Received: 19 July 2023 | Revised: 28 October 2023 | Accepted: 27 November 2023
DOI: 10.1002/cpe.7987

REVIEW ARTICLE

WILEY

The blockchain conundrum: An in-depth examination of challenges, contributing technologies, and alternatives

Iraq Ahmad Reshi | Sahil Sholla

Department of Computer Science and Engineering, Islamic University of Science and Technology, Awantipora, India

Correspondence
Iraq Ahmad Reshi, Department of Computer Science and Engineering, Islamic University of Science and Technology, Awantipora, Kashmir, J&K, India.
Email: rshiraq333@gmail.com

Summary

The accelerated development of information and communication technologies has generated a demand for data storage that is effective, transparent, immutable, and secure. Distributed ledger technology and encryption techniques such as hashing and blockchain technology revolutionised the landscape by meeting these requirements. However, blockchain must overcome obstacles such as low latency, throughput, and scalability for its full potential. Investigating blockchain's structure, types, challenges, promises, and variants is necessary to understand blockchain and its capabilities comprehensively. This paper overviews various aspects, such as emergent blockchain protocols, models, concepts, and trends. We classify blockchain variants into five essential categories, DAG, TDAG, Sharding, Consensus, and Combining methods, based on the structure each follows, and conduct a comparative analysis. In addition, we explore current research tendencies. As technology progresses, it is essential to comprehend the fundamental requirements for blockchain development.

KEYWORDS

blockchain privacy, blockchain review, blockchain scalability, blockchain variants, IoT, smart contracts

1 | INTRODUCTION

Sensitive data transactions usually require an independent third party to operate separately from the communicating nodes. The server provides third-party trust in the client-server model, which handles the responsibility of trust and various communication parameters. However, the censorship of data by governments and large corporations has resulted in a shift from centralized to decentralised technology models. Furthermore, centralizing information on third-party software such as the cloud and other infrastructures compromises user privacy and confidentiality.[1]

With the increasing use of technology, individuals are exposed to additional threats to their human rights, as evidenced by governments' routine curtailment of freedom of expression through online content filtering. The right to privacy in the digital environment has also garnered significant attention in recent years due to the ease with which private data can be accessed. The growth of software like Pegasus,[2] Stuxnet,[3] and Petya[4] in the past few years highlights the problem of data centralisation. The European Union (EU) must link and coordinate control surfaces on human rights and digital policy, according to a report by Reference 5 to ensure that technologies do not negatively impact human rights.

In addition to the issues related to centralized architectures, single-point failures increase the need for a distributed system. While a single system is needed to monitor the entire network, maintaining availability without compromising security parameters is challenging, especially in cases where traffic generation is high. Following the financial crisis of 2008 and the failure of centralized systems, Satoshi Nakamoto published a paper on cash systems using peer-to-peer networks, eventually leading to the development of Bitcoin.[6] The underlying principle of Bitcoin is to

move away from third-party trust and instead focus on peer-to-peer communication. This technology stores information in blocks linked in a chain structure, hence blockchain technology.

Since the commencement of Bitcoin by the face-name Satoshi Nakamoto in 2008, this technology came to the limelight. Blockchain enables value exchange or transaction processing without a centralized issuer's trust authority. Unlike a centralized institution like a bank database, the transaction log is maintained on a decentralized ledger, constituting many peer-to-peer systems. Before accepting a transaction, the blockchain system undertakes an autonomous verification (i.e., validation), which is critical in ensuring security. Blockchain is unique in its operational functioning as it requires no trust, and safety and reliability are achieved by using particular computations or code.[7] Most blockchain networks were utilized for Bitcoin transactions until 2016. Recently, blockchain applications expanded beyond cryptocurrency and are now being used in a variety of fields like the Internet of Things (IoT), Machine earning (ML), Voting, Agriculture, and so forth, after the introduction of Ethereum Blockchain.[8] Ethereum enhanced the features and laid the foundation for developing decentralized applications using scripting called Smart Contracts.[9] Even though Bitcoin supports decentralized applications, they are platform-dependent. However, the latter supports vital features like smart contracts, which, once deployed to the network, are not controlled by the user; instead, they run as programmed.

Blockchain combines cryptography for encryption and hashing, a distributed ledger for decentralised databases and a consensus mechanism for participating parties. It ensures data integrity, confidentiality, and the elimination of third-party trust from the systems. However, in this concrete technology with decentralization and enhanced security, there is a cost of scalability. Similarly, if decentralization and privacy are kept in focus, the cost of implantation would increase; otherwise, one of the two has to be conceded.[10] Hence, having a highly secure, perfectly decentralized, and highly secure blockchain is nearly impossible, as perfectly decentralized blockchains like Bitcoin and Ethereum can process a small number of transactions per second. The transaction number in Bitcoin is far small (i.e., 7), and in Ethereum, the number ranges from 15 to 20. A specific window for research lies in this field to utilize the blockchain to its full potential and make it fully capable of carrying out all the operations it desires.

1.1 | Motivation and contribution

We came across different reviews, papers and proposals on blockchain technology that discuss applications,[11] consensus mechanisms,[12] modeling and tools,[13] and so forth. To understand blockchain better still, many comprehensive surveys need to be done. Owing to the lack of information regarding the challenges, their counter-strategies, and the different modifications of blockchain, some of the reviewed papers[14–21] provide specific insights regarding the topic. Blockchain as technology seeks certain modifications in terms of Scalability, Privacy, and Consensus.[22,23] Among the numerous blockchain platforms, apart from the most prominent ones, we have reviewed several platforms. We comprehensively analyze how well different blockchain variants are designed to achieve specific goals. These designed variants, too, seek the attention of researchers and engineers to improve their performance in terms of scalability and minimize resource utilization. Moreover, here is a pointwise contribution of this paper:

1. This paper offers insights into the different scalability challenges and a concise overview of countermeasures in the form of variants developed to address the issues.
2. A structural division of variants for scalability is done based on the mechanism they adhere to. Based on this, we classify the variants into five categories: DAG, TDAG, Sharding, Consensus, and Combined methods.
3. Blockchain solutions designed to counter privacy issues public blockchains face are mentioned alongside the prominent use cases.
4. Vulnerabilities in Smart Contracts and issues regarding computation power are described briefly, along with recently proposed solutions.
5. A section on recent research trends, blockchain promises, and their application in different sectors is reviewed.

1.2 | Selection criteria

Tables 1,2, and 3 present the introduction and comparison of the proposed work. Based on the analysis, it is observed that there is a requirement for a comprehensive survey that addresses blockchain challenges and the various variants available to counter them. This article aims to bridge the gap between existing surveys and current research on blockchain challenges, solutions, and variants. Its primary objective is to identify the multiple solutions and variants available for addressing various technical challenges when dealing with blockchain. Apart from these, we have listed the latest privacy-preserving means in different use cases in blockchain technology. Also, we identified various research areas in the blockchain field. Through this study, we hope to contribute to advancing blockchain technology and its applications in various fields. Table 2 highlights the most recent surveys and the primary areas of study tackled. Some surveys address privacy concerns and scalability issues. However, a state-of-the-art survey in this field is missing that includes all blockchain concerns and possible solutions. Similarly, Table 3 summarizes the surveys on blockchain

TABLE 1 Inclusion and exclusion criteria for selection of studies.

Inclusion criteria	Exclusion criteria
Study available in English language	Study is not available in English
Full text available	Full text is not available or partially available
The primary focus of the paper is on blockchain as a technology	Primary focus on economics
Focus on blockchain variants	Focus entirely on consensus mechanisms

TABLE 2 Summary of related work I.

Reference	Year	Main Topic	Privacy	Computation Power	Smart Contracts	Scalability
24	2018	Survey on applications of blockchain specific to IoT	✓	–	–	–
23	2019	Survey on privacy-preserving techniques	✓	–	–	–
25	2020	Comprehensive survey on blockchain scaling	–	–	–	✓
26	2021	Security enhancement techniques for blockchain	–	–	✓	–
27	2021	Survey of State-of-the-art on blockchains theories, modelings, and tools	–	–	–	✓
28	2022	Challenges of blockchain in new generation energy systems and future outlooks	✓	–	–	✓
This survey	2023	Survey on enhanced blockchains	✓	✓	✓	✓

TABLE 3 Summary of related work II.

Reference	Year	Main Topic	Sharding	DAG	TDAG	Consensus	Miscellenious
24	2018	Survey on applications of blockchain specific to IoT	–	✓	✓	–	–
29	2019	Survey on consensus, membership and structure	–	✓	–	✓	–
25	2020	Comprehensive survey on blockchain scaling	✓	✓	–	–	–
30	2021	Research and applied perspective to blockchain technology a comprehensive survey	–	–	–	✓	–
27	2021	Survey of State-of-the-art on blockchains theories, modelings, and tools	✓	✓	–	–	–
31	2022	Survey of application research based on blockchain and smart contracts	–	✓	–	–	–
This survey	2023	Survey on enhanced blockchains	✓	✓	✓	✓	✓

variants. A survey that incorporates all blockchain variants is not present up to date. In this paper, we have identified and classified blockchain variants based on the structure they follow. We have included a miscellaneous column in the table that follows a different structure apart from the mentioned ones.

1.3 | Review plan and taxonomy

A comprehensive systematic review explored solutions to challenges encountered in blockchain technology, including various variants. The review process involved accessing a range of review articles, with several excluded based on predetermined inclusion and exclusion criteria as outlined in Table 1. Relevant review articles are identified to address gaps in the current knowledge base. Various academic sources, including Wiley Online, ACM Digital Library, Science Direct, IEEE Explore, SpringerLink, Google Scholar, and Scopus, are utilized to ensure a comprehensive and rigorous review. The search terms "Blockchain Challenges", "Blockchain Variants", and "Blockchain surveys" are used across all databases. Additional advanced search terms, such as "Sharding blockchain", "DAG blockchain", "TDAG Blockchain", "Blockchain privacy", and "Blockchain scalability" are

also employed. In addition to peer-reviewed journal articles, conference papers, thesis, white papers, pre-prints, and books published in recent years are included in the review process. The basis for this classification is the structure a variant follows. Researchers try to impart different optimized structures in the blockchain to manage the number of transactions per second. For example, DAG-based blockchain systems hold the potential to achieve rapid transaction conformations while also offering scalability by allowing transactions to proceed in parallel. Another approach that enhances horizontal scalability by dividing the network's nodes into distinct shards. Each shard is responsible for a specific subset of transactions. It facilitates concurrent transactions as multiple shards work in parallel. Similarly, the innovative structure of TDAG, which is transaction-focused, excels in scalability and confirmation speed. There is no separation of roles between transaction approvers and issuers, which further simplifies network structure. Consensus is the core component of blockchain technology. Certain blockchain variants show improvement over traditional ones by altering their consensus mechanism. We included combined or miscellaneous approaches in our classification apart from the four mentioned blockchain variant classes. In this particular class, we have variants that fall in more than one class or does not fall in any of the mentioned class, that is, use new novel approaches to enhance scalability.

1.4 | Research questions

The rationale behind conducting this survey paper stems from the necessity to thoroughly investigate several critical research inquiries concerning the dynamic nature of blockchain technology. Firstly, an exploration is conducted into the present condition of solutions that are accessible for a wide range of issues encountered by blockchain ecosystems. It involves a range of challenges about scalability, security, consensus processes, and other related aspects. Our investigation aims to evaluate current options, elucidating their efficacy and constraints comprehensively. Furthermore, we explore the approaches employed by different iterations of blockchain technology in addressing these complex difficulties. Gaining insights into the varying tactics employed to overcome these difficulties necessitates a comprehensive understanding of the nuanced approaches and adjustments implemented by various blockchain implementations. Finally, the survey aims to identify the areas of research that will significantly impact the future development of blockchain technology. Identifying these gaps and areas requiring additional exploration plays a crucial role in guiding the trajectory of blockchain research and innovation. This process ensures that this disruptive technology continues to progress and adjust to the dynamic environment of the digital realm. The following research inquiries are addressed in this survey.

1. **RQ1**: What is the scenario of current solutions to various blockchain challenges?
2. **RQ2**: How do Blockchain variants address the various issues in blockchain?
3. **RQ3**: What are the various research gaps for the future?

1.5 | Structure of paper

The paper is structured as follows: Section 2 provides an overview of the core features and operational principles of blockchain, including its structure, parameters, and different types. Section 3 introduces blockchain platforms' challenges, and a survey of various strategies to counter these challenges is presented. This section discusses the challenges of scalability and solutions concerning scalability. Section 4 summarizes various blockchain platforms or variants for scalability enhancement and their comparative analysis. Sections 5 and 6 discusses privacy concerns of blockchain platforms and privacy-preserving variants. Section 7 introduces the latest use cases based on privacy-preserving blockchains. Sections 8 and 9 review smart contract vulnerabilities, computation power issues, and their proposed solutions. Finally, Section 10 discusses recent research trends in various blockchain application areas.

2 | BLOCKCHAIN: STRUCTURE AND OPERATIONAL PRINCIPLES

A blockchain is an increasing chain of Blocks where miners add and validate the Blocks. Blockchain can be thought of as a ledger where entries are chronologically timestamped. Network peers must offer the following functions to maintain and operate the blockchain-routing, storage, wallet services, and mining.[32] The blockchain protocol organizes data into blocks, each containing a list of Bitcoin or any other crypto transactions completed at a specific time. Chain structure is formed by every block linked by a pointer to the preceding block.

2.1 | Structure of blockchain

Every block consists of a header and a body. The diagrammatic representation is shown in Figure 1. The header encompasses the hash code of a block's transactions, the preceding block's hash code, a string called a nonce, and a timestamp to keep track of transactions while the body contains the transactions.

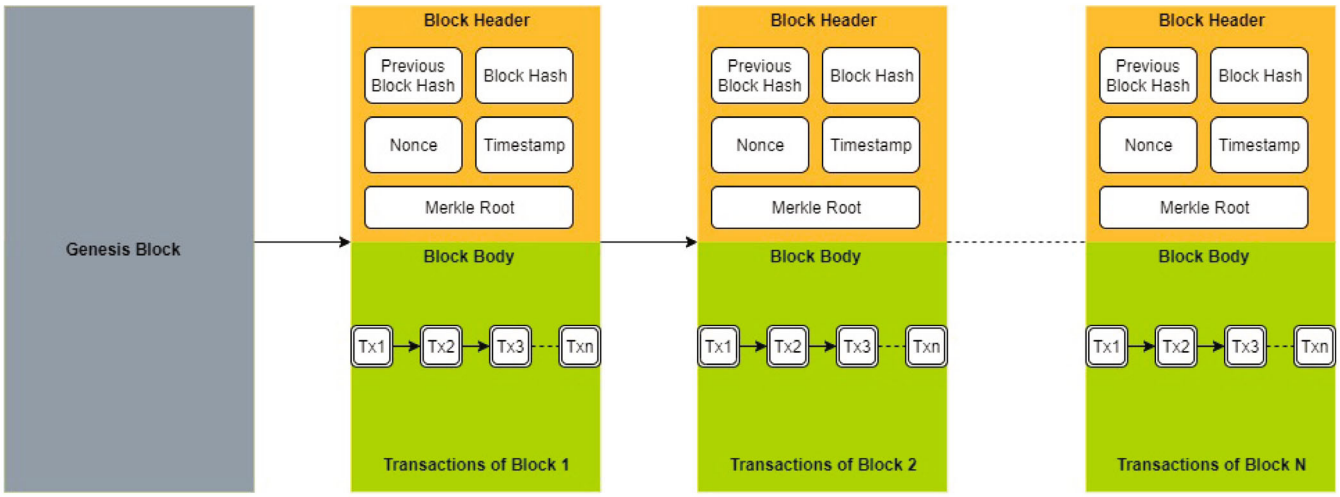

FIGURE 1 A simple representation of a blockchain.

The block from where the chain originates is a genesis block, characteristic of a particular chain. The first block does not contain the previous hash block, as its previous hash field is null. The other fields are briefly described here:

2.1.1 | Block hash

Hashing is an objective approach that converts a variable-length input into a fixed-length cryptographic output. As a result, regardless of the amount of data or file size involved, its unique hash will remain the same size. Hashes are used in various stages in a blockchain system. Each block in a blockchain carries the hash of the preceding block header, guaranteeing that nothing is tampered with when additional blocks are added. Every block in the chain, except for the first, includes a prior and current block hash. The Secure Hashing Algorithm 256 of Bitcoin is a prime illustration (commonly shortened to SHA-256). The output data of SHA-256 is always of a predefined length of 256 bits (the output is 32 bytes).

