IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 March 2023, accepted 3 April 2023, date of publication 13 April 2023, date of current version 25 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3267047

SURVEY

A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues

SAMINUR ISLAM[1], MOHAMMAD JAMINUR ISLAM[2], MAHMUD HOSSAIN[3], SHAHID NOOR[4], (Associate Member, IEEE), KYUNG-SUP KWAK[5], (Life Senior Member, IEEE), AND S. M. RIAZUL ISLAM[6], (Senior Member, IEEE)

[1]Department of Computer Science, North Carolina State University, Raleigh, NC 27606, USA
[2]Department of Computer Science, University of California at Riverside, Riverside, CA 92521, USA
[3]Department of Private Certificate Authority, Amazon Inc., Seattle, WA 98109, USA
[4]Department of Computer Science, Northern Kentucky University, Highland Heights, KY 41099, USA
[5]Department of Information and Communication Engineering, Inha University, Incheon 22212, South Korea
[6]Department of Computer Science, University of Huddersfield, HD1 3DH Huddersfield, U.K.

Corresponding authors: Kyung-Sup Kwak (kskwak@inha.ac.kr) and S. M. Riazul Islam (s.mr.islam@hud.ac.uk)

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (Ministry of Science and ICT) under Grant NRF-RS-2023-00208462.

ABSTRACT Recently, Blockchain-based applications have become immensely popular because of limited reliance on a single entity, unlike a centralized system. However, reaching a consensus among blockchain networks is a challenging and vital aspect of blockchain-based applications. There are various types of blockchain networks for different kinds of application scenarios. Among all of them, the consensus algorithm is the most crucial part of reaching an agreement in the complex blockchain network. Over the years, researchers have focused on dealing with the challenges like distributed computing, storage, transaction speed, security, validity, interoperability, and many more. However, only some of them are appropriate for all domains. Therefore, this paper presents an extensive study of different types of consensus protocols used in existing blockchain solutions with the strength and limitations of each algorithm. We also provide an inherent comparison among different algorithms to understand consensus protocol selection better. Moreover, we investigate operational and interoperability issues in existing blockchain-based applications to understand challenges and provide recommendations for future developers.

INDEX TERMS Blockchain, consensus algorithm, interoperability, cross-chain transactions, architecture, operational issues, applications, research directions.

I. INTRODUCTION

The blockchain concept was first introduced by Haber and Stornetta [1], which is considered one of the technologies with the most potential. After that the introduction of Bitcoin by Nakamoto [2], it has attracted intense attention from all over the world. In Blockchain systems, different cryptographic protocols, like hash functions, digital signatures, etc., are used to maintain the authenticity and security of the data. Blockchain is a distributed ledger system that keeps data secure from unauthorized access. Blockchain technology allows users to add, view, and validate transactions to the distributed ledger. These transactions often take place with the consent of all involved users. Blockchain uses a consensus mechanism to ensure that all transactions are accurate.

In a trustless environment, blockchain provides users with desirable qualities like decentralization, autonomy, integrity, immutability, verification, fault-tolerance,

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

anonymity, auditability, and transparency, which have received significant academic and industrial attention recently years [3], [4], [5], [6]. However, the blockchain system is trustless and ensures blockchain-enabled trust through other cryptographic peer-to-peer communication in the decentralized network. Further verification and validation mechanisms are employed across the decentralized network as the computation parts to simplify and ease transactions. However, there are a ton of dependencies that must be met for blockchain transactions to be successful. Typically, participating users and nodes are free to leave at any moment. Blockchain requires universal consensus, which is challenging to get, making it challenging to complete a transaction. Furthermore, each node must establish its competency before adding a block to the existing blockchain. As a result, consensus is an essential component of Blockchain applications. It's also been used in embedded architecture to improve the power consumption and execution time [7]. However, the researcher has recently expressed a strong interest in inter-blockchain operations, known as interoperability. But gaining interoperability among different blockchains is still an important field to explore. Interoperability does not only conflate flexibility and application portability. It also has the potential to solve some of the biggest blockchain research challenges. In particular, interoperability encourages blockchain scalability because it offers a means to offload transactions to other blockchains, such as via sharding [8], [9]. It can also encourage privacy by enabling end users to use different blockchains for data objects with various privacy requirements [10]. At this stage, a comprehensive understanding of current research and practices on consensus algorithms in the blockchain context is expected to be useful for various stakeholders. This paper examines the trends in consensus algorithms in blockchain research and uncovers various issues that must be addressed to transform blockchain innovation. From a general viewpoint, some of the consensus issues in blockchain systems have been discussed in [11], [12], [13], [14], and [15]. In [11], authors mainly focused on giving an overview of lesser-known consensus protocols other than widely used ones. Therein, they tried to provide an overview of all the alternative consensus protocols, including their advantages and disadvantages. The survey, presented in [15], also provided an in-depth overview of different consensus protocols. However, there is no evidence of discussing the comparative analysis of all the protocols and discussion of suitability on different platforms. In contrast, our survey focuses on discussing all the consensus protocols in three levels, 1≈ giving an overview of each protocol, 2≈ providing an application perspective of each protocol, and 3≈ in-depth analyses of the existing issues in each protocol. In particular, the main contributions of this paper are as follows:

- We provide the general architecture of blockchain applications and the transaction mechanism.
- We present a simple taxonomy of the consensus algorithms and discuss each branch, including proof-based and voting-based consensus algorithms.
- We provide a comparative discussion about the algorithms of interest in terms of performances, efficiencies, and their uses in blockchains.
- We extensively analyze application domains of consensus algorithms in terms of development tools, uses, and environments.
- We highlight the challenges in Blockchain applications regarding functional and non-functional issues.

The remainder of the paper is organized as follows. In section II, we provided a detailed overview of our literature review methodology. Section III provided a high-level review of blockchain characteristics and operational concepts. Section IV addressed various consensus algorithms, and Section V gave detailed information on the uses of different consensus algorithms in various applications. Section VI gave a comparative analysis of consensus algorithms in terms of Verification and performance. Section VII provided information about functional issues in blockchain applications. Finally, Section VIII is devoted to the discussion and conclusion.

II. LITERATURE REVIEWS METHODOLOGY

Literature reviews are essential in any academic research to understand existing knowledge and identify research gaps. Our main purpose of the literature survey was to provide a comprehensive overview of the current state of blockchain technology research, focusing on consensus algorithms, architecture, application domains, operational issues, and interoperability. To achieve this, we followed Two step review process, which includes a scoping review and a systematic literature review.

In Fig. 1, we showed a two-step process including a scoping review and a systematic review for our literature survey focused on the different contexts of blockchain technology.

A. SCOPING REVIEW

A scoping review is a process of identifying a particular field's existing literature and research gaps. This review process is iterative, involving several stages of searching relevant literature and screening based on chosen inclusion and exclusion criteria.

In our scoping review, we used specific keywords like blockchain technology, distributed ledger, Consensus protocols, comparative analysis, blockchain architecture, blockchain applications, issues in blockchain, issues in consensus algorithms, comparative analysis of the blockchain, and many more. We screened the title and abstracts of the articles and selected those that met our inclusion criteria. Then we reviewed each of the selected articles to find out the queries which were used to perform a systematic literature review.

B. SYSTEMATIC LITERATURE REVIEW

In the Systematic Literature Review, we categorized the review process based on our queries or research questions we found from the scoping review.

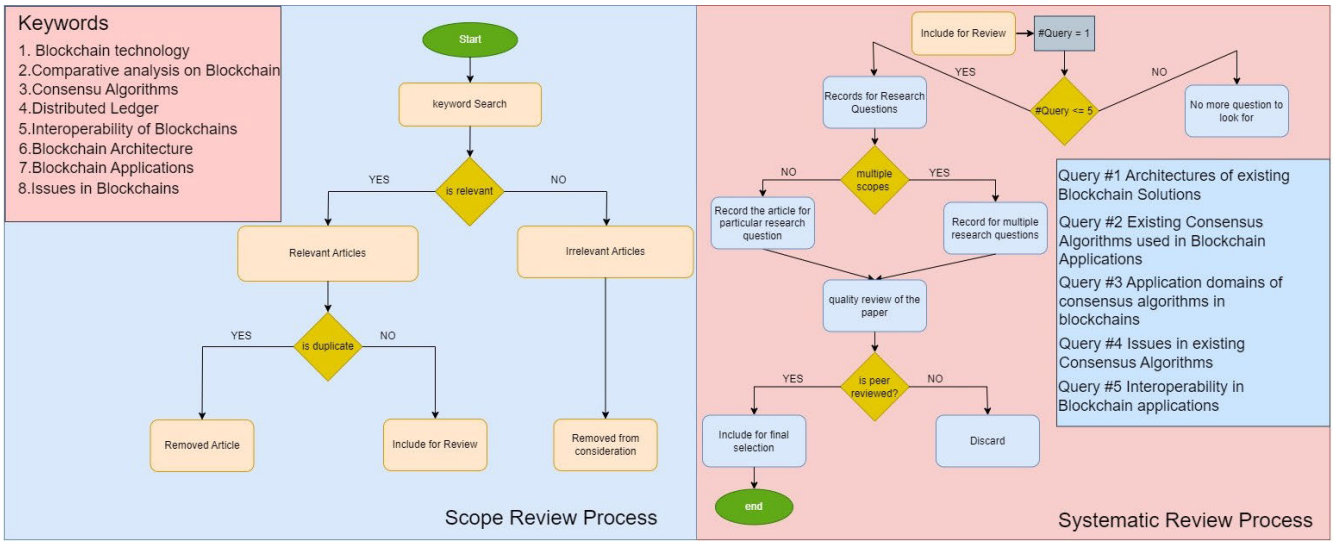

FIGURE 1. Overview of literature review process for blockchain technology research.

- **Architecture of existing blockchain solutions:** We found that researchers have used various techniques to explore blockchain architecture, including conceptual frameworks, system design, and analysis of existing systems.
- **Existing consensus algorithms used in blockchain:** We found that researchers have used techniques such as simulation models, analysis of existing consensus algorithms, and experimental studies to explore consensus algorithms used in blockchain applications.
- **Application domain of consensus algorithms in blockchain:** Researchers have used different techniques, such as case studies and empirical studies, to explore using consensus algorithms in various application domains.
- **Issues in existing consensus algorithms:** Researchers have used techniques such as analyzing existing consensus protocols to explore challenges and issues in existing consensus algorithms.
- **Interoperability in blockchain application:** In this query, we found that researchers have used techniques such as analyzing existing protocols and experimental studies to explore interoperability in blockchain applications.

