International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Blockchain for Secure Networking: A Review of Privacy and Security Applications

Harris Frank DJ[1], Thansil Ahamed S[2], Ms. B. Vinitha[3]
[1,2]Department of Data Science, Sri Krishna Adithya Arts and Science College.
[3]Assistant Professor, Department of Data Science, Sri Krishna Adithya Arts and Science College.

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 and Security.

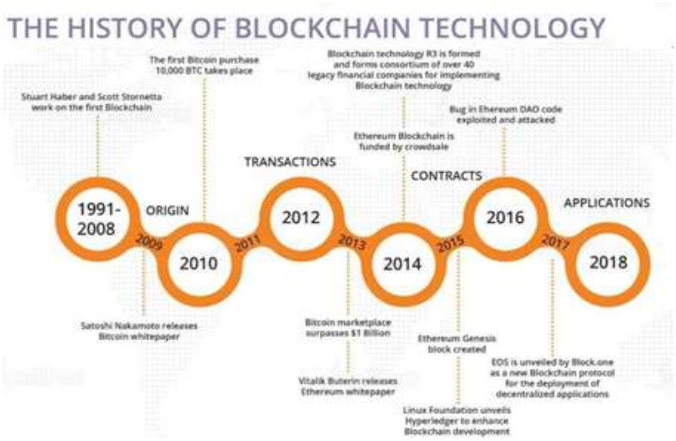
I. INTRODUCTION

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.

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 applicatio 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.

© 2026 IJSRET



These phases of BC can be conceptualized with regards to the value factor and level of maturity of the technology. Transactions, digital payment systems, currency transfers and remittances are the main applications for BC version 1.0. The initial application of BC technology was Bitcoin. Smart contract is one example of BC 2.0, with added value and protection of the users' privacy. Application developers can implement transactions through a platform referred to as a decentralized application (dApp), an open-source software platform based on BC 3.0. Upcoming technologies are BC 4.0, which is based on a decentralized AI system due to automatic decisions making.

The BC technology connects numerous blocks of data in a traceable, unalterable, and decentralized sequence. It was initially created for transaction monitoring, such as decentralized digital currency. Updated information on various transactions validated within a decentralized and distributed database can be received by each node of the P2P network. When there is a new transaction, a new block has recent data acquired and a unique hash value obtained from complicated computations. The blocks are highly securely connected. In today's time, privacy protection is an essential aspect that comes into play during any transaction. The use of BC technology can introduce a significant difference in how authentication and privacy are managed. Incorporating this technology can eliminate security, risk management, and resource allocation concerns. Since information contained in a BC cannot be altered in any manner, there was no need for the centralized database or involvement of the service offered by third-party. Because of this, overhead costs involved in dealing with intermediary services offered by different organizations and businesses are avoided.

BC Key Features:

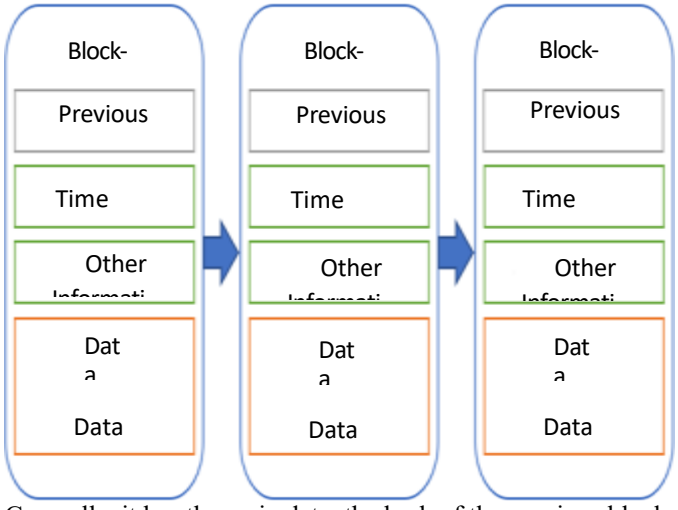
- Cryptographic key pair.
- Decentralized consensus mechanism.
- Distributed shared ledger.
- Access and identity management.
- Smart contracts.
- Immutable records.
- Improved security.
- Transparency and traceability in transactions.
- P2P network.

