Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 02
2025

Research Article
https://doi.org/10.56979/802/2025

Blockchain in the Digital Age: Challenges, Opportunities, and Future Trends

Khushbu Khalid Butt[1], Muhammad Yousif[2*], Irshad Ahmed Sumra[1], Abubakar Qazi[1], Sajid Khan[3], and Muhammad Amjad khan[2]

[1]Department of Computer Sciences, Lahore Garrison University, Lahore, Pakistan.
[2]Department of Computer Sciences, Minhaj University, Lahore, Postcode, Pakistan.
[3]College of Computer Science and Technology,Zhejiang Normal University, Jinhua, China.
*Corresponding Author: Muhammad Yousif. Email:myousif.cs@mul.edu.pk

Accepted: January 21, 2025 **Published:** March 01, 2025

Abstract: Blockchain technology offers a massive network with built-in security features that encompass cryptography, decentralization, and consensus, which foster trust in transactions. IoT further looks as an emerging in finance and security that are the application of blockchain. The basic need for every blockchain consumer is the first to prioritize data confidentiality, integrity, and availability. In the era of 2025, trust is a necessary part of security for third parties, which handle the privileges of private and public. The mentioned advantages and disadvantages motivated us to provide an advancement and comprehensive study regarding the applicability of blockchain technology. This paper focuses on blockchain security issues for blockchain and sorts out the security risks in six layers of blockchain technology by comparing and analyzing existing security measures. The text also investigates and describes various security threats and obstacles associated with implementing blockchain technology, fostering theoretical inquiry and the creation of strong security protocols in current and forthcoming distributed work settings.

Keywords: Blockchain; Security; Privacy; Healthcare; Six-Layer; Parallel Security.

1. Introduction

Initially presented in 2022, blockchain serves as the distributed ledger that records bitcoin transactions, with the mining of the genesis block by Nakamoto in 2009 confirming the viability of the blockchain concept [1]. The conceptual framework included an E-cash system utilizing a peer-to-peer (P2P) network, encryption, timestamps, and blockchain technology [2]. This application permits peers to exchange value through transactions without the necessity for a central authority, thus protecting consumer privacy and preventing identity theft [3]. Blockchain technology has been utilized in various sectors as part of the framework for businesses that need openness, reliability, and trustworthiness [4] since its early days, expanding from its origins in cryptocurrency to modern blockchain applications for Industry 5.0[5-7]. Nevertheless, with the widespread use of blockchain technology and the ongoing emergence of new advancements, the challenges and risks associated with it are increasingly growing. In the Ethereum network, a smart contract refers to a piece of code that is deployed so that it is accessible to all users [8]. The adoption of blockchain technology in the healthcare industry can cover various facets of hospital operations, including processes, oversight, data management, financial transactions, auditing, and record keeping, while also offering essential technical support for reorganizing the hospital's information systems and workflow. Advances in blockchain technology from versions 1.0 to 5.0 [9–13] enhance its suitability and reliability for commercial applications and business needs: Blockchain 1.0, 2.0, 3.0, 4.0[14,15], and 5.0[16,17] represent distinct stages of application rather than successive advancements. Each version, from 1.0 to 5.0, operates within its area of development, contributing to different sectors. Figure 1 illustrates the extent of technical progress within the blockchain, while Figure 2 illustrates the differences between traditional networks and those utilizing blockchain for transparency.