C. FREQUENTLY USED TECHNIQUES

We found that the frequently used techniques in the selected articles were analysis of existing systems, case studies, and empirical studies. These techniques were used to explore various aspects of blockchain technology, including architecture, consensus algorithms, application domains, issues, and interoperability.

Overall, our literature survey methodology was designed to provide a comprehensive and unbiased review of the current state of blockchain technology research, focusing on consensus algorithms, architecture, application domains, and interoperability. We hope our review will provide a valuable resource for researchers, practitioners, and other stakeholders interested in this rapidly evolving field.

III. BLOCKCHAIN STRUCTURE AND TRANSACTION FLOW

Blockchain-based frameworks combine cryptography, public key infrastructures, and economic modeling to achieve distributed database synchronization through peer-to-peer networking and decentralization consensus. Blockchain is a secure and distributed system in which the entire network is broadcast on every transaction. It can record and secure transactions or transnational events using cryptography [16]. Each transaction has one signature. This signature is used to verify the transactions on the users based on cryptographically secured blocks. Each user here is known as a block miner who created the block as a consensus problem and solved it in a distributed manner. The miners who solve the consensus problem broadcast their new blocks throughout the network [17]. In order to understand the potential applications of blockchains in the Internet of Things, it is essential to understand the working principles of blockchains and how they achieve decentralization.

In the following subsection, more detailed descriptions will be provided on the key components of blockchains like data structure, consensus algorithms, smart contracts, and security analysis on blockchain.

The transaction is the basic unit of blockchain, which the miners in the network observe. Each transaction initiates with a private key to indicate the miner who requests the transaction. Each of the private keys corresponds to a public key for the verification of the validity of the transaction [2]. The transaction was first used in Bitcoin to capture the financial interactions between two financial parties. Transactions have also been used to elaborately

assign the ownership rights and realize programmable events [18]

Being the element of the distributed ledger, every block encapsulates a batch of verified transactions. Each block is uniquely identified by a hash value generated using the cryptographic hash algorithm on the header of the block [12]. Every block also has a header containing a link to the parent (previous) block (which is the hashed value of the parent block, e.g., in Bitcoin Blockchain) and an answer in response to the consensus problem, as will be described shortly. Depending on specific demands, the block header may contain other fields, such as timestamps. An ordered backward-linked list of blocks is maintained, as a local record of transactions, at every network miner.

In Fig 3, a general structure of blockchain has been shown, and how the transactions usually happen in the blockchain network is explained with a flow diagram.

A. NODE/USER

The core part of the blockchain architecture [19] is the node. Normally, any devices able to connect with cloud or network servers are considered nodes or users. Whenever a transaction happens the nodes act as transaction requesters and receivers. Each of these nodes maintains a copy of the entire blockchain ledger to do any transactions in a blockchain.

B. MINERS

The nodes capable of adding new blocks are known as miners [20]. Miners are responsible for the validation, and verification of the transactions as well as their authenticity. Miners add a transaction message to the publicly shared blockchain ledger for the verification and the validity of the request. This process of adding a block to the existing blockchain is known as blockchain mining. It happens through blockchain miners.

C. BLOCK

A block is a representation of transaction details. When a transaction request is initiated in the blockchain, it implies the building of a new block. The blocks can be added to the blockchain, only if they are successfully verified by the miners. A block has two major parts, namely the header and transaction details [21].

D. VERIFICATION MECHANISM

To have a successful transaction in a blockchain network, the transaction needs to be verified through two steps. The first step involves the use of a smart contract to facilitate the transaction between two parties. The second step involves the use of a consensus algorithm to reach an agreement on the state of the transaction. We will discuss both of these steps in detail below.

1) SMART CONTRACT

Smart contracts are normally computer-based transaction protocols that can document, control, execute legal events, and perform actions based on the contract agreement [22]. The main objectives of integrating smart contracts in blockchain technology are to reduce the need for trusted intermediates and fraud losses and to reduce the malicious, enforcement costs, and accidental exceptions [23]. Blockchain technology is built on top of a smart contract. When two parties enter into a smart contract and agree to all of its terms, the contract is instantly added to the blockchain, and the transaction is carried out when specified terms or circumstances are met [24].

2) CONSENSUS ALGORITHM

Consensus algorithms aim to securely update replicated shared states and are the essential piece of the puzzle in the working principles of the blockchain. In the blockchain, a system based on state machine replication, consensus protocols ensure all replicas of the shared state are synchronized and in agreement at any given point in time [3]. There are different types of decentralized consensus algorithms that exist in which the core principles of designing the algorithms are safety, liveness, and fault tolerance. Here we will discuss the different types of blockchains which will cover all variants of consensus algorithms used in different blockchain types. However, we can generalize different blockchains into either permissioned or permissionless. Our discussion over the consensus algorithms would be based on these two categories.

E. TYPES OF BLOCKCHAIN

There are normally two types of blockchains: 1) permissioned blockchain 2) permissionless blockchain. In 2, We showed the detailed categorization of existing blockchain technologies. Here we discussed each type shortly.

- Permissioned Blockchain: In permissioned blockchain deployments such as private and consortium blockchains, only a limited number of known participants carry a copy of the entire blockchain [25]. Maintaining consensus, therefore, is much more straightforward and doesn't require costly proofs for publishing a new block. Since participants are known, there is no risk of a Sybil attack, therefore voting mechanisms are used to achieve consensus. By this virtue, permissioned blockchains have a much higher performance than permissionless blockchains.
  - Private Blockchain: Private blockchain is a type of blockchain which restricted by a single authority for any transactions or changes on nodes. There is a central authority controlling access to the functionalities. Private blockchains are normally partially decentralized due to this reason.
  - Hybrid Blockchain: A hybrid blockchain [26] combines the features of public and private blockchains. It makes use of both the private permission-based system and the public permission-less system aspects of blockchains. Users may manage who has access to what data is stored in the blockchain with the help of such a hybrid network. Only

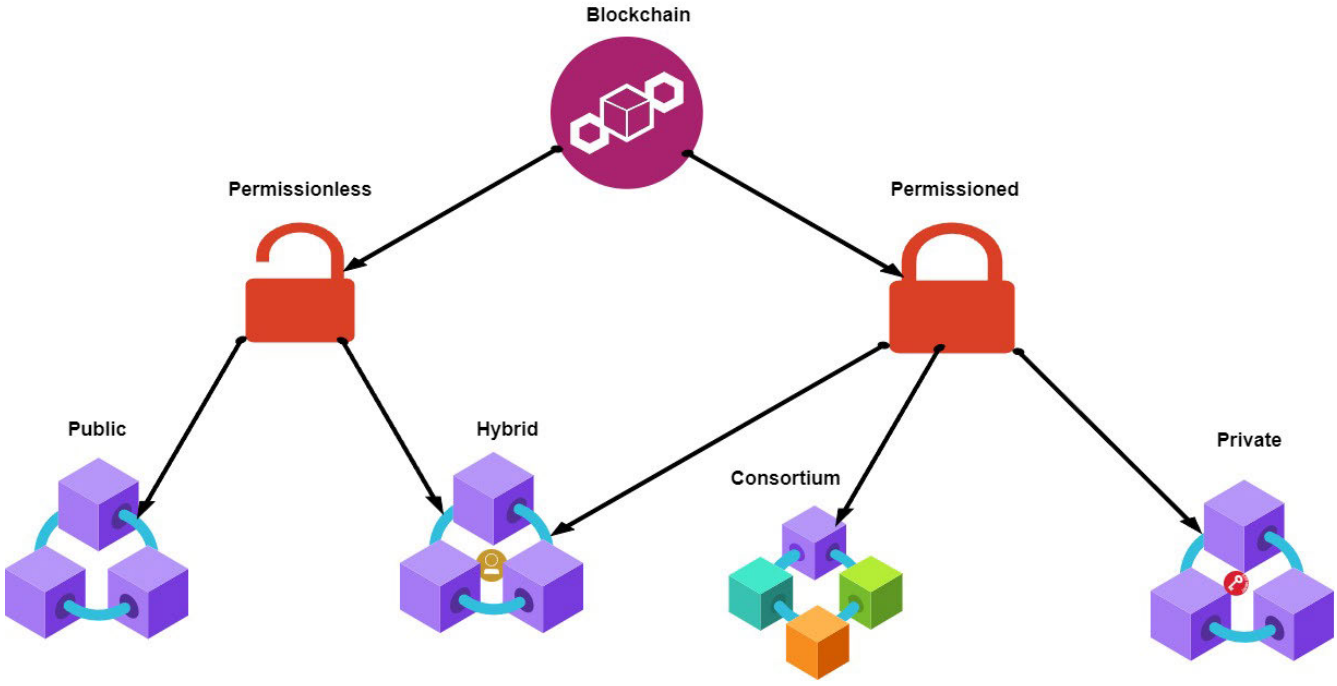

FIGURE 2. Classification of blockchains. Permissionless blockchain could be public and will be fully decentralized. There could be Hybrid blockchains that could be considered both permissioned and permissionless blockchains. Permissioned blockchains can classify into three categories. Private would be controlled by a single authority; consortium is a type of blockchain that is controlled by a group of authorities.

a certain subset of the blockchain's data or records may be made public, keeping the remainder secret and confidential. Users may simply combine a private blockchain with many public blockchains thanks to the flexibility of the hybrid blockchain technology. A hybrid blockchain's private network is often used to verify a transaction. However, users can also publish it on the open blockchain in order to be confirmed. The hashing is increased and additional nodes are used for verification on public blockchains. As a result, the blockchain network's security and transparency are improved.

- Consortium Blockchain: A consortium blockchain is a semi-decentralized kind in which a blockchain network is managed by more than one entity. This contrasts with what we saw in a private blockchain, which is administered by a single entity. In this sort of blockchain, more than one organization can operate as a node, exchanging information or mining. Consortium blockchains are commonly utilized by banks, government agencies, and other organizations.

