Journal of Soft Computing and Computer Applications

Volume 2 | Issue 1 Article 1015

2025

Enhancing Cybersecurity based on Blockchain Technology: A Systematic Review

Sarah Mohammed Shareef
University of Technology- Iraq, Department of Production Engineering and Metallurgy, Department of Computer Science Al-Sina'a St., al-Wehda District, 10066 Baghdad, Iraq, sarah.m.ali@uotechnology.edu.iq

Rehab Flaih Hassan
University of Technology- Iraq, Department of Computer Science Al-Sina'a St., al-Wehda District, 10066 Baghdad, Iraq, rehab.f.hassan@uotechnology.edu.iq

Recommended Citation
Shareef, Sarah Mohammed and Hassan, Rehab Flaih (2025) "Enhancing Cybersecurity based on Blockchain Technology: A Systematic Review," *Journal of Soft Computing and Computer Applications*: Vol. 2: Iss. 1, Article 1015.
DOI: https://doi.org/10.70403/3008-1084.1015

Scan the QR to view
the full-text article on
the journal website

REVIEW

Enhancing Cybersecurity based on Blockchain Technology: A Systematic Review

Sarah Mohammed Shareef [a,*], **Rehab Flaih Hassan** [b]

[a] University of Technology- Iraq, Department of Production Engineering and Metallurgy, Al-Sina'a St., al-Wehda District, 10066 Baghdad, Iraq
[b] University of Technology- Iraq, Department of Computer Science, Al-Sina'a St., al-Wehda District, 10066 Baghdad, Iraq

ABSTRACT

Cybersecurity is a crucial component of the security system that guards against unauthorized access to digital transactions. Blockchain is a decentralized ledger used to securely exchange digital currencies and conduct trades and transactions. Blockchain technology has led to significant changes in electronic transactions. The enormous potential is being exploited in many areas such as financial services, real estate, supply chain, and the Internet of Things. Despite being a security system, it has suffered from security threats to sensitive data. Phishing and 51% attacks can circumvent blockchain security, highlighting the need for thorough user education and awareness. Additionally, blockchains based on digital transactions require more robust and resilient cybersecurity solutions to protect their software and databases. This paper focuses on the latest research on blockchain in cybersecurity, its various applications in digital transactions, and potential challenges including security issues such as various types of cyberattacks and scalability in blockchain technology. This study aims to improve knowledge about the cyberattacks that blockchain security and transaction privacy face. It also strives to summarize the strengths and weaknesses of previous studies in general, and discuss the various challenges and security issues faced, in particular. In each study, new solutions were proposed that could be used for future development and potential future research solutions were identified.

Keywords: Cybersecurity, Blockchain, Smart contract, Decentralization, Consensus mechanisms

1. Introduction

Blockchain technology is an increasing combination of documents, recognized as blocks, that are joined (chained) by encryption. The block includes an encrypted hash of the preceding block, a timestamp, and information about the transaction (which is frequently

Received 26 May 2024; revised 22 July 2024; accepted 27 January 2025.
Available online 14 June 2025

* Corresponding author.
E-mail addresses: sarah.m.ali@uotechnology.edu.iq (S. M. Shareef), rehab.f.hassan@uotechnology.edu.iq (R. F. Hassan).

https://doi.org/10.70403/3008-1084.1015

displayed as a Merkle tree). A blockchain is a distributed ledger that is managed by a network of nodes. It uses a protocol for inter-node interaction and fresh block verification. This method requires creating reliable data in a distributed database to enroll the date of immutable transactions. When sent to the blockchain, the record is stored in a distributed network framework consisting of numerous ledgers [1]. Blockchain enables parties to authenticate information based on predefined rules and roles, guaranteeing data integrity. Hence, it will prevent the system from coercive assaults. Other areas, such as real estate, the Internet of Things (IoT) and healthcare have begun to experiment with blockchain technology. In this scenario, various applications have evaluated the potential of providing secure data simultaneously by delivering more efficient and real-time information about land parcels, such as land tenure, vegetation, and electronic voting. However, thus far, applications have been restricted and have not been completely explored for more complicated purposes [2]. Blockchain is similar to every emerging financial services technology. It must be estimated in terms of cybersecurity danger, both to financial institutions and the larger financial services industry, to make cybersecurity a top priority for policymakers and fiscal institutions. One of blockchain's features is its natural impedance to cyberattacks. While blockchain is not immune to all types of cyber risks, its structure gives it cybersecurity features that traditional ledgers and other legacy technologies lack. Despite the numerous cybersecurity benefits of blockchains, the system, like any other, is susceptible to cybersecurity risks, particularly ones caused by human error [3]. Human mistakes can comprise software coding faults and errors caused by deficiencies in participants' data security policies. Blockchain systems are furthermore vulnerable to identity-based assaults, in which thieves distort the consensus process of a specific blockchain by obtaining dominance of the majority of the blockchain's nodes. To relieve these threats, effective cyber risk management methods are needed [4].

As a result of the huge development that is happening to digital transactions based on blockchain technology, it has been exposed from time to time to fraud or theft of sensitive data. Therefore, previous studies have examined the most important security issues, and proposed solutions were presented in terms of many challenges and cyberattack types of blockchain technology.

By surveying existing research and freely available information on cybersecurity using blockchain technology, this study contributes to providing the best innovative solutions for secure digital transactions and avoiding cyber-attacks. It collects essential cybersecurity information using blockchain technology and standardizes cyber risk data for educational comparability and repeatability.

This study is structured in the following manner: Section 2 offers a theoretical basis and a literature assessment regarding the integration of blockchain technology and cybersecurity for digital transactions. Section 3 explains the principles of cybersecurity. Section 4 presents a summary and future directions for blockchain cybersecurity. Finally, Section 5 provides the conclusion of this study.

2. Theoretical background and literature review

2.1. Blockchain technology

The blockchain is made up of blocks having a secure copy of its initial, a time stamp, and significant information about transactions that are connected together, protecting against unauthorized alterations. In this scenario, resistance to alteration is an intrinsic feature of blockchain architecture that ensures the data's legitimacy and validity [5, 6]. Blockchain, a decentralized ledger, eliminates the need for an intermediary, speeds up transactions, and

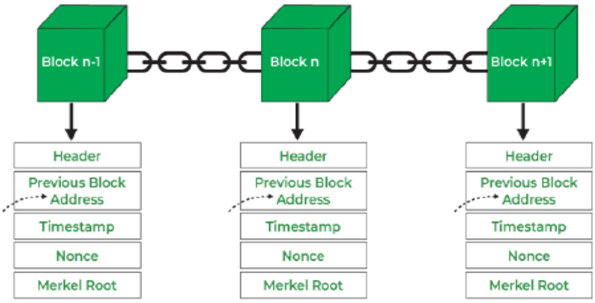

Fig. 1. Blockchain Structure [5].

ensures that each one on the blockchain knows the same version of the original. It also utilizes completely digital technology, removing the inadequacies and inconsistencies of sheet-based transactions [7]. The decentralization part of the blockchain is critical since it does not need an intermediary, and hence, it cancels the risk of one-point failure on the part of criminal alters. Blockchain enrolls personal property sales, such as bitcoin exchanges between two parties. Land transfers are registered by the assessor's residence, tax department, and public records residence after two residents trade property. Blockchain offers speedier transactions, increased data accessibility, and higher accuracy [8], as shown in Fig. 1.