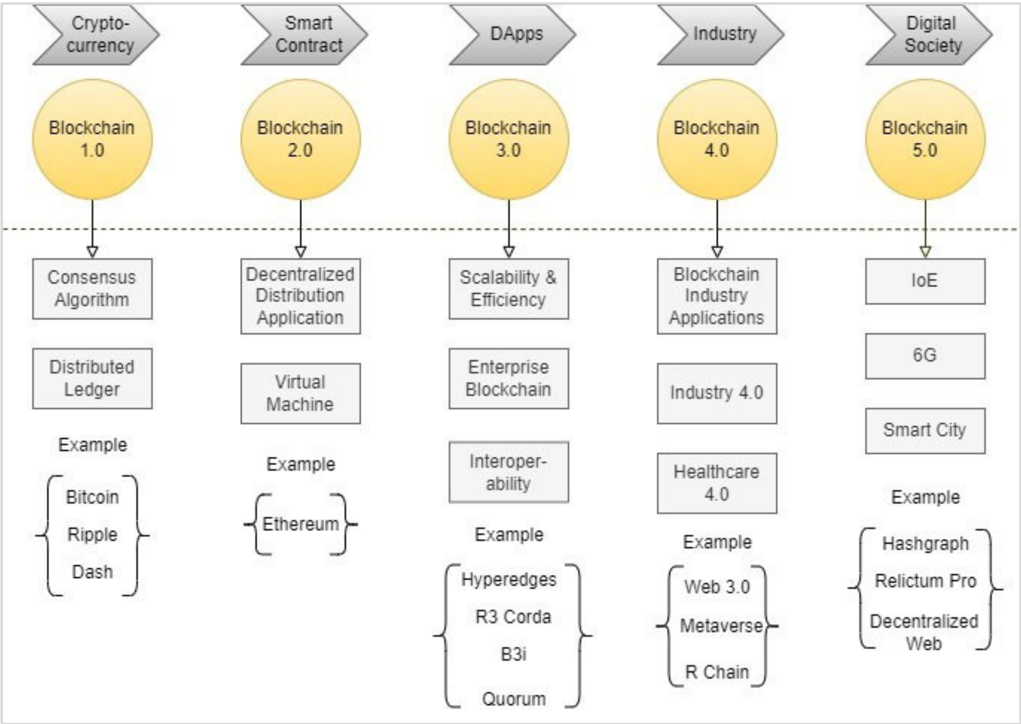

Figure 1. The extent of technological advancement in blockchain [122].

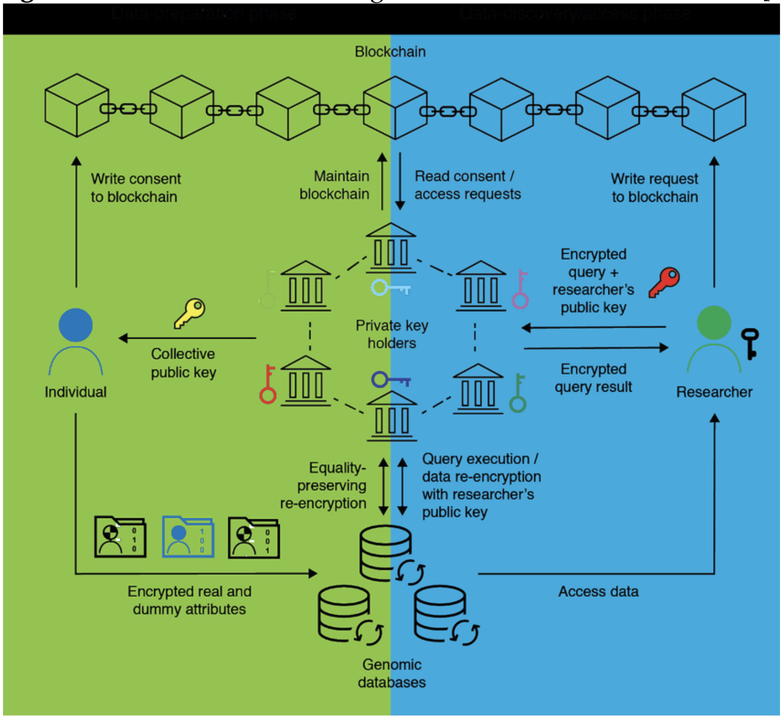
Blockchain
Write consent to blockchain
Maintain blockchain
Read consent / access requests
Write request to blockchain
Encrypted query + researcher's public key
Private key holders
Collective public key
Individual
Encrypted query result
Researcher
Equality-preserving re-encryption
Query execution / data re-encryption with researcher's public key
Encrypted real and dummy attributes
Access data
Genomic databases

Figure 2. The comparison of transparency networks between conventional systems and blockchain technology[123].

Since the introduction of blockchain 2.0, the technology has moved beyond being limited to currency transactions, exploring its applications in various financial and inter-organizational interactions, with the rise of multiple sources without sacrificing privacy. It ensures transparency without revealing digitalization, and blockchain 3.0 offers enhanced distributed storage and scalability while maintaining security and facilitating data integration ownership, guarantees interoperability without adding unnecessary complexity, and establishes a means of authentication. The adaptability and diverse functionalities of blockchain technology present vast opportunities for innovation, integration, and sustainability in healthcare.