- Permissionless Blockchain: This is a type of blockchain in which anonymous participants are termed p̃ermissionlessãnd can be a member of blockchain networks. Normally those anonymous users gain their consensus in the permissionless blockchain using the voting technique. But there is a problem with that where an attacker can create multiple accounts to launch a Sybil attack [27] can lead to a false representation to drive the outcome toward their favor.

  Therefore, in permissionless blockchain implementations, the consensus algorithms are based on a lottery-based selection of a single node that publishes a new block onto the blockchain. To ensure security in public blockchains where anonymous participants are required to transact in a trustless manner, block creation needs to be ẽxpensiveõ that the resources of one entity are insufficient to bias the consensus decisions in its favor [3].

  - Public Blockchain: Public blockchain is a fully decentralized blockchain where each node or user will have equal rights for performing any functionalities like transactions or data sharing.

IV. CONSENSUS ALGORITHMS

When distributed systems first appeared, consensus algorithms first appeared as coordinated transitions inside these networks. For Blockchain technology, multiple consensus techniques are used. Consensus algorithms are classified into two types: proof-based consensus algorithms and voting-based consensus algorithms [28], [29]. The sections that follow examine and offer instances of these two categories in terms of permissioned and permissionless blockchains [12], [13], [30], [31], [32], [33], [34].

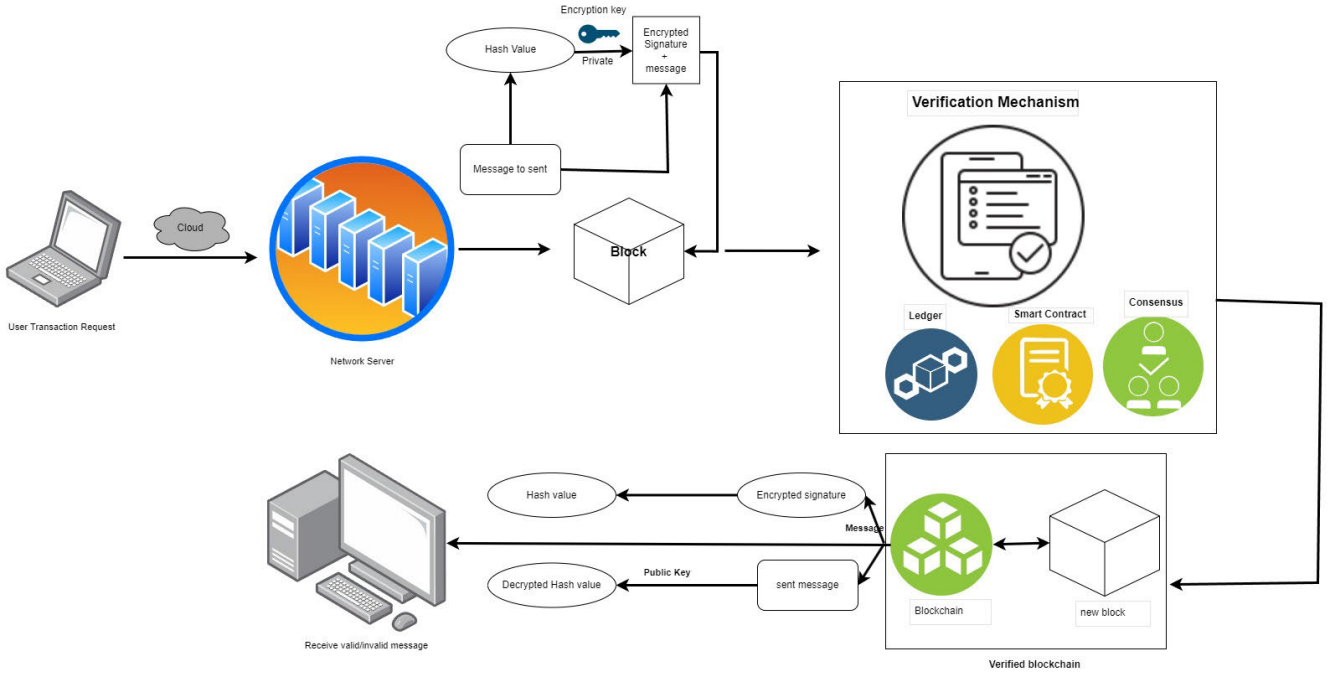

FIGURE 3. Blockchain structure and transaction flow diagram.

A. PROOF OF WORK

The first blockchain consensus protocol was the Proof-of-work (PoW) consensus [14], [15], [35], [36]. Normally, blockchain security is based on this concept and a transaction is only considered valid once the system obtains proof that enough computational work has been exerted by authorizing nodes. The miners (responsible for creating blocks) constantly try to solve cryptographically puzzles (named PoW) [29] in the form of hash computation. The process of adding new blocks to the blockchain is called mining. Each block in the chain is identified by a hash in the header. The hash is unique and generated by the Secure Hash Algorithms (SHA-256). SHA takes any size plaintext and calculates a fixed size 256-bit cryptographic hash. Each header contains the address of the previous block in the chain. The inability to delete or change information from blocks makes blockchain the best appropriate technology for most blockchain applications. However, there are some drawbacks to Blockchain applications using PoW. Applications must have the capacity to provide high computational power to solve PoW, low scalability, and long latency for transaction confirmation over the network.

B. PROOF OF STAKE

The Proof-of-Stake (PoS) algorithm aims to cut back on the ever-increasing electricity consumption of the PoW blockchain network [14], [15], [35], [36]. As an alternative to computationally expensive puzzle solving, proof of stake aims to stake peers' economic share in the network. Here the term miners are replaced with the validators and similar to the proof of work algorithm, one of the validators is chosen to publish a block onto the blockchain [29]. The difference lies in how the validator is chosen. In proof of stake, a validator is selected in a pseudorandom fashion, with the probability of being selected proportional to the validatorš share in the network. Naive Proof of Stake consensus mechanisms are prone to attacks like the ñothing at stakeãttack and require further considerations for them to be consensus-safe. Block finality in PoS blockchains is faster compared to PoW blockchains since there is no computational puzzle-solving involved in choosing the validator.

C. DELEGATED PROOF OF STAKE (DPoS

DPoS [15], [37] has been proposed as an underlying consensus mechanism that outperforms its counterparts, such as PoW and PoS using a block generation procedure that leads to faster transactions. DPoS reduces energy consumption by incorporating a one vote per share mechanism that enhances the number of process coins [29]. Since stakeholders vote for randomly selected witnesses to preserve consensus, they are incentivized and penalized concerning their generated blocks and accomplishments, respectively. However, DPoS suffers from a lack of decentralization as it incorporates an extensive number of validators to reach a consensus.

D. PROOF OF REPUTATION- X (PoRX)

Further alternative consensus algorithms for public blockchain deployments came about, and are classified as Þroof of X-. Cachin and Vukolic [38] present an exhaustive study of these algorithms.

PoX is a set of consensus algorithms that depends on the Proof of things like PoW (Proof-of-Work), PoA (Proof-of-Activity), PoS (Proof-of-Stake), and PoET. PoX can be extended to another consensus protocol known as Proof of reputation, where a reputation module can be integrated with a PoX protocol (Proof-of-Elapsed-Time). PoRX [39], therefore, makes use of two factors for choosing block issuers: reputation and another factor as determined by the base PoX, such as a stake, activity, elapsed time, and work. The following is a better explanation of PoRX: To ensure their legitimacy, integrity, validity, and uniqueness, all nodes taking part in the consensus have their identities recorded in a register and signed by the declarer. Upon admission, a new node is given a default reputation value, while an existing node's reputation is retrieved upon recognition. When it comes time to issue/generate a new block (update the ledger), two processes are completed: estimation of the reputation rewards and punishments for the nodes and calculating the mining difficulty of a specific node wishing to create a block. In the incentive scheme, a node is rewarded for successfully mining its block with a certain quantity of tokens, transaction fees, and reputation fees. Finally, because the consensus nodes are dynamic, it is necessary to update the protocol settings.

E. PROOF OF ACTIVITY

An alternative to Bitcoin mining was proposed by extending Bitcoin's proof of work via proof of stake, which combines aspects of both proof of work and proof of stake to achieve consensus. The objective is to reward stakeholders that actively participate in the network. Peers start with mining potential blocks, similar to the proof of work. Decred [29], [40] uses proof of activity to achieve distributed consensus. Computational puzzle solving in proof of activity only involves finding proof of work against the block header, without the transactions in the block. Beyond this point, a random group of validators is chosen to vote on the validity of the mined block header. Similar to the proof of stake, the probability of the validators being chosen is proportional to their share in the network. The block is considered valid if all the validators vouch for its validity. If some of the validators are offline, the next mined block is chosen, along with a new set of validators, till a block is voted as valid. Transaction fees in this case are split between the miner and validators. Criticism of proof of activity includes concerns pertinent to proof of work and proof of stake. It requires higher computational power, and a naive implementation can be prone to nothing-at-stake attacks.

F. PROOF OF ELAPSED TIME

Hyperledger Sawtooth [15], [41] is an open-source project with its consensus algorithm called proof of elapsed time. Proof of elapsed time runs in a Trusted Execution Environment (TEE), like Intelš Software Guard Extensions (SGX) [29], [42]. A trusted voting model built on the SGX helps elect a validator for publishing a new block. Proof of elapsed time is another lottery-based consensus algorithm; however, it foregoes the need for expensive computational puzzle-solving. The Sawtooth blockchain network node requests a wait time from a trusted function within the SGX. The validator with the shortest wait time is selected as the leader as soon as its waiting time runs out. Another trusted function attests to the fact that the validator waited an allotted time before publishing a new block. This second function thus provides proof of the validator being chosen after its allotted time had elapsed. The probability of being elected here is proportional to the resources (general-purpose processors running TEE) contributed to the network. The algorithm meets the prerequisites of a viable lottery-based consensus algorithm; however, its limitation is in its use of specialized hardware.