2.1.2 | Nonce

A nonce is a number or string appended to a hashed transaction in a blockchain that, when rehashed, fits the difficulty criteria. The nonce is the number that blockchain miners try to compute. When a solution is found, blockchain miners are rewarded with cryptocurrencies.

2.1.3 | Merkle tree

The concept of the Merkle tree was first introduced by Ralph Merkle in 1987 in his work "A Digital Signature Based on a Conventional Encryption Function". A data structure used to store transaction hash values is a Merkle Tree.[33] The hashing algorithm used is SHA256. The Merkle root is kept in the block header. A combined hash of all the transactions processed inside a block is placed in this structure. Merkle tree reduces the effort to verify any transaction in a particular lock. As the Merkle tree root is kept in the block's header, there is no need for the whole copy of the transaction to verify it. The major advantage of utilizing a Merkle tree is that numerous essential pieces of information about a specific data element or the data set as a whole may be validated without requiring access to the entire data set.[33] Instead, we search in that particular branch only, thus reducing the complexity from (n) to (logn). Thus, to verify a particular transaction, there is no need to download the entire blockchain.

2.1.4 | Timestamp

The timestamp stores the timing of transactions since it stores the moment the data block is mined and validated. Its function is to avoid the double-spending attack.

2.1.5 | Consensus

A consensus mechanism is a fault-tolerant technique used in blockchain technology. It mainly establishes agreement amongst distributed components or multi-agents on a particular data value or network state. It is handy for keeping track of stuff, among other things. A consensus mechanism is required in a blockchain to carry out transactions smoothly. A variety of consensus mechanisms exist in present-day blockchain systems. When implementing blockchain technology in various circumstances, distributed technology overcomes the limitations of centralization but also introduces a slew of new challenges. Bitcoin, for example, relied on the inefficient Proof-of-Work consensus mechanism. It needs the nodes to use energy for mathematical calculations. So, it becomes inefficient for systems like banks where we need more transactions to use a public blockchain. Blockchains are not completely anonymous; partial anonymity, called pseudo-anonymity, is achieved only, which proves costly in certain situations. So, in general, privacy concerns remain.[23] The other major concern to be dealt with when the chain's size keeps increasing is scalability.[34] Based on the user operation, security, and scalability, Blockchains can be of different kinds. We have different types of Blockchains depending on the problem being addressed. A brief description is provided below, and a table describes the comparison.

2.2 | Blockchain types

To summarize in brief, the various reasons that led to the cornerstone in the development of different types of blockchains are:

1. Any specific type of blockchain carries out no specific agenda.
2. Scalability and security issues with a public blockchain.
3. Pure centralization of private blockchains.

The different types of blockchains based on the above points are:

2.2.1 | Public Blockchain

Also known as a public Ledger or permissionless blockchain. Here, anyone can join the network and become a part of the chain. Because of its decentralised nature, it necessitates some method of data authentication. That approach is a consensus algorithm that allows blockchain participants to agree on the present state of the ledger. The commonly used consensus algorithm is proof of work (PoW),[35] which allows the decentralized network to agree on variables like account balances and transaction order. At the same time, more new mechanisms are being proposed and tested. The lack of the need for trust is one of the most significant advantages of the public blockchain. Everything is recorded, public, and unchangeable. The disadvantages include the need for processing power, little or no transaction privacy, and scalability. These are critical concerns of blockchain application usecases.

2.2.2 | Private blockchain

In this type of chain, a limited number of nodes get access to be a part of the chain. This type of blockchain is somewhat centralized because a single unit manages it, and only that unit provides access to different nodes. It achieves a highly scalable chain of nodes. As this type of blockchain is permission-based, there is not even partial anonymity. Its main motive is to prevent the misuse of organizational details. Depending on the use case, it can maximize the participant's trust and confidence. A private blockchain can be administered behind a business firewall and even hosted on company premises. The private blockchain has increased transactions per second (TPS) and enhanced scalability over the public blockchain. However, these blockchains did not guarantee immutability as the organization can roll back their transactions anytime. Also, security concerns increase as the number of nodes is less and malicious users can penetrate the network easily.[36] Hyperledger Fabric is designed for this type of blockchain.[37]

2.2.3 | Hybrid blockchain

A blend of permissionless and permissioned blockchain technologies. The private blockchain fixes the scalability issues, whereas the Public blockchain seeks Transparency. Moreover, the processing of sensitive data is performed on the private blockchain. Privacy is achieved using

hybrid architecture as the number of nodes involved in sensitive transactions is less specific. Hybrid Blockchains have enhanced scalability and decentralization mechanisms; they still lack control over data variables, unlike private and consortium blockchains.

2.2.4 | Consortium blockchain

This version of the blockchain is decentralized to some extent. In consortium blockchain, a group of private Blockchains collaborate. Consortium and hybrid blockchain may sound similar, but they are entirely different, the former being a combination of public and private while the group manages the latter. Examples of this type of blockchain are Quorum and Corda.[38,39] Consortium comes up with advantages like limited access, which means increased TPS, better scalability, and privacy. It helps to maintain partial transparency across the different organizations, but it is not entirely free from censorship and centralization.[40]

Table 4 demonstrates how different kinds of blockchain systems are compared. A blockchain can differ from other blockchains in terms of another parameter called consensus mechanism, as mentioned in section 2.1. A consensus mechanism is a medium by which a blockchain agrees or disagrees with a certain transaction. Different blockchains follow numerous consensus mechanisms. The underlying consensus mechanism is a critical component of a blockchain network, as it determines the performance, throughput and security. As a result, several current and unique consensus mechanisms are created to overcome the constraints of various blockchain systems. A thorough examination of these mechanisms and algorithms aids in determining how and why each blockchain performs as it does. The next section overviews basic consensus mechanisms followed by different blockchain technologies. The two most common consensus approaches are proof of work (POW) and proof of stake (POS). The most common example of this type of blockchain is Bitcoin[6] and Ethereum.[8] Adding a new block to the chain involves solving a cryptographically difficult puzzle or staking a part of the owned currency. The former is proof of work, and the latter is proof of stake. Bitcoin and Ethereum use proof of work.

2.3 | Why is consensus needed?

It's not as hard to spot double-spending as in a centralised system when one entity controls a ledger of all transactions. When Alice sends Bob $1, the central ledger manager takes $1 from Alice and provides $1 to Bob. PayPal and other payment systems meet this criterion. Cryptocurrencies, on the other hand, are not like that. The goal is to avoid having a single leader or entity in charge of the system, which complicates record-keeping as it has to be kept decentralized. To keep a decentralised system working, we need a consensus mechanism where the decisions are carried out so that we may not suffer from double-spending.

2.3.1 | Proof of work

Proof-of-Work (POW) is the initial consensus mechanism in a blockchain network. This mechanism is being used in the blockchain to verify transactions and add new blocks to the blockchain. Miners compete in POW to finish network transactions and are rewarded for their efforts. The network

TABLE 4 Comparative analysis of various types of blockchains.

Parameter	Public blockchain	Private blockchain	Hybrid blockchain	Consortium blockchain
Resistance to censorship	Achieved	Not achieved	Partially achieved	Achieved
Scalability	Scalability is a limitation	Scalability is user-specific	Highly scalable	Scalability by joint consortium
Security	Algorithm dependent	Voting based	Combined	Depends on voting of approved/multiple participants
Immutability	Immutable	Can be tampered	Immutable	Can be tampered
Chain nature	Permissionless	Permissioned/centralized	Private permissionless	Permissioned
User identity	Pseudoanonymus	Known/Approved	Pseudoanonymus/Known	Known/Approved
Use case	Cryptocurrency, electronic notarization	Internal voting, banking	Research, medical supply chain	Business consortium, research
Platform	Ethereum,[8] Litecoin[41]	Multichain,[42] Hyperledger[37]	Dragonchain[43]	Energy web foundation, R3

users trade digital tokens. A decentralized ledger organizes all transactions into blocks. However, considerable caution should be used while verifying transactions and organizing blocks. This is the duty of certain types of nodes known as miners. The primary operating concepts are the mathematical challenges and the ability to verify the answer[35] quickly.

2.3.2 | Proof of stake

Proof of Stake (POS) is a new form of consensus that blockchain technologies use to reach an agreement on a single genuine record of data history. POS validators contribute their part of currency or stake to certify (or validate) blocks into existence. In contrast, POW miners spend energy (usually electricity) to mine blocks into creation. Validators are network participants that run nodes (known as validator nodes) to propose and implement a POS blockchain. A part of cryptocurrency is staked on the chain, and nodes make themselves accessible to be picked randomly to propose a block. Other validators "attest" to seeing the block. After a specific number of attestations for a block are obtained, it is time-stamped and appended to the chain. Validators are rewarded for successfully proposing blocks (as in POW) and attesting to blocks observed.[44]

Besides these basic consensus mechanisms, blockchain technology is adapting new consensus rules to change its appearance. This field has huge advancements, and many consensus mechanisms have been developed lately. Some other consensus mechanisms proposed include References 19,45. The introduction of Green Blockchain[46] has shifted the focus towards computation-efficient mechanisms instead of the traditional blockchain, which is computationally hard. The main focus is shifting towards developing chain systems where resource consumption is not so high. We mention some of the blockchain variants based on different consensus mechanisms in the latter part of this paper.

3 | CHALLENGES AND SOLUTIONS CONCERNING SCALABILITY

The most important challenge in a blockchain is its scalability. We have a limit on the number of transactions. For example, with Bitcoin, we may produce a block after 10 min because that is the expected block time, and it can handle 3 to 7 transactions per second; also, in Ethereum, it is 15 to 20 transactions every second. The anticipated block time is fixed to a constant number to ensure miners do not compromise the chain's security by adding additional processing power. The average block time of the blockchain network is evaluated after n blocks. If the block time is longer than expected, the level of difficulty of the Proof of Work technique is reduced. In the reverse case, if the block time is shorter, the difficulty level increases, and the block time is based on this design idea. Mechanisms like sharding, sidechaining, and subchaining are proposed for countering this problem.

3.1 | Sharding

It divides the blockchain into smaller sections to scale the platform to serve more users. Compared to other shards, each shard comprises its data, making it separate and autonomous. Because sharding divides a blockchain network into distinct shards, it can assist in minimizing network latency or slowness. However, sharding has significant security issues, such as the possibility of shards being attacked.[47] Sharding is a conventional database technique presented primarily for optimizing big commercial databases. The fundamental concept of sharding technology is divide and conquer. As a result, sharding technologies divide a blockchain network into various separate networks, each comprising a subset of peers known as a shard. Sharding allows multiple parallel transactions to occur simultaneously, resulting in improved performance from the Merkle root of the transaction group. Any transaction receipt is conveniently retrieved via numerous Merkle trees. The receipts are also kept in a distributed shared memory that other shards may see but cannot modify.[48] Figure 2 depicts a sharding architecture separating the blockchain network into four shards. The network's transactions are split into shards, so each node has to process a tiny portion of the transactions that stream in.

3.2 | Sidechaining

Technologies that allow tokens and related valuable contracts and assets from one blockchain to be safely utilized on a different blockchain before being returned to the original blockchain when required.[49] A sidechain is a secondary blockchain with a two-way connection to the main blockchain. Currently, sidechains are in two platforms: (i) RSK (short for Rootstock). RSK (short for Rootstock) has built an open-source testnet named Ginger for its sidechains. RSK aims to provide smart contract capabilities on the Bitcoin blockchain, allowing quicker payments. (ii) Ardor's Blockchain Ardor's sidechains are referred to as "childchains" and are intimately linked to the main chain. Because the parent mainchain keeps few functionalities, most transactions are moved down to the childchain level. Childchains provide access to global entities like assets and currencies across chains.

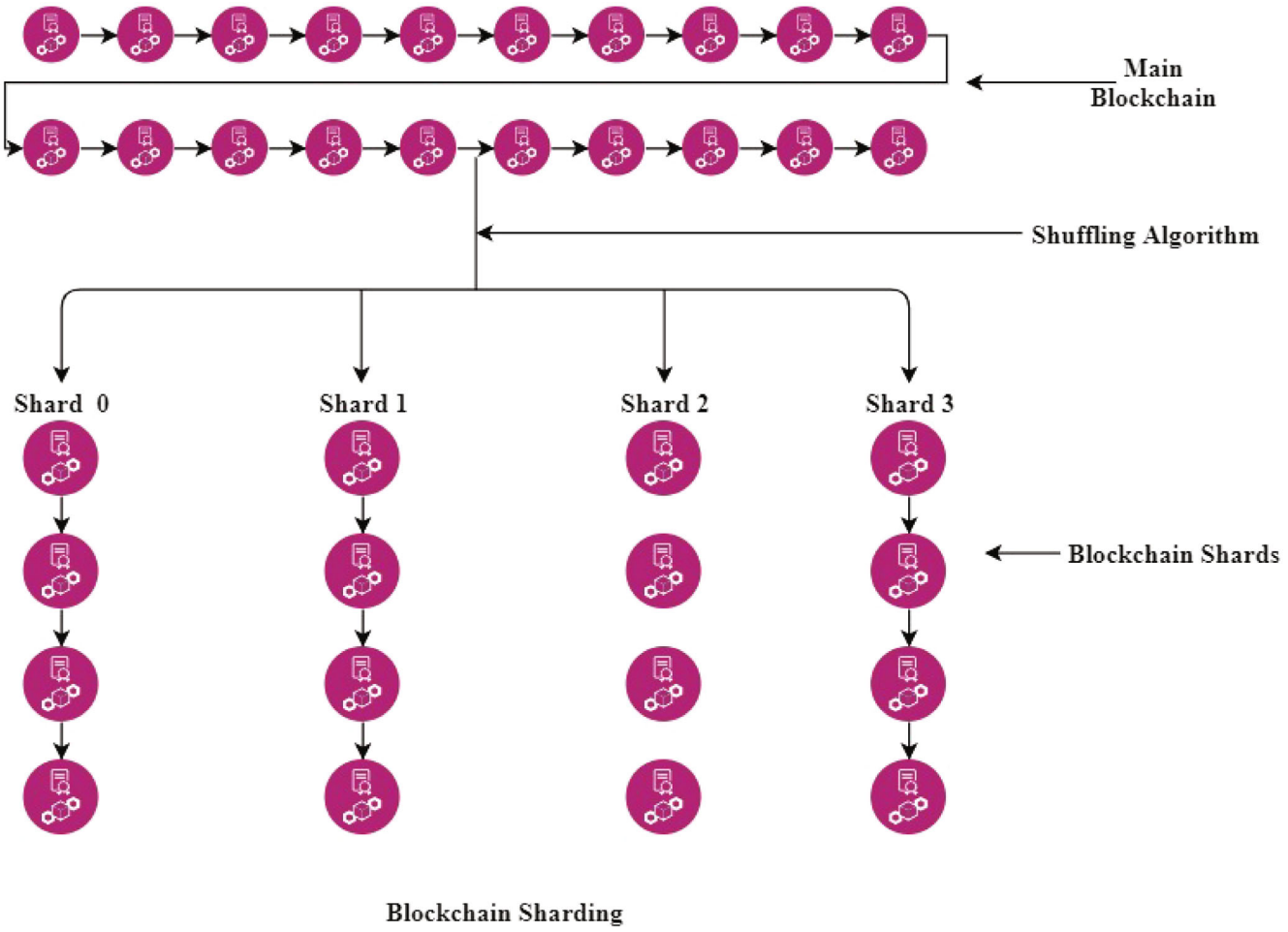

FIGURE 2 A sharding-based blockchain structure.

3.3 | Subchaining

A SubChain is a complete and self-contained blockchain. On the SubChain, the process for achieving all functionalities and consensus is the same as on the MainChain. The MainChain serves as a witness, while SubChains send data to the main chain in their blocks regularly.[34] This technique guarantees that the sub-chains and the main chain are in sync.

3.4 | Payment channel networks

Payment channel networks (PCNs) are new emerging solutions to scalability issues. Based on the concept of payment channel, which enables parties to engage in multiple transactions while updating pre-established balance commitments.[50] Despite a promising solution, PCNs face issues in routing payments effectively. Payments need to find paths having enough funds. Moreover, while flowing in one direction through a channel, payments can become exhausted, rendering routing approaches ineffective and potentially disrupting network.[51] More information about PCNs is elaborated in Reference 52.