1.1. Understanding the Concept and Features of Blockchain:

To begin with, from a technical standpoint, blockchain is not a new concept but rather a combination of pre-existing technologies:

- A pe.39er-to-peer network with an immutable distributed ledger: this ensures that the ledger maintained by a single node is fundamentally unchangeable due to the architecture of the blockchain.
- Security mechanisms such as encryption: cryptographic techniques and hashing algorithms provide protection and confidentiality for transactions.
- Consensus algorithms: these are purely mathematical methods used for the collective verification of the blockchain, fostering a trusting relationship among all parties while utilizing technology to uphold the agreement results.
- Smart contracts: Introduced by Billy in 2021, this notion of a contract is termed "smart" as it encompasses a collection of arrangements that participants can uphold. Smart contracts facilitate trustworthy business transactions without the need for intermediaries, aiming primarily to enhance security and lower transaction costs associated with traditional contracts. Consequently, they ensure that every transaction among nodes is credible and dependable.[18]

Secondly, from a principled perspective, blockchain represents a distributed-shared ledger technology, which establishes a decentralized, machine-trusted, and widely distributed shared ledger system, employing an optimal mathematical solution to create a framework for trust and consensus among all entities involved.

1.2. Blockchain characteristics:

1.2.1. Transparency and accessibility:

The system is accessible to all participants, granting them the right to be informed and to benefit equally from blockchain data.

1.2.2. Consensus:

Specific nodes vote to expedite verification and transaction confirmation; when multiple nodes agree on a transaction without any vested interests, it reflects the consensus of the network.

1.2.3. Equitable competition:

The actions of all nodes are governed by algorithms, which also dictate the rights to accounting.

1.2.4. Accuracy and Completeness:

Every record is documented accurately and comprehensively under oversight.

1.2.5. Secure and Trustworthy:

Data encryption and cryptographic techniques safeguard against data tampering and forgery; a sophisticated checksum-sharing approach ensures integrity, availability, and confidentiality. Multiple threats are identified through an encryption standard (digital signature) where each node possesses its key, and packet transmission occurs only when the key is valid [19].

1.2.6. Limitations and Challenges of Blockchain Security

Health information is gathered from various medical data sources and complex data formats. While data sharing enables the interaction of electronic health records (EHR) across different healthcare platforms, it also poses risks to patient privacy. Several technical challenges hinder the widespread adoption of blockchain technology in the healthcare sector [20–24].

1.2.7. *Limited transaction performance and scalability:*

The blockchain suffers from restricted transaction processing capabilities and delays in forming transaction blocks. The proposed solutions for expansion include:

1.2.8. Sharding:

This approach involves splitting the overall state of the blockchain into separate blocks that can be processed simultaneously.

1.2.9. Off-chain:

Moving the computation and verification processes to a separate protocol off-chain can lead to higher transaction throughput; in this scenario, the blockchain serves merely as an agreement layer to oversee a series of transactions.

1.2.10. DAGs:

(Directed acyclic graph): a graph structure that comprises vertices and edges (vertices represent entities within the graph, while edges indicate relationships between these entities). A DAG ensures that no cycles exist, facilitating the arrangement of nodes following a topological order.

1.3. Limited privacy protection:

Although blockchain is decentralized and tamper-proof, its transparent nature allows participating organizations to access the user's ledger. This openness can increase the risk of privacy breaches, as unmasked users' data on the blockchain heightens the potential for privacy violations. In current public chain systems such as Bitcoin, all transaction details are visible (including the amounts involved). This transparency does not comply with certain regulatory privacy standards, like the General Data Protection Regulation (GDPR) [25].

There is a pressing need for advancements in associated security technologies to address these issues:

1. Homomorphic encryption (HE) secures transaction data by encrypting it with a public key. Transactions are conducted as operations on ciphertext, and the resulting ledger remains encrypted and stored. Even if a node is compromised, the ledger information cannot be decrypted. The HE process is illustrated in Figure 3.
2. Zero-knowledge proof (ZKP) allows for verification without providing any valuable information from the verifier while keeping the message being proven hidden during the verification process.
3. A trusted execution environment is a secure area within the main processor that guarantees the confidentiality and integrity of the code and information processed inside it.
4. Storage limitations pose a significant challenge because the blockchain database is permanently recorded and can only be appended to, not altered. As a result, the cost of data storage becomes a major burden for the distributed network, requiring each full node to continually store an ever-growing amount of data. Thus, storage represents a substantial hurdle for any practical blockchain-based application.