No central authority or requirement for the involvement of a trusted third party. Recent research has revealed that several DL techniques, most commonly DNNs (deep neural network), Deep Convolutional NN (DCNN), GoogleNet, DBN (deep belief network), VGGNet, RNNs (Recurrent NN) etc., among them CNNs are extensively applied in fields like computer-based applications, speech, audio and video recognition, natural language processing for text search (NLP), game development, social network filtering, constructing translation machines, designing drug discovery methods, bioinformatics, medical image analysis, and histopathological diagnosis. these new technologies have the potential to enhance diagnostic efficiency and accuracy in cancer detection. Furthermore, DL-based CAD has also been shown to be accurate in the early detection of breast cancer. The current work is intended to review the existing literature regarding DL architectures employed for breast cancer detection using models to perform BC diagnosis with performance measurement. The survey is presented in the following order: In Section 2, a discussion of breast cancer diagnosis using DL is given, including datasets information for some imaging modalities. Section 3 provides performance metrics for the analysis of research methodology results. Section 4 concludes the article by providing issues and possible directions for research.

II. OVERVIEW OF BC ARCHITECTURE

Every block has two parts, i.e., a header and a body. The header contains a hash value and the hash references to the block's hash that is shown in front of it. Since the hash references all the blocks point to the blocks shown in front of it, forming the chain that links the blocks. All the block transactions were input into the ledger that is available to every linked network node and distributed among them. When a block is added, the nodes merely verify a transaction as having occurred. Each block requires individual validation and upkeep through a consensus protocol. This is because the interlinked nature of several nodes or systems creating a chain, and each node keeps a copy of the main chain; hackers cannot access the information easily. If attackers want to break into a block, they first have to break into the hash references to the hash presented prior to it. By this time, the chain is impossible to break because blockchain technology has secure processes. Participants have control over the blockchain through consensus protocols such as Proof-of-Work (PoW), Proof-of- Elapsed Time (PoET), and Proof-of-Stake (PoS).

© 2026 IJSRET

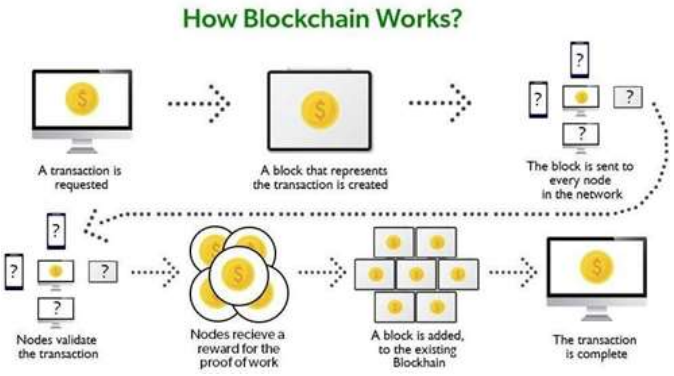


Generally, it has the main data, the hash of the previous block, the current block's hash, the time stamp, and other metadata.

Figure 2 illustrates the organizational structure of the BC.

- Main data: This could be either a record of transactions or contracts, a record of clearance of banks, or IoT recordings based on the services this blockchain application provides.
- Hash: Once the transactions are completed, it is hashed into a code shared with all the nodes. The blockchains used the Merkle tree algorithm to compute the ultimate hash values, which themselves are also Merkle tree roots. This was done because each node's block could have thousands of transaction records. The regular hash values would be incorporated in the block header. Using the Merkle tree functionality would drastically cut down on computing resources and data communications.
- Timestamp: The time when the block was originally created.
- Additional Information: For instance, the signature of the block, the Nonce values, or any other information as defined by the user.

As is evident in Figure 3, a standard BC system is divided into a total of six main layers. The below is a thorough elaboration of the descriptions and the functions of the layers, including the data layer, the network layer, the consensus layer, the incentive layer, the contract layer, and the application layer. The data layer consisted mostly of blocks and transactions, which are tasked with holding the data produced by the different applications. Each block is part of a ordered list of blocks by referencing the one found before it and holding a specified number of transactions per block. The block's metadata is described in the block header, where there are block versions, prior block and current block hashes, the time stamp, the Merkle root, and extra data. The time stamp holds data for the block's production time. The main data in the block holds a list of every transaction ever made. The type of data is set by the blockchain service. The generated data from the data layer is passed to the network layer, where it is broadcasted, forwarded, verified, and audited. The network layer provides the special networking technique utilized in the blockchain. Typically, the network is based on a peer-to-peer network, whereby the nodes exchange the transaction and block in a decentralized way. In decentralized systems, it is necessary to achieve consensus on certain information among parties that cannot be trusted. To do this, a specific consensus algorithm must be used. This layer determines which algorithm to use. There are now a number of consensus protocols used in BC systems. These consensus protocols can be categorized as follows: PoW, PoS, PoET, etc. Consensus protocols are selected in a way that is unique for each blockchain.