2.2. Types of blockchain technology

Blockchain frameworks have three types: private, public, and hybrid. A public blockchain does not contain any restrictions. The ability of anyone with internet communication can deliver transactions and function as a validator in a consensus mechanism. A public blockchain could consist of thousands of devices. Storing data redundantly across several systems increases its availability and transparency to all stakeholders, making it significantly more difficult to manipulate or attack. Bitcoin and Ethereum are two of the largest and best-known public blockchains. More specifically, to participate in a private blockchain, network administrators must first provide authority. Participant and validator access is limited. Private blockchains are sometimes called Distributed Ledgers Technology (DLT) to recognize them from open blockchains' peer-to-peer, decentralized database frameworks that do not need ad-hoc computation chunks. Popular private blockchains include Hyper Ledger Fabric (HLF) and Ripple. A hybrid blockchain consists of both private (centralized) and public (decentralized) components, as shown in Table 1 [9–11].

2.3. Blockchain with smart contract

Smart contracts, based on blockchain, are systems that function on distributed nodes without a major authority, allowing firms to collaborate while easily executing contract terms. Each smart contract is assigned a unique address. To carry it out, a transaction needs to take place between the sender and the smart contract, where executing the transaction could incur a computational cost. Transaction costs are expressed in terms of gas, where gas consumed refers to the block miner in which the transaction is stored. The blockchain network is classified as a distributed Virtual Machine (VM) since it comprises several nodes. The smart contract's original code has been disclosed, and once deployed, it cannot be amended. As a result, the run code must be error-free while ensuring confidence and achieving deliberate utilization. Solidity, a programming language specifically built for

Table 1. Blockchain types summary.

Key differences	Public blockchain	Private blockchain	Hybrid blockchain
Accessibility	Public blockchains are open to the public, allowing anyone to append the network, legitimize transactions, and share in consensus mechanisms.	Private blockchains are limited, allowing only specific participants or organizations to join the network. Access to the blockchain is controlled, and participants need permission to join and validate transactions.	Hybrid blockchains incorporate elements from both public and private blockchains. They contain a public-facing component that allows for public involvement, as well as limited portions that only particular individuals can access.
Decentralization/ Centralization/ Flexibility	Public blockchains which decentralized, meaning there is no main leverage dominating the network. Consensus is finished through mechanisms similar to Proof of Work (PoW) or Proof of Stake (PoS), where participants collectively check and agree on the blockchain.	Private blockchains are more centralized compared to public blockchains. Usually, an individual entity or a society of trusted entities governs the network and makes decisions regarding consensus and network rules.	Hybrid blockchains provide more flexibility in governance, allowing companies to choose which areas of the blockchain are public and which are private. This enables modification based on individual use cases and requirements.
Transparency/ Privacy/ Scalability	Public blockchains are transparent, as all transactions and data stored on the blockchain are visible to all participants. This transparency ensures accountability and trust in the system.	Private blockchains often provide privacy features, allowing participants to have restricted visibility of transactions and data. This is especially important for enterprise use cases where sensitive information needs to be protected.	Hybrid blockchains could resolve scalability concerns by leveraging private chains for faster and more secure transactions, while occasionally anchoring data to a public chain for consistency and transparency.
Examples	Bitcoin and Ethereum are instances of public blockchains	Hyperledger Fabric and Corda are two examples of such kinds of blockchain.	Ripple and Dragon chain are examples of hybrid blockchains.

smart contracts, is used to build them. Programmers mostly utilize it, and it is comparable to an object-oriented language [12–15].

2.4. Blockchain with consensus techniques

In a distributed situation, consensus approaches are used to verify that all scenario replications adhere to predefined case transitions and norms. Consensus techniques used in blockchain topologies must be robust to node setback, network partitioning, message postponement, ordering, and corruption [16]:

2.4.1. Proof of work

Satoshi Nakamoto [17] picked PoW as a Bitcoin consensus technique after Dwork and Naor [18] recommended it to prevent phishing emails. PoW requires miners to generate a nonce n that meets hardness level L, with the total hashing of nonce n and block elevator b being less than the predetermined hardness level. In mathematics, L can be written as in Eq. (1):

$$\mathrm{H}\left(\mathrm{n}\backslash\backslash\mathrm{H}\left(\mathrm{b}\right)\right) < \mathrm{L} \tag{1}$$

When a nonce is discovered, the miner creates a block and broadcasts it to the network. The block is then validated by multiple nodes in the chain by calculating the hash and comparing the criteria. Altering anything in the block requires doing the work again. Changing history is significantly more difficult since a user must recompute that accepted for all blocks mined next to the current block that was attacked. This demands substantial processing power, recognized as the hash rate [14, 19, 20].

2.4.2. Proof of stake

This technique is the most popular substitutional PoW and has been proposed for Peercoin. A 51% attack occurs when an adversary controls over 50% of the network's computational input and can generate his copy of the blockchain records or stop transactions from earning confirmation consensus. However, proof of stake relies upon the nodes to store their coins to suggest blocks and the safety of the network. The probability of getting chosen to produce the following block is determined by a combination of the tokens held by a node and the currency age. The block proposer must stake their coin period to attach it to the blockchain. If the node behaves maliciously, it loses its stake. Once the checker appeals the award, the coin period is broken, letting others "prevail the lottery" [14, 21].

2.4.3. Practical byzantine fault tolerance

The Practical Byzantine Fault Tolerance (PBFT) refers to a device replication system that can survive (n-1)/3 errors. The grid consists of chief and legitimate peer nodes and block installation takes place in rounds. At the end of each round, the controller authorizes the transactions and places them in a block. The block creation operation consists of three phases: pre-prepares, prepares, and commits. The controller communicates the proposition block to the peers. During the preparation and commit phases, the peers save the block locally before broadcasting it to others. After receiving two-thirds of the effectiveness of peers, miners will implement the block and insert it into their stream chain [22, 23].

2.5. Blockchain cyberattack

In this part, Klynveld Peat Marwick Goerdeler (KPMG) member firms apply their substantial experience to determine eight major risk categories connected with blockchain deployments. These risk groups influence the overall stability of the blockchain system. The following is a classification of blockchain risks [24, 25]:

Double spending: This is a type of fraud in electronic currency systems in which the same unit of currency is used more than once. This constitutes a serious issue in decentralized digital assets like Bitcoin, as the currency's integrity depends on blocking such transactions.