Apart from these fundamentals, various researchers proposed some more mechanisms to enhance scalability. A survey on various scalability resolving techniques like off-chain, cashing, sidechain, interchain, and deep learning-based methods was carried out in Reference 53. Apart from the mentioned techniques, a lot of research in this direction has recently gained momentum. Some recent works are mentioned below. Moreover, researchers introduced a probabilistic verification (PV) scheme that efficiently reduces block propagation delay and fork formation.[54] PV scheme is found resistant to double-spending attacks and fake blocks. To examine the trade-off between scalability and security in sharding-based blockchain networks, a probability distribution model is suggested in Reference 55. Hypergeometric distribution and Chebyshev's inequality are commonly employed for this purpose. The top boundaries of hypergeometric distributed transaction processing and shard failure probability are primarily

assessed. A unique permissioned blockchain platform, "Rahasak," for corporate applications that require extremely high scalability is proposed. To manage real-time transaction executions on the blockchain network, the Rahasak Blockchain uses Apache Kafka-based consensus on top of a "Validate-Execute-Group" blockchain architecture.[56] In Reference 57, the efficacy of sharding remains a challenge because of the unequal distribution of malicious nodes. The many-objective optimization method based on the dynamic reward and penalty mechanism (MaOEA-DRP) is proposed to optimize the shard validation. The best blockchain sharding strategy is then found. It is evident from References 34,47,49,53–58 that a lot of research to improve scalability is going on. Still, a lot needs to be done to improve the overall system.

4 | BLOCKCHAIN VARIANTS DEVELOPED ACROSS YEARS TO COUNTER SCALABILITY ISSUES

Blockchain technology has revolutionized various industries by providing secure, transparent, decentralized solutions to many problems. However, as the popularity of blockchain has grown, so have the scalability issues that come with it. Numerous blockchain variants have been developed to address these challenges over the years. These variants employ various transaction processing and validation approaches, including sharding, directed acyclic graph (DAG), temporal DAG (TDAG), and consensus mechanisms. In addition, miscellaneous approaches have also been explored to enhance the scalability of blockchain technology. This paper provides a comprehensive overview of these blockchain variants and their comparative analysis, focusing on their ability to address scalability issues and promote the wider adoption of blockchain technology.

4.1 | Sharding based mechanisms

Sharding has emerged as a promising approach to address the scalability issues of blockchain technology. Sharding involves breaking down a blockchain network into smaller, more manageable partitions called shards, each of which can process transactions independently. This allows for greater parallelism in transaction processing, enabling blockchain networks to handle more transactions and scale more efficiently. In recent years, various sharding-based methods have been proposed and implemented in different blockchain networks, each with unique features and limitations. In this paper, we explore these sharding-based methods and their comparative analysis, focusing on their ability to enhance the scalability of blockchain technology.

4.1.1 | Monoxide

It enables system scalability while maintaining decentralization and security by operating multiple distinct and concurrent instances of solitary chain consensus systems known as zones. As the network expands, the consensus occurs autonomously inside each zone with little connectivity, dividing the effort of the whole network and ensuring a manageable load for individual nodes. As Blocks and transactions are zone-specific and maintained solely in their very own zone, the entire Monoxide network is separated into multiple parallel zones, each of which is only accountable for itself. Monoxide is the first scalable blockchain system that implements complete sharding of the consensus protocol and resource use for scalability while retaining the decentralization guarantees of POW and maintaining the same degree of security as Bitcoin and Ethereum.[59] Chu-ko-nu mining, a unique proof-of-work system, is introduced to prevent the attack bar from being lowered when mining power is distributed over many zones, and it further magnifies mining power and enables miners to create and add blocks in multiple zones. Handling transactions between shards or zones is a critical challenge in sharding-based blockchain systems.

4.1.2 | Elastico

It is the first permissionless blockchain sharding system. Participants in each Elastico consensus epoch solve the POW challenge to determine the consensus council.[60] In Elastico, the number of unit-time transactions rises linearly with available computer power—the more computing power in the network, the more transaction blocks are selected per unit of time. Elastico's network connections are efficient, and it can outperform byzantine adversaries as little as one-fourth of the total computational capabilities. Elastico secures the mining network by dividing or parallelizing it into narrower committees, each executing its transactions. Although sharding seems prevalent in non-byzantine contexts. Elastico is the first protocol contender enabling sharding with byzantine adversaries that is secure. Moreover, Elastico promises enhanced scalability by utilizing sharding mechanisms. In each epoch, Elastico creates identities and committees. Such frequent operations may harm the efficiency of transaction execution. Even though each node needs to validate transactions within its shard, nodes must keep all network data, which is a disadvantage in Elastico. It tolerates 1/4 of faulty nodes.

4.1.3 | OmniLedger

A modern decentralized ledger implemented upon Sharding and built on Elastico attempts to overcome issues surfacing Elastico. Built on OmniLedger, Atomix is a two-phase client-driven lock/unlock technology ensuring the atomicity of cross-shard transactions. OmniLedger utilizes blockDAG too, to parallelize the commitment of blocks and enhance transaction performance using Trust-but-Verify Validation. It assures security and accuracy by employing a bias-resistant public-randomness method to pick big, statistically meaningful shards to execute transactions and a fast cross-shard commit method to handle transactions affecting numerous shards atomically. OmniLedger also boosts efficiency by employing collectively signed state blocks for simultaneous intra-shard transaction execution and ledger pruning and low-latency "trust-but-verify" transaction confirmation. OmniLedger needs users to actively participate in cross-shard transactions, which makes satisfying lightweight users difficult.[87] After each epoch, OmniLedger utilises UTXO pool checkpoints, but the state is not broadcast to the network. As a result, OmniLedger is vulnerable to attackers who can corrupt a shard from a prior epoch before the new nodes of the shard bootstrap to the state during the epoch shift. This attack violates the system's liveness property.[61] It has 1/4 resilience to byzantine faults.

4.1.4 | Rapidchain

A public blockchain based on sharding that can withstand Byzantine flaws up to a third of the participants is far better than OmniLedger's 1/4 percentage. RapidChain demonstrates that in prior sharding-based protocols, transaction communication overhead significantly hinders transaction speed and response time.[62] RapidChain uses a speedy cross-shard verification mechanism to reduce the data sent per transaction, thus eliminating the need to broadcast transactions to the entire channel. RapidChain employs a provably secure re-configuration mechanism and an optimized intra-committee consensus mechanism capable of achieving extremely high system capacity through block parallel execution. Bootstrap, Consensus, and Reconfiguration are the three major components of RapidChain. The protocol begins with Bootstrap and continues in epochs, each including several epochs. A Reconfiguration step follows consensus iterations. RapidChain lets new leaders propose a different block while repositioning old block headers, which enables RapidChain to pipeline consensus iterations, increasing throughput.[62] The protocol, in particular, only permits a certain number of parties to join or depart, and the adversary may only corrupt a fixed number of additional parties with each epoch transition. RapidChain's synchronous consensus process is another flaw. In the event of a temporary loss of network synchronization, the consensus of cross-shard transactions is susceptible, and therefore consistency may fail. However, a decent tradeoff between performance and security will make Rapidchain pretty efficient.

4.1.5 | Ziliqa

It is a new blockchain framework built on Sharding technology that overcomes the scalability issue of conventional blockchain platforms.[86] The sender address allocates transactions to shards such that the same shard handles transactions from the same address. Nonces prevent double spending; when an address submits a transaction, the nonce in the account and the global state are updated.[63] Zilliqa has a unique special-purpose smart contract language and execution environment uses the underlying architecture to create a large-scale, extremely efficient computation platform. Transaction sharding is provided by Zilliqa, not state sharding. This implies that each node stores the data with terabytes of storage.[64] Ziliqa's smart contract language is based on dataflow programming, making it suited for large-scale, readily parallelized calculations. Simple computations like search, sort, and linear algebra are examples of more sophisticated computations like training neural nets, data mining, financial modeling, scientific computing, and any map reduce task.

However, some more sharding-based techniques include PolyShard,[65] which is a "polynomially programmed sharding" technique that establishes information-theoretic upper constraints on storage efficiency, system throughput and trust, allowing for a genuinely scalable system. The PolyShard system's scalability and performance advantages over the state-of-the-art are quantitatively demonstrated in simulation results. Also, Harmony[66] was proposed, which solves the issues with existing blockchains by integrating the greatest research and engineering practices into a finely tailored solution. Furthermore, owing to its distributed random-generating mechanism, Harmony was prepared to illustrate that its sharding method possesses enough security. Table 5 provides a comparative analysis of blockchain variants based on basic sharding mechanisms.

The issue of improving its efficiency without compromising any of the other two, that is, security and decentralization, is the main challenge in all existing sharding systems. Only a few efficient sharding protocols currently provide high decentralization, scalability, and security levels. As a result, there is still a lot of room for research in this area. While sharding-based approaches have been shown to enhance blockchain scalability significantly, we feel that further research and observations into the operations of several of these protocols are required. The first operation is partitioning the network into shards, the second is choosing a consensus that assures security and protection inside a cluster, and the last is picking the optimum

TABLE 5 Comparative analysis of different blockchain variants based on sharding mechanism.

Variant	Consensus	Topology	Throughput	Transaction confirmation time (s)	Fault tolerance
Monoxide	PoW with Chu-ko-nu mining	Sharding	11696 TPS	13–21	1/2
Elastico	Byzantine, PoW	Sharding	40 TPS	800	1/4
Omniledger	Byzantine, PoW	Sharding	3500 TPS	800	1/4
Rapidchain	Optimal intra committee, PoW	Sharding	7380 TPS	8.7	1/3
Ziliqa	PBFT, PoW	Sharding	1218 TPS	1800	1/3

Note: Fault tolerance indicates the fraction of tolerating the fraction of faulty nodes.

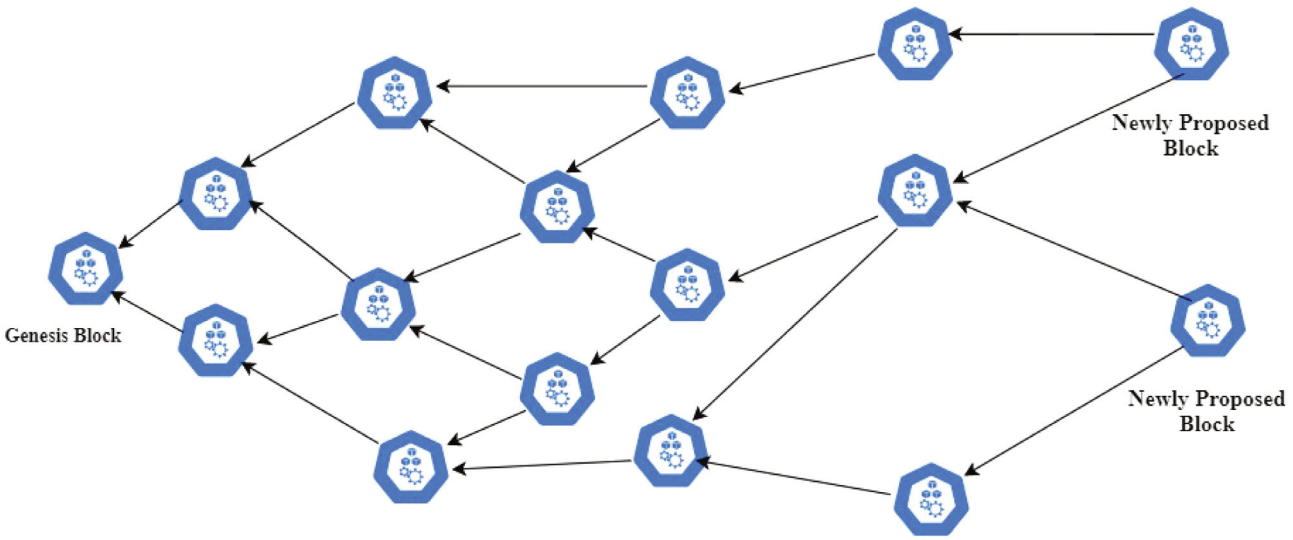

FIGURE 3 A directed acyclic graph (DAG) structure: The key distinction here is that in the blockchain, each block always refers to the previous block, but in the block-DAG, a block might refer to many prior blocks.

consensus among the committees. Moreover, authors in Reference 65 have explored the vulnerability to Sybil attacks of sharding-based blockchains. If an attacker has the enormous computational capacity to produce numerous Sybil committee members (by producing multiple legitimate node IDs), it can easily manipulate the underlying consensus mechanism. However, if the design is carried out properly, the attack can be avoided.[67]

4.2 | Directed acyclic graph based mechanisms

The directed acyclic graph (DAG) has transformed blockchain technology. DAG is quickly eclipsing older methods, given its improved validation mechanism, high scalability, efficient provenance, support for IoT, and multi-party engagement. The basic concept here is to increase the scalability of a decentralized ledger by using DAG instead of a single series of blocks. BlockDAG is based on a data structure in which blocks are arranged in a graph-like structure called DAG, as defined in Reference 68. Figure 3 describes the structure of DAG. The edges in this DAG indicate the previously published blocks to which each is related, whereas the vertices represent a single block. BlockDAG does not try to remove POW mining or transaction fees, but it uses the DAG's structural features to address the problems associated with high orphan rates in blockchains. Orphan blocks are created due to inevitable network propagation delays produced outside the longest chain. DAGs are a mathematical structure utilized by several projects not based on Satoshi's proof-of-work mechanism. BlockDAGs, conversely, are DAG applications to a Nakamoto-based system (in particular, proof-of-work), with just the data structure and consensus layer redesigned.

BlockDAG is a structural modification of blockchain, not a new consensus or any other medium. Some of the blockchain variants based on BlockDAG are:

4.2.1 | Spectre

In Spectre,[69] transactions can be verified in seconds, and throughput can be increased by magnitudes over Bitcoin; it is only restricted by network infrastructure and ability. As a result, the protocol eliminates the Nakamoto Consensus security-scalability trade-off. Spectre's key technique is a voting algorithm that determines the order of each pair of blocks in the directed acyclic graph (DAG). The voters are blocks (not miners), and each block's vote is interpreted algorithmically (rather than interactively) based on its position in the DAG. Spectre transactions can be completed in seconds, and throughput can be increased by orders of magnitude above Bitcoin; it is only limited by network infrastructure and capacity. Unlike Bitcoin and its numerous variations, Spectre is safe against attackers with less than 50% of the processing power, even when its throughput is raised and the propagation delay becomes significant. However, the increased flexibility in parent selection may increase the attack surface, like in a balancing attack. The willingness to postpone decisions on clearly double-spent transactions has been critical to Spectre's success. As a result, it addresses a weaker problem than typical consensus methods. This makes it less suited for systems requiring total order over transactions, such as Bitcoin and Ethereum.[6,8]

4.2.2 | Phantom

A protocol based on Nakamoto's longest-chain protocol. Unlike Bitcoin blocks, which include a previous block's hash on the chain they are extending, Phantom organizes blocks in a Directed Acyclic Graph, or BlockDAG. As a result, each block might include several hash references to predecessors. Phantom then orders all blocks and transactions and returns a consistent list of approved transactions. Unlike the Bitcoin protocol, which discards blocks that are not on the main chain, Phantom includes all blocks in the BlockDAG into the ledger but places attacker-created blocks lower in the order.[61,67] PHANTOM addresses scalability, trade-offs, and security concerns while ensuring a quick voting process, making it more generic and scalable than other blockchain protocols.[67] Phantom contains a parameter k that regulates the protocol's tolerance to blocks produced simultaneously, which can be adjusted to allow larger throughput. It, therefore, avoids the security-scalability tradeoff that Nakamoto's protocol suffers from. Phantom utilises a greedy algorithm on the BlockDAG to differentiate between blocks mined by non-cooperating nodes diverting from mining protocol and those created by honest nodes. The procedure for mining Phantom generates a solid overall order based on this differentiation. All honest nodes finally agree on a strategy to implement BlockDAG. Phantom is vulnerable to live-ness attack. Even if all honest nodes are perfectly synchronized, attackers with limited computational power can postpone transaction confirmation indefinitely with high probability.

4.2.3 | Conflux

Conflux is a decentralized blockchain platform that is quick, scalable, and secure. It uses intrinsic parallelism in blockchain transactions. It employs a DAG-based method to defer entire order reconciliation while maintaining the same external interface compared to traditional chain-based methods.[70] Conflux answers the scalability issue by providing a unique tree-graph consensus mechanism. The processing power of each node limits flux throughput rather than the consensus mechanism. Conflux arranges blocks into a new tree-graph structure, a tree within a (DAG). Concurrent blocks are not regarded as harmful in Tree-Graph but also contribute to the Conflux ledger. Their POW solutions enhance the finality of all of their ancestors, and their transactions are put in the ledger total order in the most efficient way possible. This protects Conflux against double-spending attacks while also increasing its throughput.[70] Conflux's consensus protocol intrinsically incorporates two alternative block generation methods to combat liveness attacks: an optimistic strategy that allows quick confirmation and a conservative strategy that assures consensus progress. Conflux combines these two techniques into a single consensus process using its innovative adaptive weight mechanism. Table 6 analyses different DAG-based Blockchain variants based on throughput, consensus and other characteristics.