The incentive layer is what gives a financial reward to nodes to help them validate information in blockchain networks, motivating nodes to contribute efforts to the network. It's critical to how the decentralized blockchain network operates because it has no central authority controlling it and ensures that it remains operational. Blockchain systems' contract layer is responsible for allowing programming within those networks. Smart contracts, various script codes, and other program codes may be implemented to facilitate more complex programmable transactions. They have embedded within the blockchain some essential scripts named smart contracts; everyone has its own unique address. Providers and operators are able to reasonably set the rules and criteria and develop the rules of business along with the additional possibility of setting penalty mechanisms by using smart contracts. Application layer contains numerous applications such as IoT, smart city, edge computing, security system, digital identities, etc. These applications could make these aspects undergo a revolution and offer management and optimization which is efficient, secure, and decentralized.

Blockchain Applications in Security Applications

Security of IoT: With the heightened use of IoT and AI, there has never been a serious concern regarding shielding data and systems from cyber threats. To make the IoT safe, one potential application of blockchain technology is that it can be used to encrypt data exchanges among devices, utilizing key management practices, and identifying users. This kind of

© 2026 IJSRET

utilization of blockchain technology may enhance the security of the IoT system.

- Software download integrity: BC technology would be used to authenticate software installers and updates, lowering the risk of malware-infected machines being used by malicious software. In this scenario, hashes are included in the BC, and new software identities can be compared with the hashes to ensure that the downloads are authentic.
- Data protection in transit: Encrypting the data in a way that unauthorized individuals can't read it while it's being transferred is one way to offer this protection.
- Decentralized storage of critical data: As the quantity of data being generated every day is increasing exponentially, blockchain-based storage solutions can help in reaching decentralized storage, thus protecting digital information.
- Prevention of DDoS Attacks: This attack is one of the most prevalent cyberattacks today. Hackers conduct these attacks to create an influx of Internet traffic and, consequently, hinder the flow of services. Blockchain, because of its immutability and cryptographic features, can potentially be an effective defense against such attacks.
- DNS Security: DNS was the public directory's equivalent in the matching of the domain names and the respective IP address. In due course of time, hackers tried to avail the use of DNS and access the links through it to deface websites. DNS can be housed with tighter security because the BC technology offers it immutability and de-centralization.

Blockchain Usage in Network Security

In network security, the CIA triad model is the standard to use in determining an organization's overall security model. The three elements of the triad are confidentiality, integrity, and availability. Blockchain technology allows us to verify that all these policies are being followed.

- **Confidentiality:** Confidentiality is maintained by ensuring that only those who are legitimately interested and permitted to do so have access to the respective data. Full encryption of information stored on a blockchain ensures unofficial parties would never view the data even when it is sent through networks that do not have the ability to trust. It becomes necessary to provide security measures right at the level of the application, like access controls, so that attacks through the network do not occur. Using important public infrastructures for authenticating parties and encrypting communications between them, blockchain technology can potentially offer improved security mechanisms. Alternatively, utilizing secondary storage for private key backup poses a high risk of private key loss or theft. Using key management procedures such as RFC or IETF and cryptographic methods based on integer factorization problems is suggested to avoid this.
- **Integrity:** The immutability and traceability inherent in blockchains are two of the inherent features that help organizations secure the integrity of their data. In a cyber control attack employing 51% of the network's resources, consensus model protocols can also help organizations put in place mechanisms to secure and handle ledger splitting. The original state of the system is stored within the blockchain as every new cycle begins, which builds up a history log traceable from end to end. Smart contract implementations enable parties to verify and enforce norms against one another that may prevent blocks of data mining.
- **Availability:** Recently, there was growth in the cyberattacks that are aiming to disarrange the technology services availability, with DDoS being the cool kind of attack. But DDoS attacks cost money in blockchain-based systems because the hacker attempts to overloading the networks using a large scope of comparatively little transactions. Since in a blockchain, there is no point of failure, the threat of IP-based DDoS attacks influencing its overall functioning decreases considerably. Data remains accessible by different nodes, and full copies of the ledger are present always. Systems and platforms become stable because they use multiple nodes and operations distributed-wise.

