SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I6P107

Volume 10 Issue 6, 69-91, June 2023
© 2023 Seventh Sense Research Group®

Review Article

A Study on Blockchain Technologies for Security and Privacy Applications in a Network

T. Rajendran[1], S. V. Shri Bharathi[2], S. Sridhar[3], T. Anitha[4]

[1, 3]Center for AR/VR, Hologram and Metaverse, Rajalakshmi Institute of Technology (Autonomous), Chennai, Tamilnadu, India.
[2]Department of Data Science and Business Systems, School of Computing , SRM Institute of Science and Technology, Kattankulathur campus, Chennai, Tamilnadu, India.
[4]Department of Information Technology, SNS College of Engineering (Autonomous), Coimbatore, Tamilnadu, India.

[1]Corresponding Author: rajendrant@ritchennai.edu.in

Received: 30 March 2023 Revised: 26 May 2023 Accepted: 14 June 2023 Published: 30 June 2023

Abstract *- Integrating the Internet into many applications has made securing users' data and maintaining their privacy a significant concern. In recent years, blockchains (BC) have garnered much attention due to their distinctive properties, which include decentralization, immutability, anonymity, security, and auditability. BC technology was utilized in various non-financial applications, like the Internet of Things (IoT), wireless sensor networks (WSN), and cloud computing. The objective of this study is to conduct an analysis of previously published research and provide a summary of the efforts put into researching BC applications for network security. In this study, many networking technologies, including IoT, Industrial IoT, Cloud, WSN, VANET, and MANET, were used in conjunction with BC technology to investigate applications for network security. This study presents an analysis of network security, along with its limitations and contributions, with an overview of the BC evolution, BC architecture, its working principle, and its application, as well as the advantages and disadvantages associated with BC. In this study, recently published articles on BC-based solutions for network security and privacy preservation that were published between 2018 and 2022 are analyzed. The surveyed articles are categorized according to the network application, methodology, and contribution. In conclusion, an analysis of the implementation of BC technology across various networks and their issues and challenges are presented.*

Keywords *- Blockchain, IoT, Network applications, Network protection, Privacy, Security.*

1. Introduction

The term "blockchain" refers to a tamper-resistant, immutable, auditable, permanent, timestamp blocks ledger utilized to share and store information in a peer-to-peer (P2P) way. The information kept in the BC could be anything from the payment history to a contract or private information about an individual. The issue of double spending in cryptocurrency led to the creation of BC technology, which was initially developed as a solution. Intriguingly, BC is utilized in industries apart from cryptocurrency due to its unique and alluring properties like security, integrity, transactional privacy, system transparency, data immutability, authorization, censorship resistance, fault tolerances and auditability. A few examples include mobile crowd sensing, identity management, intelligent transportation, industry 4.0, healthcare, management of supply chains, smart grids, agriculture, and mission-critical system security. BC technology has attracted much focus in the last decade due to its anonymity, auditability, and security [1].

In 2008, Satoshi Nakamoto published an article called "Bitcoin: A peer-to-peer electronic cash system," he presented the idea of BC as a new data structure to store financial transactions and the related protocol for assuring BC's validity in the networks. This article also introduced the concept of a distributed ledger, also known as a blockchain [2]. People frequently get blockchain and Bitcoin confused with one another. On the other hand, Bitcoin cryptocurrency utilizes the BC scheme, enabling it to engage in available and worldwide trading without the intervention of a single central authority. In simple terms, Bitcoin is just a financial application that uses BC technology.

The evolution of a BC can be broken down into four stages, which are depicted in figure 1 as follows: blockchain 1.0 to 4.0 [3].

- Blockchain 1.0: The first commercial blockchain application was a digital currency like Bitcoin. This version was released in 2010.

- Blockchain 2.0 refers to applications used in the financial and economic sectors, like Ethereum.
- Blockchain 3.0 is a term that refers to applications associated with the digital community, like healthcare, education, and government, where there is no involvement of monetary value.
- Blockchain 4.0: Solutions based on Blockchain 4.0 will give enterprises access to more secure, self-recording applications based on distributed, trust-less, and encrypted ledgers.

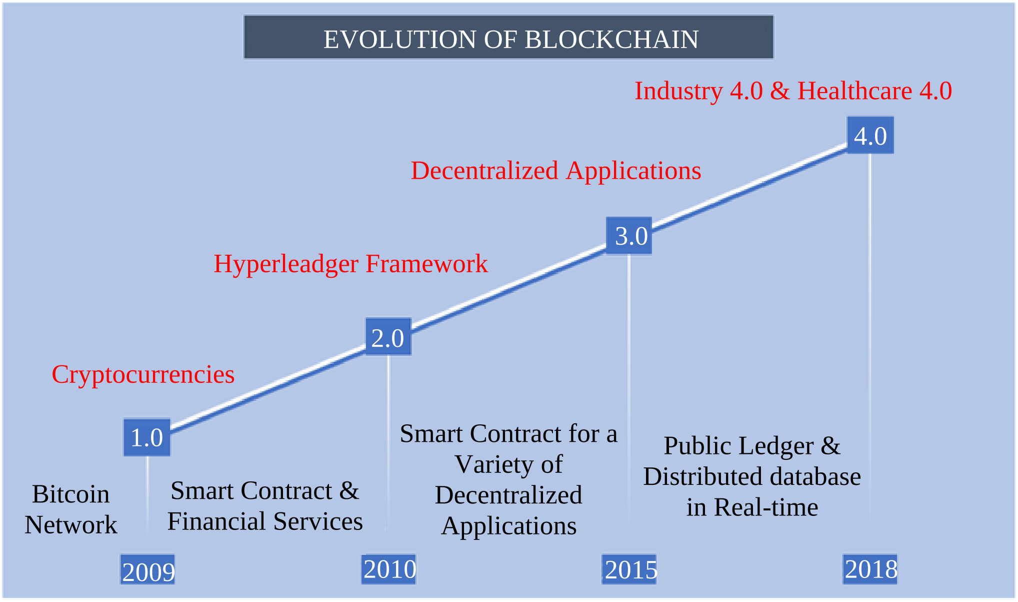
EVOLUTION OF BLOCKCHAIN
Industry 4.0 & Healthcare 4.0
Decentralized Applications
Hyperleadger Framework
Cryptocurrencies
1.0
2.0
3.0
4.0
Bitcoin Network
Smart Contract & Financial Services
Smart Contract for a Variety of Decentralized Applications
Public Ledger & Distributed database in Real-time
2009
2010
2015
2018

Fig. 1 Blockchain evolution

These stages of BC can be thought of in terms of the value factor and maturity of the technology. The primary focus of the applications for BC version 1.0 is on transactions, including digital payment systems, currency transfers and remittances. The first implementation of BC technology was Bitcoin. One example of BC 2.0 is a smart contract, which adds value and helps protect users' privacy. Application developers can carry out transactions using a platform known as a decentralized application (dApp), an open-source software platform that uses BC 3.0. Emerging technologies include BC 4.0, which utilizes a decentralized AI system resulting from automatic decisions making [4].

The BC technology links many data blocks in a decentralized, traceable, and unchangeable order. Initially, it was developed for monitoring transactions, including decentralized digital currency. Each node in the P2P network can receive updated information regarding the different transactions validated in a decentralized and distributed database. When a new transaction occurs, a new block contains recently acquired data and a distinct hash value derived through complex calculations. The blocks are connected highly securely [5]. These days, protecting one's privacy is a crucial concern involved in any transaction. Implementing BC technology can bring about a considerable variation in how authentication and privacy are handled. Integrating this technology can resolve security, risk management, and resource allocation issues. Because the information included in a BC cannot be changed in any way, there was no requirement for the centralized database or the participation of the service provided by third-party. Due to this, the overhead expenses associated with managing intermediary services provided by various businesses and organizations are eliminated [6]. BC Key Features:

- Cryptographic key pair.
- Decentralized consensus mechanism.
- Distributed shared ledger.
- Access and identity management.
- Smart contracts.
- Immutable records.
- Improved security.
- Transparency and traceability in transactions.
- P2P network.
- No central authority or requirement for the involvement of a trusted third party.

Recent studies have shown that various DL methods, widely DNNs (deep neural network), Deep Convolutional NN (DCNN), GoogleNet, DBN (deep belief network), VGGNet, RNNs (Recurrent NN) etc., among them CNNs are frequently used in areas such as computer-based applications, recognizing audio, video and speech, natural language processing for text retrieval (NLP), game development, filtering of social networks, developing translation machines, designing methods for drug discovery, bioinformatics, analyzing medical images, and histopathological diagnosis

[7]. These novel technologies can increase cancer detection diagnostic accuracy and efficiency [8]. In addition, DL-based CAD has been proven accurate in detecting breast cancer early [9]. This study aims to explore the literature related to DL architectures used for detecting breast cancer by utilizing models for BC diagnosis with performance metrics. The survey is ordered as follows: In Section 2, there is a review of breast cancer diagnosis methods employing DL, which includes datasets details for several imaging modalities. Section 3 gives performance metrics for research methodology result analysis. Section 4 finishes the article by presenting problems and potential research directions.

2. Overview of BC Architecture

Each block consists of two components, namely a header and a body. The header includes a hash value and the hash references pointing to the block's hash presented before it. Because the hash references every block point to the blocks presented before it, establishing the chain that connects the blocks. Every block transaction was entered into the ledger accessible to each linked network node and shared among them. When a block is added, the nodes only confirm a transaction as having taken place. Every block necessitates separate validation and maintenance through a consensus protocol. This is due to the interconnected nature of multiple nodes or systems forming a chain, and every node stores a duplicate of the primary chain; hackers cannot quickly access the information. If attackers wish to breach a block, they must first breach the hash references pointing to the hash presented before it. At this point, breaking the chain is impossible because blockchain technology has secure processes. Participants control the blockchain using consensus protocols like Proof-of-Work (PoW), Proof-of-Elapsed Time (PoET), and Proof-of-Stake (PoS) [10].

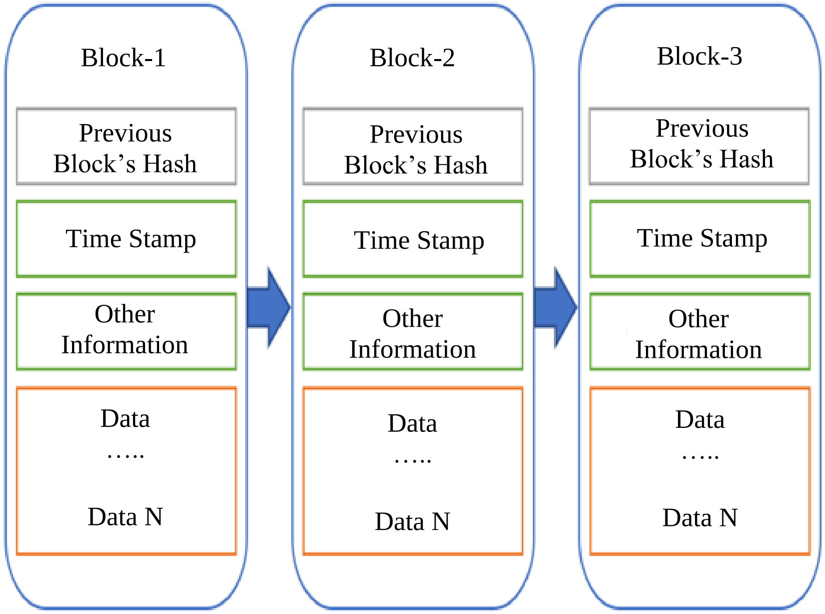

Fig. 2 Blockchain structure

In general, each block contains the primary data, the previous block's hash, the present block's hash, the time stamp, and other metadata. Figure 2 depicts the organizational framework of the BC.