Currently, the storage options available on public blockchains include the following:

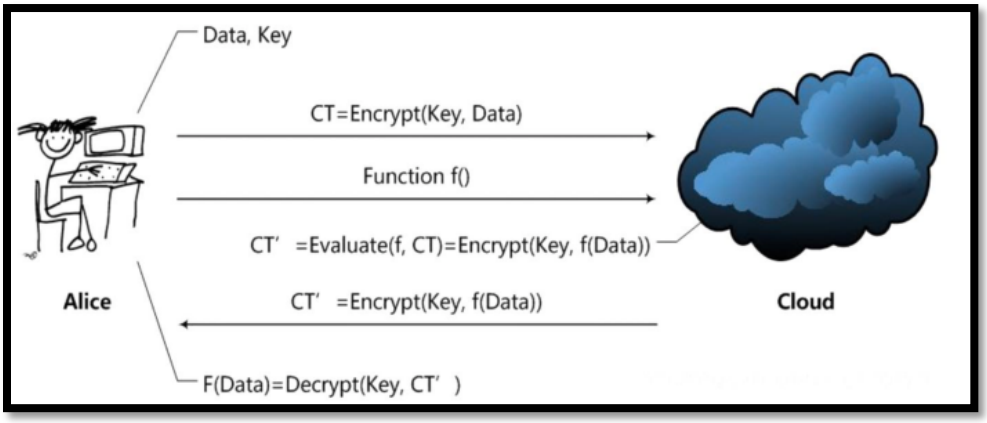
Data, Key
CT=Encrypt(Key, Data)
Function f()
CT' =Evaluate(f, CT)=Encrypt(Key, f(Data))
Alice
CT' =Encrypt(Key, f(Data))
Cloud
F(Data)=Decrypt(Key, CT')

Figure 3. The advancement of homomeric encryption [124].

1.3.1. Swarm:

A peer-to-peer sharing protocol built on Ethereum that enables users to save application code and data within swarm nodes beneath the main chain, allowing data exchange via the blockchain.

1.3.2. The Storj network:

This approach breaks files and data into smaller pieces, encrypts them, and distributes them across various nodes, ensuring that each node holds only a fraction of the total data.

1.3.3. *The IPFS:*

An optional hypermedia protocol that facilitates a peer-to-peer model for block storage based on content-addressable links, allowing for the permanent and distributed storage of files and providing historical access to versions, thus eliminating duplicate files.

1.3.4. Decent:

A decentralized platform for content sharing that enables users to upload and monetize their works (such as videos, music, e-books, and electronic health records) without the need for a centralized third-party service.

1.3.5. Alliance chain:

Data can be stored on the alliance chain, where the blockchain operating system retains only the most recent information while archiving historical data for preservation. Table 1 outlines the benefits and drawbacks of blockchain technology [26–28].

Table 1. The benefits and drawbacks of blockchain technology.

Lower expenses and enhance productivity.	The effectiveness in terms of cost has not been established.
Safe, reachable, and instantaneous.	Concerned about the problem of data leakage.
Database of network transactions	Regulatory challenges and technical issues.
Enhanced protection against "pushing."	Possible threat to the integrity of the data set.
Simple interaction in the broader network.	Less extensive networks raise the same issue.

Blockchain technology is utilized in the healthcare industry to tackle security risks, while homomorphic encryption is a popular technique for ensuring the privacy and security of electronic health records. Table 2 illustrates a comparison between the use of blockchain technology and homomorphic encryption.

Table 2.The examination of how blockchain technology and homomorphic encryption are implemented.

References	Application Domain	Implemented Algorithm	Summary
[29]	Healthcare insurance claims utilizing blockchain technology	Paillier cryptographic system	The hospital receives a request from the insurance company to confirm the accuracy of the patient's electronic health record.
[30]	Digital Copyright Safeguarding for Property	Algorithm for large prime numbers (LPN)	Auctioning on a blockchain platform to safeguard the digital copyright of a property practically and efficiently.
[31]	Auctioning on a blockchain platform to safeguard the digital copyright of a property practically and efficiently.	HE(Homomorphic Encryption), Completely homomorphic encryption (CHE)	The document outlines a variety of possible uses for HE across different fields to assess the significance of data privacy and security.
[32]	Sharing sensitive biomedical information in the public cloud.	EIGamal, Discrete Algorithms	Reduce the risk associated with sharing medical information on public cloud platforms. This model's drawback is that it requires an online connection.

