into a formalized Blockchain-enabled authentication protocol for secured personal identity assurance," in *International Conference on Future Data and Security Engineering*, Ho Chi Minh City, Vietnam, 2017, pp. 181–196.

[93] C. Sullivan and E. Burger, "E-residency and Blockchain," *Comput. Law Secur. Rep*, vol. 33, no. 4, pp. 470–481, 2017.

[94] "Cisco Visual Networking Index: Forecast and Trends, 2017–2022", 2018. [Online]. Available: https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf. [Accessed: 25- Jul- 2022].

[95] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications Of Blockchain In unmanned aerial vehicles: A review," *Veh. Commun*, vol. 23, pp. 1–28, 2020.

[96] P. Sharma, S. Moon, and J. Park, "Block-VN: A distributed Blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst*, vol. 13, no. 1, pp. 184–195, 2017.

[97] D. B. Rawat and C. Bajracharya, *Vehicular Cyber Physical Systems*, Cham, Switzerland: Springer, 2016.

[98] C. Akmeemana, Blockchain Takes Off: How Distributed Ledger Technology Will Transform Airlines. Blockchain Research Institute, 2017.

[99] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, 2017, pp. 618–623.

[100] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure Internet -Of- Battlefield Things (IoBT) architecture," in *MILCOM 2018-2018 IEEE Military Commu- nications Conference (MILCOM)*, Los Angeles, CA, USA, 2018, pp. 593–598.

[101] L. Serrano, O. S. Santos, and M, "Blockchain and the decentralisation of the cybersecurity industry," *DYNA*, vol. 96, no. 3, pp. 1–4, 2021.

[102] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of Blockchain in IoT: Challenges and solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, pp. 1–49, 2021.

[103] "Cryptocurrency Prices, Charts and Market Capitalizations", *Coinmarketcap.com*, 2022. [Online]. Available: https://coinmarketcap.com/. [Accessed: 14- Jul- 2022].

[104] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain based data provenance architecture in cloud environment with enhanced privacy and availability," in *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid, Spain, 2017, pp. 468–477.

[105] "IBM Food Trust - Blockchain for the world's food supply", *Ibm.com*. [Online]. Available: https://www.ibm.com/in-en/blockchain/solutions/food-trust. [Accessed: 21- Jul- 2022].

[106] A. Tanzarian, "Understanding Smart Property", *Cointelegraph*, 2014. [Online]. Available: https://cointelegraph.com/news/understanding_smart_property. [Accessed: 22- Jul- 2022].

[107] D. Rawat, A. Alshaikhi, A. Alshammari, C. Bajracharya, and M. Song, "Payoff optimization through wireless network virtualization for IoT applications: A three layer game approach," *IEEE Internet of Things J*, vol. 6, no. 2, pp. 2797–2805, 2019.

[108] D. B. Rawat, M. S. Parwez, and A. Alshammari, "Edge computing enabled resilient wireless network virtualization for Internet of Things," in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, San Jose, CA, USA, 2017, pp. 155–162.

[109] D. B. Rawat and A. Alshaikhi, "Leveraging distributed Blockchain based scheme for wireless network virtualization with security and QoS constraints," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, 2018, pp. 332–336.

[110] M. Sharples and J. Domingue, "The Blockchain and Kudos: A distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, Lyon France, 2016, pp. 490–496.

[111] A. Kamišalić, M. Turkanović, S. Mrdović, M. Heričko, "A preliminary review of blockchain-based solutions in higher education," in *International Workshop on Learning Technology for Education in Cloud*, Zamora, Spain, 2019, pp. 114-124.

[112] P. Franks, "Blockchain for Identity Management: Can a Case be made to Begin at Birth? - SJSU | School of Information", *SJSU | School of Information*, 2019. [Online]. Available: https://ischool.sjsu.edu/ciri-blog/Blockchain-identity-management-can-case-be-made-begin-birth. [Accessed: 30- Jul- 2022].