- Primary data: Depending on the services offered by this blockchain application, this may be a record of transactions or contracts, a record of bank clearance, or recordings of IoT.
- Hash: When the transactions are finished, it is hashed into a code disseminated to all the nodes. The blockchains utilized the Merkle tree algorithm to generate the final hash values, which are also Merkle tree roots. This was done since each node's block might comprise thousands of transaction records. The traditional hash values would be included in the block header. Utilizing the Merkle tree function could significantly reduce the resources required for computing and data communications.
- Timestamp: The point in time when the block was initially created.
- Additional Information: For example, consider the block's signature, the Nonce values, or any other information that the user specifies [11].

As can be seen in Figure 3, a typical BC system is split into a total of six primary layers. The following is a detailed discussion of the descriptions and the roles of these layers, which include the data layer, the network layer, the consensus layer, the incentive layer, the contract layer, and the application layer [12]. The data layer was primarily made of transactions and blocks, which are responsible for storing the data generated by the various applications. Every block forms part of an ordered list of blocks by linking to the one present previously and containing a certain number of transactions each. The metadata for the block is specified in the block header, which includes the block versions, the hash of the prior and present blocks, the time stamp, the Merkle root, and additional data. The timestamp contains information about the time the block was produced. The primary data in the block contains a record of every transaction that has ever been carried out. The data type is determined by the blockchain service [13]. The produced data from the data layer is sent to the network layer, where it is broadcasted, forwarded, verified, and audited. The network layer offers the specialized networking method employed in the blockchain. Generally, the network is modelled after a peer-to-peer network, in which the nodes circulate the transaction and block in a decentralized manner. In decentralized systems, reaching a consensus on some information among parties that cannot be trusted requires using a particular consensus algorithm. This layer decides which algorithm to use. Currently, several consensus protocols are being implemented in BC systems. These consensus protocols can be classified as follows: PoW, PoS, PoET, etc. Consensus protocols are chosen in a manner that is distinct for each blockchain.

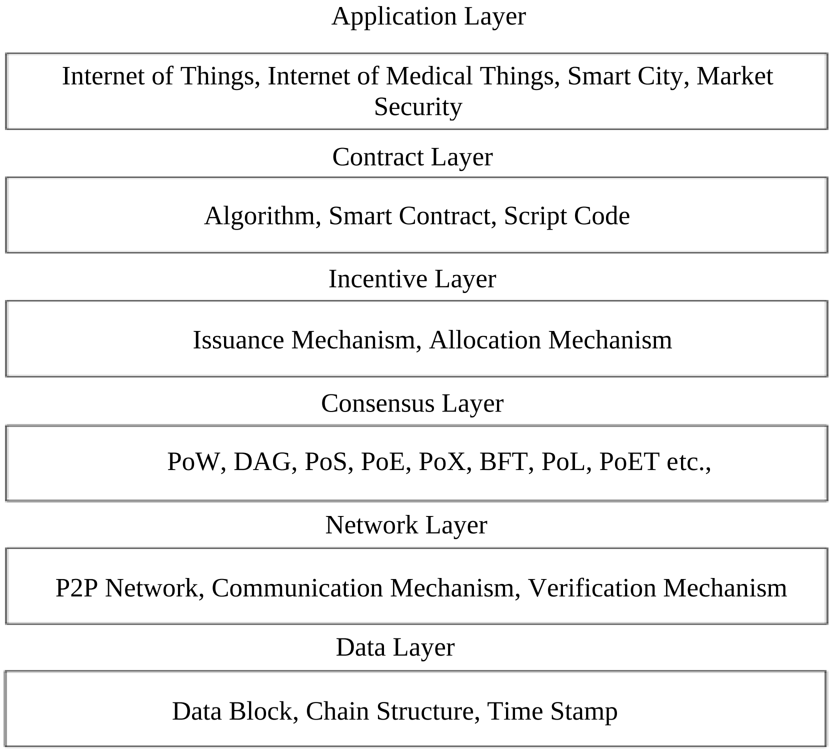
Application Layer
Internet of Things, Internet of Medical Things, Smart City, Market Security
Contract Layer
Algorithm, Smart Contract, Script Code
Incentive Layer
Issuance Mechanism, Allocation Mechanism
Consensus Layer
PoW, DAG, PoS, PoE, PoX, BFT, PoL, PoET etc.,
Network Layer
P2P Network, Communication Mechanism, Verification Mechanism
Data Layer
Data Block, Chain Structure, Time Stamp

Fig. 3 Blockchain architecture

The incentive layer provides nodes with a financial incentive to verify data in blockchain systems, encouraging the nodes to donate their efforts to the system. It is essential to the operation of the decentralized blockchain system, which has no centralized authority, and plays a crucial role in doing so. The contract layer in blockchain systems is what permits programmability in those systems. Smart contracts, different script codes, and other program codes could be applied to enable more complicated programmable transactions. Embedded on the blockchain are vital scripts known as smart contracts; each has its unique address. The providers and operators can adequately establish the criteria and create the rules of business, with the potential addition of penalty mechanisms, with the assistance of smart contracts. The application layer comprises many applications, like the IoT, smart cities, edge computing, security systems, digital identities, etc. These apps could potentially bring about a revolution in these areas and provide administration and optimization that is effective, secure, and decentralized [14].

2.1. Blockchain Uses in Security Applications

- Security of IoT: With the increased use of AI and IoT, there has always been a big issue over protecting data and systems from cybercriminals. To keep the IoT secure, one potential use case for blockchain technology involves encrypting communications between devices, using essential management methods, and authenticating users. This type of usage of blockchain technology could increase security in the IoT system [15].

- Software download authenticity: BC technology could be leveraged to validate software installers and updates, reducing the risk of infected machines being used by malicious software. In this process, hashes are added to the BC, and new software identities can be compared to the hashes to validate the downloads' authenticity.
- Protection during data transmission: Encrypting the data so that unauthorized parties cannot read it while it is in transit is one method of providing this protection [16].
- The decentralized storage of essential data: Since the amount of data created each day is growing exponentially, blockchain-based storage solutions can assist in achieving decentralized storage, thereby safeguarding digital information.
- Protecting Against DDoS Attacks: This attack is among today's most common cyberattacks. Hackers carry out these attacks to cause a surge in Internet traffic and, as a result, disrupt the flow of services. Blockchain, due to its immutability and cryptographic capabilities, has the potential to be an efficient defence mechanism against these threats.
- Security of the DNS: The DNS was comparable to the public directory in associating domain names with their corresponding IP address. Hackers have, with time, attempted to use the DNS and use these links to bring down websites. The DNS can be stored with increased security due to BC technology's immutability and decentralized nature [17, 18].

2.2. Blockchain Application in Network Security

In network security, the CIA triad model is the reference for determining an organization's overall security model. The three components of the triad are confidentiality, integrity, and availability. Blockchain technology enables us to check that all these policies are followed.

- Confidentiality: Maintaining confidentiality requires ensuring that only parties who are legitimately interested and allowed to do so have access to the relevant data. Complete encryption of the data stored on a blockchain guarantees that unofficial parties would not see the information even when it transmits over networks that cannot be trusted. It is important to establish security measures directly at the application level, such as access controls, to prevent attacks within the network. By utilizing vital public infrastructures for authenticating parties and encoding communications between them, blockchain technology has the potential to provide enhanced security measures. On the other hand, using secondary storage for the backup of private keys creates a high risk of loss or theft of private keys. Implementing key management processes like RFC or IETF and cryptographic approaches based on integer factorization problems is recommended to prevent this.
- Integrity: The immutability and traceability built into blockchains are two of the built-in properties that assist organizations in securing the integrity of their data. In a cyber control attack using 51% of the network's resources, consensus model protocols can further assist organizations in implementing methods to secure and manage ledger splitting. The system's initial state is saved in the blockchain at the beginning of each new cycle, creating a history log that can be followed entirely. The implementation of smart contracts allows for the verification and enforcement of norms between parties, which can prohibit blocks of data mining.
- Availability: Recently, there was an expansion in the cyberattacks that are seeking to disrupt the technology services availability, with DDoS being the trendy sort of assault. However, DDoS attacks are expensive in blockchain-based systems because the hacker tries to overwhelm the networks with a large scale of relatively minor transactions. Because there is no single point of failure in a blockchain, the likelihood of IP-based DDoS attacks affecting its general operations is significantly reduced. The data continues to be accessible through various nodes, so complete copies of the ledger are always available. The systems and platforms are resilient due to integrating several nodes and operations in a distributed manner [19].

Table 1. Advantages and disadvantages of blockchain in cybersecurity

Advantages	Disadvantages
User confidentiality	Reliance on private keys
Data transparency and traceability	Adaptability and scalability challenges
Secure data storage and processing	High operating costs
No single-point failures	Lack of governance
Safe data transfers	Blockchain literacy

3. Blockchain Types

Blockchains can be classified as public, private, and consortium blockchains [20].

3.1. Public Blockchain

In this BC, anybody can connect to the network and read the block information whenever they want. It utilizes a technology known as public distributed ledgers, which allows anybody with access to the internet to connect and become a legal miner to mine a block of cryptocurrency. Even in this BC network, a user's address of identity was produced utilizing hash values with pseudo-anonymous. Anybody can know that somebody has that identity, but they do not know who it is. Once the user joins the network, they may verify transactions and block mining to be combined into the networks. The successful miner on a public BC of this kind will typically be rewarded monetarily for their contribution to solving PoW problems [21].

3.2. Private Blockchain

In terms of its operation and algorithms, this blockchain is comparable to a public blockchain in numerous respects. However, it serves a different purpose than the other. A private blockchain is essentially the same as a restricted or permissioned blockchain. Within a closed network that is both dispersed and centralized, it is managed using a set of access control rules as the basis for its operation. This kind of blockchain is typically utilized within an organization, where one or many nodes manage which nodes could carry out transactions, operate as miners, or carry out intelligent contract functionality.