In a recent study, Zhou et al.[71] proposed DLattice, a public blockchain framework with a novel double-DAG architecture. DLattice employs a novel protocol, DPOS- BA-DAG (PANDA), to achieve a consensus among users. DAG-based systems offer new models with great throughput and

TABLE 6 Comparative analysis of different blockchain variants based on DAG mechanism.

Variant	Consensus	Topology	Throughput	Transaction confirmation time (s)	Technique	Smart contract support	Ledger
Spectre	PoW	DAG	1000+ TPS	10–120	Pairwise Vote	No	Permissionless
Phantom	PoW	DAG	1000+ TPS	10–120	K-cluster	Yes	Permissionless
Conflux	PoW	DAG	6400 TPS	Less than minute	Adaptive weighted protocols	Yes	Permissionless

scalability because of their underlying architecture. However, the area has become increasingly complicated, with various shapes and patterns that might confuse novices. In conclusion, combining PHANTOM and SPECTRE allows quick confirmation times and liveness. It is still uncertain to accomplish a linear ordering without jeopardizing the speed of confirmation. Conflux's unique consensus process protects it from double spending and liveness attacks, even when the block creation rate is high. Conflux offers a potential solution to the blockchain's performance constraint and opens up many blockchain applications. Future advancements, particularly structural shifts, have a range of effects on performance, scalability, and security.

4.3 | TDAG based mechanisms

TDAG is a DAG structure made out of transactions rather than blocks. Each transaction has a list/Merkle tree of hashes from previous transactions. Particularly because of the ever-increasing data expansion, TDAG systems have two advantages over blockchain or blockDAG designs, that is, speed and scalability. Once put onto the network, each new transaction receives at least partial confirmations from peers very quickly, meaning no longer delays for miners to secure a new block. In terms of scalability, TDAG surpasses blockchain and blockDAG. Local peers confirm each transaction for faster mining. With many transactions, the TDAG structure expands and is not restricted to linear processing like other non-TDAG blockchains. This structure is extremely beneficial where the number of transactions per second is more like IoT networks.[18] Transactions in a TDAG merely reference parent transactions that are visible immediately to the issuer. As a result, TDAG outperforms blockDAG techniques since there is no need to wait for new blocks to be mined, and transactions may be confirmed instantly. The following provides a review of some of the best-known TDAG-based approaches.

4.3.1 | Tangle (IOTA)

Tangle is for the Internet of Things. Tangle is believed to be an evolutionary step after blockchain and offers features needed to create a machine-to-machine micropayment framework. With essential characteristics, including micropayment support and no transaction fees, IOTA is a potential platform for Internet-of-Things (IoT) applications.[72] It is employed when someone wants to keep a distributed ledger without blockchain technology. Tangle does not need total node miners. Validating new transactions requires comparing them to two prior transactions, thereby reducing time and memory needs.[73] The consensus process of the IOTA protocol has its basis in the Markov Chain Monte Carlo (MCMC) algorithm.[73] Transactions are connected using a weighted random walk. The focus of this stroll is on heavy transactions or ledger branches. Heaviness is a metric that reflects how many more transactions in the DAG directly or indirectly reference a specific transaction. The integer holding this is called cumulative weight. The higher a transaction's cumulative weight, the more likely it is to be included in the DAG's main, agreed-upon branch.[74] Because all data in the Tangle are permissionless, the privacy level provided by IOTA is unknown. Parasitic chain attacks are a vulnerability for IOTA, where a parallel chain intermittently connects to the DAG.[75] There is a scope for further improvement in the MCMC algorithm.

4.3.2 | Avalanche

Avalanche is a consensus system that uses random network sampling and a metastable mechanism. Avalanche refers to a specific instance of a broader family of consensus procedures based on DAGS.[47] Metastability denotes a lack of equilibrium, which is crucial for blockchains as they lean in one direction to achieve consensus. Avalanche is intended to shift consensus towards one choice in an ultra-decentralized (no leader) and secure (probabilistic selection) way. This suggests that the most potent miners or the nodes with the highest stakes (effectively, network leaders) need to be in control of the network. Instead, all nodes come to a consensus using probabilistic sampling, which involves selecting sets of nodes and their decisions at random and accepting the majority decision.

4.3.3 | Byteball

Instead of using the blockchain, Byteball stores and transfers data using directed acyclic graph (DAG) technology. This system operates similarly to blockchains in that a new block scans all previous blocks to complete the transaction. Blackbytes[76] are a second currency utilized on the Byteball platform. Blackbyte transactions are much less traceable than byte transactions, accessible on the DAG. Instead of being stored in a public database, blackbyte data is transmitted directly from peer to peer.[77] Byteball arranges transactions in a network topology, but with the help of trustworthy and reputable witness nodes, it finally creates a main chain. These nodes separate themselves from other nodes by creating witness units regularly.

TABLE 7 Comparative analysis of different blockchain variants based on TxDAG mechanism.

Variant	Consensus	Topology	Throughput	Transaction confirmation time	Smart contracts supported
IoTA (Tangle)	Total weight of transactions, PoW	TxDAG	1500 TPS	1–5 min	Yes
Avalance	Metastable BFT protocols	TxDAG	1300-5000 TPS	4.2 s	Yes
Byteball	Validation by witness	TxDAG	10 TPS	30 s	Yes
Nano	Weighted voted on conflicting transactions, PoW	TxDAG	1000+ TPS	0.14 s	No

A Main Chain Index (MCI) that connects to a witnessing unit identifies each unit. The MCI is allocated to each vertex v, corresponding to the height of the nearest central chain vertex with a directed path to that vertex. When a node wishes to link a new connection with a tip, it must first assess its legitimacy and MCI. Meanwhile, the MC is picked collaboratively between the witness group and the network. Byteball's witness group, which consists of 12 trustworthy entities, decides the next vertex of MC. Witness participation in the blockDAG allows assigning a witness degree to contender nodes or vertices. The witness with the highest witness index is assigned to MC.

4.3.4 | Nano

Nano is a permissionless cryptocurrency with a unique lattice-based design that achieves consensus using delegated Proof of Stake voting.[78] Nano obtains consensus by a weighted vote on competing transactions. While retaining a robust and decentralized system, this consensus mechanism allows for faster, more deterministic transactions. Nano is still growing and has established itself amongst the effective cryptocurrencies in terms of performance. Nano provides fee-free transactions and possesses a huge scaling capacity. In nano, each user possesses their blockchain, which they maintain asynchronously to the blockchain network, leading to fast transactions with minimum bandwidth.[79] Account balances, instead of transaction amounts, are tracked by transactions, allowing for aggressive database cleaning while maintaining integrity. The initial beta version of Nano (RaiBlocks) was published in December 2014, establishing it as one of the earliest Directed Acyclic Graph-based cryptocurrencies.[78] Analysis of different TDAG based blockchain variants is provided in Table 7.

TDAG protocols are perfect for permissionless networks because they scale with more participants. To address the scalability limitations of current blockchains, they allow users to choose or configure a plug-and-play consensus algorithm. This architecture also addresses the issue of transaction fees and costly blockchains. The optimal TDAG, according to Nano, must have minimal latency and great efficiency. For transaction validation, proof of work, provenance, dynamic contract creation, negotiation/renegotiation, and other purposes, clever and cost-effective algorithms must be designed and developed.

4.4 | Consensus

Consensus protocols are the foundation of a blockchain network because they ensure consistency and integrity, resulting in tamper-proof and immutable features. The POW and POS are the most typical blockchain protocols, as mentioned in section 2.3. Alternative consensus protocols develop specific blockchain variants.

4.4.1 | Stellar

Stellar is a well-known cryptocurrency project that specializes in payment processing. The Stellar project aims to close the gap between cryptocurrencies and centralised financial institutions like banks. The Stellar consensus protocol (SCP) is an open-membership quorum-based Byzantine agreement system. Individual node local configuration decisions are combined to form quorums. SCP is a novel, fully accessible Byzantine agreement protocol that uses the peer-to-peer structure of the financial network to obtain global agreement underneath a unique premise. This allows for the atomic commitment of irreparable transactions between untrusting parties. There is much debate among cryptocurrency users about whether Stellar, a fork of Ripple, should be considered as the genuine coin or the fork.[80]

4.4.2 | Ripple

Ripple works on the Ripple protocol consensus algorithm (RPCA) consensus mechanism. The main motive behind its introduction is latency with other variants. Within the broader network, the proposed technique featured collectively-trusted subnetworks. The confidence needed for these

TABLE 8 Comparative analysis of different blockchain variants based on consensus mechanism.

Variant	Consensus	Topology	Throughput	Transaction confirmation time (s)	Smart contracts supported
Stellar	SCP	Open ledger	2000 TPS	5	Yes
Ripple	RPCA	Open ledger	1500 TPS	3–5	No
EOSIO	BFT, DPOS	Shared ledger	4000 TPS	30	Yes

subnetworks could be higher and much lower with careful selection of member nodes.[81] Ripple serves the banking and finance industries. Rather than revolutionizing how ordinary people trade or hold wealth, its primary goal is resolving difficulties inside the banking industry. Each server compiles a list of all legitimate transactions it has witnessed before the start of the consensus. This list is known as the "candidate set." The candidate sets of all servers on its Unique Node List (UNL) are combined, and voting on the authenticity of all transactions is conducted. A transaction requires agreement from at least 80% of a server's UNL in the last consensus round.

4.4.3 | EOS.IO

A decentralized, open-source platform that permits decentralised apps to scale vertically, for example, explore sophisticated database technologies to increase exibility and throughput). Moreover, horizontally, for example, investigate parallel execution of smart contracts). Byzantine fault tolerance (BFT) and Delegated proof of stake consensus (DPOS) techniques are being used by EOSIO. With no transaction fees, a high transaction rate, and exceptionally low latency, EOS.IO claims to be able to service millions of users. However, with EOS.IO, a block can be validated by 15 or more producers out of the 21 available.[82,83] EOS.IO suffers from a lack of decentralisation due to this small number of producers. EOSIO further suffers from bot accounts.

Table 8 provides a comparative analysis of different blockchain variants based on a consensus mechanism. The consensus protocol, among others, is the fundamental mechanism underpinning blockchain's security and efficiency. Numerous consensus methods, from modest tweaks to several replacement consensus algorithms, are proposed to improve the blockchain's performance directly or fulfil specific application demands. The primary goal is to enhance the scalability and security of the blockchain. While developing a consensus mechanism, the focus is on developing a blockchain that consumes less computation power.

4.5 | Miscelleneous approaches

Besides utilizing DAG, TxDAG, sharding, and consensus mechanisms, there are certain variants of blockchain that either fall in more than one mechanism or entirely use different underlying technologies. These variants produce enhanced scalability and throughput and are currently under research. Some of the variants in our survey are:

4.5.1 | Hashgraph

Hashgraph, a successor to blockchain, offers better speed, fairness, lower cost, and security. A blockchain is like a tree that needs pruning as it grows to prevent the branches of blocks from expanding out of reach. It ensures that the ledger has only one chain of blocks. In Hashgraph, instead of removing new growth, it is incorporated into the ledger. This ensures that the network grows and evolves over time without losing any important information.[84] Hashgraph is more effective than blockchains since any transaction container is inserted into the ledger, and none are discarded. Both of the divisions exist indefinitely and are intertwined into a single whole. Moreover, Hashgraph is inexpensive, fast, and more efficient than blockchain.

4.5.2 | Graphchain

A system that avoids blockchains in favor of constructing a distributed ledger in the form of a self-scaling graph. The transactions occurring in the system are cross-verified. Newly generated transactions validate previous ones, establishing a thin network. The system employs a cumulative consensus mechanism of the Proof of Work type, ensuring that each participant receives fair rewards.[85] It provides a

better technique for building blockchain systems by replacing the original chain's structure with the graph data structure. Additionally, everyone knows that a single miner processes all transactions in the Bitcoin system, resulting in much pointless work. Consequently, an alternative approach to optimize resource efficiency is to switch from competition to voting and concurrent mining.[86] Increasing the number of miners reduces the likelihood of all nodes going offline. Parallel mining proves beneficial in the development of high-availability blockchain systems.

4.5.3 | Chainweb

The Chainweb design maintains a consistent global hash rate and energy demand while providing high levels of Proof-of-work throughput. A chain with a concurrent POW architecture that aggregates hundreds (if not thousands) of independently mined peers into a unified platform with throughput surpassing 10,000 transactions per second. Peer chains combine their Merkle roots together to produce a single mega-chain with a total hash power equal to the sum of each chain's hash rates.[87] Each network chain mines the same currency, which is sent from one chain to another via a two-step, trustless Simple Payment Verification (SPV) at the smart contract level. Chainweb provides increased security by substantially minimizing confirmation depth and significantly increasing performance. Chainweb avoids the liquidity and centralisation issues of employing dedicated channels for scalability while complying with current worldwide regulations. Chainweb delivers these advancements while retaining POW's fundamental trustless, decentralized character. This protocol allows for greater practical decentralization and an environment where companies, individual users, and big mining pools may coexist happily by acting selfishly.

4.5.4 | Blockclique

The restriction is addressed with the Blockclique design, which shards transactions in a block graph with a fixed number of threads. The design enables the simultaneous generation of inherently compatible blocks, with each block referencing one preceding block of each thread.[88] It was the first to use transaction sharding with a directed acyclic block graph structure. The Blockclique design divides blocks of transactions into several threads based on the input address of the transaction, allowing nodes to parallelize block creation while prohibiting nodes from spending the same coins in many threads simultaneously. The blockclique consensus rule makes an ideal clique of suitable blocks, allowing a block generated in one thread to be coherent with a block formed in another thread at the same time, allowing the rate of compatible blocks and transactions to be broadcasted to the network to scale while trying to keep the fork rate low.

4.5.5 | Polkadot

A heterogeneous multichain with scalability. Unlike earlier blockchain implementations, which focused on providing a single chain with various degrees of generality across potential applications, Polkadot is meant to have no intrinsic application functionality. On the other hand, Polkadot offers the foundational "relay chain" upon which a considerable variety of validatable multiple coherent dynamic data structures coexist side by side, called parachains. Polkadot is a sharded multichain network. It can process many transactions on multiple chains simultaneously, bypassing the bottlenecks plaguing traditional networks that process transactions one at a time.[89] This parallel processing capacity enhances scalability and offers the ideal environment for greater adoption and future growth. It is compatible with other blockchains inside and outside of cryptocurrency, allowing for the construction of smart contracts and new blockchains (and tokens) and transmitting information across blockchains. Although the Polkadot project is marketed as highly compatible, its compatibility has some limitations. External blockchains, like Ethereum, need a bridge to interface with the Polkadot Relay Network. Nevertheless, bridging protocols for Polkadot, like ChainX and Clover, are gaining ground, which needs further development.[90]

4.5.6 | Cosmos

Cosmos is a network of interconnected blockchains. The main goal of Cosmos is to create a crypto ecosystem of independent parallel blockchains that can scale and communicate with one another. The network comprises several blockchains, each referred to as a zone. Those zones communicate with one another through the use of the Inter-Blockchain Communication (IBC) protocol, which uses consensus techniques like Tendermint consensus to allow heterogeneous chains to interchange values which are either token or data.[91] Tendermint BFT is a mechanism used to protect the network, validate transactions, and commit blocks to the blockchain by a distributed network running the Cosmos Blockchain. Tendermint Core

TABLE 9 Comparative analysis of different blockchain variants based on combined approaches.

Variant	Consensus	Topology	Throughput	Transaction confirmation time	Smart contract supported
Hashgraph	Randomised gossip	Multiple parallel chains	10,000+ TPS	3–5 s	Yes
Graphchain	Proof of luck (POL)	Natural expanding graph	Limited by communication networks	Bandwith limited by communication networks bandwith	Yes
Chainweb	Parallelized POW	Multiple parallel chains	Limited by communication networks bandwith	Limited by communication networks bandwith	Yes
Blockclique	PoW	Multithreaded and transaction sharding	10,000 TPS	0–59 s	Yes
Polkadot	Nominated POS	Sharding and cross-chain paralell	1000 TPS	60 s	Yes
Cosmos	Tendermint BFT	Parallel chains	1000 TPS	6 s	Yes

is the heart of Tendermint, a proof-of-stake (PoS) governance mechanism that maintains Cosmos Hub's distributed network of computers in sync. Unfortunately, prominent PoW-based blockchains like Bitcoin and Ethereum cannot link directly to Cosmos Hub. In such a scenario, bridges are necessary for connecting reasons, just as in the case of Polkadot. Comparative analysis of the variants based on combined approaches is provided in Table 9.