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

III. TYPES OF BLOCKCHAIN

Blockchains are public, private, and consortium blockchains.

Public Blockchain

Here, anyone can join the network and access the block data at any time. It uses a technology called public distributed ledgers, which enables anyone with an internet connection to join and become a legitimate miner to mine a block of cryptocurrency. Even in this BC network, an address of identity of a user was generated using hash values with pseudo-anonymous. Anyone can be aware that someone has that identity, but they do not know who. Once the user is part of the network, they can authorize transactions and block mining to be bundled into the networks. The successful miner on a public BC of this type will generally receive monetary compensation for his or her part in solving PoW issues.

© 2026 IJSRET

Private Blockchain
In its operation and algorithms, this blockchain is no different than a public blockchain in many aspects. It is just not doing the same thing. A private blockchain is exactly the same as a permissioned or restricted blockchain. In a closed network that is dispersed and centralized, it is controlled by a set of access control rules as the foundation for its functionality. This type of blockchain is generally used within an organization, where one or multiple nodes control which nodes might perform transactions, act as miners, or perform intelligent contract functionality. A TTP organization is responsible for managing controlling the safety, accessibility, permissions, and authorization of the system. Supply chain management, electronic voting, digital asset management, and data preservation are common uses of this type of blockchain. The Hyperledger Fabric and the Ripple blockchains are good examples of private blockchains. No one will be admitted to a private blockchain network without being first invited by the administrators of the network. Besides, it consumes less power compared to the public blockchain, and it can append blocks on the chain more quickly [22].

Consortium Blockchain
Since the word "blockchain" sometimes sounds unfathomable, the simplest method of knowing this blockchain is by comparing it with public and private blockchains. To explain this partly, it is centralized and partly decentralized. At first, it was not extended within a single business; it was used by several organizations at once.

On the contrary, it is only accessed by node groups that have previously been registered, meaning that a person cannot obtain a direct connection to the networks unless they have already been a registered user. One organization in consortium BC cannot commit any criminal activity since it is not possible to conduct any transaction without the permission of other organizations. The whole concept of consortium blockchain was created to help companies collaborate to build their businesses.

Consensus Mechanism
The consensus mechanism is a critical part of BC technology since they safeguard the information in a BC from being tampered with by double spending attacks and also guarantee that the data in the BC is not destroyed. The ultimate aim is to reach consensus among all the participants in a decentralized network, and therefore, there is no requirement for centralized authorities. The participants do not have to trust each other.

The basic principle on which these algorithms are founded is choosing a leader responsible for authenticating and broadcasting the newer block across the networks. All the nodes in the network must participate in the process of validation for a block to be added to the network because a fixed number of nodes have authenticated it. Review Pattern.

Data Source
To find the relevant research, major data sources are electronic databases like IEEE Explorer, Science Direct, Springer, and MDPI websites.

Keywords Searched
These search terms were used to find a list of data sources: Blockchain technology; Blockchain- based security; Blockchain in network applications; and Challenges of Blockchain in security.

Inclusion and Exclusion Standards
The relevant research was fetched from different data sources based on the inclusion and exclusion criteria mentioned below. Included: Research pertaining to Blockchain technology; Research not regarded as Blockchain- based security but addressed related issues; Research that appeared in a journal or peer- reviewed conference; and research that appeared between 2018 to 2022.

Excluded: Research not regarded as Blockchain technology; Research that appeared in non- standard journals; and Research without validation and internet sources.

IV. IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN NETWORK APPLICATIONS

The subsequent part elaborates on the deployment of BC technology used in different network applications over the past few years and the areas in which BC technology can be implemented, as well as image representation.

Blockchain for IoT
In order to develop a reliable IoT network for the next generation of CPS, a method called blockchain technology, enabling secure P2P connections between unapproved parties, has become the top choice. CPS constructed a protection system for its operational and data security relying on BC technology [25]. Blockchain was applied to look for a solution to the information security problem, to protect the functional safety of the CPS, and to research the safety of the Cyber-physical machine tool system.

The use of distributed deep learning together with blockchain technology can potentially provide a learning task that is effective and secure, hence alleviating some of the challenges that are as yet related to edge and cloud intelligence. The merging of distributed deep learning and BC resulted in the creation of a secure and decentralized deep learning method for the IoT network known as Deep Block IoT Net.