A TTP organization oversees controlling the safety, accessibility, permissions, and authorization of the system. The management of supply chains, electronic voting, the management of digital assets, and the preservation of data are typical applications of this form of blockchain. The Hyperledger Fabric and the Ripple blockchains are notable instances of private blockchains. No one can become a member of a private blockchain network unless they first receive an invitation from the network's administrators. In addition, it has a lower power consumption than the public blockchain, and it may add blocks to the chain faster [22].

3.3. Consortium Blockchain

As the term "blockchain" can sometimes sound incomprehensible, the easiest way to understand this blockchain is by comparing it to public and private blockchains. One way to describe this is partially centralized and partially decentralized. Initially, it was not expanded within one business; it was utilized by multiple organizations simultaneously.

Contrarily, it can only be accessed by node groups that have already been registered, which means that an individual cannot gain a direct link to the networks unless they have first been a registered user. A single organization in the consortium BC cannot engage in any criminal behaviour because it is impossible to carry out any transaction without the approval of the other organizations. The entire notion of consortium blockchain was developed to assist businesses in working together to strengthen their businesses [23].

3.4. Consensus Mechanism

The consensus mechanism is an essential component of BC technology because they protect the data in a BC from being corrupted by double spending attacks while also ensuring that the information in the BC remains intact. The end goal is to achieve consensus among all the participants in a decentralized network, so there is no need for centralized authorities. Participants do not need to trust one another.

The fundamental tenet upon which these algorithms are based is selecting a leader accountable for certifying and disseminating the newer block throughout the networks. All participants in the network are required to take part in the validation process for a block to be integrated into the network since a predetermined count of nodes has validated it. The most critical need is that most nodes are trustworthy [24].

Table 2. Comparison between blockchain types

Feature	Private	Public	Consortium
Efficiency	High	Low	High
Immutability	Partial	Yes	Partial
Centralized	Yes	No	Partial
Read Permission	Restricted or Public	Public	Restricted or Public
Consensus Process	Permissioned	Permissionless	Permissioned
Consensus Determination	One Organization	All Miners	The selected set of Nodes
Participants	Permissioned, Identified and Trusted	Free Anonymous could be malicious	Permissioned, Identified and Trusted

Table 3. Comparison between consensus mechanisms

Consensus Mechanism	Type	Mechanism	Mining	Scalability	Transaction Rate
PoA (Proof of Authority)	Permissioned/ Permissionless	Reputation-based	The identity of the validator executes the role of stake	Higher	Higher
PoS	Permissioned/ Permissionless	Tokens/coins number of locked accounts	No mining Selection of verifier randomly	Good	Higher
PoW	Permissionless	Proof-based	Based on computational power	Not scalable	Low
PoET	Permissioned	Lottery	Election of verifier	Good	Medium
DPoS (Delegated Proof-of-Stake)	Permissionless	Vote based	Democracy	Higher	Higher
PBFT (Practical Byzantine Fault Tolerance) & Variants	Permissioned	Vote based	No PoW-based mining	Medium	Higher
RR (Round Robin)	Permissioned	Vote based	Pseudo-randomly selection Turn base on the interval time	Poor	Higher

4. Review Pattern

4.1. Data Source

To search for relevant research, significant data sources include electronic databases such as IEEE Explorer, Science Direct, Springer, and MDPI websites.

4.2. Keywords Searched

The following search phrases were utilized to compile a list of data sources: Blockchain technology; Blockchain-based security; Blockchain in network applications; and Challenges of Blockchain in security.

4.3. Inclusion and Exclusion Standards

The relevant research was retrieved from various data sources using the inclusion and exclusion criteria described below.

Included: Research related to Blockchain technology; Research not considered Blockchain-based security but solved related problems; Research published in a journal or peer-reviewed conference; and research published between 2018 to 2022.

Excluded: Research not considered Blockchain technology; Research published in non-standard journals; and Research with no validation and internet sources.

5. Implementation of Blockchain Technology in Network Applications

The following section discusses the implementation of BC technology utilized in various network applications in recent years and the domains in which BC technology could be applied, along with image representation.

5.1. Blockchain for IoT

To create a trustworthy IoT network for the future generation of cyber-physical systems (CPS), a technique known as blockchain technology, which makes secure P2P connections among unauthorized parties, has emerged as the preferred option. CPS developed a protection mechanism for its operational and data security based on BC technology [25]. The blockchain was utilized to find a solution to the problem of information security, to safeguard the functional safety of the CPS, and to explore the safety of the Cyber-physical machine tool system.

The utilization of distributed deep learning in conjunction with blockchain technology has the potential to deliver a learning task that is both safe and effective, thereby mitigating some of the issues that are currently associated with edge and cloud intelligence. Combining distributed deep learning and BC led to the development of a decentralized and secure deep learning approach for the IoT network named DeepBlockIoTNet [26].

A functional design for deploying distributed deep learning was presented within blockchain technology. To deliver a decentralized and secure deep learning task, it supports the secure gathering and collection of the local deep learning models from many edge servers using BC transactions. Although, DeepBlockIoTNet faces difficulties regarding cross-communications among IoT's multiple domains. In this context, sensors change, and various sensors gather different knowledge types, resulting in diverse deep learning models for diverse domains.

Intrusion detection and blockchain technology can prevent cyberattacks and protect sensitive data on IoT and cloud computing networks. A deep blockchain architecture was built to provide protection based on distributed intrusion identification and privacy using BC technology with IoT's smart contracts [27]. To protect the confidentiality of the distributed intrusion identification engines, the privacy-focused BC and smart contract technologies have been built with the help of the Ethereum library. This model may be subject to a few drawbacks, like communication difficulty, which reflected the communication costs of propagating the newer blocks to all stakeholders in the system in every iteration. Another potential drawback of this model is that it may be prone to scalability issues. The effectiveness of finding complicated attack events in real-time and aggregating alarms would suffer.

Identifying intrusions in smart homes is still difficult, particularly in prediction and evaluation. Simultaneously, recent advancements in BC technology and ML have shown they have much potential to accomplish such goals. A deep extreme learning machine architecture based on blockchain was developed to facilitate identifying and predicting intrusions in smart homes [28]. The security of the BC-based smart home architecture was ensured by thoroughly assessing the technology's dependability concerning the primary security objectives of maintaining accessibility, integrity, and privacy.

To alleviate some difficulties, it was investigated whether combining blockchain technology and software-defined networking (SDN) would be possible. A blockchain-enabled SDN controller architecture that is safe and energy-efficient has been designed for IoT networks. This architecture uses a cluster scheme and a novel protocol for routing [29]. This model removes proof-of-work using private and public BCs for P2P communications among IoT systems and SDN controllers. It also uses the effective authentication approach with a distributed trust, making the BC appropriate for IoT systems with minimum resources.

A BC-based secure information-sharing platform with access control was employed to address the privacy leakage challenges arising during sharing in the IoT [30]. The Fabric BC technology was developed to address the issue of prohibitively expensive decryption for users in the IoT. A high-complexity partial decryption method is executed by smart contracts in blockchain technology, which helps to reduce the decryption overhead for users. The security criteria of open data limitation and transparent supervision can also be met by realizing the traceability of historical actions due to blockchain's capabilities.

A dedicated blockchain-enabled IoT system can be easier to develop if one understands the interaction between communications and BC and the performance limitations posed by the alternatives. It was decided to create the analytical framework for the BC-enabled IoT [31]. Transactions occur directly between peers instead of going through a central server, and the information regarding every transaction is sent to all other network nodes. These are the fundamental concepts that underpin the blockchain. Each node that is part of the blockchain can access the full database and the right to contribute to the computation and authentication of the new blocks formed by the transaction that was gathered.

Recent advancements in IoT and fifth-generation mobile networks (5G) will substantially increase the amount of big data collected by 5G-enabled industrial automation[32]. However, building an efficient deep learning paradigm for IoT has several obstacles, including a single point of failure, the potential for IoT devices to leak personal information, a shortage of meaningful data for deep learning purposes, and data poisoning attacks. Because of this, a secure distributed ledger based on blockchain was developed. This ledger combines deep learning with blockchain to facilitate secure collaborative deep learning in IoT [33, 34]. Collaborative machine learning was executed at the device level to prevent privacy leaks and collect enough information for deep learning. In contrast, BC was used to assure the integrity and confidentiality of collaborative deep learning in IoT. Both goals were accomplished by ensuring that the data was stored securely.

The high costs associated with computing and storage make it impossible for most IoT devices to participate as blockchain nodes. As a result, a blockchain is typically deployed on a single delegate node, such as an edge device or the cloud. This approach has several potential drawbacks, including a single point of failure when the number of delegate nodes is restricted, the disclosure of private information when a delegate node replicates blockchain data, and susceptibility to a DDoS attack[35]. It is possible to turn IoT devices into specialized blockchain nodes by reducing the amount of redundant blockchain functionality. Establishing a BC-based access control system for IoT devices can be done with the help of hyper ledger fabric [36]. A blockchain-based IoT monitoring framework based on Hyperledger Fabric was developed to identify and isolate a device hacked by malicious firmware attacks or physical intrusions [37].

To protect IoT networks and to make their deployment easier, a multi-layer blockchain security architecture was devised [38]. A distributed ledger like this one improves security and credibility assurances while offering a way to authenticate networks. The open-source Hyperledger Fabric Blockchain technology facilitated the model's development. Using a global blockchain as the method for secure communication between base stations was investigated. A deep learning-based blockchain-driven scheme was developed for a secure smart city. This scheme leveraged blockchain distributed at the fog layers to ensure integrity, data security and decentralization [39]. At the cloud layer, deep learning was applied to increase productivity, data analysis automation, and expand communication bandwidth between innovative manufacturing applications and the industry used in smart cities. To ensure users' privacy and safety in IoT-enabled smart cities, an elegant blockchain architecture that combines traditional blockchain technology with machine learning approaches has been developed [40]. An improved PoW method for ensuring that data has not been tampered with, using blockchain technology and smart contracts as the underlying infrastructure.

5.2. Blockchain for Industrial and Smart Factory

The IIoT aims to advance smart industrialization to benefit businesses and industries. However, the ever-increasing data quantities produced by IIoT environments bring security difficulties, such as system scalability and data integrity. The ongoing growth of the data volumes causes these problems. Because it supports distributed system design principles, blockchain technology is a better method for solving these difficulties. To fully achieve Industry 4.0, which has been hampered by various restrictions on the scalability of networks and the robustness of their security, IIoT is of the utmost importance. Therefore, blockchain technology in its original form, with the more conventional PoW consensus, is not appropriate for addressing these issues. Considering this, an alternative blockchain design that combined a checkpoint mechanism with dynamic PoW (dPoW) consensus was developed [41]. Unlike the traditional PoW-based mechanism, which typically has a constant difficulty level, dPoW performs with changing mining levels of difficulty. This enables the system to scale effectively with an expansion in the IIoT communication traffic environment and the devices connected with those environments.