RQ1: What is the scenario of current solutions to various blockchain challenges?

Researchers and the industry have focused on developing multiple blockchain variants to address multiple blockchain challenges. The variants work on a similar underlying principle as that of the blockchain. However, it comes up with certain advantages as well as disadvantages. Considering the blockchain trilemma, its developers have developed a keen interest in catering to the various security vulnerabilities and scalability issues. The main motive behind various variants is to develop a scalable, secure, and purely decentralized blockchain system. Figure 4 depicts graphical representation of transaction time with transactions per second of different blockchain variants. In our survey, we have mentioned some of the variants based on scalability and energy consumption.

RQ2: How do blockchain variants address the various issues in blockchain?

In this paper, we examine some of the most well-known scalability methods. We create a taxonomy to identify and assess the already proposed solutions by analyzing and having a comparative analysis of their capabilities, strengths, and limitations. A hybrid model of techniques needs to be designed to have a proof, scalable and secure system. Protocol designers must consider the tradeoff between decentralization and scalability based on actual requirements.

5 | CHALLENGES AND SOLUTIONS CONCERNING PRIVACY

As blockchain technology expands into various industries, privacy concerns are increasingly pressing. While blockchain is renowned for its transparency and immutability, these features occur at the cost of privacy, particularly in public blockchain networks. This has led to a growing need for solutions that can strike a balance between privacy and transparency. In this paper, we explore the challenges and solutions concerning privacy in blockchain technology. We examine the various privacy issues associated with blockchain networks, such as pseudonymity, traceability, and information leakage, and the solutions proposed to address these challenges, including zero-knowledge proofs, ring signatures, and homomorphic encryption. By providing a comprehensive overview of the privacy concerns and solutions in blockchain technology, we aim to contribute to developing more secure and privacy-enhanced blockchain systems. In permissionless blockchains that form the major portion of blockchain networks, one can be a part of the chain, and the platform provides pseudo-anonymity from which inferences are drawn to expose the real ID, using various techniques like graph modeling.[92] Once the ID is revealed, every operation related to that ID is exposed, including transactions, wallet details, and so forth. Real privacy implies the user should be completely obfuscated by design. In this section, We will discuss certain solutions regarding blockchain privacy.

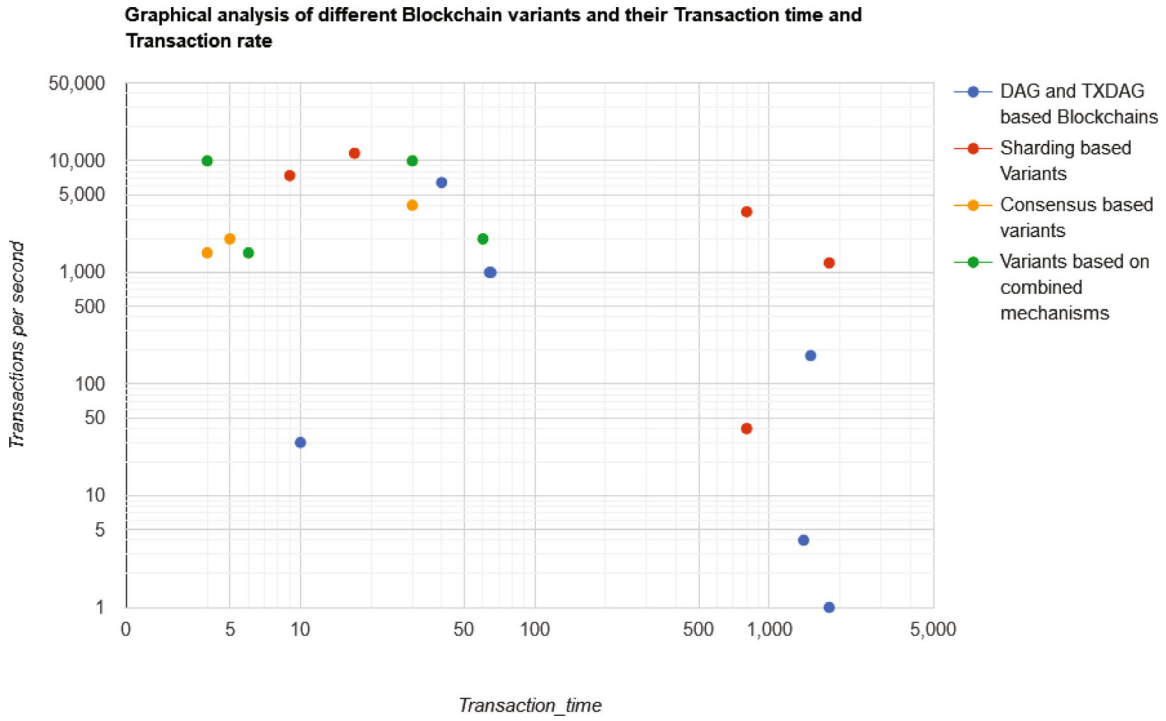

FIGURE 4 Graphical representation of transactions per second and transaction time of various blockchain variants.

5.1 | Privacy solutions

In response, various privacy solutions are proposed to enhance the privacy and security of blockchain networks. These solutions include advanced cryptographic techniques such as zero-knowledge proofs, ring signatures, and homomorphic encryption. Additionally, privacy-focused blockchains, such as Monero and Zcash, emerged with unique features that aim to provide greater anonymity and confidentiality. In this paper, we explore these privacy solutions and their comparative analysis, focusing on their ability to enhance the privacy and security of blockchain networks. Mixing[93] strategy to preserve privacy in the blockchain environment. The working mechanism is to collect inputs from the different transactions and hide values from intermediaries after proper mixing. Another approach is to apply a differential privacy preservation strategy that enhances data privacy by adding some noise during query evaluation and separating noise and data at the output.[94] Moreover, some encryption techniques are used to enhance privacy in blockchain, but these methods are computationally efficient and a handsome trade-off between computation and privacy is needed.[95,96] Privacy is something that is still a broader research area in blockchain and a lot more needs to be done in this particular area.

6 | VARIANTS OF BLOCKCHAIN FOR PRESERVING PRIVACY

The importance of privacy cannot be overstated; that is why various iterations of blockchain are developed. These innovative technologies provide a secure and reliable way to protect sensitive information, ensuring data is never compromised. These variants employ different approaches to address privacy concerns and provide greater confidentiality and anonymity. We explore these variants of blockchain and their comparative analysis, focusing on their ability to enhance the privacy of blockchain networks. We examine different variants of blockchain that are proposed and implemented, such as privacy-focused blockchains, hybrid blockchains, and permissioned blockchains, and assess their effectiveness in preserving privacy. By providing a comprehensive overview of blockchain variants for preserving privacy, we aim to contribute to developing more secure and privacy-enhanced blockchain systems.

6.1 | Zcash

Zerocash's implementation ensures complete anonymity by utilizing cutting-edge cryptographic technology, widely recognized for its reliability. It incorporates the present transparent payment mechanism of Bitcoin with a protected payment method protected by non-interactive

zero-knowledge arguments (zk-SNARKs).[97] This implementation, however, has a small scope for further development as it needs more support for solid user interaction.

6.2 | Hawk

A decentralized smart contract system does not record plaintext monetary transactions on the blockchain network, protecting transaction anonymity in the eyes of the public. Hawk programmers build private smart contracts in an effortless manner that does not need encryption.[98] A proper cryptographic protocol is generated automatically by the compiler. Contracting parties communicate with the blockchain and employ zero-knowledge proofs based on cryptographic primitives. Hawk programmers maintain the privacy of the system and provide user interactive platforms in the form of contracts.

6.3 | Ring signature blockchains

Ring signing is an encryption system that allows anyone participating in a group to produce signatures in the name of participants without disclosing the individual signer's identity.[99] This gives group members anonymity that a universal digital signature system cannot provide.

6.4 | Monero

Monero is a privacy-focused cryptocurrency that aims to give users greater anonymity and confidentiality than other cryptocurrencies like Bitcoin. Monero uses various techniques to obfuscate transaction details, including ring signatures, stealth addresses, and confidential transactions, making it difficult to trace transactions back to specific individuals or addresses. Monero has recently gained popularity among those prioritising privacy and anonymity in their financial transactions.[100]

6.5 | Traceable monero

Monero provides a high level of anonymity to users and transactions by including "chaff coins" or "mixins" with actual coins spent, making it difficult to trace the source of transactions. However, anonymity in cryptocurrency transactions is exploited for criminal activities, making user accountability or traceability necessary. The paper introduces a new cryptocurrency, Traceable Monero, that balances user anonymity and accountability by overlaying Monero with two tracing mechanisms–tracing one-time addresses with money flows and tracing long-term addresses. This framework relies on a tracing authority but is optimistic that it is only involved in investigations when required. Traceable Monero is secure and has minimal overhead compared to regular Monero transactions.[101]

7 | PRIVACY PRESERVING BLOCKCHAIN USE-CASES

We will have an overview of various privacy-preserving blockchain systems.

7.1 | Score voting

Score voting is a type of voting in which voters assign a number score to each candidate instead of just choosing one. By enabling a more precise and sophisticated representation of the voter's decisions, we can better understand their choices. However, traditional voting methods have several privacy and security issues, such as the potential for vote tampering and vote purchasing. By offering a decentralized and immutable platform for vote recording and counting, blockchain technology is utilized to overcome these issues. Voters protect the privacy of their vote while allowing for public verification of the vote count by employing cryptography. Moreover, by eliminating the need for a central authority to oversee the voting process, blockchain-based score voting boosts democratic confidence and transparency. Based on blockchain technology, an e-voting system that protects privacy and lets people vote from afar while keeping the privacy and integrity of their votes.[102] The proposed system lets people vote by score and protects the votes with encryption. So that wrong voters cannot change the score value, the scheme lets voters show that the score they submit falls within a range already set before the vote is added to the blockchain. Simulations are conducted to test the scheme's safety and capacity

to handle up to 10,000 transactions concurrently. The plan uses blockchain technology to deal with concerns about privacy and security in remote voting systems.

7.2 | Tracing model

The pandemic of COVID-19 has created an urgent need for contact tracking to halt the spread of the virus. A contact tracing approach built on a privacy-preserving blockchain assists in safeguarding user privacy while enabling efficient contact tracing. With this concept, an individual's personal information and location data are encrypted and anonymized before being stored on the blockchain. When a user tests positive for COVID-19, the test result is recorded on the blockchain. Users with close contact with the infected individuals are notified without revealing the individual's identity. Using blockchain technology can assist in verifying the data's integrity and provide a secure platform for contact-tracing activities; privacy-preserving algorithms make such systems user-friendly. The protocol in Reference 103 employs an auditable ABE scheme built on blockchain technology and local differential privacy (LDP) to provide user privacy. The suggested approach offloads encryption and decryption to service providers, easing the computing burden on mobile devices. The method also employs smart contracts to prevent unfair execution and fix the issue of malicious cloud servers providing misleading search results. The accuracy of the data, the computational overhead, the storage performance, and the fairness of the proposed method are all assessed. The findings demonstrate that the scheme's efficiency and privacy protection are at their peak. It is fantastic to witness the amalgamation of LDP technology and blockchain, significantly improving tracing systems' dependability. This is a crucial step towards disease prevention and control. With these cutting-edge advancements, we can all be more assured of our ability to ensure our safety and communities.

7.3 | Data sharing

In numerous industries, including healthcare, finance, and supply chain management, blockchain-based data sharing is growing in popularity. Sharing sensitive data between businesses in these sectors is a cause of worry. A privacy-preserving blockchain provides a secure platform for sharing information without revealing identities. The use of encryption in blockchain-based data sharing protects the confidentiality and safety of the exchanged information. In addition, smart contracts can be utilized to enforce access control restrictions, thereby giving granular access control over shared data. In addition to facilitating effective data management and reducing data duplication, blockchain-based data exchange also improves data integrity. To ensure the efficacy of blockchain-based data exchange, it is necessary to design and implement stringent privacy and security safeguards. A framework for private and secure data sharing on permissioned blockchains using Groth signatures and anonymous credentials to verify users without revealing their true identities is presented in Reference 104. The proposed protocol also provides an anonymous authentication technique based on ElGamal commitment and one of many proofs to protect sensitive information from snoopers further. Data storage, ACLs, and storage addresses are all recorded by the blockchain platform, making the protocol more secure. The protocol has been installed and tested on several devices with positive results. A proposal for a vital use case of data sharing in Blockchain-based Internet of Vehicles (IoVs) using lightweight-BIOV is presented in Reference 105. The findings demonstrate that the BIoV architecture effectively decreases the computational power costs and significantly enhances the generation and exchange of robust nodes.

7.4 | Mining pool selection

Mining pools are group of miners who combine computer resources to maximise their likelihood of mining blocks in a blockchain network. However, mining pools might offer privacy hazards to their members because they demand that miners reveal their wallet addresses and divulge other sensitive information. In the context of mining pool selection, blockchains provide a privacy-preserving solution by enabling miners to join mining pools anonymously and earn rewards without revealing their wallet addresses. One way is using zero-knowledge proofs (ZKPs) to establish that miners can join a specific mining pool without revealing their identity. An alternative method is a decentralized identity management system that enables miners to create and manage their identities on the blockchain without releasing personal information. Miners can preserve privacy while participating in the blockchain network by incorporating privacy-preserving features into mining pool selection. The study in Reference 106 presents a verifiable and privacy-preserving cloud mining pool selection strategy (VPP-CMPS) for Internet of Things (IoT) devices to deal with privacy and scalability concerns. The suggested strategy employs the additively homomorphic ElGamal cryptosystem to safeguard information during the selection process, while the improved time-locked puzzles technique is used to detect fraudulent mining pools. Moreover, the strategy uses a cooperative, somewhat dishonest cloud server to lessen the computing burden on IoT devices throughout the selection process. The experimental outcomes demonstrate the suggested strategy's effectiveness and low computing cost.

7.5 | Healthcare

Blockchain-based systems provide the healthcare industry with numerous advantages, such as safe and efficient management of electronic health records (EHRs) and optimized medical billing procedures. However, when deploying such systems, privacy considerations need to be addressed to protect patient confidentiality. Solutions constructed using privacy-preserving blockchain technology can provide confidentiality features such as selective disclosure of information, secure data sharing between healthcare providers, and anonymous data analysis for research purposes. For instance, an EHR based on the above system can enable consumers to maintain control of their medical data and select which healthcare providers can access it. Moreover, smart contracts streamline and protect the medical billing process, lowering the possibility of false claims and billing errors. To ensure patient data privacy, robust encryption and access control system needs to be implemented. A blockchain-based system for sharing EMRs that protects patient confidentiality is proposed in Reference 107. The approach provides no single point of failure in the interplanetary file system and identity-based sign encryption for granular access control (IPFS). Smart contracts and blockchains can track and log who has accessed what data and when. Experimental results demonstrate that the suggested approach satisfies data privacy and integrity requirements at a lower computing cost than other relevant works.

7.6 | Identity management

Identity management has become a key concern for individuals and enterprises in the digital era. By providing a secure, decentralized, and irreversible system that may prevent identity theft, fraud, and data breaches, blockchain technology provides the ultimate answer for identity management. Identity management systems based on blockchain technology can speed up identity verification processes for enterprises, save expenses, and increase productivity. To fully reap the benefits of blockchain-based identity management, various privacy problems, such as the risk of data breaches, inadequate data protection regulations, and user control over their data, must be addressed. To ensure that personal information stays secure and private in blockchain-based identity management systems, it is vital to adopt the proper privacy-enhancing technology. To secure users' privacy without compromising authentication, researchers in Reference 108 have proposed a privacy-preserving identity management (PPIdM) system built on blockchain technology. The system uses cryptographic techniques such as zk-SNARK and SSS to safeguard user privacy and identify policy violations by bad actors. Game theory is used to examine and prove the system's security requirements informally.