The 51% attack, also known as the "gold finger,": It occurs when an attacker gains control of more than 50% of the network's mining power, allowing them to change transactions, double-spend bitcoin, or shut down the network's operations.

Smart Contract Threats: They represent Intelligent contract weaknesses that can be used to steal funds or alter contract behavior. These assaults are typically based on coding errors or logic flaws.

Routing Attacks: This type changes the direction of network traffic to intercept or redirect transactions.

Phishing Attacks: This is an attack in which attackers deceive victims into surrendering private keys or credentials via bogus websites or emails, enabling them to steal funds.

Real DOS attack against the Ethereum network: Overloading the network or nodes with traffic to disrupt normal operations or services.
Sybil Attack: An attacker creates multiple fake identities (nodes) to gain a disproportionate influence over the network, potentially disrupting consensus mechanisms.
Ransomware: It is an example of harmful software (malware) that encrypts or locks a victim's files, making their data unusable**.** The attacker then requests a ransom, usually in a cryptocurrency, to be exchanged for a decryption key or the ability to recover system access.

2.6. Literature review

As previously stated, the use of blockchain technology is the most widely contested topic between corporate and academic people. Several previous works will be studied and reviewed in terms of the challenges and cyberattacks types [11]. Table 2 contrasts previous studies for blockchain-based cybersecurity. For example:

The authors in [8] presented a blockchain-based secure solution for mobile phone commerce, which is an important tool for promoting social entrepreneurship and sustainable development. It has the ability to contribute to the development of reliable and long-lasting mobile commerce platforms that promote social responsibility, customer confidence, and company ethics. Researchers as well as developers can utilize it to enhance social commerce platforms and hence improve the effectiveness of m-commerce. The authors in [15] presented a comprehensive review of blockchain-based smart contract issues, concentrating on smart contract execution, privacy problems, encoding, and security. Blockchain-enabled smart contracts are exposed to a range of assaults, including the decentralized autonomous group and the ParitySig bug on the platform known as Ethereum. Downloaded numerous publications and found new dangers that fit into one of the categories. The appropriate answers to the new risks are offered, and they can also be applied to current problems. The authors in [16] highlighted current research insights on several blockchain applications in cybersecurity. The researchers prioritized protecting IoT systems, networks, and data. They concluded that blockchain can safeguard data from being viewed or altered by intruders by using encoded blocks that can only be read by designated parties. The authors in [24] highlighted the impact of blockchain security function and privacy challenges to predict the possible damage and the researchers classify several critical cybersecurity threats and vulnerabilities occurrences in blockchain software and describe the ways of risk management based on the Information Security Risk Assessment (ISRA) frameworks. The authors in [25] suggested that the technique of blockchains be used with the data encryption standard algorithm to increase the degree of security of the shared photographs by enhancing the key used in the method of encryption, as well as boosting the amount of authentication between the person who sent them and the recipient. The testing results reveal that the security of the encryption image made using the recommended technique is higher, fulfilling the goal of protecting medical image features, as evidenced by the results in Entropy, Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The authors in [26] provided a detailed overview of blockchain applications in retail cybersecurity, focusing on supply chain authenticity, data protection, and transaction security. They also investigated how blockchain can help with provenance and traceability, as well as fraud prevention and improved vendor management throughout the supply chain. It also looked at how blockchain-powered payment frameworks and fraud detection systems could improve transaction security. Furthermore, the study evaluated blockchain's potential to safeguard data through privacy and permission management, as well as robust and immutable data storage. The authors in [27] presented a scope of cyber defense and examined blockchain study and development trends according to the

Table 2. Comparison of research cybersecurity based on blockchain technology.

Ref.	Research Name	Blockchain Type	Cyber-attack Type	Challenges	Solutions	Research Findings
[8]	Blockchain-based cybersecurity approach for e-commerce mobile applications, social and sustainability companies	A blockchain-based secure mechanism for mobile platform	Platform risk	An absence of trust and security, particularly in sustainable and successful crowdfunding networks	Combining cyber security mechanisms into sustainable mobile commerce channels and assessing their efficacy in promoting mobile commerce sustainability	A blockchain-based security framework for m-commerce can encourage social business and long-term success
[15]	Smart contracts security threats and solutions	Public and private	Smart contract exploits	Transactional privacy	Encryption technique applied to smart contract	Embrace mostly codifying privacy, safety, and efficiency challenges and their corresponding solutions
[16]	Improving cybersecurity through the use of blockchain technology	Blockchain-based cybersecurity	Malicious botnet networks	A serious worry is their vulnerability to hacking	Blockchain can safeguard data from being altered by intruders using encoded blocks	Safeguard IoT data from being viewed or altered by intruders by using encoded blocks that can only be read by the designated parties
[24]	Cybersecurity risks of blockchain technology	Public and private	51% attack real DOS attack against the Ethereum network	Identifying, analyzing, and controlling the relevant risk events	Risk analysis includes: activity, threat analysis	risk measures based on the ISRA
[25]	Cybersecurity for healthcare image protection using circular blockchain systems based on the modified DES Algorithm	Circular blockchain	Hacking by unauthorized persons	Maintain the integrity of the patient's medical information	Blockchain technology was combined with the DES mechanism to improve the security of the sent photos	Higher security, achieving the goal of safeguarding medical imaging information, as demonstrated by the Entropy, MSE, and PSNR statistics
[26]	Blockchain technologies for retail cybersecurity: Improving supply chain protection, secure transactions, and safeguarding information	Blockchain-based payment mechanisms	Phishing attacks	Regulatory and scalability considerations	Blockchain applications in the retail lead to increased efficiency, transparency, and trust across providers and consumers	Blockchain technology presents significant prospects for innovation and development in retail cybersecurity
[27]	Blockchain for cyber defense: Prospects, application development, and challenges	Blockchain-based payment	Double-spending	Cyber threats at the national defense level	Blockchain technology is growing as a security and defense tool	Reduced the gap in blockchain for cyber defense

(Continued)

Table 2. Continued.