The IIoT has enabled a smart factory to enter a phase of rapid expansion. Though, as the total network size and the number of nodes increase, the conventional architecture of IIoT cannot effectively support such an enormous system any more. As a result, Blockchain technology can be utilized to establish dispersed networks, which can help reshape the conventional architecture of the IIoT. A new architecture for the IIoT based on blockchain was developed to assist in constructing an IIoT system that is more reliable and secure [42]. Blockchain technology and the Bitcoin design were merged to create an IIoT architecture for the smart factory that was privatized, lightweight, easily expandable, and decentralized. The privacy and security model was presented to assist in the analysis of the crucial components of the architecture.

Asymmetric encryption, safe listing and other approaches are implemented to improve the privacy and security of the IIoT architectures. As a result, the design modified the automatic production platform; furthermore, the platform will serve as an example while discussing the defensive measures. Figure 4 depicts the architecture of a smart factory that Blockchain-based IIoT powers. The layers like sensor, storage, management hub, application and firmware layer comprise the five layers inside this design.

The most recent data transmission solutions using blockchain in IIoT have a low level of security, high administrative costs for the trading centre, and a significant challenge in terms of oversight. To solve this issue, a data transmission approach for industrial IoT based on a secure fabric BC was utilized [43]. This approach utilized a mechanism for dynamic secret sharing that depended on BC technology. A dependable trading centre was created with the power blockchain sharing model, which also allows for sharing power trading books. The consensus mechanism dynamic link storage and power data were developed to make it possible to match the power data securely. Because of its reliable and trusted security approach, blockchain could help protect data used in IIoT and maintain users' privacy. The overall scalability and throughput of blockchain networks can be helped to be improved using sharding technology.

However, sharding is still challenging to implement due to the uneven distribution of malicious nodes. A many-objective optimization approach based on penalty and dynamic reward mechanism was used to optimize the shard validation model to enhance the BC networks' performances and lower the likelihood of malignant node aggregations [44]. To assist manufacturing organizations (for example, automotive) in gaining in-depth knowledge of the various stages of production, IIoT devices are installed in factories. This helps these companies improve production efficiency and achieve cost reductions. It might be challenging to create robust security solutions for embedded devices because of the limited resources and functionalities they offer. A software condition monitoring framework dependent on BC was developed to monitor the IIoT device's software condition to identify and respond to recognized dangerous actions [45]. The blockchain is utilized as the distributed ledger to keep snapshots of the software's current state so that the information's integrity may always be maintained.

To deliver a trustworthy software-defined industrial network, a blockchain architecture powered by deep learning was developed [46]. In this context, a blockchain-based system was devised to register, validate and verify each switch in the BC utilizing a voting-based consensus scheme. Mitigating and identifying potential threats in real time inside the IIoT network can be accomplished through machine learning and BC [47, 48]. Similarly, it lessens the amount of work required by the network nodes if no intruders are on the network and no additional encryption procedures are being carried out.

5.3. Blockchain for Healthcare and Medical Data

The presence of diseases, their progression, and the methods used to treat them have all been documented in electronic health records or EHRs. This indicates that it possesses significant potential for medical use. Data sharing and protecting patients' privacy are two of the most important concerns with EHR due to the private and sensitive nature of patients' medical information.

Since blockchain technology possesses the characteristics of decentralization and tamper resistance, it can be a promising solution for the difficulties outlined above. To enhance the electronic health system of the hospital, a plan for the security and sharing of medical information based on the hospital's private blockchain was developed [49].

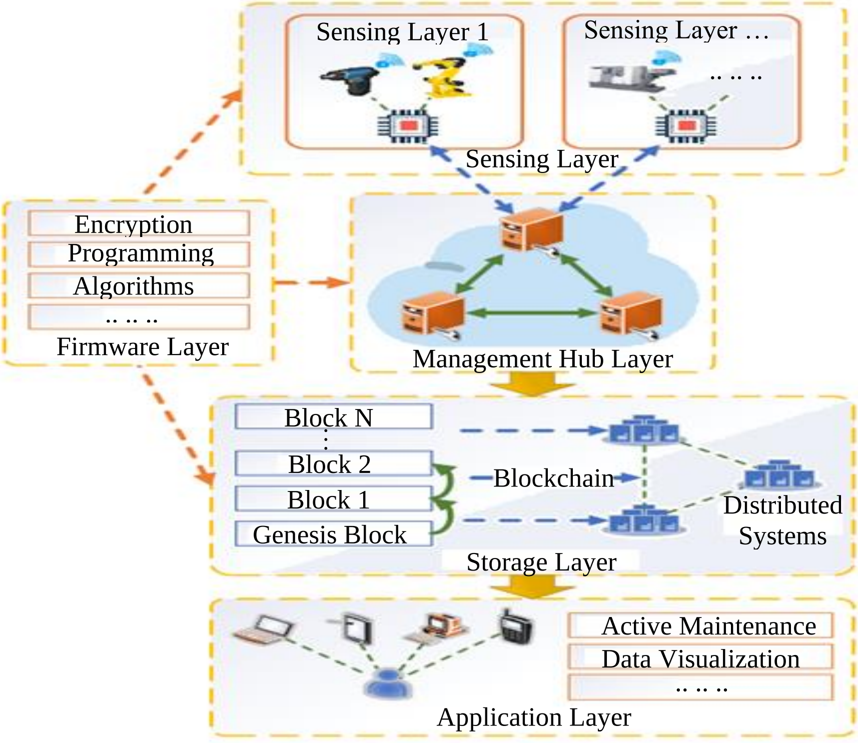

Fig. 4 Architecture of BC-based IIoT for a smart factory [42]

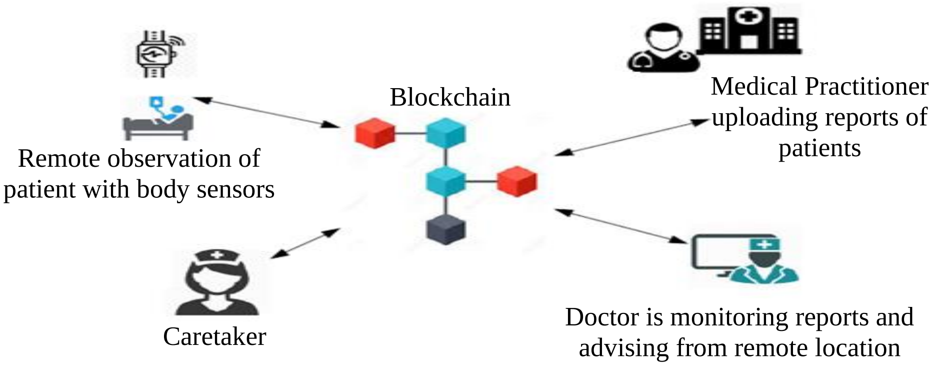
Blockchain
Medical Practitioner uploading reports of patients
Remote observation of patient with body sensors
Caretaker
Doctor is monitoring reports and advising from remote location

Fig. 5 Architecture of blockchain-based IoMT [50]

The model could facilitate data sharing between medical professionals in different hospitals using proxy re-encryption technology. The fact that the stored medical information is kept in a blockchain makes it highly secure and makes it extremely difficult to make any changes to it. By enhancing the conventionally delegated PoS process, it was hypothesized that a better consensus mechanism might be created. It is safe, dependable, and effective all at the same time. In addition, a technique for matching patients' symptoms was developed for those patients who registered at separate hospitals despite having the same disease symptoms. After the patients' mutual validation, a session key could be generated among them. The method can assist individuals in communicating information regarding their ailment. EHR presents significant issues in the areas of data consistency, data privacy, and data confidentiality. Users of healthcare services are increasingly turning to EHR solutions based on blockchain technology because of their inherent trustworthiness, security, and confidentiality. Blockchain-based deep learning is a service with blockchain technology and deep learning techniques to facilitate the exchange of EHR information across various users in the healthcare industry [51].

An EHR sharing protocol that is secure and protects users' privacy has been designed [52]. The data requester searches for key terms from the information providers to identify related health records on the consortium BC. After obtaining the data owner's approval, the requester retrieves the re-encryption cipher text from the server. For the most part, the strategy relied on conditional re-encryption and searchable encryption of proxy to accomplish the goals of information security, the protection of privacy, and access control. PoA was developed to serve as the consensus mechanism for the consortium BC to ensure the framework's availability. Authentication, Authorization, and Audit Logs are three of the most important characteristics of network security. While these features may be easily obtained in legacy systems, obtaining them in IoT is impossible. To accomplish these goals of IoT network security, a model based on fuzzy logic and blockchain was devised [53]. Since Hyperledger is a well-known blockchain technology for providing anonymity and rapid response, it was optimally appropriate for use in healthcare IoT environments. The large volume of information inside the clinical system makes it complex to guarantee data security and perform diagnostic processes. To address these concerns, a hyper ledger BC-based system for secure clinical data management that employs a deep learning-based diagnostic model has been developed [54]. Several separate stages of activities, including diagnostics, encryption, and optimal key generation, as well as hyper ledger blockchain-based secure data management, are included in this approach. This approach ensures the user can regulate data access, allows the medical authorities to write and read the information, and notifies those who need to be notified in an emergency. A system for the efficient exchange of medical files based on BC technology and decentralized attributes-based encoding has been devised [55]. The blockchain did record both the request for authorization and its subsequent approval. The adoption of smart contracts gives all participants in the system access to an interactive platform. Fine-grained access control of medical information was implemented by leveraging decentralized attribute-based encryption. This was done to assure the security and privacy of the files and to prevent a single point of failure.

5.4. Blockchain for Smart Grid and Energy Applications

The smart grid is quickly becoming the industry standard for electricity distribution networks of the future. Despite its numerous successful applications, P2P trading in the local energy market (LEM) was still difficult.

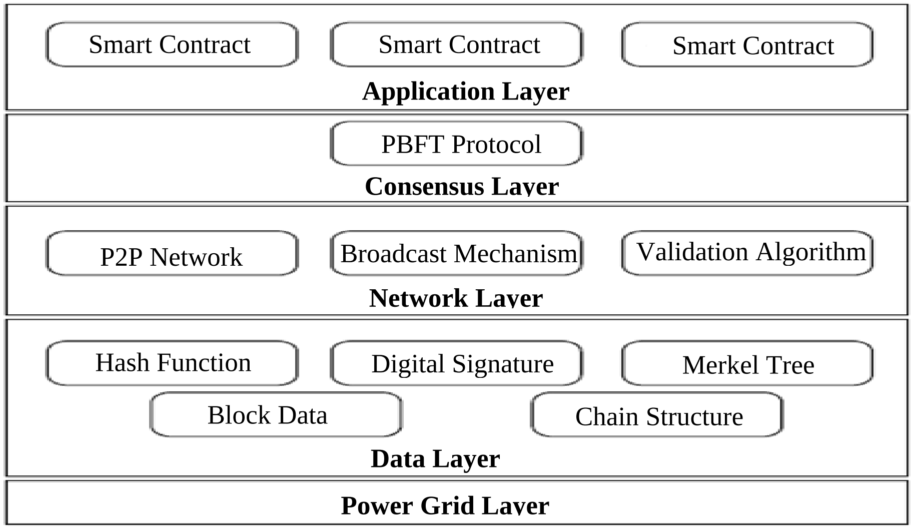

Fig. 6 Architecture of blockchain-based LEM [53]

This is primarily due to the absence of trade methods and security measures. Blockchain technology is a data-driven, secure, and intelligent solution for the smart grid that has been built [56]. The P2P commerce in BLEM was modelled as an online optimization issue in this scenario. This model was constructed using a BLEM architecture with five layers, and it was then deployed on a private Ethereum blockchain. CPSs are essential to the operation of modern power systems because they link physical devices with control technology. When putting smart power networks in place, ensuring that there is as little potential for a data privacy breach as possible is a primary priority. Protecting the datasets of smart power networks and identifying potential threats required utilizing a framework that preserved users' privacy and was built on blockchain technology and deep learning techniques [57].