[33]	Collection and storage of personal health data.	BGV(Brakerski-Gentry-Vaikuntanathan) scheme, Leveled homomorphic using modulus switching	The writer suggested a system that utilized homomorphic encryption to ensure the security of personal health information gathered, stored, and transmitted in the cloud.
[34]	Healthcare system for querying medical side effects.	Smart and Vercauteren, Style	An implementation model for a privacy-preserving query system that is efficient in terms of time applied to a real-world medical side effect inquiry system. Although there is an increase in communication costs, whether using threads or not, it remains feasible.
[35]	Gathering medical information	Fan and Vercauteren Lattice-based homomorphic encryption	He applied clinical research to assist patients and physicians in speeding up the process of learning from real-world data.

Motivation and Contribution The characteristics of cryptography require substantial hardware infrastructure and software tools for effective data processing and computational tasks; it is unrealistic to rely on standard computing components (like CPU or GPU) to achieve an adequate performance level. Moreover, the operation of large-scale machinery, particularly during encryption and decryption operations, generates significant noise and heat, which present considerable challenges to computation speed and memory management. While the academic community has explored blockchain technology's architecture, privacy, and network security extensively, there has been limited thorough investigation into its applications within the medical sector. This article begins with a foundational overview of blockchain theory and advances to its security architecture, performing a detailed analysis of the challenges and future directions for blockchain in healthcare while integrating prospective medical innovations with contemporary cryptographic encryption techniques. Additionally, it aims to serve as a practical guide for advancing blockchain technology in the healthcare sector, offering comprehensive theoretical insights and robust security protocol development to foster the adoption and progress of blockchain in medical applications. From this introduction, we can gain an understanding of the blockchain concept, its operational mechanics, as well as its limitations and challenges.

The subsequent sections of the paper are organized as follows: Section 2 provides a review of existing literature. Section 3 examines the security challenges across six layers of blockchain technology. Section 4 discusses a comparative analysis of blockchain-based healthcare applications and data management practices. Section 5 delves into prospective research areas concerning blockchain security, while the concluding section presents the overall conclusions drawn from this study.

2. Literature Review

With the extensive adoption of Bitcoin and the rapid advancement of decentralized platforms in both financial and non-financial domains, blockchain technology has sparked a surge of global research interest. Blockchain facilitates the sharing of electronic health records (EHR) between end-users and healthcare systems without hindering communication[36]. This is achieved through trust lines and interoperability certifications enabled by distributed ledger technology. Contemporary healthcare applications prioritize user privacy and the safeguarding of shared data to thwart unauthorized access by malicious actors. Consequently, trust, authentication, and privacy are essential for the exchange of EHRs among various participants[37]. Vulnerabilities in mechanisms, attack strategies, and security protocols are critical factors contributing to security threats at all levels within the blockchain[38,39]. While it offers security assurances in a trustless setting, it also encounters a range of security and privacy challenges. Numerous countries and organizations have shifted their research focus toward enhancing blockchain security. This article addresses security concerns related to blockchain technology and its applications in the healthcare sector, organizing the security risks according to a six-layer architectural model to evaluate and analyze current security strategies to develop a more robust secure protocol in the blockchain context. The conceptual framework of parallel security offers valuable technical and theoretical support for research initiatives on blockchain security. A framework that centers on a parallel healthcare system is suggested to model and illustrate a patient's condition, diagnosis, and treatment journey, aiming to provide accurate predictions and guidance for disease diagnosis and treatment through parallel execution [40].

2.1. The Importance and Study of Security in Blockchain

From the beginning of blockchain technology, there have been five evolutions of technological advancements, and the array of applications has expanded significantly [41]. It is crucial to explore and analyze the security challenges related to blockchain technology. Examining blockchain security promotes accelerated innovation development. Blockchain encompasses various elements such as cryptographic fundamentals, distributed consistency, economic incentives, and network security. Investigating blockchain security fosters the advancement of technology. Inadequate theoretical security assessments, insufficient code reviews, and recurring security issues hinder blockchain development. Researching secure and efficient solutions can be applied to various healthcare contexts, and an increasing number of application cases can further evaluate the practical security of blockchain. Studying blockchain security contributes to establishing a reliable programmable society. The programmability and automated execution of smart contracts exhibit their intelligent characteristics; investigating the security of blockchain can enhance the security standards and design principles of smart contracts, streamline the development process, and improve interoperability. A secure blockchain framework and self-executing smart contracts can technically enforce agreements, minimize default risks, and create a trustworthy programmable society. Examining blockchain security aids in achieving manageable oversight. The unchangeable and anonymous nature of blockchain poses difficulties for regulatory enforcement. A supervisory mechanism can identify and prevent illicit activities within the system, serving as a security response following a system compromise. Analyzing current blockchain vulnerabilities, possible attack vectors, and privacy protection strategies is advantageous for developing network monitoring approaches and creating more effective and secure regulatory frameworks.