Ref.	Research Name	Blockchain Type	Cyber-attack Type	Challenges	Solutions	Research Findings
[28]	Blockchain's potential for digitizing lands and real estate property documents	Blockchain-based real estate	Risk of fraud	Interoperability, data privacy, scalability	Decentralization, immutability, smart contracts	Increased openness, decreased errors and delays, and enhanced overall industry efficiency
[29]	A blockchain solution for protecting real property transactions: A case investigation in Serbia	Permissioned public blockchain	Tamper attack	Speed and expense of real estate transactions	Permissioned public blockchain built on the peak of the Ethereum infrastructure	Represent an illustration of how multiple government registries can be established on top of a blockchain as part of the proposed blockchain-based electronic government in Serbia
[30]	Worm computing is a blockchain-based resource collaboration and cybersecurity system	Blockchain-based worm computing concept	Malicious URLs	Integrating network resources and successfully improving defense capabilities is a pressing topic	Extend the schemes of the worm computing concept based on blockchain technology, and store transaction data and cooperative info by supplying a private chain	The effectiveness of the suggested worm computing system in terms of resource usage and network security
[31]	Comprehensive review of cyber security in blockchain-based IoT	Blockchain-based IoT	Mining attacks	Protecting the privacy of private data collected by IoT devices	The Scrypt cloud mining algorithm is presented as a means of securing the IoT blockchain against crypto-mining-based attacks	Mining attackers can be tracked down in a number of ways, including by exploiting text patterns, blacklists, CPU utilisation, and drive-through mining
[32]	Machine learning and blockchain-based systems can improve cybersecurity in connected vehicles	Blockchain-based CAVs security	Reply, Sybil, malware attacks	Future self-driving vehicles have to be secured from cyberattacks during their routines on the road.	Intrusion detection using machine learning and data mining, as well as other protection mechanisms.	A reliable network for CAVs must be deployed utilizing security mechanisms against various cyber threats

established cyber defense, studies, national programs, and restrictions. Government data, interviews, pertinent news, technical papers and research publications from 2016 to 2021 were also analyzed. As a consequence, this study tried to minimize the gap in blockchain for cyber protection by conducting methodical inquiry and evaluation, and it concluded with recommendations for future studies in the field of distributed ledger, evaluation, and survey. The authors in [28] studied the existing scenario and related problems in recording land and real estate ownership records, particularly in developing countries, and identified the obstacles and prospects for the use of blockchain technology in this industry. They examined whether blockchain technology has the ability to bring about beneficial changes and play a fundamental role in the real estate market. It certainly has the potential to carry out a positive change and play a vital part by increasing transparency, decreasing errors and delays, and enhancing the overall efficiency of the industry. The authors in [29] proposed a system construction for a blockchain-based Laboratory Information System (LIS) that maintains track of transactions in LIS in an immutable and tamper-proof manner, increasing safety and, as a result, transaction speed, effectiveness, and data integrity without significantly impacting current laws and rules. To facilitate and embrace blockchain technology, Serbia is currently developing a legislative framework. Since geography plays a significant role in decision-making at all government stages, a complete and compatible geospatial solution for blockchain must be developed. The authors in [30] introduced the concepts of worm nodes and worm computing, as well as provided a formal explanation. Effective data from the internet is obtained in a timely manner to enable resource sharing and collaborative defensive services. Then, using blockchain technology, the authors develop the algorithms of the worm computing model and store transaction data plus cooperative information via a private chain. The findings suggested that the proposed worm computing model is excellent at improving the utilization of resources and cybersecurity. The authors' intention in [31] was entirely professional and directed towards counter-mining attacks. Scrypt is a cloud mining algorithm designed to discourage selfish mining and effectively encourage more honest mining practices. Mining attackers can be tracked down in a number of ways, including by exploiting text patterns, blacklists, CPU utilization, and drive-through mining. It has been established that mining attacks waged against the blockchain can be tracked and foiled by introducing future blockchain security measures. The authors in [32] focused on crossovers between relationships, control, artificial intelligence, fusion of sensors, and cybersecurity, with a detailed look at a system-integrated method for intelligent cars. It conducted a thorough investigation of communication analytics influencing traffic flow, use cases, protection, and privacy in Connected and Autonomous Vehicles (CAVs) from both traditional and machine learning viewpoints. As a result, it is necessary to safely build a network for CAVs by utilizing defense mechanisms against various cyber threats.

3. Cybersecurity principles

Existing laws, regulations, and industry guidelines provide crucial controls for an effective blockchain cybersecurity program. Many financial authorities have offered specific guidelines for financial institutions' cybersecurity procedures, which include [33–35]:

1. Access controls on customer information systems, such as those that authenticate and restrict access to only authorized users.
2. Encryption of electronic customer information, particularly when it is in the passage or stored on networks or frameworks to which unauthorized persons can get access.
3. Employees having responsibility for or access to client information must follow dual control processes, segregate duties, and undergo employee background checks.
4. Systems and processes for detecting real and tried assaults on or intrusions into client information systems.
5. Response protocols that describe measures to be performed when the financial establishment believes or discovers that unauthorized people have acquired incoming client information systems, including suitable reporting to regulatory enforcement bodies.

3.1. Blockchain for cybersecurity

Blockchains offer unique characteristics for reducing cybersecurity risk in an Information Technology (IT) system. The blockchain architecture enables additional security measures, as illustrated by the examples below [36–38]:

1. A blockchain-distributed architecture strengthens the whole network's robustness against exposure from a single access point.
2. Consensus mechanisms, a crucial component of blockchains, increase the inclusive resilience and integrity of participated ledgers because consensus among network members is required for verifying new blocks of data, and mitigates.
3. Blockchains also give manipulators increased transparency, making it far harder to disrupt blockchains via malware or manipulative acts.
4. Blockchains housed on a cloud program, like Microsoft Azure, have enhanced cybersecurity safeguards caused by the platform's incoming restrictions and other safeguards.

3.2. Blockchain applications in cybersecurity

There are several applications of blockchain in cybersecurity, some of them are as follows [39–41]:

Secure Data Storage: The blockchain technique displays a decentralized and tamper-proof ledger for keeping sensitive data, including digital certificates, cryptographic keys, and identity information. By spreading and protecting information throughout a network of nodes, blockchain increases data security and resilience against illicit access or alteration**.**

Identity Management: Blockchain technology enables decentralized and self-governing authentication systems in which individuals keep their identification data. This reduces the risks related to central identification systems, including single points of failure and information leaks, by allowing users to identify themselves without the need for third-party intermediaries**.**

Secure Authentication: Blockchain-based authentication methods, such as decentralized authentication systems and digital signatures, boost authentication security by reducing the requirement for common passwords and standardized authentication mechanisms.

Secure Communication: The blockchain can establish secure communication channels across parties by encrypting and timestamping messages. This guarantees messages' secrecy, integrity, and non-repudiation making them resistant to eavesdropping, manipulation, and spoofing assaults.

Supply Chain Security: Blockchain makes supply networks transparent and traceable by documenting the origin and movement of commodities across the supply chain network.

Immutable Audit Trails: Blockchain's immutable ledger allows for the production of visible and auditable logs of cybersecurity events, such as security incidents, access control modifications, and data breaches.