G. PROOF OF SPACE

Proof of Space is a consensus algorithm that is cheaper than PoW in terms of required computing infrastructure, as it requires the use of hard disks or cloud storage systems [15], [37]. Their multiplicity enhances the probability of mining a new block for the corresponding node. The proof of space is executed in two stages. The first stage is plotting, where the hard disk capacity that the miner has devoted is evaluated by incorporating Shabal [29], [43] hash function and plotting the hard disk. The hash function is then seeded using the minerš ID and nonce [44]. Mining is performed during the second stage. It refers to the most recent block on the chain to calculate the generation hash. The total number of scoops is then calculated by incorporating the hash module to generate the target value that also uses the outputs of the plotting stage. Afterward, the network re-calculates each hash's scoop to validate each miner's deadlines. The miner that correlates the shortest published deadline generates the next block and receives a reward for the transaction. The advantage of PoSpace is its energy efficiency, as it does not impose high requirements on hardware.

H. PROOF OF APPROVAL

Proof of approval [37] is acknowledged as a permissionless consensus that intermittently publishes blocks within predefined intervals. Each node can propose a new block; however, nodes that do not indicate valid transactions are eliminated, and stakeholders with a minimum stake are authorized to compete in the block creation procedure. Once the block generator has been selected, it broadcasts its corresponding approval block containing the acquired confirmations and is rewarded with the transaction fees of the proposed block and coins [45].

I. PROOF OF EXISTENCE

Proof of existence [37] as an online service exploits a decentralized certification SHA256 [29]. PoE permanently validates the existence of data by storing its cryptographic digest and the corresponding submission date using blockchain. This service can publicly prove the ownership of data without

revealing the data itself. It also eliminates the requirements for trusting any central authority. This approach provides anonymity, privacy, and decentralized proof that does not rely on a single centralized entity.

J. PROOF OF ENERGY

Proof of Energy [37] is a consensus mechanism for administration of the P2P energy trading using DLTs. PoE uses smart contracts for regulating energy transactions without excessive energy consumption. After the validation of each smart contract, the next block generator needs to be elected to decide on the next offer. The block generator is elected using the proof of energy that incorporates a consumption production function to calculate the self-consumption proportion of each prosumer. The user that retains equal consumption and generation is chosen as the block proposer and incentivized accordingly. This approach empowers the prosumers to enhance the operation of both distribution and transmission systems [46].

K. SIEVE

SIEVE [37] was initially employed by Hyperledger as an underlying consensus mechanism that tolerates nondeterminism. Once performed by distinct replicas, it results in contrasting outputs. SIEVE considers the blockchain as a block box that compares the results from different replicas to sieve out the sequence of diverging outputs. If the diverging values within a procedure reach a certain threshold, the procedure is eliminated [47], [48], [49].

L. PROOF OF OWNERSHIP

Proof of ownership has been proposed to ensure a trusted execution environment for participants. This procedure can be employed to certify the integrity and ownership of contracts. The proof is established using a block header and pseudonym. The consensus is met when a proposed block generated by a particular trusted execution environment retains most proofs with unique pseudonyms [50].

M. RIPPLE/PROOF OF CORRECTNESS

Ripple is a consensus mechanism that incorporates validating nodes to preserve a set of trusted nodes acknowledged as a Unique Node List (UNL). To append transactions into the ledger, UNL is required to maintain agreement among 80% of the nodes. UNL nodes verify the transactions and broadcast their corresponding votes to the network. Unverified transactions are discarded and retained in the open ledger until meeting the validation criteria. As long as the number of faulty nodes remains under 20%, the ledger is authentic [51], [52], [53].

N. PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

PBFT [15], [29], [54] algorithm involves multiple rounds of voting by all nodes of the network in order to commit state change [14], [35], [36]. PBFT consensus provides high throughput and low latency in validating transactions, however, the overhead incurred by broadcasting blocks and votes in PBFT consensus makes it unable to scale beyond a network with tens of validators.

O. TENDERMINT TENDERMINT (TT)

TT [55]uses proof of stake in combination with principles of PBFT to provide security, high throughput, and low block processing times of 1-3 seconds. While in PBFT, a leader node is used to get chosen pseudorandomly, Tendermint uses the lottery-based properties of proof of stake and chooses the leader node with probability proportional to the stakeholdersshare in the network. Tendermint provides a safety guarantee that no conflicting blocks are created, and no forks appear in the blockchain. Tendermint is compatible with public or private chains; however, it does not enjoy the same level of scalability as proof of work or proof of stake blockchains.

P. FEDERATED BFT

Blockchain implementations in Ripple [51] and Stellar [56] extended the traditional Byzantine Fault Tolerance and made it open-ended for participation in scenarios involving a consortium or federation of nodes. Ripple allows open-ended participation of users, market entities, and gateways to other subnetworks [29]. Stellar provides flexible trust, and low latency, since it is computationally inexpensive, and quorums contain a limited number of nodes that share vote messages.

Q. PROOF OF AUTHORITY

Proof of Authority [37] has been proposed as an underlying consensus algorithm for permissioned blockchains [29]. This algorithm substitutes a lighter message transmission scheme in comparison with BFT algorithm, which has led to the superiority of this approach concerning its performance.

R. MACHINE LEARNING-BASED APPROACHES

Machine learning has a wide range of uses and applications, and we see them every day all around us. Recently, its benefits in blockchain consensus are also emerging. For example, authors in [57] proposed a machine-learning-based consensus mechanism called Proof-of-Learning (PoL) that establishes a cooperative relationship between two complex and unrelated tasks. Its transaction is validated through a machine learning task inspired by machine learning competitions like those hosted in Kaggle. WekaCoin, a blockchain-based cryptocurrency, currently uses PoL. Conventional consensus algorithms, such as PoW-based protocols, routinely perform a massive amount of computation to solve a cryptographic puzzle. To overcome the computational complexity, the researchers in [58] introduced a variation of PoL that directs the computation spent for block consensus toward optimizing neural networks. As a result, the algorithm achieves a stable block generation rate without significantly losing training performance. Machine learning-based consensus protocol is

also effective in IoT-based smart cities, where various kinds of transaction prioritization are often a feature [59].

V. APPLICATION PERSPECTIVE BASED ON CONSENSUS ALGORITHMS

Blockchain has now been deployed in not only cryptocurrency but its underlying technology is used in various applications [60], [61], [62], [63]. Different application scenarios required types of consensus protocols. For example, public blockchains are more suitable for an open environment, whereas consortium blockchains are more appropriate for enterprise cooperation [14]. So the requirement of consensus protocols constantly changes based on the application requirements. Researchers developed various consensus protocols for that reason with different aspects kept in mind. As a result of facts, the blockchain technologies with each consensus protocol have different development tools, [64], [65], [66], [67], [68], [69], [70] technologies and platforms. Some consensus mechanisms are used for public blockchains, and some are for private ones. Some protocols are used on both private and public blockchains. Some of the consensus mechanisms were used in a blockchain because of their node size, and some were used based on the transaction frequencies. Blockchain Types also play a vital role in selecting consensus algorithms in a blockchain application.

We investigate the literature regarding the development tools and application platforms for different consensus protocols and put them in a tabular form. In Table 1, we presented the consensus protocols with their applications and development platforms and the application platforms in detail [60], [71], [72], [72], [73], [74], [75], [76], [77], [78], [79], [80]. It also provided development languages for each consensus protocol, including their uses in different blockchain applications. The table shows a detailed comparative analysis of the uses of consensus algorithms in different industries. The blockchain consensus protocol has several specific goals, including agreement, cooperation, collaboration, mandatory participation of each node in the consensus process, and equal rights for all nodes. As a result, a consensus algorithm seeks to identify a standard agreement that benefits the entire network. Here, we categorically discuss some selected domain-specific applications with their respective consensus protocols as follows.

A. FINANCIAL MANAGEMENT

P2P and third-party payment systems have accelerated the development of financial decentralization with the emergence of Internet finance. Due to the innovation in data storage and transmission, blockchain is a fundamental technological advance in financial systems and the FinTech sector [81]. In the financial sector, digital currencies have utilized blockchain to gain faster payment methods. Most of the discussed consensus algorithms in this paper are used in cryptocurrency applications. Different consensus algorithms are used in different applications to address different challenges in the developed solutions. Some of the consensus algorithms have limitations in energy consumption; some have problems in centralization, and some have economic security [82]. Blockchain is used not only in cryptocurrency for financial management but also to transform traditional financial systems into a cross-border transaction industry. Ripple consensus algorithm has been vastly popularized, based on the crypto tokens ensuring low cost of transactions and revolutionizing the remittance industry [83].

B. HEALTHCARE

Blockchain Technology has tremendous potential in healthcare. It can be used to manage data that could benefit the potential to connect disparate systems and increase the accuracy of EHR. It can also be used to support drug prescriptions and supply chain management, pregnancy and any risk management, as well as to support access control, data sharing and managing audit trail of medical activities [84]. Proof of Interoperability, Proof of Movement (share transportation data with the community and get the reward) and PBFT are some of the most well-known consensus protocols in blockchain-based healthcare [60]. Fast Health Interoperability Resources (FHIR) profile that shows elements and data formats, along with providing publicly accessible application programming interfaces (APIs) for the reason of exchanging EHR [60]. Hyperledger Fabric technique is also used in privacy-preserving medical systems [60].

C. SUPPLY CHAIN MANAGEMENT

The capacity of blockchain to guarantee the reliability, traceability, and validity of information, as well as smart contractual connections for a trustless environment, all point to a major rethinking of supply chains and supply chain management (SCM) [85]. All the changes made during the supply chain process are recorded in the transactions ledger keeping it secure and unchangeable [60]. Public blockchain consensus has slow speed, which is a limitation for blockchain to use in SCM, but a weighted variation of Proof of Stake is being used for this type of blockchain application to reach out to underdeveloped and remote areas [60].

D. NFT MARKETPLACES

A Non-Fungible Token (NFT) is a blockchain-based ownership record (such as the Ethereum blockchain). While digital assets such as photographs and movies are the most commonly exchanged as NFTs, the sale of physical assets such as postal stamps, gold, real estate, physical artwork, and so on is also gaining popularity [86]. Several NFT marketplaces (NFTMs), e.g., OpenSea, Rarible, and Axie emerged in recent years to facilitate buying and selling NFTs [86]. An NFT is the equivalent of a traditional proof-of-purchase in the world of cryptocurrencies, such as a paper invoice or an electronic receipt. NFTs are appealing due to their verifiability and trustless transfer, among other reasons [87]. Verifiability

TABLE 1. Comparative analysis of application perspective of consensus algorithms.