2.2. Goals for Security in Blockchain

Based on the security requirements of the network system, the fundamental objective of building a blockchain system is to utilize cryptography, network security, and various technical methods to safeguard all aspects of the blockchain security framework [42]. Security goals like consensus security, smart contract security, privacy safeguards, and content protection are intricately linked to data security [43]. The advancement of quantum technology based on digital and networked resources will lead to quicker and more sophisticated blockchain solutions, along with opportunities to enhance security and efficiency within blockchain systems [44-46]. Kashyap explores a method to incorporate blockchain and quantum cryptography into a quantum cryptosystem [47]. The advancement and safety of network technology go hand in hand and are closely aligned, and the security weaknesses and privacy threats present in IoT systems can be effectively tackled using blockchain technology[48]. The IoT applications in the healthcare sector help reduce communication barriers between healthcare professionals and patients, allowing for remote diagnoses during emergencies via smart devices and sensors. In healthcare, blockchain technology is primarily utilized as it provides decentralization, ensuring immutability, security, privacy and transparency [49]. Healthcare systems, the Internet of Things (IoT), and blockchain are interconnected and utilize dependable resources. During the process of technical integration,[50] investigated a new paradigm concerning security risks and challenges. In Monrat's study[51], conducted a comparative analysis of various consensus mechanisms and explored the challenges.

2.3. Agreement on Security

Blockchain 2.0, as it is often called, allows for the use of a full programming language to develop smart contract applications on the blockchain[60]. The security of smart contracts is a critical consideration, as they involve financial elements that attract various hacking attempts and make the blockchain network vulnerable to attacks. Given the characteristics of smart contracts, they activate across the blockchain network to each node when certain predefined conditions are satisfied. This system is intended to ensure that all parties involved in transactions receive their fair share or contract amount once the specified conditions are fulfilled. They are automatically triggered and cannot be halted. However, there are several disadvantages, such as the potential for exploiting smart contracts to carry out unwanted actions on the targeted machine without the user's awareness, including attacks that can withhold access to blockchain services [61,62].Pool attacks [63]. And unobtrusive snares [64].

2.4. Protection of Privacy and Content

A significant aspect of the blockchain is the confidentiality of a user's identity while engaging with the network and concealing transactions involving other individuals. However, achieving this is challenging since the blockchain network operates as an open system, allowing every node to validate the authenticity of the blocks. The anonymity feature is maintained in the blockchain to safeguard user privacy, yet it can be compromised in various ways [65]. De-anonymization can be achieved through various types of attacks, some of which are typical of network attacks while others are specifically targeted at blockchain. A straightforward network scan or analysis may reveal information about the incoming blocks and their sources [66]. Address clustering can be utilized to distinguish the creators of the initial block, typically miners, by identifying blocks that lack an origin-destination pair [67,68], While it's challenging, it is achievable. An effort to remove anonymity from user data was conducted in [69]. By employing transaction fingerprinting, which analyzes the hour of the day, minute of the hour, coin movement, and input/output balance, it is possible to identify nearly 40% of Bitcoin users. Different forms of mixing services exist [70,71] that can help safeguard the user's identity and transactional data. In addition, utilizing a VPN and the Tor network can enhance online anonymity and shield user identification within the blockchain network.

2.5. Concurrent Security of Blockchain

The parallel security theory of blockchain employs parallel intelligence along with the AHP(Analytic Hierarchy Process) method, which consists of artificial systems, computational experiments, and parallel execution [72,73] to understand the process of making security decisions [74]. Revised security theory formulates synthetic blockchain architectures by precisely outlining the static attributes and dynamic functions of essential components, including consensus protocols, node statuses, network conditions, and incentive mechanisms tied to security. Figure 4 illustrates the idea of revised security[75], By employing the artificial system (A) approach, we can model the actual blockchain system to accurately represent its operational state. We conduct method calculation experiments (C) to distinguish artificial attack scenarios, perform analysis, and evaluate results within the artificial system to understand the evolution patterns and develop countermeasures for the actual blockchain system in response to various attacks. Furthermore, we aim to create an optimal "scenario-response" knowledge database utilizing the parallel execution (P) technique, where both the parallel execution and artificial systems evolve alongside real systems under identical attack conditions, facilitating training, learning, experimentation, education, and management of the actual blockchain system.