3.2.1. Blockchain application in real estate

One area where blockchain has the potential to shine is in land registration systems. Ylii H. [42] suggested the development method and utilized a decentralized database to demonstrate that businesses may sell their properties in a virtual environment, potentially representing a revolutionary solution. Land registration operations will be carried out

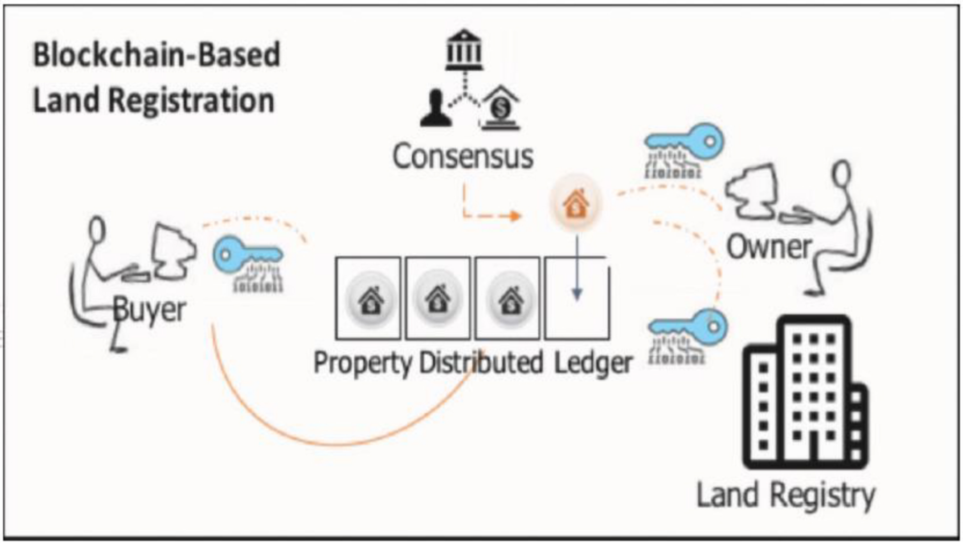

Fig. 2. Basic Work Flow of Blockchain Land Registry Systems [41].

using a blockchain, which will assist to decrease or remove middlemen while also providing a safe and transparent transaction environment. Land registration using blockchain can improve processing efficiency, eliminate fraud in property exchange, boost security, accountability, and transparency, and reduce vulnerability to natural or man-made catastrophes, as shown in Fig. 2.

Some significant examples of governments with pilot initiatives for blockchain-based cadastre and land registration options [43]:

- **Brazil**

The Brazilian real property registry “Cartorio de Registro de Imoveis” has launched a pilot project with blockchain startup “Ubiquity” to record land registrations on the blockchain. Addresses, cadastral zoning, and ownership details are all encoded and linked to a colored coins blockchain. Brazil’s experimental program comprised the settlements of Pelotas and Morro Redondo. The project’s goal was to establish a pilot program for official land registration in the region, lower expenses, and increase the accuracy, security, and transparency of property records. After assessing the data collected through the blockchain application, mistakes in the registration system were decreased, and archiving became significantly easier.

- **Dubai**

The land department in Dubai employs blockchain software to track real estate transactions. The system links the real estate to the Dubai Electricity and Water Authority and contains renter information and immigration status. This blockchain platform is an essential part of Dubai blockchain planning, which was deployed in October 2016 to ensure that all transactions occur on blockchain by 2020.

- **United States of America**

The Chicago Cook County Recorders of Deeds has begun a pilot investigation into the usage of blockchain registers in property records. The pilot project looked at the combination of property ownership and digital assets in around 2,000 unoccupied residences in Chicago.

- **India**

The Indian state of Andhra Pradesh has partnered with start-up “ChromaWay” to create a blockchain-based land register. To increase data transparency for citizens, the blockchain backend was connected with a front-end website.

- **Sweden**

Sweden’s land record authority “Lantmäteriet” has completed a two-phase operation to migrate property transactions to blockchain. This initiative sells real estate using smart contracts, which are overseen by banks and intermediaries. According to the “World Bank Business Index” statistics, Sweden has one of the most precise property registration systems in the world, therefore its shift to blockchain technology was not motivated by fraud or irregularities in its operations, as was the case in Brazil. A notary lawyer does not take part in the initiative. The pilot project data was gathered between July and October 2017.

3.2.2. Blockchain application in supply chain integrity

K. R. Rejon et al. [44] proposed a novel blockchain simulation scenario as a reference for identifying altered phishing assaults, facilitating traceability, preventing fraud and increasing client control in supply chains. Additionally, they discussed how blockchain-based payment and fraud detection technology can improve transaction security. The simulation makes use of a Mersenne Twister pseudorandom number generator. This random number generator will be used to add variation to the test programs, allowing for the modeling of both faulty and genuine messages, similar to the characteristics of a phishing assault. This simulation attempts to mimic the actions of both legitimate recipients and email senders, as well as phishing recipients and senders. To enable a simple and user-friendly program execution, the simulation was built with JavaScript as the runtime environment. The blockchain implementation uses the SHA256 hashing method. The findings demonstrate blockchain technology’s capacity to reduce risks, increase transparency, and strengthen confidence in retail cybersecurity. While issues with scalability and legality persist, the advantages of the distributed ledger in retail cybersecurity are tremendous, making it an appealing source of future innovation and development in the field.

4. Discussions and future directions

The study provides a systematic overview of blockchain technology to improve cybersecurity. Below is a basic description of the key challenges of previous studies, as well as suggestions for new solutions to these challenges in terms of strengths and weaknesses:

- **Strength Points**

1. **Smart contracts** are self-executing contracts that have stated basic conditions secured on the blockchain, and can automate cybersecurity guidelines and processes, such as access control regulations, threat detection, and incident response actions, reducing manual intervention and increasing security efficiency.
2. **Blockchain technology can enhance cybersecurity monitoring and threat detection systems** by combining security incident records and sensor data, as well as other pertinent information, into a blockchain that simplifies the detection of abnormalities, identifying trends, and connecting events across several systems. This can boost the efficacy and reliability of intrusion detection systems and early warning systems.

- **Weakness Points**

1. **Scalability** is one of the most pressing problems concerning the application of blockchain technology. As the size and volume of blockchain transactions increase,

Table 3. Proposed solutions for previous studies' challenges.