An enhanced PoW technique based on blockchains was developed to mitigate data poisoning attacks and check data integrity. Simultaneously, the variational autoencoder was utilized to convert data into an encrypted type and secure it from inference attacks. Conventional cloud-based smart grid systems face several significant obstacles: obtaining low latency and offering real-time services. As a result, there has been a growing tendency toward moving towards edge computing. Existing cryptographic methods typically do not enable conditional anonymity or flexible key management, even though many cryptographic protocols were developed to make it easier to maintain secure communications in smart grid systems. A mutual key agreement and authentication protocol based on BC can be used for smart grid systems dependent on edge computing [58].

DeepCoin is an energy framework based on deep learning and blockchain technology designed for Smart Grids [59]. Users can use the extra energy and sell it to other users in the area while maintaining anonymity due to short signatures and hash functions. This concept can reach consensus within the BC-based energy network by utilizing the viable fault tolerance mechanism based on the Byzantine consensus model. DeepRing is a model that uses the learnt parameter of the standard DNN and is protected from adversaries externally with encryption and the process behind blockchains [60].

A BC-based access control protocol in an IoT-based smart grid system has been developed. With this protocol, the data was delivered to the service provider from the corresponding smart meters safely and securely [61]. The participant service provider established the P2P network. Within this network, the peer nodes were accountable for constructing the blocks based on the information accumulated safely from their respective smart meters. These blocks were then added to the blockchain following validation by an algorithm based on voting to reach a consensus on the blocks.

5.5. Blockchain for WSN Applications

BC-based multi-WSN authentication system was created to prevent the single point of failure in standard authentication approaches used in the IoT [62]. A hybrid BC model was developed to accommodate the multi-WSN network great. Under the varying energies and abilities of the various nodes, a local BC and a public BC were implemented among the base station and cluster head node. This allows for the formation of the hybrid blockchain model. A private BC was created among the cluster head of a WSN, and the base station of each WSN was integrated into the public BC. This combines the decentralized nature of BC with the distributed condition of the nodes that make up the IoT. Between all the network nodes, a hybrid blockchain model was developed. The local and public BC are the two components of the hybrid BC paradigm, as seen in Figure 7.

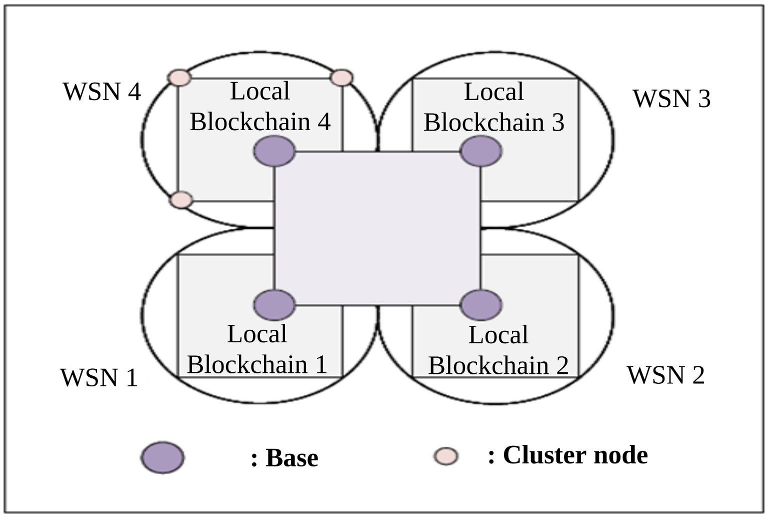

Fig. 7 Hybrid blockchain WSN model

It was decided to utilize an architecture of trust management based on BC to improve the trust connection within beacon nodes and eliminate rogue nodes in WSNs [63]. The evaluation of data-based trust considers both direct and indirect trust within the participant beacon nodes, which are essential components of information trust. This comprehensive trust assessment considers trust based on behaviours and trust based on statistics. To construct a blockchain of the values of trust, the composite value of trust of every beacon node, which considers both its behaviour and data, is broadcast to base stations. After that, the model will eliminate the signal node with the lowest trust rate, guaranteeing the dependability and consistency of the localization process in WSNs. A decentralized model that ensures the independence and safety of the IoT-based WSN. This contributes to preserving data integrity and availability due to the numerous security benefits offered by blockchain technology and the utilization of various cryptographic technologies. This blockchain project was built on a private blockchain mechanism; as a result, it uses the security characteristics of blockchain technology [64].

Identifying malicious nodes in WSNs often takes the form of a single centralized decision. It was impossible to find where the original data came from, the detection process was difficult to duplicate and check, and it was challenging to find a solution to the problems of inaccuracy and false positives. It is accomplished by utilizing BC intelligent contracts and WSN quadrilateral measurements for the localizations of the malicious node detection, and the outcomes of the voting that led to the consensus are recorded in a spread blockchain [65].

The data security of WSNs may be improved with the applications of technologies based on BC. Technology based on blockchain and data transfer creates a WSN framework that is exceptionally safe [66].

The ledger that first used blockchain technology in the financial sector can be considered the sensory database WSN uses. A timestamp that cannot be fabricated is included in every block that uses blockchain technology, and each block also contains a more restricted record database. Processing through cryptography and decoding public keys are two processes that are essential to the linking process in every blockchain[67]. In addition, to send data in the first place, the previous and most recent sequences of a link need to be confirmed before a new blockchain can be created. As a result, a few problems need to be resolved before instantaneous data storage, and update can be achieved.

5.6. Blockchain for MANET

In Mobile Ad Hoc Networks (MANET), the collecting of data about security is a crucial component for both the detection of attacks and the measurement of security. When discovering viable routes for the collection nodes for data collections, a detection node (also known as a collector) should collect security data to determine which routes may be relied upon. To gather information concerning network safety, the B4SDC blockchain technology was utilized [68]. The collector can limit the amount of money it pays out by controlling the scale at which Route REQuests, also called RREQs, are forwarded during route discovery. This allows the collector to simultaneously ensure that each forwarder of control information, also called Route REPlies, or RREPs and RREQs, receives as many rewards.

Simultaneously, B4SDC prevents spoofing attacks by adopting secure digital signatures and collusion attacks with cooperative receipts reporting. Both types of attacks are pretty dangerous. Based on a PoS consensus mechanism, which accumulates stakes via forwarding messages, this model offers rewards for every participant node, prevents forking, maintains high efficiency, and enables genuine decentralization. The application of BC technology in an ad-hoc network presents several challenges, the most significant of which are determining which kinds of nodes must be included in the process of validation and how to appropriately adopts the heavy computational block validation complexity while still preserving the original blockchain features. The distributed ledger technology-based trust management solution uses the lightweight consensus scheme for MANET [69]. This presents a tamper-proof distributed trust framework for use in MANETs’ routing nodes, which is enabled by blockchain technology.

5.7. Blockchain for VANET

One of the most exciting and potentially valuable applications in communications between smart vehicles and smart transportation systems is the vehicular ad-hoc network, often known as VANET. Nevertheless, authentication and protecting users’ privacy are still two of the most critical concerns in VANETs. A decentralized and traceable internet of vehicle framework was used for communications between smart vehicles by applying the authentication of secure access approach among vehicles and roadside units. This framework was built using blockchain technology for communication among smart vehicles [70]. The technology delivers a trustworthy vehicle communication model and protects users’ anonymity by concealing their true identities and preventing the disclosure of sensitive information.

It is integrating BC and the critical derivation approach allowed for the development of a conditional privacy-preserving authentication protocol based on BC. This protocol was developed to make secure communication on VANETs more feasible [71]. This eliminates the requirement placed on participating vehicles to keep a significant quantity of private keys in their possession and enables efficient certificate administration. Using Ethereum, a public blockchain, helps make secure communication in VANETs possible.

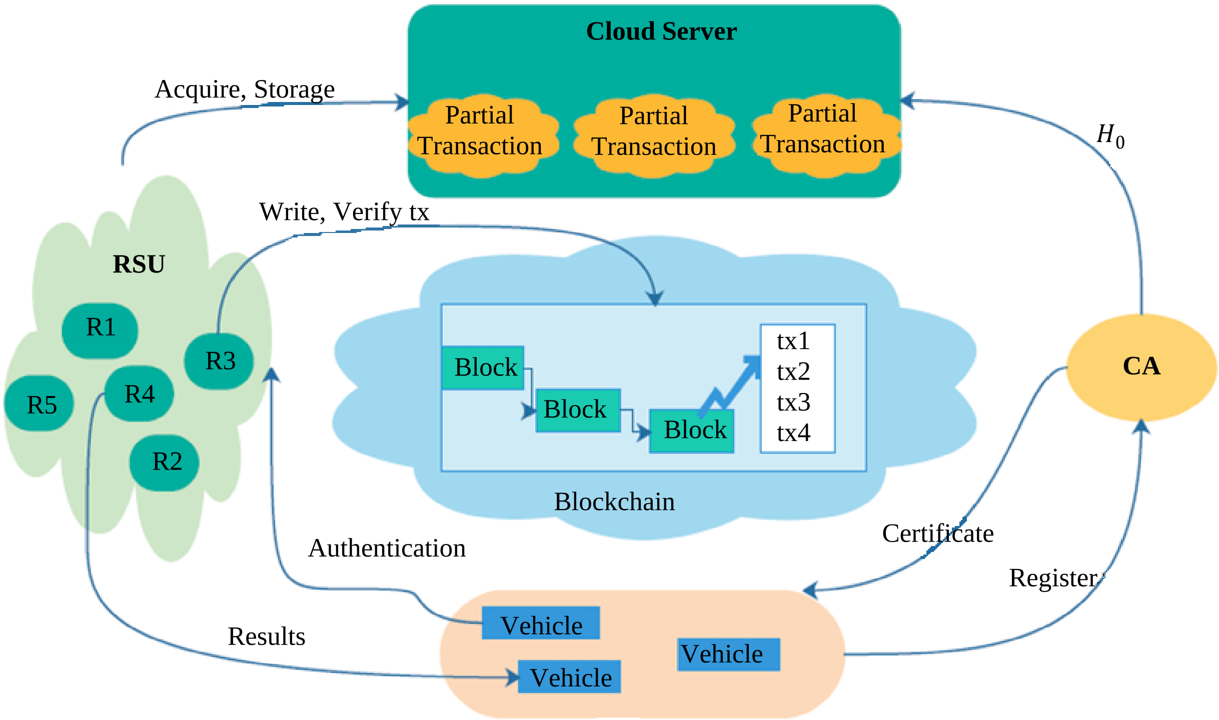

Fig. 8 Architecture of blockchain-based VANET [68]

Management of a trust mechanism for ensuring location safety in VANET based on blockchain technology has been created [72]. Using certificates enables vehicles to make LBS requests without disclosing their private information. Management of trust algorithm was used to limit and generalize the behaviour of vehicles, and the BC was used for implementing the vehicle's data security. The region of anonymous cloaking ensures the privacy and security of vehicles and that the data security of vehicles is implemented. For the IoT environment seen in SDN-enabled 5G-VANETs, a security architecture based on decentralized blockchain technology was developed. A P2P network established by all the active nodes in the automobile system is responsible for maintaining the blockchain [73]. Utilizing the blockchain's immutable property makes verifying the message's origin and accountability possible. Suppose hostile nodes claim fraudulent messages or messages might be tampered with. In that case, the trust management for the vehicular model has been presented with the assistance of a BC-based framework.