7.7 | Certificate management

Certificate management based on the blockchain has emerged as a solution to the problem of certificate counterfeiting in online education and job applications. These technologies must offer privacy and security to prevent malicious behaviors such as cyber-attacks and identity theft. Using cryptographic hash and digital signature in blockchain-based peer-to-peer networks helps alleviate numerous security and privacy concerns. One approach involves creating and storing student identities using IPFS tokens. To protect the privacy and security of certificate management, the suggested system can employ techniques such as EdDSA (Edward-curve Digital Signature Algorithm) for digital signature and verification and SHA-256 for cryptographic hashing. The potential of blockchain technology for certificate administration in online education is explored in Reference 109 but admits the security and privacy risks associated with such an implementation. The suggested system produces and stores student IDs in IPFS using tokens, EdDSA for digital signature, and SHA-256 for cryptographic hashing. In terms of privacy, transaction cost, colossal file storage, blockchain implementation, and registration cost, the system's performance is compared to previously implemented alternatives. The outcomes demonstrate that the suggested system has a faster transaction speed and reduced transaction and registration costs, making it a more practical option.

The proposed schemes leverage the benefits of blockchain technology, such as immutability, transparency, and distributed storage, to address issues such as privacy breaches, forgery of certificates, identity theft, and cyber-attacks. These schemes use cryptographic techniques such as digital signatures, cryptographic hashing, and zero-knowledge proofs to ensure data privacy and security. Experimental results demonstrate these schemes' efficiency and lower computational cost than existing systems. Future work in this area may include exploring new cryptographic techniques, developing efficient consensus algorithms, and exploring the potential of other privacy-preserving algorithms for other blockchain use cases.

8 | VULNERABILITIES IN SMART CONTRACTS

A smart contract denotes a code computer program or transaction protocol intended to automate the execution, control, and recording of legally required events and activities in line with the provisions of a contract or agreement.[9] Since blockchain technology has implicit protection features, like immutability and transparency, the weakest link is susceptible to flaws within smart contracts. One area of blockchain research

is the development of security requirements for scripting smart contracts so that no vulnerabilities jeopardize the security of the devices in the network.

In Reference 110, they researched solidity smart contracts. They summarized that the Ethereum blockchain is a dynamic and volatile environment that requires significant upgrades to become a trustworthy digital medium. This study enables us to understand and classify errors in the probable. The comprehensive classification of research allows smart contract developers to fully comprehend the flaws and vulnerabilities, enhancing smart contracts' overall reliability and safety. Li et al.[111] offer extensive explanations of previously established security measures and improvements, including SmartPool,[112] a mining pool system that aims to avoid the 51% attack. Tikhomirov et al.[113] categorize smart contract bugs into four categories: security, functional, operational, and developmental. SmartCheck, a static analyzer capable of identifying these issues, is presented. The findings of the experimental evaluation, which employed more than 4000 working smart contracts, demonstrate that SmartCheck is exceptionally successful. According to Reference 114, multi-player games, Rubix, the DAO attack, GovernMental, King of the Ether throne, and dynamic libraries are among the six types of attacks found in Ethereum smart contracts. There is a thorough description of each sort of assault. These attacks involve vulnerabilities with Solidity, EVM byte code, and fundamental blockchain technology flaws. A vulnerability analysis tool, Oyente, a smart contract analysis tool, can be applied to avoid malicious contracts.[115] Another tool called Neucheck uses a syntax tree in conversion from source code to intermediate representation, and then open-sourced libraries of XML are used to evaluate these trees.[116] Smartshield is another rectification system that handles the errors in bytecode itself and makes a contract secure for deployment.[117]

Because of the immutability of blockchain, existing security response techniques (such as code patching) must be altered to address insecure smart contracts. Before a smart contract is put on the blockchain, the only correct method to safeguard it is to fix any potential vulnerabilities in its code. Much research in this field is required to deploy smart contracts on a blockchain platform safely.

9 | COMPUTATION POWER

Before a transaction is added to the network, it is verified and trusted via the Proof-of-Work method. This method requires substantial processing power to analyze, validate, and, most importantly, secure the whole network. POW is the consensus method used by both Bitcoin and Ethereum. However, to eliminate this computation overhead, Ethereum 2.0 is a planned upgrade that will use POS as a consensus protocol. In POS, we have validators who validate blocks instead of miners. A part of currency as the stake is required to become a validator. Moreover, Proof of work works on brute force, and miners must know how far they lie from the solution. Various researchers have published much research to cater to this infeasibility by proposing algorithms with less computational power. There has been published a lot of significant work in this area. In References 15,19,21,45, authors have reviewed a lot of consensus mechanisms like Proof of burn, Proof of activity, Proof of capacity, Proof of elapsed time, and so forth, and their comparative analysis. Each of these mechanisms performs better in aspects like time, energy consumption, currency consumption, resource consumption, and so forth. This paper has mentioned some computationally easy mechanisms that consume a few resources.

The paper[118] suggested using Alt-POW as an alternative mechanism for solving puzzles based on progression. This Alt-POW method gives users an enhanced network picture of each miner's performance in the block-finding process, allowing them to determine whether it is in their best interests to drop out of a block competition or continue to devote energy to it. It also gave a mechanism that allows for multiple interconnected chains rather than a single blockchain, allowing for parallel block discovery. Participants can choose which chain to devote their resources to based on which chain has the best chance of allowing them to mine successfully at any given time. The paper[119] presents a unique lightweight proof of block and trade (POBT) consensus method for IoT blockchains and an integration framework for it. This approach speeds up the validation of transactions and blocks. Proof of Block and Trade algorithm ensures block security during trade validation and generation phases. Furthermore, a lightweight consensus method that integrates peers based on the number of nodes in a session is employed. This lowers the computing time peers require and enables more excellent transaction rates for resource-limited transactions in IoT devices with limited capabilities. In Reference 53 presented Proof-of-Useful-Randomness (POUR), a novel useful POW that reduces energy loss by integrating pre-computed (disclosable) randomness into the POW. The basic idea is to incorporate unique randomness into puzzles using algebraic commitments that may be saved and later revealed. Unlike inefficient POWs, this technique allows for the use of pre-computed commitments by a wide range of public-key cryptography methods that need offline-online processing (e.g., digital signature, key exchange, zero-knowledge protocol). PoUW generates usable randomness, reducing energy waste and avoiding the high transition costs of other consensus algorithms while retaining POW's architecture. The original POW mining approach awarded the first successful finisher of a computing race for a single block at a time. The runners in the first round are granted some exclusivity in the next round for solving the puzzle. The number of competing nodes in the following round, as well as the number of resources wasted, will be significantly reduced as a result of this. This is the basis of a new emerging technology called Green Blockchain.[120] A software-defined networking (SDN) approach integrated with blockchain to overcome the high energy consumption of POW consensus mechanism.[121] This approach makes blockchain appropriate for IoT devices with limited resources, and testing results showed its supremacy over a classical blockchain. An optimization framework for integrating blockchain with IoT was proposed with decreased consumption.[122] This work performed dynamic offloading through mobile edge computing (MEC). The problems of prominent dimensional characteristics were solved using deep reinforcement learning (DRL). Table 10 provides an overview of the challenges and various countermeasures to tackle these issues.

TABLE 10 The table provides an overview of various challenges and their countermeasures.

Challenge	Proposed tackling mechanisms	Contribution
Scalability	Sharding[47]	Blockchain is divided into multiple shards, thereby reducing slowness utilizing parallelism.
	Sidechain[49]	Allows some computation-intensive operations to be performed on the sidechain, reducing the burden on the original chain.
	Subchain[34]	Utilizes the concept of layering; the more layers in the chain increase, the more scalability.
	Payment channel netwoks[52]	Allows multiple transactions while updating pre-established balance commitments.
	Offchain, interchain and DL[58]	Survey on scalability resolving techniques like offchain, cashing, sidechain, interchain, and deep learning approaches.
	PV scheme[54]	Scalability and efficiency enhancement of blockchains using probabilistic verification and clustering.
	Probability distribution[55]	Comprehensive direction for developing efficient sharding protocols using mathematical probability.
	Rahasak[56]	Rahasak, a highly scalable blockchain with increased throughput.
	MaOEA-DRP mechanism[57]	Optimization of sharding with MaOEA-DRP mechanism.
Privacy	Zcash[97]	A shielded pool-based privacy preservation mechanism over Bitcoin protocol.
	Hawk[98]	Interactions on blockchain between the contracting parties occur using cryptographic primitives like zero-knowledge proofs.
	Ring signature[99]	A communication signed with a ring signature has been approved by someone from a certain group of individuals.
	Mixing[93]	Random mixing of transactions to remove linkability.
	Differential privacy[94]	Addition of random noise so that the inferences drawn from statistical analysis are infeasible.
	Encryption based privacy[95]	Protection using public and private keys.
Smart contracts	SmartPool[112]	A mining pool for subverting attacks.
	Smartcheck[113]	Static analyzer for detecting bugs.
	Oyente[115]	Tool for bug analysis and returns attack possibility.
	Neucheck[116]	Tool based on syntax analysis that looks for vulnerabilities.
	Smartshield[117]	Automatic bytecode rectification tool.
Computation power	Alternative PoW[118]	Based on progression while solving puzzles.
	Proof of block and trade (PoBT)[119]	Addressed this problem by decreasing the number of peers involved and restricting verification to trades only.
	Proof-of-useful-randomness (PoUR)[53]	The basic idea is to incorporate unique randomness into puzzles using algebraic commitments that may be saved and later revealed.
	Green POW[120]	The runners who have mined previously are given an advantage.
	SDN with blockchain[121]	Software defined networking architecture provides a programmable interface for the network and makes it independent of the data plane, thus reducing unnecessary computations.
	MEC with DRL[122]	Used deep reinforcement learning for computation offloading in blockchain powered MEC.

The consumption of resources by the traditional POW algorithm for blockchain systems is a concern and needs immediate addressing. A survey on electricity consumption by blockchain systems indicates the importance of research in this particular area.[111] Despite existing techniques and algorithms, more solutions are needed to tackle this problem.

RQ3: What are the various research gaps for the future?

10 | RECENT RESEARCH TRENDS

Blockchain technology has garnered considerable attention over the past decade, and this trend shows no sign of abating. Researchers and practitioners continuously seek new ways to use blockchain technology to enhance existing systems or establish new ones. In a recent survey by Huang et al.,[82] they mentioned IoT and IIoT, consensus protocols, and security and privacy as the three most surveyed topics in blockchain. Researchers are addressing the privacy, scalability, interoperability, and energy consumption issues that come with the increasing deployment of blockchain technology across multiple businesses. Current advances in blockchain research have been on improving the security and privacy of blockchain-based systems, examining novel consensus processes, enhancing the scalability of blockchain networks, and building interoperability solutions to enable cross-chain communication. This section will highlight new research trends in blockchain technology and explore their potential implications for the future of blockchain. Figure 5 highlights the recent research trends of blockchain.

10.1 | Internet of things

In the past decade, the issue of single-point failure in IoT networks has been a significant challenge that required a decentralized mechanism provided by blockchain technology.[20] Integration of blockchain with IoT has become a popular research trend as IoT devices generate large amounts

FIGURE 5 Depicts the various recent research directions in blockchain technology.

of data that require a secure, transparent, and decentralized platform for storage, management, and sharing.[18,19,123] Blockchain and IoT integration can revolutionize various industries, such as supply chain management, healthcare, energy, and transportation. However, addressing the integration challenges requires in-depth research focusing on efficient and scalable consensus algorithms, lightweight cryptography, privacy-preserving techniques, and energy-efficient mining algorithms.[22] Apart from providing a trustless environment for IoT devices, researchers are implementing blockchain for the security, data management, and monetization of IoT devices. Designing a secure and energy-efficient protocol that considers both IoT and blockchain technology is still an open issue, and there is a need to converge the technologies to make IoT devices scalable for particular blockchain types. To summarize, research on blockchain-based IoT includes, Examining the potential of blockchain to increase the security and privacy of IoT devices and networks, such as by protecting data transmissions and regulating access to IoT devices. Investigating the potential of blockchain to provide smooth interoperability between heterogeneous IoT devices and networks, including facilitating cross-device data sharing and compatibility between various IoT platforms. Exploring the potential for blockchain to provide autonomous and decentralized governance of IoT networks and devices, such as enabling distributed decision-making and resource distribution. Investigating the potential of blockchain to enable secure and decentralized storage, processing, and sharing of Internet of Things (IoT) data, such as enabling data marketplaces and promoting data sharing amongst stakeholders.

10.2 | Agriculture

Due to its potential to enhance food quality and transaction speeds, blockchain technology is gaining traction in the agriculture business. With food safety concerns that directly impact public health, the lack of transparency and quality control in food supply chains has been a long-standing issue. To address these issues, experts have investigated blockchain technology, which offers a unique level of credibility and traceability that can improve food quality.[124] Safeguarding agricultural forecasting events and node transactions within the distributed and decentralized network are discussed in Reference 125. However, blockchain technology in agriculture is in its infancy, and additional research is required to reach its full potential.[126,127] With the rise of smart farming techniques employing IoT sensors in agriculture, blockchain can play a significant role in preserving the immutability and transparency of the food supply chain. In addition to the existing blockchain research in agriculture, several more areas require further investigation. One such field is the creation of efficient and scalable supply chain management solutions for agricultural products based on blockchain technology. Integrating blockchain with other developing technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), for effective administration and monitoring of crop development and disease prevention is an additional study direction. Additionally, there is a need for research to determine the ideal use cases for blockchain in agriculture and assess the economic feasibility of integrating blockchain technologies into the business. In addition, creating interoperability standards for blockchain-based agricultural systems would facilitate frictionless data exchange across stakeholders. Lastly, tackling the issue of scalability in agricultural blockchain systems is a crucial research path. There is a need for additional research to grasp blockchain technology's benefits in agriculture fully. More insights into blockchain in agriculture are: Using blockchain to provide end-to-end traceability and transparency of agricultural products, such as tracing the origin, quality, and safety of food products. For example, investigating the potential of blockchain to improve the efficiency and sustainability of agricultural production by enabling precision farming and resource optimization. Exploring the potential for blockchain to allow safe and decentralized identity management and financial services for smallholder farmers, including access to loans, insurance, and market data. Investigating the potential for blockchain to facilitate decentralized and collaborative agricultural research and development, including data sharing and intellectual property management.

10.3 | Business applications

Blockchain technology has the potential to alter several industries radically. Integration of blockchain technology can result in increased transaction speed, decreased transaction costs, and increased security. Blockchain can streamline supply chains, improve inventory control, and automate payments. Moreover, blockchain can provide a secure and tamper-proof way for authenticating documents and intellectual property rights. Various business sectors are extensively studying blockchain technology for implementation.[128,129] However, we must actively explore the full potential of blockchain technology in commercial applications and develop more efficient and scalable solutions.[130] The application of smart contracts in business is also a fascinating field of research, as it can help automate complex business operations and decrease the need for intermediaries. Further possible research insights include, Examining the potential of blockchain-based solutions for various industries, including healthcare, finance, and logistics. Exploring the use of blockchain technology for digital identity management and verification, which has the potential to increase security and reduce fraud across a variety of corporate operations. Creating smart contract-based solutions for supply chain management and other business operations that are more efficient and secure. Solving the scalability and interoperability issues between blockchain networks and commercial processes.

10.4 | Healthcare

The medical industry needs help adjusting to an increasing technological infrastructure that includes Internet-enabled devices, Internet of Things (IoT), smart devices, and sensor data. Blockchain technology can solve some of the medical sector's problems. Given the ledger and block-related architecture, blockchain technology's most promising uses in the healthcare sector are due to its features like integrity, confidentiality, and immutability. Blockchain technology can efficiently facilitate drug tracing, supply chain management, and infection tracing in pandemic scenarios. Some more possible directions could be, using blockchain to safely store and share electronic medical records (EMRs) to promote data privacy and interoperability across healthcare providers. Examining the potential for blockchain-based healthcare systems to minimize healthcare fraud and abuse, better supply chain management, and improve patient outcomes. Assessing the ethical and legal consequences of implementing blockchain technology in healthcare, including data ownership, consent, and liability issues.[131–133]

10.5 | Integration with other recent technologies

Surveys are looking into combining blockchain with fog/edge nodes, AI, ML, and big data. Blockchain technology improves security and reliability. Also, it can benefit ML for trusted decision-making, decentralized intelligence, and data and model sharing. The challenges are being addressed and are the focus of researchers from various backgrounds, including big data processing, scalability of integration, and resource management.[134–136] A state-of-art review about power automation and distribution using Artificial intelligence and blockchain is presented in Reference 137. A Digital Forensics Chain-of-Custody for surveillance mechanism is proposed in Reference 138. The process establishes a Blockchain network to facilitate the exchange of investigation information among involved stakeholders. This information includes details related to video surveillance, the pre-processing of frames, and the chain of custody. The experimental results demonstrate that the proposed solution offers superior performance, with robust tracking of real-time video surveillance, automatic frame filtering redundancy, and efficient investigation of objects of interest. Moreover, other insights in this field include, Exploring how blockchain can protect and certify machine learning models and data across multiple industries, including finance, healthcare, and transportation. Exploring the potential of merging blockchain with deep learning algorithms to provide decentralized and privacy-preserving artificial intelligence applications, such as fraud detection and medical diagnosis. Creating novel cryptographic primitives and algorithms to integrate blockchain technology and machine intelligence.