Ref.	Challenges	Proposed Solutions
[8]	Lack of assurance and confidence, particularly on sustainable and social business networks	– Blockchain Technology • Smart Contracts include automating and enforcing deals transparently, eliminating the need for middlemen. • Immutable Records: Use blockchain's immutability to keep a secure and transparent record of transactions, building trust among users.
[15]	Transactional privacy	– Smart Contract Privacy • Create privacy-enhancing smart contracts to limit access to transaction details to just appropriate parties. • Use Zero-Knowledge Proofs to validate transactions without disclosing sensitive information. • Use homomorphic encryption to protect sensitive information while performing computations on encrypted data.
[16]	An absence of security and confidence, especially in sustainable and profitable social enterprise systems	– Enhance Network Security • Firewalls and Intrusion Detection Systems (IDS) Configure robust firewalls and IDS that track and manage network traffic both incoming and outgoing and observe suspicious activity. • Network segmentation can restrict access to essential data and reduce the impact of a compromise.
[24]	Identifying, assessing, and managing relevant risk events	– Risk Analysis • Qualitative Risk Analysis: Use a grading system to evaluate hazards based on their probability and impact (high, medium, or low). This helps identify and prioritize risks. • Quantitative Risk Analysis: Use statistical approaches, such as Monte Carlo simulations, to assess potential consequences on the goals of the project. – Risk Identification • Conduct Risk Assessment Workshops with stakeholders to identify potential hazards in processes, projects, or services. • Analyze previous data to identify patterns and risks that may affect future activity.
[25]	Maintain security of the patient's medical information	– Implement Strong Access Controls • Use Role-Based Access Control to control access to medical data based on client responsibilities, ensuring only authorized staff can access important information. • Enforce Multi-Factor Authentication for accessing Electronic Health Record (EHR) systems to enhance security. • Encrypt patient data both at rest and in transit using strong encryption methods.
[26]	Regulatory and scalability considerations	– Regulatory Adaptation • Create a Regulatory Task Force to monitor rules and adjust processes for compliance in a changing environment. – Scalable Architecture • Cloud-Based Solutions: Scale resources based on demand without considerable upfront expenditure.
[27]	Cyber threats at the national defense level	– Continuous Monitoring and Threat Intelligence • Use real-time monitoring technologies to detect and handle threats efficiently. • Use threat intelligence solutions to collect and evaluate data on new threats, risks, and attack trends.
[28]	Interoperability, Data privacy, Scalability	• Implement tight access control mechanisms to limit sensitive data access to approved users. Use Role-Based Access Control (RBAC) to limit data access. • Use Layer 2 scaling answers, such as a lightning network for Bitcoin and Plasma for Ethereum, to increase transaction performance and reduce primary network traffic.

(Continued)

Table 3. Continued.

Ref.	Challenges	Proposed Solutions
[29]	Speed and expense of real estate transactions	• Collaborate with financial institutions to simplify loan funding and approval processes that fit with property transaction timelines.
[30]	Integrating network assets and effectively enhancing defense capabilities is a pressing topic	• Use virtualization and cloud technologies to combine network resources, improving flexibility, scalability, and centralized management. • Integrate automation threat intelligence feeds into security systems to receive fast information on threats and vulnerabilities.
[31]	Safeguarding the privacy of sensitive information gathered by IoT instruments	• Encrypt all data exchanged between devices in the IoT and servers to prevent unauthorized manipulation. • Strong authentication techniques, such as multi-factor authentication, are required for accessing IoT equipment and data.
[32]	Modern interconnected and autonomous automobiles must be safeguarded against cyberattacks for their actions on routes	• Compliance with Industry Standards: Adhere to established standards (e.g., ISO/SAE 21434, NIST cybersecurity framework) to ensure systematic risk management and security practices. • Secure Coding Practices: Implement secure coding standards throughout the software development lifecycle to minimize vulnerabilities in vehicle software.

the network may become overcrowded, causing transaction processing times to lag. This could limit the widespread adoption of blockchain for high-volume applications such as payment processing and supply chain management. To address this issue:

a) Reducing codes in storage systems can enhance scalability by reducing data collection per block and increasing storage capacity.
b) Blockchain sharding creates independent shards for parallel transaction processing. Sharding represents one of the scalability techniques utilized in the latest version of Ethereum.
c) Utilize decentralized storage platforms, like InterPlanetary File System (IPFS) or Sia, to offload huge data assets from the chain of ledgers, reducing storage requirements and enhancing scalability.

2. **Many distributed ledger networks,** particularly those that depend on PoW consensus (such as Bitcoin), require tremendous computing power and energy to check transactions and protect the network. This has sparked worries about blockchain technology's environmental impact, particularly as energy usage rises due to greater network activity. The suggested remedy to these concerns is:
a) Use PoS consensus, which is more energy-efficient than PoW in traditional blockchains like Bitcoin. PoS algorithms rely on staking, in which inspectors lock up their cryptocurrency tokens to verify transactions rather than energy-intensive mining.
b) Optimize energy consumption by implementing dynamic energy management strategies, such as adjusting mining difficulty or selectively active nodes based on network traffic.
c) Using alternative sources of energy, such as solar or wind, to supply the blockchain nodes and mining activities can reduce the overall carbon footprint and environmental impact.

Specifically, the summary of prior studies covers multiple problems. As shown in Table 3, new solutions were proposed in each study.

In particular, the summary of previous studies discusses the safety issues. As shown in Table 4, new solutions were proposed in each study.

Blockchain technology can be connected with IoT devices, sensors, and Radio Frequency Identification (RFID) tags to provide real-time tracking and surveillance of supply chain

Table 4. Proposed solutions for previous studies of blockchain cyberattacks.

Ref.	Cyberattacks Types	Proposed Solutions
[8]	Platform risk	– Comprehensive Risk Assessment • Conduct Regular Risk Assessments: Evaluate the platform's architecture, operations, and third-party integrations to identify vulnerabilities and potential risks. • Identify Critical Assets: Determine which assets are most critical to the platform's functionality and security, prioritizing their protection.
[15]	Smart contract Exploits	– Security Best Practices • Limit External Calls: Minimize the reliance on external contract calls that can introduce vulnerabilities or unexpected behaviors. • Use Safe Libraries: Utilize well-audited libraries (e.g., OpenZeppelin) for common functionalities to reduce the risk of implementing insecure code.
[16]	Malicious botnet networks.	– Strengthening Network Security • Use robust firewalls and intrusion detection systems to detect traffic and avoid botnet activities. • Botnet Mitigation Strategies • Implement rate limitation on network traffic to prevent Distributed Denial of Service (DDoS) assaults from botnets and limit bandwidth to key services. • Use traffic filtering to prevent botnet activity by blocking known malicious IP addresses and behaviors.
[24]	51% attack Real DOS attack against the Ethereum network	– Strengthening Network Consensus Mechanisms • Adopt PoS to prevent 51% attacks by asking validators to stake huge sums of cryptocurrency, rendering attacks economically untenable. • Combine PoW and PoS consensus models to enhance security and attack resilience.
[25]	Hacking by unauthorized persons	– Monitoring and Logging • Use real-time monitoring to recognize and respond to illegal access attempts quickly.
[26]	Phishing attacks	– Email Filtering and Security Tools • Use machine learning to detect and eliminate phishing emails in consumers' inboxes. • Use URL scanning technologies to detect fake emails and warn consumers before hitting on potentially harmful links.
[27]	Double-spending	– Use strong consensus mechanisms like PoW and PoS to examine transactions and avoid double-spending among multiple participants. • Set confirmation criteria. Multiple confirmations must be obtained for major transactions to avoid double-spending.
[28]	Risk of fraud in real estate	– Enhanced Verification Processes • Identity of all parties engaged in property deals, such as consumers, sellers, and agents.
[29]	Tamper attack	– Data Integrity Measures • Use cryptographic hash methods to ensure data integrity. Any modification in the data creates a unique hash value, confirming manipulation.
[30]	Malicious URLs	– User Education and Awareness • Training consumers about the risks of clicking on unknown or suspect URLs, such as phishing and social engineering. • Use phishing simulations to assist consumers detect and reporting malicious URLs.
[31]	Mining attacks	• Use robust consensus methods, such as PoS, to prevent attackers from obtaining control of the network through mining.
[32]	Reply, Sybil, malware attacks	• Use the lightweight cryptographic technique.