The sharing and storing of a data security system based on the consortium BC were built to meet security problems like data leaking and malicious tampering. This was done to address these issues [74]. The new blockchain technology, developed by a consortium, offers a decentralized, safe, and dependable database. Every node on the network maintained this database. When sending and storing data, smart contracts were utilized to constrain the conditions that can trigger specific nodes, and they are also used to distribute data coins to vehicles that contribute data as part of their participation in the process.

5.8. Blockchain for Cloud and Internet Security

Cloud computing allows sharing and supporting pervasive computing of on-demand access. This model offers the processing of new data and services for various industries, significantly reduces the costs of user computing and storage, and improves the system's usability. Security in the cloud has emerged as a primary concern in cloud computing as a direct result of the expansion and intensity of the cloud. Access control is an essential security solution businesses and people should implement to secure sensitive data in the cloud. As a result of the adoption of a cloud's centralized access control, sensitive information stored in the cloud was at a greater risk of being altered or disclosed, whether at the hands of hackers or cloud internal managers. As a result, BC technology may be utilized to address the concerns regarding the cloud's level of data protection.

To ensure the safety of cloud computing environments, AuthPrivacyChain, a BC-based access control system with privacy protection, is utilized [75]. Authprivacychain designed the process of authorization, access control, and revocation of authorization and then used the decentralized and tamper-proof BC to maintain access control rights. Additionally, the BC account address was used to identify each user. Because of blockchain's inherent transparency, exposing users' private information is simple. Using encryption and the storage of access control rights in blockchain, Authprivacychain can adequately secure the privacy of its users. Not only can Authprivacychain guarantee the resources' integrity, confidentiality, authenticity, availability, and accountability, but it can also withstand attacks from the outside and the inside of the organization. Ciphertext-policy attribute-based encoding system based on BC was utilized for safe information sharing in the cloud, which eliminated the need to rely on any third parties that could be trusted [76]. Traditional encryption methods include rotating through several keys to generate several encoded versions of similar data for individuals. It was no longer relevant when discussing the safety of cloud data sharing. The issues can be solved using attribute-based encryption; however, it is necessary to depend on a reliable third party to protect the user's privacy. A ciphertext-policy attribute-based encryption technique based on BC technology can preserve the rights of data owners and keep their data secure. The internet would not function properly without the Domain Name System, also known as DNS. However, it is susceptible to various assaults, including cache poisoning and distributed denial of service attacks. A domain name system built on blockchain technology can provide a safe and effective DNS service [77]. By developing a PoS mechanism and domain index, Blockchain-DNS addresses two deficiencies in the existing blockchain-based DNS system. These deficiencies are a computation-intensive PoW protocol and an inefficient query. To successfully provide a safe protection scheme for satellite communications, the authentication of privacy protection techniques based on BC data storage could be used [78].

Bitmessage was a popular decentralized message system that allowed users to communicate through messages while preventing inadvertent eavesdropping by utilizing the BC flooding propagations method and an asymmetric encoding approach. It can maintain its users' anonymity and privacy. Unfortunately, Bitmessage relies on PoW as the solution to the problem of spam prevention; however, this approach wastes computational energy and renders it ineffective for use in actual practices. To solve this issue, an enhanced version of Bitmessage that includes a new antispam method based on proof-of-space was utilized [79]. To send a message, the user must allocate a particular amount of space on their disk. By removing computationally taxing hash processes, this enhancement saves time and computer resources while reducing prices.

Table 4. Comparison of blockchain implemented in network applications

Author Reference	Year	Methodology	Application	Contribution
Shailendra R & Jong H P	2021	DeepBlockIoTNet	Cybersecurity in CPS	Integration of BC, IoT and deep learning for cybersecurity.
Jaifu W et al.,	2021	BC-based Smart Factory	IIoT	Privacy and security solution based on BC.
Xiaoguang L et al.,	2019	BC-based medical data protection & sharing	Healthcare	Privacy preservation and security of medical data using BC.
Uzair J & Biplab S	2021	BC for Industry 4.0	IIoT	Solving the security issues of IIoT, such as system scalability and data integrity, based on BC.
Zeng Z et al.,	2021	BC-based Local Energy Market	Smart Grid	BC-based approach for security and trading mechanisms.
Osama A et al.,	2021	BC-enabled Collaborative IDS	IoT & Cloud	BC and deep learning-based IDS for delivering additional privacy and security in the cloud for IoT networks.
Zhihua C et al.,	2020	BC-based authentication	WSN	BC-based multi-WSN authentication model for IoT.
Muhammad A K et al.,	2020	BC-based Network Security	Smart Home	A resource-efficient BC-based solution for secure and private IoT smart homes.
Tai H K et al.,	2019	Block-based Trust Management	WSN	Enhancing trust among beacon nodes and eradicating malicious nodes in WSN.
Marwa K et al.,	2020	BC-based Privacy Preserving Model	Smart Power Network	A privacy-preserving system based on BC and deep learning to obtain both security and privacy in the smart power network.
Wei L et al.,	2019	Fabric BC-based Data Transmission	IIoT	A secure fabric BC-based transmission of the data model for IIoT using a BC-based dynamic secret-sharing approach.

Xingjuan C et al.,	2021	BC-based IIoT	IIoT	Privacy preservation and Security in IIoT using BC and improving the overall scalability and throughput of BC networks using a sharding scheme.
Dong Z et al.,	2019	BC-based authentication and privacy preservation	VANET	BC-based decentralized and traceable internet of a Vehicle model for vehicle communications by applying a safe access authentication approach.
Abbas Y et al.,	2020	BC-based IoT Security	IoT	An energy-efficient and secure BC-enabled model of SDN controller for IoT network utilizing the cluster model with a protocol for routing.
Caixia Y et al.,	2020	AuthPrivacyChain	Cloud	BC-based access control system with privacy protection for the cloud.
Gao L et al.,	2022	BC-based Security	MANET	BC system for security-related collection of data in MANET.
Yuting Z et al.,	2021	BC-based Encryption Model	Cloud	BC-based encryption model for cloud data safe sharing without depending on any trusted third parties.
Chao L et al.,	2021	BC-based Privacy-Preserving Authentication	VANET	Combination of BC and key derivation approach to realize reliable certificate management in VANET.
Zecheng L et al.,	2021	BC-based Efficient and Secure DNS	Internet Security	BC-based DNS for providing an efficient and secure DNS service.
Hong X et al.,	2020	BC-based Data Security	IoT	BC-based safe information-sharing platform with access control for the issue of privacy leakages in IoT.
Pronaya B et al.,	2021	BC-based Deep-Learning as-a-Service	Healthcare	Integrating BC and deep-learning models for sharing the EHR records between multiple healthcare users.
Liucheng S et al.,	2021	BC-based Communication Protocol	Data Security	Improved Bitmessage with an antispam mechanism based on proof-of-space communication protocol for data security.
Jing W et al.,	2020	BC-based Authentication with Key Management	Smart Grid	BC-based key agreement protocol and mutual authentication for computing-based smart grid frameworks.
Alma E. G. S et al.,	2020	BC and Symmetric Encryption	WSN	IoT-WSN protection of availability and integrity of data based on the benefits of security given by BC and the utilization of cryptography schemes.
Wei S et al.,	2019	BC Trust Model	WSN	BC trust model for malicious node detection in wireless sensor networks.
May T L et al.,	2020	BC-based Trust Management	MANET	BC-based management of trust with a lightweight consensus scheme for MANET.
Bohan L et al.,	2021	BC-based Trust Management	VANET	BC-based management of trust for privacy preservation of location in VANET.
Shuang S et al.,	2021	BC-Based Access Control System	IoT	A BC-based IoT access control system to establish a lightweight local BC ledger for each IoT domain.
Lixia X et al.,	2019	BC-based Trust and Security Model	IoT-VANET	A decentralized BC-based security framework for vehicular IoT environment in SDN-enabled 5G-VANETs.
Yao S et al.,	2019	BC-IoT	IoT	A framework for the BC-enabled wireless IoT system design through a detailed spatiotemporal model.

Shailendra R et al.,	2019	BlockDeepNet	IoT	BC-based secure deep learning that combines deep learning and BC to support secure collaborative deep learning in IoT.
Sen H et al.,	2020	BC-based Status Monitoring System	IIoT	BC-based software model to monitor the software status of IIoT devices and detect and respond to detected malicious behaviours.
Yong W et al.,	2019	Security and Privacy Preservation through BC	Healthcare	BC-based privacy-preserving and secure cloud-assisted protocol for sharing data.
Xiaohong Z & Xiaofeng C	2019	BC-based data security sharing & storage	VANET	Data storage and security sharing based on the BC for malicious tampering and data leakage in VANET.
Maninderpal S et al.,	2021	BC-based Security	SDN-Industrial Network	A deep learning-based BC model for providing improved decision-making in smart factories and for providing seamless data transfer.
Sushil K S et al.,	2021	DeepBlockScheme	IoT Smart City	BC to limit control of central authority and present a safe IoT smart city application environment.
Mohamed A F et al.,	2020	BC-based Energy Exchange System	Smart Grid	DL and BC-based energy framework for Smart Grids, where users could exploit the excess energy and sell it to neighbouring users while preserving privacy.
Akhil G et al.,	2019	DeepRing	Deep Neural Network	Integrating deep neural network and security of BC to create tamper-proof models.
Basudeb B et al.,	2020	BC-based Access Control Protocol	Smart Grid	IoT-enabled framework by developing a decentralized BC-based protocol for access control without involving a trusted third party.
Henry V et al.,	2021	BC-based Attack Detection	IIoT	Integrating machine learning and BC to provide a strategy for mitigating and identifying intruders in an IIoT model.
Chengjie L et al.,	2021	BC-based Security	Network Security	BC model comprised of ground equipment and satellite that combines communication network privacy protection and authentication.
Sung J H et al.,	2021	BC-based Security	WSN	BC-based technology with data transfer to strengthen the data security of WSN.
Zeeshan Z et al.,	2022	BC-based Security	Healthcare	Integrating BC and fuzzy logic to achieve authentication, authorization, and audit logs in healthcare IoT.
Naresh S & Latha P	2022	BC-enabled Medical Record Management	Healthcare	Hyperledger BC enabled secure medical data management with deep learning for security and diagnostic processes.
Ai G et al.,	2020	BC-based Security	CPS	BC-based information protection and functional safety mechanism for CPS.
Sreenivas S S et al.,	2021	BC-based Monitoring System	IoT	A BC-based IoT monitoring framework to detect and isolate a device that malicious firmware attacks or physical attacks have compromised.
Houshyar H P et al.,	2021	BC-based Security	IoT	Multi-layer BC security model to protect IoT networks while simplifying the implementation.
Prabhat K et al.,	2021	BC-based Privacy Preservation and Security	Smart City	BC framework that integrates BC with machine learning techniques to protect privacy and security in IoT-driven smart cities.
Jiyu T & Li L	2021	BC-based Security	Healthcare	BC and decentralized attribute-based encryption model for practical medical file sharing.