Consensus Algorithm	Platform	Programming Language	Public/private	Application
PoW	Cryptocurrency, Governance, Entertainment,Real Estate, Power	Solidity,Golang	Public	Ethereum, Bitcoin, Monoxide,Litecoin
PoS	Cryptocurrency, Governance, Entertainment	Solidity, Java, C++,Python, Go	Public/Private	Ethereum, Cosmos,Casper, QTUM,Peercoin
DPoS	Cryptocurrency	JavaScript,Python, Ruby	Public/Private	EOS,Bitshares
TaPoS	Cryptocurrency	Not Known	Public/Private	BitCoin, Peercoin
PoA	Cryptocurrency	Solidity, Java, Python	Public	Bitcoin or bitcoin related technologies, Decred
PoSpace	Cryptocurrency, Cellular Networks	Java	Public	Brustcoin,Chia and Spacemint,IPFS
PoAu	Cryptocurrency	Golang	Public	PoA.Network,Ethereum,Kovan testnet,vechain
PoET	Cryptocurrency	Python, JavaScript, Golang, C++, Java, Rust	Public	Hyperledger sawtooth
PBFT	Cryptocurrency, General Consensus Algorithm	Java,Golang,Node	Public/private	Hyperledger
DBFT	Cryptocurrency	C#, Python, .NET, Java, C++, C, Golang, Kotlin, JavaScript	Public/private	Neo
Ripple	Cryptocurrency	Java,C++,Node.js	Public	Ripple (XRP)

*PoW = Proof of Work, PoS = Proof of Stake, DPoS = Delegated Proof of Stake, TAPoS = Transactions as Proof of Stake, PoA = Proof of Activity, PoSpace = Proof of Space, PoAu = Proof of Authority, PoET = Proof of Elapsed Time, PBFT = Practical Byzantine Fault Tolerance, DBFT = Delegated BFT NA= Not Available.

entails recording sales as blockchain transactions, enabling ownership verification [86].

E. HEAVY INDUSTRY & MANUFACTURING

The demands for smart, individualized and sustainable products lead to the emerging of new smart manufacturing paradigms, for example, cyber-physical production systems, cloud manufacturing and social manufacturing in the industry 4.0 blueprint [88]. In the Industry 4.0 vision, machines with a certain degree of interaction capability will be empowered to cooperate with each other via the Industrial Internet [89]. Heavy industry or manufacturing requires lots of data sharing and device collaboration Proof of Stake-based consensus protocols would be used if there is no need for high throughput. n the application scenario is the cooperation between a small number of companies, a Blockchain can be used to record business transactions among them [14]. PBFT-based or Hash code-based consensus algorithms could be good choices in this case [14].

F. SECURING PERSONAL INFORMATION

On the Ethereum platform, there is an identity management blockchain application where users can claim ownership of their identities. Users can request and send credentials, safely store their keys and data, sign transactions, and request and send credentials [90]. Blockchain can be used to store academic records, birth, death, and marriage certificates by making them more reliable and secure. Simply blockchain can simply be used to protect the identity of users by encrypting the data and securing it from attackers [91]. As each individual would have a node and the count of nodes would be enormous, Proof of work and Proof of stake consensus algorithms would be better choices [14].

G. SECURE IoT NETWORKS

IoT is based on a centralized network in which numerous devices are linked to one another through the cloud or any other central network [92]. The device receives the data from the cloud. This creates a scalability problem since data transmission and reception from several devices might cause the central system to lag and raise security concerns. The IoT is now more dependable, secure, and effective thanks to blockchain [60]. In IoT networks, two types of consensus are normally used, 1. The global consensus facilitates service integration and knowledge sharing 2. local consensus to achieve integration of functional capabilities and knowledge sharing. There are also consensus mechanisms merging from proof of work and proof of stake to have two-step authentication on the IoT networks [60].

VI. COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS

We provided two different types of comparative analysis of different consensus algorithms. In the first analysis, we compare and contrast different consensus algorithms based on verification mechanisms. The second type of analysis evaluates the performance of different algorithms using various performance metrics.

A. COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS BASED ON VERIFICATION MECHANISM

In Table 2 and 3, A detailed comparative analysis of the verification mechanism has been shown. In their comparison,

a detailed analysis has been found for security, energy consumption, decentralization, scalability, and interoperability.

Let's look at the verification mechanism for PoW. It can be secure and decentralized, but it will cost large amounts of energy, like electricity and processing power. this will make it slow. On the other hand, PoS is more energy efficient than PoW, but it would be less decentralized and subject to centralization risks. The variations of the PoS, like DPoS and TaPoS are even better in terms of energy consumption efficiency but the issues of decentralization and security risks remain.

PoA combines PoW and PoS to balance the trade-off between security, scalability and decentralization but doing so introduces so much complexity into the system, which is difficult to implement. PoSpace is a very effective, secure, scalable and fast consensus mechanism, but its relatively new and has a great risk of data vulnerability and tampering. PoAuthority and PoET are also fast and energy efficient, but there is a problem with decentralization in both of them. PoET requires extra hardware to make it function.

PBFT is a great consensus protocol, but it mainly works for permissioned blockchains. Though it's significantly faster than existing protocols, it can be complex and less decentralized in terms of PoW or PoS. DBFT is an updated version of PBFT, which is more robust to network failure. But it is less decentralized and susceptible to 51% attacks. PBFT and DBFT have high interoperability, as they use a widely used consensus protocol that can be adapted to work with different blockchains. And Finally, Ripple is also very fast and cost-effective, which is also a good option for achieving interoperability and scalability. But it also has some issues with Trust, and it's less decentralized than most of the protocols.

So from the analysis, we can say that the consensus mechanism will depend on the specific requirements of the blockchain applications. each mechanism has its own trade-off, and the choice of the consensus protocols will be based on the application's needs.

B. COMPARATIVE ANALYSIS BASED ON THE PERFORMANCE OF CONSENSUS ALGORITHMS

In Table 2, We compared the algorithmic level of comparisons in terms of performance, efficiency, and uses in blockchains. Our quantitative analysis of the consensus algorithms gave a brief idea about the main mechanism, cost, effectiveness, scalability, etc, to help select consensus protocols for different applications.

In Table 3, We showed extensive information on different consensus algorithm selections in blockchain networks. We addressed the challenges of each consensus algorithms [28], [93], [94], [95], [96], [97], [98]. Consensus mechanisms are responsible for the integrity of the information contained in blockchain while defending against double-spend attacks and therefore are an essential part of blockchain technology [29]. The final goal is to achieve consensus in a distributed network without central authorities and with participants who do not necessarily trust each other. There are different consensus algorithms due to different requirements in each domain. For example, some domains require low power, and others require faster processing of transactions [12], [13], [30], [31], [32], [33], [34]. In spite of having so many advantages from the consensus algorithms, there are some issues that need to be also addressed in the challenge section. However, apart from the issues we addressed in earlier descriptions, the performance issues regarding the consensus algorithms, we also address two very important challenges in blockchain-based healthcare systems.

Table 3 is providing an extensive comparative analysis of different performance metrics we defined for the comparison. From the table, we can see that PoW requires the highest processing power compared to any other consensus algorithm. Because of the intensive computational complexities in each node, nodes are required to solve complex mathematical problems. PoS and its variations are required less processing power as they rely on validators to secure the network. on the other hand, PoA came from the combination of both PoW and PoS where PoW components ensure security and PoS components help to validate transactions as a result it requires less processing power. Similarly, most of the algorithms required less processing power than PoW. If processing power is not an issue then PoW works best otherwise, the selection of consensus protocols would change.

From the table, we can also see that PoW is the most decentralized consensus algorithm because it does not depend on the validators to complete its transactions. It's also noticeable that DBFT is the least decentralized protocol used in blockchain applications because transaction validation happens based on elected validators. if we look into the hardware requirement, we can see that PoW requires hardware to participate in the blockchain, and PoET even requires dedicated hardware to approve miners. On the other hand, PoS and DBFT have very low requirements for hardware to participate in the network. In terms of security, most of the consensus protocols provide high-end security except PoS, DPoS and PoSpace. These three are susceptible to specific types of attacks in the networks. Scalability is a very important aspects of blockchain nowadays, and poW has very low scalability due to higher complexity. But DBFT and Ripple are some highly scalable consensus mechanisms as they have a large number of transactions per period. In terms of resource cost, PoW requires a very high amount of resources to participate as miners. PoS and DBFT, some examples have less resource consumption.

Difficulty means how much difficult to validate a transaction and secure the network. If we look into the table we can say that PoW is highly difficult and it can be expensive and slow and sometimes it could be susceptible to attacks if any miners have a large number of blocks. PoS and its variations are much less difficult which is making them faster and more efficient. On the other hand, PoA, and PBFT, DBFT are moderately difficult but they have a certain problem being susceptible to attacks if most of the validators are malicious.

TABLE 2. Comparative analysis on consensus algorithms.

Consensus Algorithm	Blockchain Type	Verification mechanism	Cost	Efficiency	Scalability
Proof of Work (PoW)	permissioned/permissionless	Miners go through a complex mechanism to add new blocks to the blockchain	High	Low	Low
Proof of Stake (PoS)	permissioned/permissionless	Validators need to put a portion of their tokens to participate in the verification process	Low	High	Medium
Delegated Proof of Stake (DPoS)	permissioned/permissionless	Validators need to put a portion of their tokens to participate in the verification process	Medium	High	High
Transactions as Proof of Stake (TaPoS)	permissioned/permissionless	Normally verification happened on two things 1. the number of tokens provided in the verification 2. the frequency of transactions. These two determine the verification weight to complete the process	Medium	High	Medium
Proof of Activity(PoA)	permissioned/permissionless	Validators validate new blocks produced by miners periodically, a a process that combines the verification mechanism of PoW and PoS.	Medium	High	Low
Proof of Space(PoSpace)	permissioned/permissionless	Validators needs to prove that they have a certain amount of disk space to verify transactions.	Low	High	Medium
Proof of Authority	permissioned/permissionless	Miners needs pre-approval from a group of authorities to verify new transactions.	High	High	High
Proof of Elapsed Time (PoET)	permissioned/permissionless	Successful miners wait a random amount of time to validate new blocks.	Very Low	High	High
Practical Byzantine Fault Tolerance(PBFT)	Permissioned	Miners validating new block by consensus and voting to reach an agreement on the state of the network.	Medium	High	High
Delegated BFT(DBFT)	Permissioned	Miners validating new block by consensus and voting to reach an agreement on the state of the network.	Low	High	High
Ripple	Permissioned	Transactions are validated by a network of trusted validators.	Low	High	High

So, if we look into the analysis, PoW is relatively low performance compared to other algorithms. PoS and its variations provide better performance overall compared to PoW. PoSpace, PoA, PoETand Ripple are some of the very good consensus algorithms in terms of performance but there are more issues regarding susceptible to attacks.