10.6 | Online voting

Because of its decentralized character and safety function, blockchain has recently attracted interest in decentralized application systems. It offers a whole new approach to storing, disseminating, and updating data, and it will be critical in developing the way the world looks. In the paper,[139] they discussed and contrasted current research contributions to the problems for existing blockchain-based e-voting methods. On the other hand, the growing requirement for security and privacy safeguards might be a roadblock to the development of actual blockchain applications. Therefore, much more must be done in this field to have a better and more efficient voting system.[140–142] Possible guidelines could be, Investigating the possibilities for blockchain-based voting systems to improve the security, accessibility, and transparency of online voting. Assessing blockchain-based voting systems' security and privacy concerns, such as vote manipulation, coercion, and anonymity breaches. Creating innovative consensus mechanisms and cryptographic protocols for scalability and security in blockchain-based voting systems.

10.7 | Smart contracts

The smart contract is a crucial component of the blockchain. It is a technology relevant to various applications beyond cryptocurrencies, including healthcare, IoT, supply chain, digital identification, business process management, and more. Although there has been significant development in recent years in improving blockchain technology with an emphasis on smart contracts, there needs to be more analysis of the smart contract topic.[143] The development of smart contract execution performance and the overall performance of blockchain-based apps is still in its early stages.[9] To make blockchain-based apps viable in actual markets, extensive research is necessary to close the existing gap,[114,144] which might include the following. Examining the potential for smart contracts to automate and expedite various corporate operations, including supply chain management, insurance claims, and real estate transactions. Creating new programming languages and techniques, such as formal verification and code auditing, to improve the usability and security of smart contracts. Assessing smart contracts' legal and regulatory ramifications, including contract enforceability and liability concerns.

10.8 | Security

The introduction of blockchain technology has aided the development of service-sharing techniques while appearing to be a feasible answer to some security issues.[145] The inbuilt features of technology like hashing and contract immutability provide a good scope for integrating it with vulnerable systems and improving their security.[146–148] The framework proposes distributed drone monitoring through Fog computing in Reference 149. This paper addresses the privacy and security concerns of managing UAV (Unmanned Aerial Vehicle) data through fog-cloud technology. The deployment of a blockchain-aware dynamic distributed monitoring system tackles issues related to transaction execution, security, and privacy within fog-cloud-based nodes. Furthermore, this system records node transactions and ensures integrity, transparency, and robust data scheduling, processing, and management performance. Probable research directions are, Exploring the security and privacy implications of blockchain technologies, including the dangers of 51% assaults, double-spending, and transaction forgery. Creating novel cryptographic primitives and techniques, including zero-knowledge proofs and homomorphic encryption, to improve the security and privacy of blockchain systems. Assessing the resistance of blockchain systems to assaults such as network partitioning, Sybil attacks, and insider threats.

10.9 | Banks and finance

Blockchain technology can streamline corporate operations while generating safe, trustworthy records of agreements and transactions in the banking and financial services area. For the banking and financial services industries, blockchain technologies provide several appealing features.[150] Such robust systems may function as decentralized networks without needing a central server or a single point of failure. They have integrity because they operate utilizing distributed open-source protocols and do not require the involvement of a third party to complete transactions.[151–153] Further research directions are, Investigating the potential of blockchain technology to improve the efficacy, transparency, and security of financial transactions, such as cross-border payments, trade finance, and asset tokenization. Assessing the regulatory and compliance implications of utilizing blockchain technology in the financial sector, including anti-money laundering (AML) and know-your-customer (KYC) regulations. Creating innovative financial products and services based on blockchain technology, including decentralised exchanges, stablecoins, and asset-backed securities.

10.10 | Supply chain

The applicability of blockchain technology and smart contracts to supply chain management is critically explored in Reference 154. Trustworthy blockchain-led business and supply chain transformation is still ongoing and in its early phases. Future research might proceed in this direction, with sustainability's environmental and social/humanity dimensions, such as the United Nations' Sustainable Development Goals (SDGs), being utilized to investigate the effectiveness of blockchain-enabled supply chains. Several prospects for a more profound knowledge of this technology and its implementation in supply chains go beyond standard information systems and web-based integration.[154–156] More insights could be, Exploring the potential of blockchain to improve the traceability, accountability, and sustainability of supply chain management, such as validating the provenance and validity of commodities. Creating novel consensus techniques and cryptographic protocols to enable safe, decentralized supply chain networks. Assessing the economic and environmental consequences of using blockchain in supply chain management, including the costs and benefits of blockchain-based systems compared to conventional supply chain models.

Table 11 highlights the research work conducted in the above-mentioned fields.

11 | CONCLUSION

Blockchain technology has emerged as a promising solution for attaining transactional immutability, decentralization, and transparency. It addresses the growing need for efficient, secure, and unchangeable data storage in the constantly evolving realm of information and communication technologies. However, the increasing adoption of blockchain technology presents several significant obstacles: concerns surrounding scalability, privacy, latency, and throughput. This study has comprehensively explored blockchain technology, covering its various varieties, complex structures, problems, potential benefits, and evolving iterations. Through an in-depth exploration of a wide range of blockchain variants, models, concepts, and trends, we have aimed to offer a complete comprehension of this revolutionary technology. One of the primary findings of this investigation is the classification of different types of blockchain into five distinct categories: directed acyclic graph (DAG), temporal directed acyclic graph (TDAG), sharding, consensus, and combining techniques. The classification, grounded on the structural approach employed by each variety, has facilitated a comparative examination that illuminates their merits and drawbacks. As we delve into the realm of blockchain study, it becomes apparent that there is still more ground to cover in this ongoing exploration. Blockchain technology is advancing and promising, exploring different forms and

TABLE 11 Research in various blockchain application related scnerios.

Area	References	Proposed work
Internet of things	123	Review on security threats and possible solutions for a blockchain-based IoT system.
	19	Research directions to increase the compatibility of integration of IoT and blockchain systems.
	20	Analysis of various challenges and open issues for implementing blockchain in IoT systems.
Agriculture	124	Blockchain enabled traceability in agricultural supply chain.
	126	Transparency and traceability in Soyabean utilizing smart contracts.
	127	Technical elements and applications of blockchain technology in the agricultural sector.
Business	130	Business architecture based on blockchain to avoid inconsistencies in time and consensus-based biasing.
	128	Review of blockchain-based business applications and services in the public and private sector.
	129	Analyze various ambivalent dimensions of blockchain technology for business.
Healthcare	131	Review highlights the state of the art of blockchain and its development in healthcare.
	132	Review aims to reveal various prototypes and potential health applications of blockchain technology.
	133	Research opportunities in various blockchain-based healthcare domains.
ML and DL	134	Machine and deep learning-based algorithms for cryptocurrency price prediction with high accuracy. (Tested on Monero and Litecoin).
	135	Survey on possible research gaps upon combining ML with blockchain technology.
	136	A privacy-preserving framework for blockchain called Deepchain, which utilizes deep learning methods.
Online voting	140	Practical and secure blockchain-based e-voting system catering to the problem of forgery in traditional e-voting.
	141	Blockchain-based e-voting (BEV) that enables vote casting using tamper proof IDs anonymously via smartphone or PC.
	142	A transparent and cost-efficient voting scheme built on blockchain.
Smart contracts	9	Smart contract based automation utilizing IoT and blockchain technologies.
	144	Challenges in implementing smart contracts and recent technical advances.
	114	Review on security attacks and the tackling mechanisms on smart contracts.
Security	146	Overview of various algorithms and security mechanisms including contract-based approaches for privacy and integrity preservation.
	147	Blockchain-based trusted data provenance system for cloud security.
	148	A blockchain-based system for better privacy and security in smart factory.
Banks and finance	151	Survey on challenges and opportunities for banking with integrated blockchains.
	152	Promotion of multicenter, intermediate scenarios for enhancement and improved efficiency of banking industry.
	153	Smart contract design for consent driven hyperledger blockchain platform that forms core of KYC applications.
Supply chain	155	Insights about future research propositions for adoption of blockchain technology in supply chain management.
	156	Introduction of circular economy with blockchain that eliminates weaknesses in the traditional supply chain.
	154	Discusses means to leverage blockchain technology for enhancing the supply chain in times of risk.

ongoing enhancements. This progress lays the foundation for developing a robust and scalable blockchain infrastructure. The infrastructure above possesses intrinsic characteristics such as immutability, decentralization, and transparency, potentially transforming several industries significantly. This transformation will encourage innovation and create new opportunities for developing creative solutions. We have a strong enthusiasm regarding the potential of blockchain technology to revolutionize transaction processes, enhancing their security, transparency, and efficiency. As the field of blockchain research progresses, the transformational potential of this technology is likely to become more evident, establishing a future in which blockchain functions as the fundamental basis for trust and security within an ever-changing digital landscape.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Iraq Ahmad Reshi https://orcid.org/0000-0002-6061-3488

REFERENCES

1. Kamongi P, Kotikela S, Kavi K, Gomathisankaran M, Singhal A. Vulcan: vulnerability assessment framework for cloud computing. Paper presented at: 2013 IEEE 7th International Conference on Software Security and Reliability. IEEE. 2013:218-226.
2. Chawla A. Pegasus spyware–'a privacy killer'. Available at SSRN. 2021:3890657.
3. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security. Paper presented at: IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society. IEEE. 2011:4490-4494.
4. Fayi SYA. What petya/notpetya ransomware is and what its remidiations are. *Information Technology-New Generations*. Springer; 2018:93-100.
5. Wagner B, Bronowicka J, Berger C, Behrndt T. *Surveillance and Censorship: the Impact of Technologies on Human Rights*. Publications Office; 2015.
6. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Decentral Bus Rev*. 2008;21260.
7. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inform*. 2019;36:55-81.
8. Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*. 2014;151(2014):1-32.
9. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. *IEEE Access*. 2016;4:2292-2303.
10. Kim SJ. An impossible trinity in blockchain-based transactions: decentralization, privacy, and lower transaction costs. ShanghaiTech SEM Working Paper. 2020.
11. Pilkington M. Blockchain technology: principles and applications. *Research Handbook on Digital Transformations*. Edward Elgar Publishing; 2016.
12. Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun Surv Tutor*. 2020;22(2):1432-1465.
13. Yasaweerasinghelage R, Staples M, Weber I. Predicting latency of blockchain-based systems using architectural modelling and simulation. Paper presented at: 2017 IEEE International Conference on Software Architecture (ICSA). IEEE. 2017:253-256.
14. Zheng Z, Xie S, Dai H-N, Chen X, Wang H. Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv*. 2018;14(4):352-375.
15. Lie X, Jiang P, Chen T, Xiapu L, Qiaoyan W. A survey on the security of blockchain systems future generation computer systems. 2017.
16. Lin I-C, Liao T-C. A survey of blockchain security issues and challenges. *Int J Netw Secur*. 2017;19(5):653-659.
17. Al-Jaroodi J, Mohamed N. Blockchain in industries: a survey. *IEEE Access*. 2019;7:36500-36515.
18. Dai H, Zheng Z, Zhang Y. Blockchain for internet of things: a survey. *IEEE Internet Things J*. 2019;6:8076-8094.
19. Wang X, Zha X, Ni W, et al. Survey on blockchain for internet of things. *Comput Commun*. 2019;136:10-29.
20. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and iot integration: a systematic survey. *Sensors*. 2018;18(8):2575.
21. Gao W, Hatcher WG, Yu W. A survey of blockchain: techniques, applications, and challenges. Paper presented at: 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE. 2018:1-11.
22. Reshi IA, Sholla S. Challenges for security in iot, emerging solutions, and research directions. *Int J Comput Digit Syst*. 2022;12(1):1231-1241.
23. Hassan MU, Rehmani MH, Chen J. Privacy preservation in blockchain based iot systems: integration issues, prospects, challenges, and future research directions. *Future Gener Comput Syst*. 2019;97:512-529.
24. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchains in the internet of things: a comprehensive survey. *IEEE Commun Surv Tutor*. 2018;21(2):1676-1717.
25. Yu G, Wang X, Yu K, Ni W, Zhang JA, Liu RP. Survey: sharding in blockchains. *IEEE Access*. 2020;8:14155-14181.
26. Wang Y, He J, Zhu N, et al. Security enhancement technologies for smart contracts in the blockchain: a survey. *Trans Emerg Telecommun Technol*. 2021;32(12):e4341.
27. Huang H, Kong W, Zhou S, Zheng Z, Guo S. A survey of state-of-the-art on blockchains: theories, modelings, and tools. *ACM Comput Surv*. 2021;54(2):1-42.
28. Wang T, Hua H, Wei Z, Cao J. Challenges of blockchain in new generation energy systems and future outlooks. *Int J Electr Power Energy Syst*. 2022;135:107499.
29. Natoli C, Yu J, Gramoli V, Esteves-Verissimo P. Deconstructing blockchains: A comprehensive survey on consensus, membership and structure. arXiv preprint arXiv:1908.08316. 2019.
30. Johar S, Ahmad N, Asher W, Cruickshank H, Durrani A. Research and applied perspective to blockchain technology: a comprehensive survey. *Appl Sci*. 2021;11(14):6252.
31. Lin S-Y, Zhang L, Li J, Ji L-L, Sun Y. A survey of application research based on blockchain smart contract. *Wirel Netw*. 2022;28(2):635-690.
32. Antonopoulos AM. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc; 2014.
33. Szydlo M. Merkle tree traversal in log space and time. Paper presented at: International Conference on the Theory and Applications of Cryptographic Techniques. Springer. 2004:541-554.