[113] C. Ellis, M. Last, G. Rana, J. Scottie and J. Cross, "World-Citizenship: Globally Orientated Citizenship With Private Passport Services Using Available Cryptographic Tools", *GitHub*, 2014. [Online]. Available: https://github.com/MrChrisJ/World-Citizenship/graphs/contributors. [Accessed: 15- Jul- 2022].

[114] D. B. Rawat, L. Njilla, K. Kwiat, C. Kamhoua, and Ishare, "Blockchain based privacy-aware multi-agent information sharing games for cybersecurity," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, 2018, pp. 425–431.

[115] W. Ying, S. Jia, and W. Du, "Digital enablement of Blockchain: Evidence from HNA group," *Int. J. Inf. Manage*, vol. 39, pp. 1–4, 2018.

[116] K. Bilal et al., "A taxonomy and survey on green data center networks," Future Gener. Comput. Syst, vol. 36, pp. 189–208, 2014.

[117] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A Blockchain-based smart grid: towards sustainable local energy markets," *Comput. Sci. Res. Dev*, vol. 33, no. 1-2, pp. 207–214, 2017.

[118] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in Blockchain: Comparative analysis, challenges and opportunities," in *12th International Conference on Open Source Systems and Technologies (ICOSST)*, Lahore, Pakistan, 2018, pp. 54–63.

[119] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, Blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[120] M. B. Mollah *et al*., "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things J*, vol. 8, no. 1, pp. 18–43, 2021.

[121] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Industr. Inform*, vol. 17, no. 1, pp. 3–19, 2021.

[122] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, April 2019.

[123] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction process- ing in Bitcoin," in *International Conference on Financial Cryptography and Data Security*, San Juan, Puerto Rico, 2015, pp. 507–527.

[124] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of Blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020.

[125] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[126] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad, and A. H. Embong, "A review on Blockchain security issues and challenges," in *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, 2021, pp. 227–232.

[127] T. Mcghin, K. Choo, C. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl*, vol. 135, pp. 62–75, 2019.

[128] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 254–269.

[129] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag*, vol. 67, no. 4, pp. 1008–1027, 2020.

[130] I. Lin and T. Liao, "A survey of Blockchain security issues and challenges," *Int. J. Netw. Secur*, vol. 19, no. 5, pp. 653–659, 2017.

[131] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of Blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data*, Honolulu, HI, USA, 2017, pp. 557–564.

[132] Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du, M. Guizani, and Medshare, "Trust-less medical data sharing among cloud service providers via Blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[133] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage*, vol. 3, no. 4, pp. 1–23, 2018.

[134] "Microsoft and Intel Detail the Deep-Seated Problems with Blockchain," [Online]. Available: https://www.forbes.com/sites/davidblack/2019/05/13/microsoft-and-intel-detail-the-deep-seated-problems-with-Blockchain/?sh=75da7a256b06. [Accessed: 15- Jun- 2022].

[135] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 2014, pp. 436–454.

[136]"Biggest Bitcoin mining pools 2021 | Statista", *Statista*, 2022. [Online]. Available: https://www.statista.com/statistics/731416/market-share-of-mining-pools/. [Accessed: 25- Jul- 2022].

[137]A. Roehrs, C. D. Costa, and R. D. R. Righi, "Omniphr: A distributed architecture model to integrate personal health records," *J. Biomed. Inform*, vol. 71, pp. 70–81, 2017.

[138]M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed., Beijing: O'Reilly Media, 2015.

[139]Y. Park, E. Lee, W. Na, S. Park, Y. Lee, and J. Lee, "Is Blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility," *J. Med. Internet Res*, vol. 21, no. 2, 2019.

[140]A. Shoker, "Brief announcement: sustainable blockchains through Proof of Exercise," in *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, Egham, United Kingdom, 2018, pp. 269–271.

[141]M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[142]D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, 2009, pp. 1–14.

[143]E. Kiktenko *et al.*, "Quantum-Secured Blockchain," *Quantum Sci. Technol*, vol. 3, no. 3, pp. 1–8, 2018.

[144]S. Abdulhakeem and Q. Hu, "Powered by Blockchain technology, DeFi (Decentralized Finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system," *Mod. Econ*, vol. 12, no. 1, pp. 1–16, 2021.