© 2026 IJSRET

Blockchain for Industrial and Smart Factory

The IIoT will promote smart industrialization for the advantage of industries and businesses. Yet, the continually rising amounts of data generated by IIoT environments raise security challenges like system scalability and data integrity. The constantly increasing data volumes create these issues. Since it accommodates distributed system design principles, blockchain technology is a more suitable approach to solve these challenges. In order to completely realize

Industry 4.0, which has been hindered by numerous limitations on the scalability of networks and the strength of their security, IIoT is of the greatest significance. Hence, blockchain technology in its natural form, with the more traditional PoW consensus, is not suitable for tackling these challenges. With this in mind, a different blockchain design that incorporated a checkpoint mechanism and dynamic PoW (dPoW) consensus was created [41]. In contrast to the conventional PoW-based mechanism, which normally operates with a fixed level of difficulty, dPoW operates with varying mining levels of difficulty. This allows the system to scale well with an increase in the IIoT communication traffic environment and the devices involved with those environments.

The IIoT has facilitated a smart factory to move into a phase of rapid growth. Although, as the size of the network and the number of nodes grow, the traditional architecture of IIoT cannot efficiently handle such a large system anymore. Therefore, Blockchain technology can be used to form distributed networks, which can assist in restructuring the traditional architecture of the IIoT. A blockchain-based new architecture for the IIoT was established to help build an IIoT system that is more secure and reliable [42]. Blockchain technology and the design of Bitcoin were combined to form an IIoT architecture for the privatized smart factory that is lightweight, easy to expand, and decentralized. The privacy and security model was introduced to help analyze the key elements of the architecture.

Blockchain for Healthcare and Medical Data

Diseases' existence, their evolution, and the treatments adopted to cure them have all been recorded in electronic health records or EHRs. This shows that it has enormous potential in medical application. Two of the most critical issues with EHR are data sharing and maintaining patients' privacy since patients' medical data is private and confidential.

Since blockchain technology has properties of decentralization and tamper resistance, it can be an effective solution for the above issues. For developing the security plan and sharing scheme of medical information based on the hospital's private blockchain to further improve the hospital's electronic health system, a plan was prepared.

Blockchain for Smart Grid and Energy Applications

The smart grid is rapidly becoming the industry norm for future electricity distribution networks. In spite of its many successful uses, P2P trading in the local energy market (LEM) was still challenging. This is largely because there was no trade method and security measure. Blockchain technology is a data-driven, secure, and smart solution for the smart grid that has been constructed. The P2P business in BLEM was represented as an online optimisation problem in this case. The model was built from a BLEM architecture consisting of five layers and subsequently hosted on a private Ethereum blockchain. CPSs are crucial to the functioning of contemporary power systems as they connect physical devices and control technology. When implementing smart power networks, having as minimal a potential for a data privacy violation as possible is of first importance. Safeguarding the datasets of smart power networks and discovering threats involved using a system that maintained users' privacy and was developed using blockchain technology and deep learning methods [57].

Blockchain for WSN Applications

BC-based multi-WSN authentication system was designed to avoid the single point of failure of the traditional authentication methods utilized in the IoT [62]. Hybrid BC model was designed to support the multi-WSN network great. A local BC and a public BC were utilized among the base station and cluster head node under the different energies and capabilities of the different nodes. This permits the establishment of the hybrid model of blockchain. Between the head of a WSN cluster and each WSN base station, a private BC was established. Each base station of a WSN was then added to the public BC. This merges the distributed nature of BC with the condition of nodes that are in the IoT to be distributed. Among all nodes of the networks, a hybrid blockchain model was established.

Blockchain for MANET

In MANET, the gathering of information regarding security is an essential building block for both security measurement and attack detection. When finding possible routes for the collector nodes of the data collections, a detection node or a collector should gather security data in order to ascertain the routes that could be trusted. In gathering data regarding network security, B4SDC blockchain technology was employed [68]. The collector can reduce the money it pays out by regulating the size on which Route REQuests, or RREQs, are relayed in the process of route discovery. The collector is able to achieve this while still ensuring that each router of control data, or Route REPlies, or RREPs and RREQs, is paid as many rewards.

Blockchain for VANET

Perhaps the most thrilling and potentially useful communications application among smart vehicles and intelligent transportation systems is the vehicular ad-hoc network, frequently referred to as VANET. However, two of the

© 2026 IJSRET

most significant issues even today in VANETs are authentication and user privacy protection. A decentralized and traceable vehicle internet framework was utilized for communications between intelligent vehicles through the implementation of the secure access authentication method among roadside units and vehicles. Blockchain technology was employed in developing the framework for communication between smart vehicles. The technology provides a reliable model of vehicle communication and maintains users' anonymity through the masking of their actual identities and blocking the revealing of personal information.