Junyu R et al., [80]	2022	BC-based Security	Healthcare	The BC-based security model for SDN-empowered and fog-assisted healthcare IoT to solve the pressing challenges.
Ibrahim A. A. E. M. & Saad M. D [81]	2021	BC-based Routing & Security	WSN	Combination of deep BC and Markov Decision to improve the routing security and performance of WSN.
Faisal J et al., [82]	2021	BC-based Security	IoT	An IoT network based on BC to establish integrity and security and an improved smart contract-based relation.

6. Discussion

This section summarises all the earlier research regarding applications based on blockchain technology in various network aspects. By its very nature, the blockchain facilitates worldwide accessibility, openness, immutability, and the capacity to store and transfer data securely. In recent years, various applications that use blockchain technology have emerged, expanding beyond the traditional applications of cryptocurrencies. Using a blockchain can facilitate a wide range of activities, including storing sensitive information by participants, creating reliable contracts, and conducting secure transactions, all of which do away with the requirement of using third parties. Blockchain technology is anticipated to be a disruptive mechanism that will play a big role in network management, control, and, most importantly, network security. In this study, the network technologies based on BC technology are studied with various network applications, such as IoT, Cloud, IIoT, WSN, VANET and MANET. Specifically, these technologies are compared with one another. Most of these networking applications have been integrated with IoT to improve communication. In addition, to further improve the models, SDN was added to some of the research projects that utilized blockchain technology.

6.1. Issues and Challenges

The safety and robustness of the blockchain, as well as its smart contracts, database technology, security tokens, and the variations of regulatory environments, will likely significantly impact its future. However, to accomplish the objectives, the development and deployment of the BC must provide an exceptionally high level of dependability, safety, and scalability. These characteristics depend on significant technological developments, including shared ledgers, consensus, provenance, immutability, and smart contracts.

Security of the Network**:** The IoT, IIoT, Cloud, WSN, MANET, and VANET are some networking technologies that could benefit from using blockchain. The IoT is the primary architectural foundation for the IIoT, WSN, MANET, and VANET networks. The IoT is a network that links many components, like digital gadgets and computer equipment so that these components can interact without human involvement. The IoT makes use of blockchain technology for the storage and protection of data. Users remotely store information using any system and from any place. In addition, the BC effectively protects the confidentiality and integrity of the stored information. The IoT is seeing an expansion in the count of digital devices being used, and as a result, blockchain is gradually shortening the business process. Users can store data, extract it, distribute it between multiple systems, and secure it with a private key when using a public blockchain.

BC-based IoT application's privacy and security requirements are authentication, integrity, traceability, nonrepudiation, location privacy, identity privacy, scalability, anonymity, unforgeability, trust management, perfect forward secrecy, access control, data auditability and confidentiality. These requirements were determined through in-depth research and analysis. From the attacks of blockchain technologies' vulnerabilities, 19 attacks are discussed by the reviewed BC-based privacy and security system.

However, several obstacles must be overcome before the blockchain-based SDN can be implemented practically and used to replace the present systems. If there are no robust cryptographic encryption mechanisms in place within the SDN controller and the BC database, the confidentiality of communications may be compromised to a severe degree. There is currently no permanent solution to the problem of cyber security that can be found in blockchain and similar technologies. It just lends support to the efforts that have already been made to secure networks, communications, and data. The storage of immutable records in the blockchain is achieved using encryption and hashing, which are also utilized by many of the already available cybersecurity solutions. Most currently implemented safety precautions depend on a solitary reliable authority to authenticate information or store encoded data. Because of this, the system was open to attacks, and numerous hostile users could concentrate their attempts on a single target to carry out DoS attacks, inject malicious data, and extort information by stealing it or blackmailing its owners.

True BCs are decentralized and do not need the trust or authority of any specific members of the network or group. This gives blockchains a benefit over the present security mechanisms that are in place because blockchains are decentralized. The system does not demand trust because every node or member has a copy of all available information. The only way for additional data to be added to the chain of past information is to achieve consensus among the majority.

Healthcare: Scalability is one of the most crucial difficulties blockchain-based applications face in the healthcare industry. This challenge results in sluggish transaction validation, expensive transaction fees, large storage capacity requirements, and lengthy synchronization periods. As a result, scalability is an important consideration that calls for additional research and guidance. The quantity of data generated and saved in each node is a significant challenge a BC presents. This challenge will become increasingly apparent as the total nodes and transactions in the network increase. As a result, one prospective strategy that might be utilized would be to lessen the energy required while simultaneously enhancing capability. Researchers have considered the potential benefits of cloud computing in medical settings. Some healthcare research has established more efficient and reliable data management systems in distributed cloud architectures. These systems use cloud computing and BC technology to provide a stable and cost-efficient heterogeneous healthcare environment in IoT. Confidentiality is one of the most significant issues arising from implementing BC in healthcare institutions. Despite using the BC, private information gathered about specific patients and linked to the blockchain could lead to the disclosure of patients' identities.

On top of that, there is a possibility that patient privacy could be compromised because of protections being breached as a direct result of harmful attacks that have been carried out on the healthcare blockchain intentionally by criminal organizations or even by government agencies. Numerous investigations have been into cryptocurrencies and severe attacks on blockchain network infrastructure. The personal keys employed in BC for decryption and data encryption also offer the risk of unapproved access to the health data that has been preserved.

Smart City: Heterogeneous sensors were utilized by a variety of smart devices as well as people to collect the necessary data in smart city deployments. These data are then analyzed and used to improve the performance of traffic management, schools, transportation systems, trash management, water supply networks, libraries, power plants and community services. The idea of a “smart city” has recently gained significant traction due to the proliferation of technologies such as the internet, big data, and the IoT. It is necessary to have a mechanism capable of effectively resolving the issues concerning energy, transportation, government, and the environment to boost the development of smart cities. To implement innovative city projects in a way that is both effective and efficient, it is necessary to address some genuine concerns, like insufficient security in IoT, issues in maintaining and upgrading equipment, trust maintaining among internet users, cost optimization of operating data centres, privacy, damage resistance, and security. These are just some of the challenges that must be overcome. Blockchain technology can resolve all these issues; as a result, it is ideally suited for designing solutions for smart cities.

Smart Grid: The innovative grid energy infrastructure development was made possible by utilizing blockchain technology, which allows each customer to obtain emission allowances criteria to maintain the environment's integrity. Tracking and monitoring energy in any form makes it simpler to create and maintain an atmosphere that is healthy and environmentally conscious. Blockchain technology allows it to eliminate the need for intermediaries and energy sellers. As a result, customers will be able to exchange energy with one another and additionally purchase it right away from the smart grids. It was discovered that customers could cut their monthly energy bills by 38%. The blockchain peer-to-peer network built as part of the smart grid infrastructure enables individuals to directly trade energy with one another without involving brokers or paying them for their services. The procedure becomes more convenient and cost-effective for the clients. Speedy deployment of the process and accurate monitoring of energy consumption are both possible with smart meters. Because of this, there is significantly less of a need for meters to be monitored by other parties. Users could access the necessary power and load by utilizing BC-based microgrids for their power needs.

6.2. Limitation of the Work

There are some restrictions on the scope of this proposed study, which investigates the use of BC technology in various network technologies. 1) This study focused only on research articles published in reputable journals between 2018 and 2022, with no conference articles. 2) The performance analysis of the analyzed methods was not investigated in detail. 3) This study focused only on blockchain applications related to network technologies such as IoT, IIoT, Cloud, WSN, MANET, and VANET. In addition, there is a lack of performance study comparison about the representation of the best blockchain scheme examined from the entire analysis.

7. Conclusion

This study analyzed recent research on how blockchain technology might contribute to network technologies such as IoT, WSN, Cloud, MANET, and VANET. This analysis focuses primarily on protecting users' privacy and data, making security one of its primary concerns. The objective of this analysis was to analyze how the integration of blockchain technology into various network technologies can address concerns regarding privacy and security. This research began with a general introduction to blockchain, including its various forms, applications, advantages, and downsides. Following that, a discussion was held regarding analyzing recently published research articles on blockchain-based applications in different network technologies. This study research was sectioned into IoT, IIoT, Healthcare, Smart Grid, WSN, MANET, VANET and Cloud. The applications of blockchain technology were broken down and addressed in these sections, along with their advantages and disadvantages. In conclusion, the blockchain faces several significant issues while offering security and privacy protection in other network technologies. Integrating deep learning and machine learning with the blockchain supports the overall application in terms of security. In the future, a detailed analysis of performance-related surveys can be reviewed based on blockchain in IoT and other network technologies. This will be useful in finding a suitable blockchain mechanism for a suitable application.