34. Yu Y, Liang R, Xu J. A scalable and extensible blockchain architecture. Paper presented at: 2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE. 2018:161-163.
35. Liu D, Camp LJ. Proof of work can work. Paper presented at: *Weis*. Citeseer. 2006.
36. Golosova J, Romanovs A. The advantages and disadvantages of the blockchain technology. Paper presented at: 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). IEEE. 2018:1-6.
37. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference. 2018:1-15.
38. Baliga A, Subhod I, Kamat P, Chatterjee S. Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv:1809.03421. 2018.
39. Brown RG, Carlyle J, Grigg I, Hearn M. "Corda: an introduction," R3 CEV, August, vol. 1, p. 15. 2016.
40. Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J Med Syst*. 2018;42(8):1-18.
41. Lee C. Litecoin. 2011.
42. Ahmad A, Saad M, Njilla L, Kamhoua C, Bassiouni M, Mohaisen A. Blocktrail: a scalable multichain solution for blockchain-based audit trails. Paper presented at: ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE. 2019:1-6.
43. Vijai C, Suriyalakshmi S, Joyce D. The blockchain technology and modern ledgers through blockchain accounting. *Adalya J*. 2019;8(12):545-557.
44. Larimer D. Transactions as Proof-of-Stake. 2013.
45. Hazari SS, Mahmoud QH. Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technol Lett*. 2019;2(3):e100.
46. Imbault F, Swiatek M, De Beaufort R, Plana R. The green blockchain: managing decentralized energy production and consumption. Paper presented at: 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE. 2017:1-5.
47. Dang H, Dinh TTA, Loghin D, Chang E-C, Lin Q, Ooi BC. Towards scaling blockchain systems via sharding. Proceedings of the 2019 International Conference on Management of Data. 2019:123-140.
48. Han R, Yu J, Lin H, Chen S, Esteves-Veríssimo P. On the security and performance of blockchain sharding. Cryptology ePrint Archive. 2021.
49. Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo K-KR. Sidechain technologies in blockchain networks: an examination and state-of-the-art review. *J Netw Comput Appl*. 2020;149:102471.
50. Papadis N, Tassiulas L. Payment channel networks: single-hop scheduling for throughput maximization. Paper presented at: IEEE INFOCOM 2022-IEEE Conference on Computer Communications. IEEE. 2022:900-909.
51. Sivaraman V, Venkatakrishnan SB, Ruan K, et al. High throughput cryptocurrency routing in payment channel networks. Paper presented at: 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20). 2020:777-796.
52. Papadis N, Tassiulas L. Blockchain-based payment channel networks: challenges and recent advances. *IEEE Access*. 2020;8:227596-227609.
53. Seyitoglu EUA, Yavuz AA, Hoang T. Proof-of-useful-randomness: mitigating the energy waste in blockchain proof-of-work. Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021). 2021.
54. Li M, Qin Y, Liu B, Chu X. Enhancing the efficiency and scalability of blockchain through probabilistic verification and clustering. *Inf Process Manag*. 2021;58(5):102650.
55. Aiyar K, Halgamuge MN, Mohammad A. Probability distribution model to analyze the trade-off between scalability and security of sharding-based blockchain networks. Paper presented at: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). IEEE. 2021:1-6.
56. Bandara E, Liang X, Foytik P, Shetty S, De Zoysa K. A blockchain and self-sovereign identity empowered digital identity platform. Paper presented at: 2021 International Conference on Computer Communications and Networks (ICCCN). IEEE. 2021:1-7.
57. Cai X, Geng S, Zhang J, et al. A sharding scheme based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things. *IEEE Trans Industr Inform*. 2021;17(11):7650-7658.
58. Pawar MK, Patil P, Hiremath P. A study on blockchain scalability. *ICT Systems and Sustainability*. Springer; 2021:307-316.
59. Wang J, Wang H. Monoxide: scale out blockchains with asynchronous consensus zones. Paper presented at: 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19). 2019:95-112.
60. Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016:17-30.
61. Wang G, Shi ZJ, Nixon M, Han S. Sok: Sharding on blockchain. Proceedings of the 1st ACM Conference on Advances in Financial Technologies. 2019:41-61.
62. Zamani M, Movahedi M, Raykova M. Rapidchain: scaling blockchain via full sharding. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018:931-948.
63. Team Z. The zilliqa technical whitepaper. Retrieved Sept. 2017 16:2019.
64. Mechkaroska D, Dimitrova V, Popovska-Mitrovikj A. Analysis of the possibilities for improvement of blockchain technology. Paper presented at: 2018 26th Telecommunications Forum (TELFOR). IEEE. 2018:1-4.
65. Li S, Yu M, Yang C-S, Avestimehr AS, Kannan S, Viswanath P. Polyshard: coded sharding achieves linearly scaling efficiency and security simultaneously. *IEEE Trans Inf Forensics Secur*. 2020;16:249-261.
66. Hafid A, Hafid AS, Samih M. New mathematical model to analyze security of sharding-based blockchain protocols. *IEEE Access*. 2019;7:185447-185457.
67. Sompolinsky Y, Zohar A. Phantom. IACR Cryptology ePrint Archive, Report 2018/104. 2018.
68. Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive block chain protocols. Paper presented at: International Conference on Financial Cryptography and Data Security. Springer. 2015:528-547.
69. Sompolinsky Y, Lewenberg Y, Zohar A. Spectre: a fast and scalable cryptocurrency protocol. *IACR Cryptol ePrint Arch*. 2016;1159:2016.
70. Li C, Li P, Zhou D, et al. A decentralized blockchain with high throughput and fast confirmation. Paper presented at: 2020 {USENIX} Annual Technical Conference ({USENIX} {ATC} 20). 2020:515-528.
71. Zhou T, Li X, Zhao H. Dlattice: a permission-less blockchain based on dpos-ba-dag consensus for data tokenization. *IEEE Access*. 2019;7:39273-39287.
72. Guo F, Xiao X, Hecker A, Dustdar S. Characterizing iota tangle with empirical data. Paper presented at: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE. 2020:1-6.
73. Popov S. The tangle. White Paper. 2018:1(3).

74. Pervez H, Muneeb M, Irfan MU, Haq IU. A comparative analysis of dag-based blockchain architectures. Paper presented at: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). IEEE. 2018:27-34.
75. Cai D. *A Parasite Chain Attack in Iota*. B.S. thesis. University of Twente; 2019.
76. Ribero Y, Raissar D. Dagcoin whitepaper. Whitepaper. 2018 no. May:1-71.
77. Churyumov A. Byteball: a decentralized system for storage and transfer of value. 2016. https://byteball.org/Byteball.pdf
78. LeMahieu C. Raiblocks: A feeless distributed cryptocurrency network. 2017. https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf
79. LeMahieu C. Nano: a feeless distributed cryptocurrency network. 2018;16:17. https://nano.org/en/whitepaper
80. Lokhava M, Losa G, Mazières D, et al. Fast and secure global payments with stellar. Proceedings of the 27th ACM Symposium on Operating Systems Principles. 2019:80-96.
81. Schwartz D, Youngs N, Britto A, et al. The ripple protocol consensus algorithm. 2014. https://ripple.com/files/ripple_consensus_whitepaper.pdf
82. Huang Y, Wang H, Wu L, et al. Characterizing eosio blockchain. arXiv preprint arXiv:2002.05369. 2020.
83. Mokdad I, Hewahi NM. Empirical evaluation of blockchain smart contracts. *Decentralised Internet of Things: A Blockchain Perspective*. Springer; 2020:45-71.
84. Akhtar Z. From blockchain to hashgraph: distributed ledger technologies in the wild. Paper presented at: 2019 international conference on electrical, electronics and computer engineering (UPCON). IEEE. 2019:1-6.
85. Boyen X, Carr C, Haines T. Graphchain: a blockchain-free scalable decentralised ledger. Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts. 2018:21-33.
86. Kan J, Chen S, Huang X. Improve blockchain performance using graph data structure and parallel mining. Paper presented at: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE. 2018:173-178.
87. Martino W, Quaintance M, Popejoy S. Chainweb: a proof-of-work parallel-chain architecture for massive throughput. Chainweb Whitepaper. 2018 19.
88. Forestier S, Vodenicarevic D, Laversanne-Finot A. Blockclique: scaling blockchains through transaction sharding in a multithreaded block graph. arXiv preprint arXiv:1803.09029. 2018.
89. Wood G. Polkadot: vision for a heterogeneous multi-chain framework. White Paper. 2016:21.
90. Liu Z, Xiang Y, Shi J, et al. Hyperservice: interoperability and programmability across heterogeneous blockchains. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019:549-566.
91. Kwon J, Buchman E. Cosmos whitepaper. 2019.
92. Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph. Paper presented at: International Conference on Financial Cryptography and Data Security. Springer. 2013:6-24.
93. Xiao R, Ren W, Zhu T, Choo K-KR. A mixing scheme using a decentralized signature protocol for privacy protection in bitcoin blockchain. *IEEE Trans Depend Secure Comput*. 2019;18(4):1793-1803.
94. Hassan MU, Rehmani MH, Chen J. Differential privacy in blockchain technology: a futuristic approach. *J Parallel Distrib Comput*. 2020;145:50-74.
95. Yang Z, Yang K, Lei L, Zheng K, Leung VC. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J*. 2018;6(2):1495-1505.
96. Zhao H, Zhang Y, Peng Y, Xu R. Lightweight backup and efficient recovery scheme for health blockchain keys. Paper presented at: 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). IEEE. 2017:229-234.
97. Kappos G, Yousaf H, Maller M, Meiklejohn S. An empirical analysis of anonymity in zcash. Paper presented at: 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018:463-477.
98. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. Paper presented at: 2016 IEEE Symposium on Security and Privacy (SP). IEEE. 2016:839-858.
99. Mercer R. Privacy on the blockchain: Unique ring signatures. arXiv preprint arXiv:1612.01188. 2016.
100. Möser M, Soska K, Heilman E, et al. An empirical analysis of traceability in the monero blockchain. arXiv preprint arXiv:1704.04299. 2017.
101. Li Y, Yang G, Susilo W, Yu Y, Au MH, Liu D. Traceable monero: anonymous cryptocurrency with enhanced accountability. *IEEE Trans Depend Secure Comput*. 2019;18(2):679-691.
102. Alshehri A, Baza M, Srivastava G, Rajeh W, Alrowaily M, Almusali M. Privacy-preserving e-voting system supporting score voting using blockchain. *Appl Sci*. 2023;13(2):1096.
103. Qin C, Wu L, Meng W, Xu Z, Li S, Wang H. A privacy-preserving blockchain-based tracing model for virus-infected people in cloud. *Expert Syst Appl*. 2023;211:118545.
104. Wang Z, Chen Q, Liu L. Permissioned blockchain-based secure and privacy-preserving data sharing protocol. *IEEE Internet Things J*. 2023.
105. Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). *Electronics*. 2023;12(3):677.
106. Zhang M, Yang M, Shen G, Xia Z, Wang Y. A verifiable and privacy-preserving cloud mining pool selection scheme in blockchain of things. *Inform Sci*. 2023;623:293-310.
107. Shao M, Liu M, Wang Z. Privacy-preserving electronic medical records sharing solution based on blockchain. *Int J Netw Secur*. 2023;25(1):68-75.
108. Luong DA, Park JH. Privacy-preserving identity management system on blockchain using zk-snark. *IEEE Access*. 2023;11:1840-1853.
109. Dewangan NK, Chandrakar P, Kumari S, Rodrigues JJ. Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system. *Multimed Tools Appl*. 2023;82(8):12595-12614.
110. Dingman W, Cohen A, Ferrara N, et al. Defects and vulnerabilities in smart contracts, a classification using the nist bugs framework. *Int J Netw Distrib Comput*. 2019;7(3):121-132.
111. Li J, Li N, Peng J, Cui H, Wu Z. Energy consumption of cryptocurrency mining: a study of electricity consumption in mining cryptocurrencies. *Energy*. 2019;168:160-168.
112. Luu L, Velner Y, Teutsch J, Saxena P. Smartpool: practical decentralized pooled mining. Paper presented at: 26th {USENIX} Security Symposium ({USENIX} Security 17). 2017:1409-1426.
113. Tikhomirov S, Voskresenskaya E, Ivanitskiy I, Takhaviev R, Marchenko E, Alexandrov Y. Smartcheck: static analysis of ethereum smart contracts. Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain. 2018:9-16.

114. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). Paper presented at: International Conference on Principles of Security and Trust. Springer. 2017:164-186.
115. Luu L, Chu D-H, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016:254-269.
116. Lu N, Wang B, Zhang Y, Shi W, Esposito C. Neucheck: a more practical ethereum smart contract security analysis tool. *Softw: Pract Exper*. 2021;51(10):2065-2084.
117. Zhang Y, Ma S, Li J, Li K, Nepal S, Gu D. Smartshield: automatic smart contract protection made easy. Paper presented at: 2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE. 2020:23-34.
118. Sharkey S, Tewari H. Alt-pow: an alternative proof-of-work mechanism. Paper presented at: 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE. 2019:11-18.
119. Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. Pobt: a lightweight consensus algorithm for scalable iot business blockchain. *IEEE Internet Things J*. 2019;7(3):2343-2355.
120. Lasla N, Alsahan L, Abdallah M, Younis M. Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm. arXiv preprint arXiv:2007.04086. 2020.
121. Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo K-KR. An energy-efficient sdn controller architecture for iot networks with blockchain-based security. *IEEE Trans Serv Comput*. 2020;13(4):625-638.
122. Yang L, Li M, Si P, Yang R, Sun E, Zhang Y. Energy-efficient resource allocation for blockchain-enabled industrial internet of things with deep reinforcement learning. *IEEE Internet Things J*. 2020;8(4):2318-2329.
123. Sengupta J, Ruj S, Bit SD. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *J Netw Comput Appl*. 2020;149:102481.
124. Kamble SS, Gunasekaran A, Sharma R. Modeling the blockchain enabled traceability in agriculture supply chain. *Int J Inf Manag*. 2020;52:101967.
125. Khan AA, Shaikh ZA, Belinskaja L, et al. A blockchain and metaheuristic-enabled distributed architecture for smart agricultural analysis and ledger preservation solution: a collaborative approach. *Appl Sci*. 2022;12(3):1487.
126. Salah K, Nizamuddin N, Jayaraman R, Omar M. Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access*. 2019;7:73295-73305.
127. Lin W, Huang X, Fang H, et al. Blockchain technology in current agricultural systems: from techniques to applications. *IEEE Access*. 2020;8:143920-143937.
128. Konstantinidis I, Siaminos G, Timplalexis C, Zervas P, Peristeras V, Decker S. Blockchain for business applications: a systematic literature review. Paper presented at: International Conference on Business Information Systems. Springer. 2018:384-399.
129. Dierksmeier C, Seele P. Blockchain and business ethics. *Bus Ethics: Eur Rev*. 2020;29(2):348-359.
130. Viriyasitavat W, Hoonsopon D. Blockchain characteristics and consensus in modern business processes. *J Ind Inf Integr*. 2019;13:32-39.
131. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. *Healthcare*. Vol 7. Multidisciplinary Digital Publishing Institute; 2019:56.
132. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. *Symmetry*. 2018;10(10):470.
133. McGhin T, Choo K-KR, Liu CZ, He D. Blockchain in healthcare applications: research challenges and opportunities. *J Netw Comput Appl*. 2019;135:62-75.
134. Patel MM, Tanwar S, Gupta R, Kumar N. A deep learning-based cryptocurrency price prediction scheme for financial institutions. *J Inf Secur Appl*. 2020;55:102583.
135. Chen F, Wan H, Cai H, Cheng G. Machine learning in/for blockchain: future and challenges. *Can J Stat*. 2021;49(4):1364-1382.
136. Weng J, Weng J, Zhang J, Li M, Zhang Y, Luo W. Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Trans Depend Secure Comput*. 2019;18(5):2438-2455.
137. Khan AA, Laghari AA, Rashid M, Li H, Javed AR, Gadekallu TR. Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: a state-of-the-art review. *Sustain Energy Technol Assess*. 2023;57:103282.
138. Khan AA, Shaikh AA, Laghari AA. Iot with multimedia investigation: a secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth. *Arab J Sci Eng*. 2023;48(8):10173-10188.
139. Abuidris Y, Kumar R, Wenyong W. A survey of blockchain based on e-voting systems. Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications. 2019:99-104.
140. Yi H. Securing e-voting based on blockchain in p2p network. *EURASIP J Wirel Commun Netw*. 2019;2019(1):1-9.
141. Kshetri N, Voas J. Blockchain-enabled e-voting. *IEEE Softw*. 2018;35(4):95-99.
142. Hjálmarsson F, Hreiarsson GK, Hamdaqa M, Hjálmtysson G. Blockchain-based e-voting system. Paper presented at: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE. 2018:983-986.
143. Rouhani S, Deters R. Security, performance, and applications of smart contracts: a systematic survey. *IEEE Access*. 2019;7:50759-50779.
144. Zheng Z, Xie S, Dai H-N, et al. An overview on smart contracts: challenges, advances and platforms. *Future Gener Comput Syst*. 2020;105:475-491.
145. Xu Y, Wang G, Yang J, Ren J, Zhang Y, Zhang C. Towards secure network computing services for lightweight clients using blockchain. *Wirel Commun Mob Comput*. 2018;2018:1-12.
146. Arora D, Gautham S, Gupta H, Bhushan B. Blockchain-based security solutions to preserve data privacy and integrity. Paper presented at: 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE. 2019:468-472.
147. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. Paper presented at: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE. 2017:468-477.
148. Wan J, Li J, Imran M, et al. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans Industr Inform*. 2019;15(6):3652-3660.
149. Khan AA, Shaikh ZA, Laghari AA, Bourouis S, Wagan AA, Ali GAAA. Blockchain-aware distributed dynamic monitoring: a smart contract for fog-based drone management in land surface changes. *Atmos*. 2021;12(11):1525.
150. Treleaven P, Brown RG, Yang D. Blockchain technology in finance. *Computer*. 2017;50(9):14-17.
151. Cocco L, Pinna A, Marchesi M. Banking on blockchain: costs savings thanks to the blockchain technology. *Future Internet*. 2017;9(3):25.
152. Guo Y, Liang C. Blockchain application and outlook in the banking industry. *Financ Innov*. 2016;2(1):1-12.

153. Bhaskaran K, Ilfrich P, Liffman D, et al. Double-blind consent-driven data sharing on blockchain. Paper presented at: 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE. 2018:385-391.
154. Min H. Blockchain technology for enhancing supply chain resilience. *Bus Horiz*. 2019;62(1):35-45.
155. Saberi S, Kouhizadeh M, Sarkis J, Shen L. Blockchain technology and its relationships to sustainable supply chain management. *Int J Prod Res*. 2019;57(7):2117-2135.
156. Casado-Vara R, Prieto J, De la Prieta F, Corchado JM. How blockchain improves the supply chain: case study alimentary supply chain. *Procedia Comput Sci*. 2018;134:393-398.

How to cite this article: Reshi IA, Sholla S. The blockchain conundrum: An in-depth examination of challenges, contributing technologies, and alternatives. *Concurrency Computat Pract Exper*. 2023;e7987. doi: 10.1002/cpe.7987