VII. OPERATIONAL AND INTEROPERABILITY ISSUES IN EXISTING BLOCKCHAIN SOLUTIONS

The use of blockchain in smart healthcare, smart homes, and smart transportation is growing by the day. Although security mechanisms used in blockchain-based applications are inexorably connected, they are not immune. Even in blockchain securities, some concerns do not exist in centralized systems. We highlighted the problems that make a blockchain system less efficient and trustworthy in this part. These factors may expose a blockchain application to the risk of vulnerability. We thoroughly explored the issue of compatibility with existing blockchain technologies. Because of blockchain's distributed architecture, we may assume data security is granted in blockchain-based apps, although this is not the case. Several other factors contribute significantly to the security and usability of blockchain systems. However, achieving a perfect blockchain system is extremely challenging due to the diverse nature of difficulties and issues. This section addressed all the issues other than security.

A. OPERATIONAL ISSUES

In the blockchain system, a transaction is completed through a number of stages. If any process has trouble running across the entire cycle of steps, it will cause functional problems. It's crucial to meet non-functional needs also if you want a system to work successfully. A system may fail because of the problems even if it has no functional problems. Therefore, there is a significant operational difficulty that has to be resolved.

- **Smart Contract Issues:** Although there are a lot of advantages to the smart contract approach in Blockchain solutions, they are vulnerable to a series of attacks. Sometimes the execution of an authorized contract brings some problems within the computer since it makes them vulnerable to technical issues such as hacking, bugs, viruses, or communication failures. Due to the irreversibility of the contract coding bug fixing is quite critical [94].
- **Credential Security:** In Blockchain, transactions mainly depend on the private key of a given user. Due to not having multi-factored authentication in most of the current systems, it is possible to lead to a complete loss of patient data by losing private key information to other users [99].
- **Processing time:** It is necessary to implement encryption algorithms for all nodes involved in the Blockchain IoT ecosystem. Because IoT frameworks are different

TABLE 3. Issues exist in consensus algorithms based on different metrics.

Properties	PoW	PoS	DPoS	TaPoS	PoA	PoSpace	PoAu	PoET	PBFT	DBFT	Ripple
Processing power	High	Low	Low	Medium	Medium	Low	Low	Low	Medium	Medium	Low
Decentralization	High	Medium	Low	Medium	Medium	High	Low	High	Low	Low	Low
Electricity consumption	High	Low	Very low	Low	Low/Medium	Low	Low	Low	Low/Medium	Low/Medium	Low
Hardware	High	Low	Low	Medium	Medium	Low	Low	High	Low	Low	Low
Security	High	Low	Low	High	High	Low	High	High	High	High	High
Scalability	Low	Medium	High	Medium	Low	Medium	High	High	High	High	High
Interoperability	Low	Medium	Medium	Medium	Medium	Low	Low	Medium	High	High	Medium
Susceptible to attacks	Low	Medium	Low	Medium	Low	Medium	Low	Medium	Medium	Low	Low
Small Concensus Group	Not suitable	Suitable	Suitable	Suitable	Suitable	Suitable	Suitable	Suitable	Suitable	Suitable	Suitable
Authenticity	High	High	High	High	High	High	High	High	Low	High	High
Control	Low	Medium	High	Medium	Medium	Low	High	Low	Low	High	High
Consistency	Fork	Fork	Fork	NA	NA	NA	NA	NA	Not Fork	NA	NA
Resource Cost	High	Low	Low	Medium	High	Low	Low	Low	Medium	Low	High
Threshold for attack	25% hash	51%	33.33%	NA	NA	27%	NA	25% hash	33.33%	NA	20%
Transactions	Low	Medium	High	Medium	Low	Medium	High	High	High	High	High
Difficulty	High	Low	Low	Medium	Medium	Low	Low	Low	Low	High	Low
Performance	slow	Fast	very Fast	Fast	Fast	Fast	Very Fast	Fast	Fast	Very Fast	Very Fast

*PoW = Proof of Work, PoS = Proof of Stake, DPoS = Delegated Proof of Stake, TAPoS = Transactions as Proof of Stake, PoA = Proof of Activity, PoSpace = Proof of Space, PoAu = Proof of Authority, PoET = Proof of Elapsed Time, PBFT = Practical Byzantine Fault Tolerance, DBFT = Delegated BFT NA= Not Available.

have good computational capabilities due to the centralized system. But Blockchain. nodes are not identical so processing time would vary [94].

- **Limitations of cloud storage:** Due to the change of storage system from a single central storage server to a distributed cloud server, the cost of memory significantly increases in Blockchain-based IoT system [94].
- **Risk over Vendors:** As Blockchain is a comparatively new idea, companies must choose a vendor who can perfectly build applications that properly address the risks associated with the blockchains [99].
- **Resource constraints:** IoT platforms requires very few resources to compute exchange and store resource information, but Blockchain needs a lot of resources.
- **Legal and Compliance:** Itš new territory in all aspects without any legal or compliance precedents to follow, which poses a serious problem in IoT manufacturers and service [99] providers. This challenge alone will scare off many businesses from using blockchain technology.
- **Scalability Issues:** Its transaction processing speed is very slow, and it is impractical to maintain a large user base. For example, Visa processes thousands of transactions per second for tens of millions of customers. On the other hand, the Bitcoin network is capable of processing a maximum of seven transactions per second [48].

B. INTEROPERABILITY ISSUES

To discuss the interoperability issues in Blockchain technology, first, we should know what Blockchain Interoperability is. In 1996, Peter Wegner stated that ''interoperability is the ability of two or more software components to cooperate despite differences in language, interface and execution platform'' [100], [101]. Blockchain Interoperability means providing interoperability between blockchains to explore synergies between different solutions, scale the existing ones and create new use cases [102], [103]. For example, a user should be able to transfer their assets from one blockchain to another or build a cross-blockchain [100], [104].

Existing systems which ensure interoperability and their issues When blockchain was first developed, it was first thought of as a single chain meaning that all transactions to different endpoints, smart contracts, and other internal and external operations would have happened on a single chain. As such a system is not feasible due to the scalability issues and improvement constraints, a new technological advancement in blockchain has been made for communication between two relatively independent blockchains. Currently, various ways exist to achieve interoperability among blockchains.

- **Cross-chains** To avoid the limitations of a single chain, the cross-chains protocol is one of the promising mechanisms to ensure interoperability. Cross-chain implementations are mainly designed to swap assets and transfer assets among different blockchains [102], [105]. There are two types of cross chains 1. Isomorphic cross chains 2. Heterogeneous cross-chain. Though Isomorphic is, the much simpler effective grouping of isomorphic blocks remains a key challenge. On the other hand, achieving cross-chain interaction among heterogeneous chains requires third-party ancillary services. Moreover, it is block composition, and the deterministic guarantee mechanism are quite different. So direct cross-chain interaction mechanism is not easy to design. Blocknet, Polkadot, Aion, and Wanchain are some of the cross-chain solutions of interoperability [102], [103].
- **Sidechains/relays** Sidechains are like a central hub of communication of different blockchain systems. Sidechains will work as a common client for the blockchains. It will have access to user data for transactions from real blockchains and can exchange assets by using sidechains [101], [106]. The sidechain can have independent consensus algorithms and tokens. They can have even their own miners, original blockchains are not responsible for maintaining the sidechains. To work the sidechains, there should be certain features, including multi-sig capability and fast consensus

finality [101], [104]. It would be very difficult to connect existing blockchains that don̈t have those characteristics.

- **Proxy Token** A proxy token can be called a proxy contract which would implement a standard interface and act as a subdomain for the blockchains. In this approach, the blockchains will not need to change the application layer. For a blockchain, a new token will be introduced, and add the address of the proxy token into the blockchain [102], [103]. But there are several drawbacks to the approach. There will be additional function calls and making the ecosystem much slower. It will also increase the attack vectors in the blockchain ecosystem [104].
- **Atomic Swaps** Atomic swaps is a technique that allows two different blockchain networks to have transactions. These atomic swaps are also known as atomic cross-chain trading based on smart contracts, and they allow users to trade their coins directly from their crypto wallet. So atomic swaps are, essentially, peer-to-peer trades across different blockchains [107], [108]. Atomic swap protocols are designed to prevent any of the involved parties from cheating. There are some drawbacks to the protocols also and the most important among them is two different blockchains will need to share the same hash algorithm. Other than that, atomic swaps bring up concerns about users' privacy. Thatš because on-chain swaps and transactions can be quickly tracked on a blockchain explorer, making it easy to link the addresses [102], [103].
- **Notary schemes** Transactions under this method rely on a third-party notary. A trusted exchange known as a notary manages the lack of trust between the two parties to the transaction. The notary may be a network of exchanges or a controlled exchange. The notaryš integrity is the only factor affecting how well a notary scheme works [101], [104], [109].
  However, it centralizes trust which goes against the main paradigm of blockchain, namely decentralization. This consequence might be acceptable in situations where blockchain consortia members can agree on a central party to operate the notary scheme [103].
- **Oracle** Oracles fill the informational gap between on-chain and off-chain settings in the context of blockchain technology. By ensuring that multiple ecosystems are referring to a single source of truth, decentralized oracle services like Chainlink help to ensure that off-chain data is fed to blockchain-enabled smart contracts [109]. The only issue with Oracle is that it's not creating block-blockchain interoperability but making a blockchain system interoperable with non-blockchain systems [103].
- **Hashed TimeLock Contract (HTLC)** (HTLC) is also among blockchain interoperability solutions used to build smart contracts with the ability to modify payment channels [109]. It uses interconnected channels to allow users to send transactions even if they are not directly connected through a channel, a process known as network routing. This is the most practical technical method to interoperability but is also the most limiting in terms of functionality, only supporting digital asset exchange [103].