The parallel security framework can enhance the decision-making process related to blockchain security, precisely and effectively addressing the security risks faced by the system during its real-world operation [76]. Nevertheless, parallel security primarily serves as a framework for guiding both attacks and defenses. Its execution requires a gradual resolution of issues related to general modeling, attack simulation, computational experiments, intelligent blockchain analysis, bidirectional guidance, and the co-evolution of artificial systems with real-world systems.

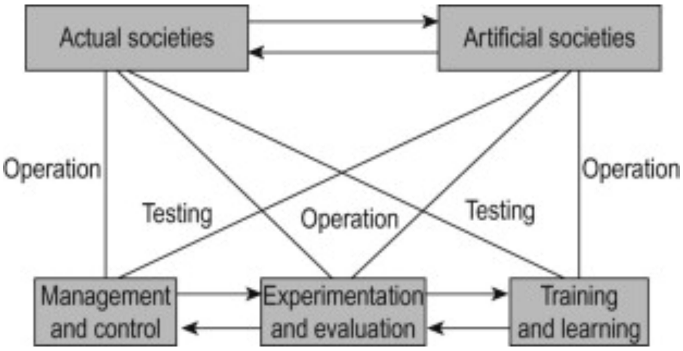

Figure 3. A structure of simultaneous security measures on the blockchain[125].

3. Materials and Methods

Reworded_TEXT:

Sybil attacks occur when hackers create fake network nodes and flood the target network with a large volume of false identities, potentially resulting in system failures and disrupting transactions on the blockchain. To guard against Sybil attacks, employ appropriate consensus algorithms, monitor the behavior of other nodes, and remain alert for nodes that are simply passing along blocks from a single user. Phishing attacks aimed at blockchain platforms are increasingly common and pose serious challenges. In a phishing scheme, the attacker seeks to gain access to the user's credentials. They might send emails that look authentic to the wallet key holder. When the user inputs their login information via a fraudulent link, the hacker acquires the credentials and other confidential information. Improve the security of your browser and devices by using software that identifies malicious links or reputable anti-malware applications, and make sure that your systems and software are regularly updated. Avoid clicking on unknown links, and when logging into an online wallet or managing sensitive data, do not enable Wi-Fi during online banking activities to reduce the chances of falling victim to phishing attacks.

Routing attacks pose a significant danger to security and privacy in blockchain systems. Cybercriminals can take advantage of account anonymity to intercept data sent to internet service providers. This type of attack can compromise sensitive information or assets without the user's knowledge. To mitigate the chances of routing attacks, users should adopt secure routing methods (using certificates), encrypt their data, establish strong passwords and change them regularly, and stay informed about the potential risks related to information security. Threats to private key security: Blockchain relies on public-key cryptography, and any mishandling or improper application of this cryptography can create notable security gaps within the blockchain. If the key signing procedure in your blockchain is not carried out correctly, an attacker might be able to obtain your private key from the public key. Holding your private key grants full control over your data stored on a blockchain.

The security of blockchain endpoints is a major concern. Cybercriminals may track user activity and target specific devices to access the user’s password. This is one of the commonly acknowledged vulnerabilities in blockchain security. To reduce endpoint risks, avoid saving blockchain keys as plain text on devices and perform regular system audits, keeping a record of the time, location, and access to devices. This section will reevaluate using the six-layer framework [82]. Each layer can be divided into two components: the fundamental module and the security module, as depicted in Figure 5. The fundamental module functions as the essential part to carry out the main tasks of this layer, while the security module serves as a safeguard to ensure the security of each layer and provide dependable technical assistance for the upper layer.

Data Layer: The security component integrated within the data layer, along with other cryptographic elements, serves as the foundation for enabling the functions of the other five layers. The data layer is confronted with several security challenges:

Quantum computing: The transactions and data blocks of the blockchain data layer rely on various cryptographic elements. To fulfill enhanced privacy protection requirements, certain blockchains necessitate the use of privacy technologies such as ring signatures and zero-knowledge proofs; however, these can compromise the security of the data layer.

Poor key management: Applications based on blockchain, particularly in the financial sector, are attractive targets for opportunistic attackers, especially concerning transactions of digital assets and healthcare that involve sensitive personal information.

Key leaks and losses: Due to inadequate usage and storage practices, users can face significant losses; therefore, it is essential to implement an effective key management strategy. Password-protected secret sharing (PPSS) is a scheme for online threshold wallets, and it is emerging as a leading research focus for achieving secure key management in the blockchain domain going forward.