References

[1] Elham A. Shammar, Ammar T. Zahary, and Asma A. Al-Shargabi, “A Survey of IoT and Blockchain Integration: Security Perspective,” *IEEE Access*, vol. 9, pp. 156114-156150, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org, pp. 1-9, 2008. [Google Scholar] [Publisher Link]

[3] Umesh Bodkhe et al., “Blockchain for Industry 4.0: A Comprehensive Review,” *IEEE Access*, vol. 8, pp. 79764-79800, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Farhana Akter Sunny et al., “A Systematic Review of Blockchain Applications,” *IEEE Access*, vol. 10, pp. 59155-59177, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Paul J. Taylor et al., “A Systematic Literature Review of Blockchain Cyber Security,” *Digital Communications and Networks*, vol. 6, pp. 147-156, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sabita Khatri et al., “A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges,” *IEEE Access*, vol. 9, pp. 84666-84687, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jiasi Weng et al., “DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438-2455, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Sungyong Cha, Seungsoo Baek, and Seungjoo Kim, “Blockchain-Based Sensitive Data Management by using Key Escrow Encryption System from the Perspective of Supply Chain,” *IEEE Access*, vol. 8, pp. 154269-154280, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yuhui Zhang, and Dejun Yang, “RobustPay+: Robust Payment Routing with Approximation Guarantee in Blockchain-Based Payment Channel Networks,” *IEEE/ACM Transactions on Networking*, vol. 29, no. 4, pp. 1676-1686, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Arzoo Miglani, and Neeraj Kumar, “Blockchain Management and Machine Learning Adaptation for IoT Environment in 5G and Beyond Networks: A Systematic Review,” *Computer Communications*, vol. 178, pp. 37-63, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Mohamed Amine Ferrag, and Lei Shu, “The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial,” *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17236-17260, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Muhammad Shafay et al., “Blockchain for Deep Learning: Review and Open Challenges,” *Cluster Computing*, vol. 26, pp. 197–221, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Nada, H. Ahmed, and B. Chaimae, “Blockchain Security in MANETs,” *International Journal of Computer and Information Engineering*, vol. 13, no. 10, pp. 542-546, 2019. [Google Scholar] [Publisher Link]

[14] Yiming Liu et al., “Blockchain and Machine Learning for Communications and Networking Systems,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392-1431, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Yong Yu et al., “Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things,” *EEE Wireless Communications*, vol. 25, no. 16, pp. 12-18, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] Minhaj Ahmad Khan, and Khaled Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sophocles Theodorou, and Nicolas Sklavos, *Blockchain-Based Security and Privacy in Smart Cities*, Smart Cities Cybersecurity and Privacy, Elsevier, Chapter 3, pp. 21-37, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Lakshmana Kumar Ramasamy et al., “Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey,” *IEEE Access*, vol. 9, pp. 128765-128785, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Bandar Alamri, Katie Crowley, and Ita Richardson, “Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review,” *IEEE Access*, vol. 10, pp. 59612-59629, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdullah Al Mamun, Sami Azam, and Clementine Gritti, “Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction,” *IEEE Access*, vol. 10, pp. 5768-5789, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Li Da Xu, Yang Lu, and Ling Li, “Embedding Blockchain Technology into IoT for Security: A Survey,” *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10452-10473, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Fang Chen et al., “Machine Learning in/for Blockchain: Future and Challenges,” *The Canadian Journal of Statistics*, vol. 49, no. 4, pp. 1364-1382, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Anusha Vangala et al., “Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective,” *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17591-17607, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Yulei Wu et al., “Deep Reinforcement Learning for Blockchain in Industrial IoT: A Survey,” *Computer Networks*, vol. 191, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ai Gu et al., “Integrated Functional Safety and Security Diagnosis Mechanism of CPS Based on Blockchain,” *IEEE Access*, vol. 8, pp. 15241-15255, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] Shailendra Rathore, and Jong Hyuk Park, “A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5522-5532, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Osama Alkadi et al., “A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks,” *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463-9472, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] Muhammad Adnan Khan et al., “A Machine Learning Approach for Blockchain-Based Smart Home Networks Security,” *IEEE Network*, vol. 35, no. 3, pp. 223-229, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Abbas Yazdinejad et al., “An Energy-Efficient SDN Controller Architecture for IoT Networks with Blockchain-Based Security,” *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-638, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] Hong Xu et al., “BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control,” *IEEE Access*, vol. 8, pp. 87552-87561, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Yao Sun et al., “Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791-5802, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[32] D. Shravani, “Research Methodology on Security Engineering for Web Services Security Architectures Extended for Integration of Cloud, Big Data and IOT,” *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 6, pp. 18-24, 2016. [Google Scholar] [Publisher Link]

[33] Shailendra Rathore, Yi Pan, and Jong Hyuk Park, “BlockDeepNet: A Blockchain-Based Secure Deep Learning for IoT Network,” *Sustainability*, vol. 11, no. 14, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] Raveendranadh Bokka, and Tamilselvan Sadasivam, “Securing IoT Networks: RPL Attack Detection with Deep Learning GRU Networks,” *International Journal of Recent Engineering Science*, vol. 10, no. 2, pp. 13-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] I. Lakshmi, “Security Analysis in Internet of Things using Ddos Mechanisms,” *SSRG International Journal of Mobile Computing and Application*, vol. 6, no. 1, pp. 19-24, 2019. [Publisher Link]

[36] Shuang Sun et al., “Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain,” *IEEE Access*, vol. 9, pp. 36868-36878, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[37] Sreenivas Sudarshan Seshadri et al., “IoTCop: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems,” *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3346-3359, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Houshyar Honar Pajooh et al., “Multi-Layer Blockchain-Based Security Architecture for Internet of Things,” *Sensors*, vol. 21, no. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[39] Sushil Kumar Singh et al., “DeepBlockScheme: A Deep Learning-Based Blockchain Driven Scheme for Secure Smart City,” *Human-Centric Computing and Information Sciences*, vol. 11, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[40] Prabhat Kumar et al., “PPSF: A Privacy-Preserving and Secure Framework using Blockchain-Based Machine-Learning for IoT-driven Smart Cities,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326-2341, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[41] Uzair Javaid, and Biplab Sikdar, “A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7679-7687, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[42] Jiafu Wan et al., “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652-3660, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[43] Wei Liang et al., “A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582-3592, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[44] Xingjuan Cai et al., “A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7650-7658, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[45] Sen He et al., “BoSMoS: A Blockchain-Based Status Monitoring System for Defending against Unauthorized Software Updating in Industrial Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 948-959, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[46] Maninderpal Singh et al., “Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 606-616, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[47] Henry Vargas et al., “Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach,” *Electronics*, vol. 10, no. 21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[48] P. Rajadurai, “Machine Learning-Based Secure Cloud-IoT Monitoring System for Wireless Communications,” *DS Journal of Artificial Intelligence and Robotics*, vol. 1, no. 1, pp. 34-40, 2023. [Publisher Link]

[49] Xiaoguang Liu et al., “A Blockchain-Based Medical Data Sharing and Protection Scheme,” *IEEE Access*, vol. 7, pp. 118943-118953, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[50] Amirhossein Adavoudi Jolfaei, Seyed Farhad Aghili, and Dave Singelee, “A Survey on Blockchain-Based IoMT Systems: Towards Scalability,” *IEEE Access*, vol. 9, pp. 148948-148975, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[51] Pronaya Bhattacharya et al., “BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1242-1255, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[52] Yong Wang et al., “Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain,” *IEEE Access*, vol. 7, pp. 136704-136719, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[53] Zeeshan Zulkifl et al., “FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs,” *IEEE Access*, vol. 10, pp. 15644-15656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[54] Naresh Sammeta, and Latha Parthiban, “Hyperledger Blockchain-Enabled Secure Medical Record Management with Deep Learning-Based Diagnosis Model,” *Complex & Intelligent Systems*, vol. 8, pp. 625–640, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[55] Jiyu Tao, and Li Ling, “Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption,” *IEEE Access*, vol. 9, pp. 118771-118781, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[56] Zeng Zeng et al., “A Data-Driven Approach for Blockchain-Based Smart Grid System,” *IEEE Access*, vol. 9, pp. 70061-70070, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[57] Marwa Keshk et al., “A Privacy-Preserving Framework Based Blockchain and Deep Learning for Protecting Smart Power Networks,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5110-5118, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[58] Jing Wang et al., “Blockchain-Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1984-1992, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[59] Mohamed Amine Ferrag, and Leandros Maglaras, “DeepCoin: A Novel Deep Learning and Blockchain-based Energy Exchange Framework for Smart Grids,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285-1297, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[60] Akhil Goel et al., “DeepRing: Protecting Deep Neural Network with Blockchain,” *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Long Beach, CA, USA, pp. 2821-2828, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[61] Basudeb Bera et al., “Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744-5761, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[62] Zhihua Cui et al., “A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN,” *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241-251, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[63] Tai-Hoon Kim et al., “A Novel Trust Evaluation Process for Secure Localization using a Decentralized Blockchain in Wireless Sensor Networks,” *IEEE Access*, vol. 7, pp. 184133-184144, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[64] Alma E. Guerrero-Sanchez et al., “Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network,” *Sensors*, vol. 20, no. 10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[65] Wei She et al., “Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks,” *IEEE Access*, vol. 7, pp. 38947-38956, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[66] Sung-Jung Hsiao, and Wen-Tsai Sung, “Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks,” *IEEE Access*, vol. 9, pp. 72326-72341, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[67] R. Surendiran, and K. Raja, “A Fog Computing Approach for Securing IoT Devices Data using DNA-ECC Cryptography,” *DS Journal of Digital Science and Technology*, vol. 1, no. 1, pp. 10-16, 2022. [Google Scholar] [Publisher Link]

[68] Gao Liu et al., “B4SDC: A Blockchain System for Security Data Collection in MANETs,” *IEEE Transactions on Big Data*, vol. 8, no. 3, pp. 739-752, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[69] May Thura Lwin, Jinhyuk Yim, and Young-Bae Ko, “Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks,” *Sensors*, vol. 20, no. 3, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[70] Dong Zheng et al., “A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs,” *IEEE Access*, vol. 7, pp, 117716-117726, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[71] Chao Lin et al., “BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7408-7420, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[72] Bohan Li et al., “Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3765-3775, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[73] Lixia Xie et al., “Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs,” *IEEE Access*, vol. 7, pp. 56656-56666, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[74] Xiaohong Zhang, and Xiaofeng Chen, “Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network,” *IEEE Access*, vol. 7, pp. 58241-58254, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[75] Caixia Yang et al., “AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud,” *IEEE Access*, vol. 8, pp. 70604-70615, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[76] Yuting Zuo et al., “BCAS: A Blockchain-Based Ciphertext-Policy Attribute-Based Encryption Scheme for Cloud Data Security Sharing,” *International Journal of Distributed Sensor Networks*, vol. 17, no. 3, pp. 1-16, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[77] Zecheng Li et al., “B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1674-1686, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[78] Chengjie Li, Xiaochao Sun, and Zhen Zhang, “Effective Methods and Performance Analysis of a Satellite Network Security Mechanism Based on Blockchain Technology,” *IEEE Access*, vol. 9, pp. 113558-113565, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[79] Liucheng Shi, Zhaozhong Guo, and Maozhi Xu, “Bitmessage Plus: A Blockchain-Based Communication Protocol with High Practicality,” *IEEE Access*, vol. 9, pp. 21618-21626, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[80] Junyu Ren et al., “Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare IoT,” *Tsinghua Science and Technology*, vol. 27, no. 4, pp. 760-776, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[81] Ibrahim A. Abd El-Moghith And, and Saad M. Darwish, “Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach,” *IEEE Access*, vol. 9, pp. 103822-103834, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[82] Faisal Jamil et al., “Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms,” *Sensors*, vol. 21, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher Link]