VIII. CONCLUDING REMARKS

This survey discussed the importance of appropriate consensus mechanisms for secure blockchain transactions. To understand the landscape of these mechanisms, the study presented a comprehensive analysis of different blockchain systems with a focus on consensus algorithms and issues with existing protocols. A comparative discussion of different consensus protocols was provided to gain insights into their performances, cost of transactions, and scalability issues. The categorical discussion on consensus algorithms helped us understand their systematic uses in distributed systems, both permissioned and permissionless blockchains. The paper also provided a critical analysis of various operational problems and challenges, emphasizing factors such as security, scalability, efficiency, and interoperability when developing new consensus protocols to ensure optimal performance and reliability.

The findings from the analysis suggested that the choice of consensus protocol significantly affects the design and operation of blockchain applications. The paper compared different consensus protocols in terms of their performance, cost, and scalability and revealed that there was no clear advantage of one protocol over another in a general sense. The most suitable protocol depends on the specific application requirements. The paper highlighted various challenges and issues that affected the operational perspectives of blockchain systems and provided possible solutions to address these challenges. Overall, the study provided a thorough understanding of blockchain and consensus protocols, along with critical insights into their operational issues and challenges. The paper can be used as a guideline for developers and researchers to design more robust and interoperable blockchain systems while addressing the identified limitations.

REFERENCES

[1] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, pp. 99–111, Jan. 1991.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, Oct. 2008.
[3] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017.
[5] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[6] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100067.
[7] T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, and A. Kerrouche, "Implementation of blockchain consensus algorithm on embedded architecture," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Apr. 2021.

[8] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "SoK: Sharding on blockchain," in *Proc. 1st ACM Conf. Adv. Financial Technol.*, Oct. 2019, pp. 41–61.

[9] G. Greenspan, "MultiChain private blockchain," Coin Sci. Ltd, U.K., 2023. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[10] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surveys*, vol. 54, no. 8, pp. 1–41, Nov. 2022.

[11] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain consensus: An overview of alternative protocols," *Symmetry*, vol. 13, no. 8, p. 1363, 2021.

[12] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[13] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, "A survey and taxonomy of consensus protocols for blockchains," *J. Syst. Archit.*, vol. 127, Jun. 2022, Art. no. 102503.

[14] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: Mechanism, design and applications," *Sci. China Inf. Sci.*, vol. 64, no. 2, pp. 1–15, Feb. 2021.

[15] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Exp. Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.

[16] S. Davidson, P. D. Filippi, and J. Potts, "Economics of blockchain," *SSRN 2744751*, Mar. 2016, doi: 10.2139/ssrn.2744751.

[17] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, "Discovering bitcoin's public topology and influential nodes," Tech. Rep., 2015. [Online]. Available: https://www.cs.umd.edu/projects/coinscope/coinscope.pdf

[18] B. Segendorf, "What is bitcoin," *Sveri gesRiksbankEconomicReview*, vol. 2014, pp. 2–71, Mar. 2014.

[19] S. Tempesta, *Introduction to Blockchain for Azure Developers: Understanding the Basic Foundations of Blockchain*. New York, NY, USA: Apress, Jan. 2019.

[20] S. Dos Santos, C. Chukwuocha, S. Kamali, and R. K. Thulasiram, "An efficient miner strategy for selecting cryptocurrency transactions," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 116–123.

[21] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustain. Energy Technol. Assessments*, vol. 52, Aug. 2022, Art. no. 102039.

[22] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, pp. 1–8, Sep. 1997. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548

[23] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021.

[24] A. Imteaj, M. H. Amini, and P. M. Pardalos, "Toward smart contract and consensus mechanisms of blockchain," in *Foundations of Blockchain*. Cham, Switzerland: Springer, 2021, pp. 15–28.

[25] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[26] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of blockchain technology: Pros, cons and SWOT," *Cluster Comput.*, vol. 22, no. S6, pp. 14743–14757, Nov. 2019.

[27] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.* Cham, Switzerland: Springer, 2002, pp. 251–260.

[28] K. Azbeg, O. Ouchetto, S. J. Andaloussi, and L. Fetjah, "An overview of blockchain consensus algorithms: Comparison, challenges and future directions," in *Proc. Adv. Smart Soft Comput.*, in Advances in Intelligent Systems and Computing, vol. 1188. Singapore: Springer, Oct. 2020, doi: 10.1007/978-981-15-6048-4_31.

[29] Y. Merrad, M. H. Habaebi, E. A. A. Elsheikh, F. E. M. Suliman, M. R. Islam, T. S. Gunawan, and M. Mesri, "Blockchain: Consensus algorithm key performance indicators, trade-offs, current trends, common drawbacks, and novel solution proposals," *Mathematics*, vol. 10, no. 15, p. 2754, Aug. 2022.

[30] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550.

[31] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[32] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Exp. Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114384.

[33] Y. Wen, F. Lu, Y. Liu, P. Cong, and X. Huang, "Blockchain consensus mechanisms and their applications in IoT: A literature survey," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* Cham, Switzerland: Springer, 2020, pp. 564–579.

[34] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103035.

[35] X. Li, Q. Zhu, N. Qi, J. Huang, Y. Yuan, and F.-Y. Wang, "Blockchain consensus algorithms: A survey," in *Proc. China Autom. Congr. (CAC)*, Oct. 2021, pp. 4053–4058.

[36] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, p. 47, Jan. 2022.

[37] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[38] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild," in *Proc. 31st Int. Symp. Distrib. Comput. (DISC)*, Vienna, Austria, Oct. 2017, pp. 1–16, doi: 10.4230/LIPIcs.DISC.2017.1.

[39] J. Bou Abdo, R. El Sibai, K. Kambhampaty, and J. Demerjian, "Permissionless reputation-based consensus algorithm for blockchain," *Internet Technol. Lett.*, vol. 3, no. 3, p. e151, May 2020.

[40] J. Wu and S. Jiang, "On increasing scalability and liquidation of lightning networks for blockchains," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2589–2600, Jul. 2022.

[41] V. Vignesh, S. H. Gopalan, M. Mohan, R. S. Ramya, and R. Ananthakumar, "A quantum-based blockchain approach to voting protocol using hyperledger sawtooth," *J. Phys., Conf.*, vol. 1916, no. 1, May 2021, Art. no. 012088.

[42] V. Costan and S. Devadas, "Intel SGX explained," Cryptol. ePrint Arch., Paper 2016/086, Feb. 2017. [Online]. Available: https://eprint.iacr.org/2016/086

[43] E. Bresson, A. Canteaut, B. Chevallier-Mames, C. Clavier, T. Fuhr, A. Gouget, T. Icart, J. F. Misarsky, M. Naya-Plasencia, P. Paillier, and T. Pornin, "Shabal, a submission to NIST's cryptographic hash algorithm competition," *Submission NIST*, pp. 1–300, Oct. 2008.

[44] G. Ateniese, I. Bonacina, A. Faonio, and N. Galesi, "Proofs of space: When space is of the essence," in *Proc. Int. Conf. Secur. Cryptogr. Netw.* Cham, Switzerland: Springer, 2014, pp. 538–557.

[45] S. Takahashi, "Proof-of-approval: A distributed consensus protocol for blockchains," Tech. Rep., 2018. [Online]. Available: https://github.com/Takanium/doc/blob/master/research/proof-of-approval.pdf

[46] P. Siano, G. De Marco, A. Rolán, and V. Loia, "A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets," *IEEE Syst. J.*, vol. 13, no. 3, pp. 3454–3466, Sep. 2019.

[47] C. Cachin, S. Schubert, and M. Vukolić, "Non-determinism in Byzantine fault-tolerant replication," 2016, *arXiv:1603.07351*.

[48] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 4, no. 1, p. 14, 2017.

[49] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Gener. Comput. Syst.*, vol. 107, pp. 760–769, Jun. 2020.

[50] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, Dec. 2016, pp. 1–6.

[51] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.

[52] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," 2017, *arXiv:1707.01873*.

[53] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *Proc. Int. Conf. Trust Trustworthy Comput.* Cham, Switzerland: Springer, 2015, pp. 163–180.

[54] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99. 1999, pp. 173–186.

[55] J. Kwon, "Tendermint: Consensus without mining," *Draft v. 0.6, fall*, vol. 1, no. 11, pp. 1–11, 2014.

[56] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Develop. Found.*, vol. 32, pp. 1–45, Jul. 2015.

[57] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, Apr. 2019, pp. 119–124.

[58] Y. Liu, Y. Lan, B. Li, C. Miao, and Z. Tian, "Proof of learning (PoLe): Empowering neural network training with consensus building on blockchains," *Comput. Netw.*, vol. 201, Dec. 2021, Art. no. 108594.

[59] S. V. Sanghami, J. J. Lee, and Q. Hu, "Machine-learning-enhanced blockchain consensus with transaction prioritization for smart cities," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6661–6672, Apr. 2022.

[60] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and applied perspective to blockchain technology: A comprehensive survey," *Appl. Sci.*, vol. 11, no. 14, p. 6252, Jul. 2021.

[61] H. T. M. Gamage, H. D. Weerasinghe, and N. G. J. Dias, "A survey on blockchain technology concepts, applications, and issues," *Social Netw. Comput. Sci.*, vol. 1, no. 2, pp. 1–15, Mar. 2020.

[62] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020, doi: 10.1016/j.jpdc.2019.12.019.

[63] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, 2020.

[64] D. Amu and S. Baskaran, "A survey of applications using blockchain technology," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2022, pp. 1–6.

[65] Q. E. Abbas and J. Sung-Bong, "A survey of blockchain and its applications," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2019, pp. 001–003.

[66] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–11.

[67] X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Appl. Sci.*, vol. 9, no. 22, p. 4731, Nov. 2019.

[68] H. Chai, X. Chen, and H. Wang, "Special issue: Blockchain technology application," *Frontiers Eng. Manag.*, vol. 7, no. 4, pp. 467–470, Sep. 2020, doi: 10.1007/s42524-020-0141-1.

[69] A. M. Kudin, B. A. Kovalenko, and I. V. Shvidchenko, "Blockchain technology: Issues of analysis and synthesis," *Cybern. Syst. Anal.*, vol. 55, no. 3, pp. 488–495, May 2019.