Blockchain for Cloud and Internet Security

Cloud computing enables sharing and supporting pervasive computing of on-demand access. The model provides processing of new data and services for different industries, lowers the costs of user computing and storage considerably, and enhances the usability of the system. Security in the cloud has become a main issue in cloud computing as a direct consequence of the growth and intensity of the cloud. Access control is one of the security solutions that companies and individuals must put in place to protect confidential information stored in the cloud. Due to the implementation of a cloud's centralized access control, confidential information stored on a cloud was more likely to be changed or revealed, either by hackers or internal managers of a cloud. Consequently, BC technology can be used to solve the issues of the degree of protection of data in the cloud.

V. DISCUSSION

This section summarizes all the previous research on applications based on blockchain technology in different network areas. By its nature, the blockchain provides global accessibility, openness, immutability, and the ability to store and transfer data securely. Over the last few years, numerous applications based on blockchain technology have been developed, going beyond the historical use of cryptocurrencies. It is possible to enable diverse types of activities through the use of a blockchain, such as holding sensitive data by participants, making secure contracts, and performing secure transactions, all of which eliminate the need for third parties. Blockchain technology is expected to be a disruptive mechanism that will play a significant role in the management, control, and, most notably, network security. In this research, the network technologies based on BC technology are examined with other network applications, including IoT, Cloud, IIoT, WSN, VANET and MANET. Of particular focus, these technologies are compared with each other. 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.

Issues and Challenges

The security and resilience of the blockchain, along with its smart contracts, database technology, security tokens, and the differences of regulatory environments, will most likely have a big influence on its future. Nonetheless, to achieve the goals, the creation and implementation of the BC must yield an extremely high degree of dependability, security, and scalability. These are contingent on huge technological advancements, such as shared ledgers, consensus, provenance, immutability, and smart contracts.

Security of the Network: IoT, IIoT, Cloud, WSN, MANET, and VANET are some of the networking technologies that may be benefited by applying blockchain. IoT is the major architectural basis for the IIoT, WSN, MANET, and VANET networks. IoT is a network that connects numerous components, such as digital devices and computer hardware so that these components can communicate without any human intervention. The IoT makes use of blockchain technology for the storage and protection of data. Users store information remotely by virtue of any system from anywhere. Moreover, the BC ensures confidentiality and integrity of stored information effectively. The IoT is experiencing growth in the number of digital devices being utilized, and consequently, blockchain is progressively shortening the business process. Users can store data, retrieve it, share it between variousn systems, and lock it with a private key while utilizing a public blockchain.

Work Limitation

There are a few limitations in the scope of this proposed work, which explores the application of BC technology to different network technologies. 1) This work considered only research papers published in peer-reviewed journals from 2018 to 2022 and did not consider conference papers. 2) The performance analysis of the compared methods was not explored in detail. 3) Only blockchain applications that pertain to network technologies like IoT, IIoT, Cloud, WSN, MANET, and VANET were considered in this study. Besides, there is no comparison study of performance regarding the representation of the best blockchain scheme studied from the whole analysis.

VI. CONCLUSION

This research discussed recent studies on how blockchain technology could contribute to network technologies like IoT, WSN, Cloud, MANET, and VANET. This study is mainly concerned with ensuring users' privacy and data, so security is one of the issues this study is mainly concerned about. The aim of this study was to examine how the integration of blockchain technology with different network technologies can solve issues of privacy and security. This research started with a general overview of blockchain, such as its types, applications, benefits, and limitations. Subsequently, a meeting was conducted for discussing the study of recently released research papers on blockchain-based applications in various network

© 2026 IJSRET

technologies. The study research in this work was divided into IoT, IIoT, Healthcare, Smart Grid, WSN, MANET, VANET and Cloud. The uses of blockchain technology were divided and covered in these areas, along with their pros and cons. Finally, blockchain has various severe issues in the context of providing security and privacy protection when it is being utilized in other network technologies. Utilizing deep learning and machine learning with blockchain contributes to the entire application based on security. Performance-related surveys are to be examined in detail with respect to blockchain in IoT as well as in other network technologies in the coming future. This will prove helpful in discovering an appropriate blockchain mechanism for an appropriate 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]

© 2026 IJSRET