assets, such as items, containers, and vehicles. In addition, blockchain-based smart contracts are being used to automate many supply chain activities, including order fulfillment, inventory management, and payments.

5. Conclusion

This study examines numerous experiments to demonstrate and examine various collaborators with the opportunity to distinguish between the limitations and move towards building unique ways to improve cybersecurity based on blockchain. This in turn achieves the comprehensiveness of data security, focusing on its ability to ensure data integrity, develop authentication mechanisms, and boost distributed authority. Blockchain technology eliminates the problems of duplicate identity and criminality by decentralizing the vital public infrastructure for authentication purposes. The blockchain's ledger also ensures data integrity because no unauthorized individual can change information inside it after recording. This review identifies the limits of each article that could be utilized for future growth and has provided a more nuanced understanding of blockchain's function in cybersecurity, and proposed solutions were presented in terms of challenges and cyberattacks facing blockchain technology. Future research leveraging blockchain technology to improve cybersecurity in real estate could focus on tokenizing real estate assets, allowing for fractional ownership and trading on a secure, decentralized network. Additionally, blockchain-based smart contracts could be used to automate and streamline real estate transactions such as property ownership exchanges, escrow management, and title transfers.

Acknowledgment

The authors would like to thank the Department of Computer Science, University of Technology—Iraq, for their cooperation in completing this study.

Conflicts of interests

The authors declare that they do not have any conflicts of interest.

Authors' contributions

Sarah Mohammed Shareef: Conceptualization, analysis, Future Visions, Writing – review and editing; Rehab Flaih Hassan: Supervision, review and editing.

Data availability

No dataset has been used in this study.

References

1. C. Papantoniou, "GeoBlockchain: The analysis, design, and evaluation of a spatially enabled blockchain," M.S. theses, CGU, Glaremont, CA, 2021. [Online]. Available at: https://dl.acm.org/doi/book/10.5555/AAI28862141.
2. D. D. H. Miriam, D. Dahiya, Nitin, and C. R. R. Robin, "Secured cyber security algorithm for healthcare system using blockchain technology," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1879–1906, July 2022, doi: 10.32604/iasc.2023.028850.

3. G. Kabanda, "Cybersecurity risk management plan for a blockchain application model," *Transactions on Engineering and Computer Science,* vol. 2, no. 1, April 2021. Art. no. 121.
4. I. Lee," Cybersecurity: Risk management framework and investment cost analysis", *Business Horizons*, vol. 64, no. 5, Sep. 2021, pp. 659–671, doi: 10.1016/j.bushor.2021.02.022, 2021.
5. D. Chatziamanetoglou and K. Rantos, "Cyber threat intelligence on blockchain: A systematic literature review," *Computers,* vol. 13, no. 3, 23 Feb. 2024, Art. no. 60, doi: 10.3390/computers13030060.
6. B. Pan, L. Zhang, C. Li, and L. Chen, "Supply chain management system's cybersecurity based on blockchain technology," *International Journal of Science and Advanced Technology*, vol. 11, no. 9, pp. 76–83, Feb. 2013.
7. Z. A. Kamal, R. F. Ghani, and A. K. Farhan, "Blockchain-based E-government system using WebSocket protocol," *Engineering and Technology Journal*, vol. 42, no. 4, pp. 421–429, Apr. 2024, doi: 10.30684/etj.2024.146559.1689.
8. B. Riskhan, S. M. H. Almassri, K. Hussain, H. A. J. Safuan, "Blockchain-based cyber-security proposal in commerce mobile platforms for social and sustainability businesses," *Metaverse,* vol. 5, no. 1, pp. 1–14, Feb. 2024, doi: 10.54517/m.v5i1.2415.
9. K. K. Vaigandla, M. Siluveru, M. Kesoju, and R. Karne," Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian journal of Cybersecurity*, vol. 2023, pp. 73–85, Mar. 2023, doi: 10.58496/MJCS/2023/012.
10. P. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, "Blockchain technology and its types—A short review," *International Journal of Applied Science and Engineering (IJASE)*, vol. 9, no. 2, pp. 189–200, Jun. 2022.
11. S. S. Abdul-Jabbar, A. K. Farhan, and R. F. Ghani, "Data analytics and blockchain: A review," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)*, vol. 23, no. 1, pp. 23–34, Mar. 2023, doi: 10.33103/uot.ijccce.23.1.3.
12. C. DeCusatis, B. Gormanly, J. Iacino, R. Percelay, A. Pingue, and J. Valdez, "Cybersecurity test bed for smart contracts," *Cryptography*, vol. 7, no. 1, Mar. 2023, Art. no. 15, doi: 10.3390/cryptography7010015.
13. S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," *IEEE Access,* vol. 8, pp. 24416–24427, Feb. 2020, doi: 10.1109/ACCESS.2020.2970495.
14. J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *Proc. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE),* Vilnius, Lithuania, pp. 1–6, doi: 10.1109/AIEEE.2018.8592253.
15. S. M. Rosaire and D. Jules, "Smart contracts security threats and solutions," *International Journal of Information Technology and Web Engineering*, vol. 17, no. 1, pp. 1–30, 2022, doi: 10.4018/IJITWE.304048.
16. V. K. Uppalapu and A. Agarwal, "Enhancing cybersecurity through the utilization of blockchain technology," *Journal of Propulsion Technology,* vol. 45, no. 1, pp. 4076–4081, 2024.
17. Sh. Lin, "Proof of Work vs. Proof of Stake in Cryptocurrency", *Highlights in Science, Engineering and Technology*, Volume 39 (2023), DOI: https://doi.org/10.54097/hset.v39i.6683.
18. A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, "Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review", *IEEE Access*, vol. 7, pp. 43622–43636, Mar. 2019, doi: 10.1109/ACCESS.2019.2904181.
19. A. R. Mathew, "Cyber security through blockchain technology," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 1, pp. 3821–3824, Oct. 2019, doi: 10.35940/ijeat.A9836.109119.
20. T. Wang, H. Hua, Z. Wei, and J. Cao, "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power and Energy Systems*, vol. 135, Feb. 2022, Art. no. 107499, doi: 10.1016/j.ijepes.2021.107499, 2021.
21. Z. Cekerevac and P. Cekerevac, "Blockchain and the application of blockchain technology," *MEST Journal,* vol. 10, no. 2, pp. 14–25, July 2022, doi: 10.12709/mest.10.10.02.02.
22. S. Gupta and M. Sadoghi, "Blockchain transaction processing," 2019, *arXiv:* 2107.11592.
23. Z. A. Kamal and R. F. Ghani, "A proposed authentication method for document in blockchain based E-government system", *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)*, vol. 22, no. 4, pp. 127–139, Dec. 2022, doi: 10.33103/uot.ijccce.22.4.10.
24. I. M. Abdelwahed, N. Ramadan, and H. A. Hefny, "Cybersecurity risks of blockchain technology", *International Journal of Computer Applications*, vol. 177, no. 42, pp. 8–14, Mar. 2020.
25. A. S. Jamil and A. M. S. Rahma, "Cyber security for medical image encryption using circular blockchain technology based on modify DES algorithm," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 03, pp. 99–112, Mar. 2023, doi: 10.3991/ijoe.v19i03.37569.
26. R. K. Ray, F. R. Chowdhury, and R. Hasan, "Blockchain applications in retail cybersecurity: enhancing supply chain integrity, secure transactions, and data protection," *Journal of Business and Management Studies*, vol. 6, no. 1, pp. 206–214, Feb. 2024, doi: 10.32996/jbms.2024.6.1.13.
27. S. LEE and S. KIM, "Blockchain as a cyber defense: Opportunities, applications, and challenges," *IEEE Access,* vol. 10, pp. 2602–2618, Dec. 2021, doi: 10.1109/ACCESS.2021.3136328.