[70] M. Maffei, R. Casciello, and F. Meucci, "Blockchain technology: Uninvestigated issues emerging from an integrated view within accounting and auditing practices," *J. Organizational Change Manage.*, vol. 34, no. 2, pp. 462–476, Mar. 2021.

[71] J. Bao, D. He, M. Luo, and K.-K.-R. Choo, "A survey of blockchain applications in the energy sector," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3370–3381, Sep. 2021.

[72] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for modern applications: A survey," *Sensors*, vol. 22, no. 14, p. 5274, Jul. 2022.

[73] C. Liu, X. Zhang, K. K. Chai, J. Loo, and Y. Chen, "A survey on blockchain-enabled smart grids: Advances, applications and challenges," *IET Smart Cities*, vol. 3, no. 2, pp. 56–78, Jun. 2021.

[74] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *J. Netw. Comput. Appl.*, vol. 177, Mar. 2021, Art. no. 102857.

[75] C. Sathish and C. Y. Rubavathi, "A survey on blockchain mechanisms (BCM) based on Internet of Things (IoT) applications," *Multimedia Tools Appl.*, vol. 81, no. 23, pp. 1–40, 2022.

[76] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Comput. Commun.*, vol. 169, pp. 179–201, Mar. 2021.

[77] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A research survey on applications of consensus protocols in blockchain," *Secur. Commun. Netw.*, vol. 2021, pp. 1–22, Jan. 2021.

[78] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.

[79] B. Tavares, F. F. Correia, A. Restivo, J. P. Faria, and A. Aguiar, "A survey of blockchain frameworks and applications," in *Proc. Int. Conf. Soft Comput. Pattern Recognit.* Cham, Switzerland: Springer, 2018, pp. 308–317.

[80] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A survey of blockchain applications in different domains," in *Proc. Int. Conf. Blockchain Technol. Appl.*, Dec. 2018, pp. 17–21.

[81] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees," *Technol. Forecasting Social Change*, vol. 158, Sep. 2020, Art. no. 120166.

[82] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2018, pp. 54–63.

[83] T. Qiu, R. Zhang, and Y. Gao, "Ripple vs. SWIFT: Transforming cross border remittance using blockchain technology," *Proc. Comput. Sci.*, vol. 147, pp. 428–434, Jan. 2019.

[84] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

[85] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019.

[86] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," 2021, *arXiv:2111.08893*.

[87] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges," 2021, *arXiv:2105.07447*.

[88] M. Moghaddam, M. N. Cadavid, C. R. Kenley, and A. V. Deshmukh, "Reference architectures for smart manufacturing: A critical review," *J. Manuf. Syst.*, vol. 49, pp. 215–225, Oct. 2018.

[89] H. Panetto, B. Iung, D. Ivanov, G. Weichhart, and X. Wang, "Challenges for the cyber-physical manufacturing enterprises of the future," *Annu. Rev. Control*, vol. 47, pp. 200–213, Jan. 2019.

[90] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, Sep. 2019.

[91] D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain: Emerging applications and use cases," 2019, *arXiv:1904.12247*.

[92] R. M. Aileni and G. Suciu, "IoMT: A blockchain perspective," in *Decentralised Internet of Things: A Blockchain Perspective*. Cham, Switzerland: Springer, 2020, pp. 199–215.

[93] H. D. Zubaydi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electronics*, vol. 8, no. 6, p. 679, Jun. 2019.

[94] M. Maroufi, R. Abdolee, and B. M. Tazekand, "On the convergence of blockchain and Internet of Things (IoT) technologies," *J. Strategic Innov. Sustainability*, vol. 14, no. 1, pp. 101–119, 2019.

[95] A. Menon, T. Saranya, S. Sureshbabu, and A. Mahesh, "A comparatýve analysis on three consensus algorithms: Proof of burn, proof of elapsed time, proof of authority," in *Computer Networks and Inventive Communication Technologies*. Singapore: Springer, Jan. 2022, pp. 369–383.

[96] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and A. Paudel, "A proof-of-authority blockchain-based distributed control system for islanded microgrids," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8287–8297, Nov. 2022.

[97] A. Welfare, "Types Blockchain," in *Commercializing Blockchain: Strategic Applications in the Real World*, Hoboken, NJ, USA: Wiley, 2019, ch. 2, pp. 37–66, doi: 10.1002/9781119578048.ch2.

[98] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, and L. He, "A comparative study of blockchain consensus algorithms," *J. Phys., Conf.*, vol. 1437, no. 1, Jan. 2020, Art. no. 012007.

[99] M. Padma, N. KasiViswanath, and T. Swathi, "Blockchain for IoT application: Challenges and issues," *Int. J. Recent Technol. Eng.*, vol. 7, pp. 34–37, Sep. 2019.

[100] P. Wegner, "Interoperability," *ACM Comput. Surv.*, vol. 28, no. 1, pp. 285–287, Mar. 1996, doi: 10.1145/234313.234424.

[101] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1298–1309, Nov. 2020.

[102] P. Lafourcade and M. Lombard-Platet, "About blockchain interoperability," *Inf. Process. Lett.*, vol. 161, Sep. 2020, Art. no. 105976.

[103] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2019, pp. 3–10.

[104] Monika and R. Bhatia, "Interoperability solutions for blockchain," in *Proc. Int. Conf. Smart Technol. Comput., Electr. Electron. (ICSTCEE)*, Oct. 2020, pp. 381–385.

[105] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Cross-chain interoperability among blockchain-based systems using transactions," *Knowl. Eng. Rev.*, vol. 35, p. e23, Jun. 2020.
[106] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153719–153730, 2020.
[107] C. Tan, S. Bei, Z. Jing, and N. Xiong, "An atomic cross-chain swap-based management system in vehicular ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–14, Jan. 2021.
[108] G. Wang and M. Nixon, "InterTrust: Towards an efficient blockchain interoperability architecture with trusted services," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 150–159.
[109] H. Wang, D. He, X. Wang, C. Xu, W. Qiu, Y. Yao, and Q. Wang, "An electricity cross-chain platform based on sidechain relay," *J. Phys., Conf.*, vol. 1631, no. 1, Sep. 2020, Art. no. 012189.

SAMINUR ISLAM received the bachelor's degree from the Bangladesh University of Engineering and Technology (BUET), in 2016, and the master's degree in computer science from West Virginia University, in 2022, under the supervision of Dr. Donald Adjeroh. He is currently pursuing the Ph.D. degree in computer science with North Carolina State University, under the supervision of Dr. Tiffany Barnes to understand students' behavior in different e-Learning platforms and understand their learning patterns. During his master's degree, he worked on predicting adverse drug events based on the drug-drug interaction network. He was a software developer for around four years in Bangladesh after completing his bachelor's degree. His research interests include blockchain, bioinformatics, educational data mining, and human–computer interaction to design human-centered computing systems to improve interactive learning systems.

MOHAMMAD JAMINUR ISLAM received the B.S. degree in computer science from the Bangladesh University of Engineering and Technology, in March 2016, and the master's degree in computer science from Western Michigan University, in May 2022, under the supervision of Dr. Shameek Bhattacharjee. He is currently pursuing the Ph.D. degree with the University of California at Riverside, under the supervision of Dr. Shaolei Ren. He is a Graduate Research Fellow with the University of California at Riverside. He was a Software Engineer at Reve Systems Bangladesh, from 2016 to 2019. His research interests include robust optimization, secure system design, AI, cyber-physical systems, and adversarial ML.

MAHMUD HOSSAIN received the Ph.D. degree from the University of Alabama at Birmingham, USA, in 2018. He is currently working as a Security Researcher at the Department of Private Certificate Authority at Amazon Inc. He is also serving as an Adjust Professor at the Department of Information Sciences and Technology, George Mason University, USA. Prior to joining Amazon, he worked as a Cyber Security Researcher at Visa Inc. from 2018 to 2022, where he developed intrusion detection and network monitoring systems for payment networks. He also served as a Software Development Lead at Samsung Research Institute Bangladesh at the Department of Solution Lab for the period June 2010 to August 2014. His research interests include IoT security, cloud security, digital forensics, blockchain, and applied cryptography.

SHAHID NOOR (Associate Member, IEEE) received the Ph.D. degree specializing in cloud, mobile, crowdsourcing, networking, and cybersecurity. He is an accomplished computer scientist with a strong academic background. He was a graduate assistant and has trained in cybersecurity and Cisco networking (CCNA). He has delivered complex academic projects on the secure IoT, medical device security, and spam e-mail detection clustering with several team members. He has published over 20 research papers in international journals and conferences. He received two Best Paper Awards from IEEE SmartCloud in 2016 and ASE Social Informatics in 2014 during his Ph.D. research, which focused on cloud systems using crowdsourced mobile devices and cybersecurity. Previously, he was a recipient of a scholarship from the Sandia National Laboratory for training in 2012.

KYUNG-SUP KWAK (Life Senior Member, IEEE) received the B.S. degree from Inha University, Inchon, South Korea, in 1977, the M.S. degree from the University of Southern California, in 1981, and the Ph.D. degree from the University of California at San Diego, in 1988. He was with Hughes Network System, San Diego, CA, USA, and the IBM Network Research Center, Research Triangle Park, NC, USA, from 1988 to 1990. Since 1990, he has been with Inha University, South Korea, as the Inha Fellow Professor, where he is currently the Inha Hanlim Professor. He received the Inha University Fellowship and the Korea Electric Association Abroad Scholarship Grants for his studies. His research interests include multiple access communication systems, mobile communication systems, UWB radio systems and ad-hoc networks, and high-performance wireless internet. He is a member of IEICE, KICS, and KIEE.

S. M. RIAZUL ISLAM (Senior Member, IEEE) received the Ph.D. degree in information engineering. He is currently a Senior Lecturer in computer science with the University of Huddersfield, U.K. Before moving to the U.K., he was an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, South Korea, from 2017 to 2022. Previously, he was with Inha University as a Postdoctoral Fellow, the Samsung Research and Development Institute as a Senior Engineer, and the University of Dhaka as an Assistant Professor in EEE. His research interests include applied artificial intelligence (AI), digital health, machine learning, data science, and the IoT and security. He received the Distinguished Research Professor Award 2020 from Sejong University.