28. V. Plevris, H. Abdallah, and A. Alnatsheh, “Blockchain and its potential in the digitization of land and real estate property records,” in *Proc. 2nd Int. Conf. on Civil Infrastructure and Construction (CIC 2023)*, Doha, Qatar, pp. 861–870, doi: 10.29117/cic.2023.0112.
29. G. Sladić, B. Milosavljević, S. Nikolić, D. Sladić and A. Radulović, “A blockchain solution for securing real property transactions: a case study for Serbia,” *ISPRS Int. J. of Geo-Inf.,* vol. 10, no. 1, Jan. 2021, Art. no. 35, doi: 10.3390/ijgi10010035.
30. L. Shi, X. Li, Z. Gao, P. Duan, N. Liu, and H. Chen, “Worm computing: A blockchain-based resource sharing and cybersecurity framework,” *Journal of Network and Computer Applications*, vol. 185, July 2021, Art. no. 103081, doi: 10.1016/j.jnca.2021.103081.
31. M. C. Raju1 and K. S. Paul, “A comprehensive review of cyber security in blockchain-based IoT,” *Mathematical Statistician and Engineering Applications*, vol. 71, no. 4, pp. 10646–10659, Dec. 2022, doi: 10.17762/msea.v71i4.1957.
32. J. Ahmad et. al., “Machine learning and blockchain technologies for cybersecurity in connected vehicles,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* vol. 14, no. 1, Feb. 2024, Art. no. e1515, doi: 10.1002/widm.1515.
33. R. A. Mallah, D. López, and B. Farooq, “Cyber-security risk assessment framework for blockchains in smart mobility,” *IEEE Open Journal of Intelligent Transportation Systems,* vol. 2, pp. 294–311, Aug. 2021, doi: 10.1109/OJITS.2021.3106863.
34. S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations”, *Sensors*, vol. 23, no. 15, July 2023, Art. no. 6666, doi: 10.3390/s23156666.
35. V. Wylde et. al., “Cybersecurity, data privacy and blockchain: A review,” *SN Computer Science*, vol. 3, Jan. 2022, Art. no. 127, doi: 10.1007/s42979-022-01020-4.
36. V. P. Sriram *et al.*, “Enhancing cybersecurity through blockchain technology enhancing cybersecurity through blockchain technology,” in *Cybersecurity Issues and Challenges for Business and FinTech Applications,* Hershey, Pennsylvania, USA: IGI Global, 2023, ch. 11, pp. 208–224, doi: 10.4018/978-1-6684-5284-4.ch011.
37. H. S. Hassan, R. Hassan, and E. K. Gbashi, “E-voting system based on Ethereum blockchain technology using ganache and remix environments,” *Engineering and Technology Journal*, vol. 41, no. 4, pp. 562–577, Mar. 2023, doi: 10.30684/etj.2023.135464.1273.
38. P. Bansal, R. Panchal, S. Bassi, and A. Kumar, “Blockchain for cybersecurity: A comprehensive survey,” in *Proc. 9th IEEE Int. Conf. on Communication Systems and Network Technologies (CSNT)*, Gwalior, India, 10-12 April 2020, pp. 260–265, doi: 10.1109/CSNT48778.2020.9115738.
39. Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, E. Akin, “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions”, *Electronics,* vol. 12, no. 6, Mar. 2023, Art. no. 1333, doi: 10.3390/electronics12061333.
40. Z. Fauziah, N. P. Anggraini, Y. P. A. Sanjaya, and T. Ramadhan, “Enhancing cybersecurity information sharing: A secure and decentralized approach with four-node IPFS,” *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 153–159, Oct. 2023, doi: 10.34306/ijcitsm.v3i2.139.
41. A. F. Al-zubidi, A. K. Farhan, and S. M. Towfek, “Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model,” *Journal of Intelligent Systems*, vol. 33, no. 1, pp. 1–24, Dec. 2023, doi: 10.1515/jisys-2023-0195.
42. A. F. Mendi and A. Cabuk, “Blockchain applications in geographical information systems,” *Photogrammetric Engineering & Remote Sensing,* vol. 86, no. 1, pp. 6–10, Jan. 2020, doi: 10.14358/PERS.86.1.5.
43. K. S. Ilesanmi and T. O. Idowu, “Possibility of land ownership transaction with non-fungible token technology: Minting survey plan”, *African Journal on Land Policy and Geospatial Sciences*, vol. 7, no. 2, pp. 488–497, Mar. 2024, doi: 10.48346/IMIST.PRSM/ajlp-gs.v7i2.41704.
44. G. Rossi, “Blockchain technology for enhancing cybersecurity in supply chain management,” *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries,* vol. 5, no. 2, pp. 1–14, Nov. 2022.