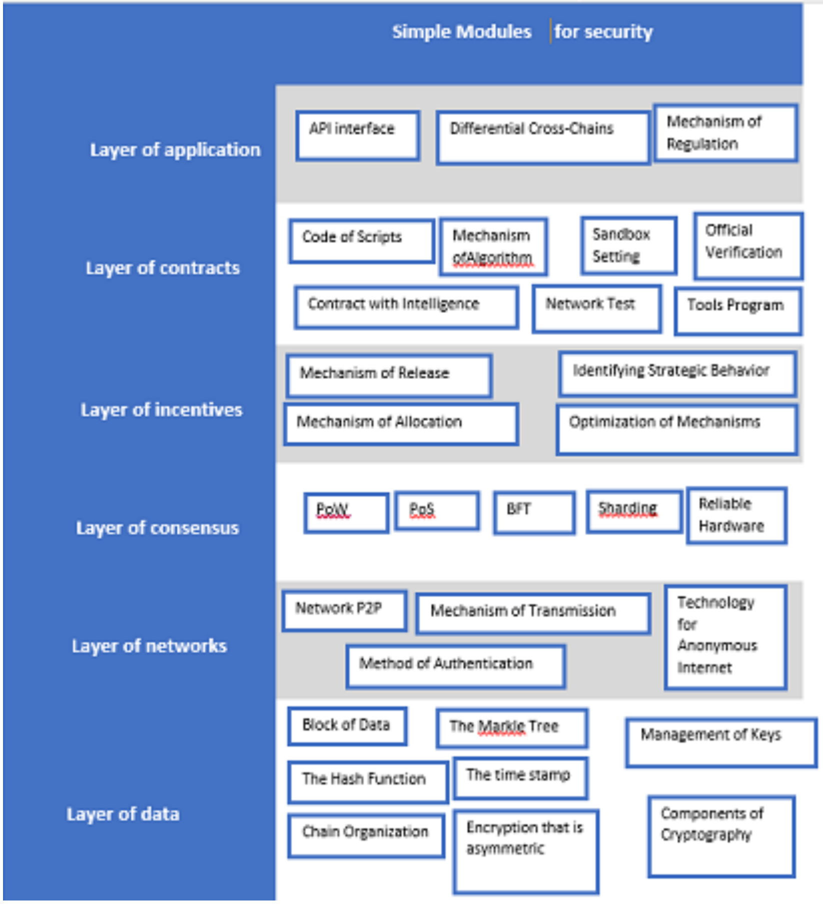

Figure 4. The blockchain system architecture.

REIated transactions: Many digital platforms utilizing blockchain technology employ digital pseudonyms, yet this technique offers only limited identity anonymity; the relationships between transactions and their amounts are visible on the blockchain. If an address is revealed, it may be possible to deduce all public key addresses associated with the user. By conducting transaction cluster analysis and transaction graph analysis, a user's actual identity can also be inferred from the statistical features of their transactions.

Code flaws: Certain cryptographic elements can contain imperfections and vulnerabilities during the compilation process. The transaction malleability attack is a type of exploit that targets weaknesses in data layer code; it takes advantage of the malleability of transactions through digital signatures during compilation and is frequently used to target bitcoin trading platforms. Initially, the attacker initiates a withdrawal from the trading platform. Subsequently, the platform generates a transaction for the attacker. The attacker then alters the transaction to create a new TXID(transaction ID) identifier, which they use to fabricate a new transaction and submit it to the network. If successful, the attacker ends up acquiring double the amount of bitcoin. Some research efforts focus on countering transaction malleability by altering the TXID(transaction ID) structure.

3.1. Network Layer:

The network layer encompasses various network technologies, with its primary role being to facilitate legitimate connection and efficient communication among blockchain nodes. The inherent security challenges of the technology will unavoidably pose security threats to the blockchain network layer:

- Security vulnerabilities in the P2P network: The peer-to-peer network [90,91] offers a distributed and self-organizing connection method for nodes within a peer-to-peer environment, but it lacks essential mechanisms such as identity verification, data validation, and network security oversight. Due to its unequal operational modes, the P2P network cannot effectively utilize firewalls, intrusion detection, and other measures for specific protection. Consequently, the nodes within the network are more susceptible to attacks.
- Network topology of nodes: The arrangement of nodes in the network can facilitate attackers in locating their targets and executing attacks. Adversaries can observe the network topology by either actively sending packets or passively analyzing the data packets exchanged between nodes. The eclipse attack [92] serves as a common attack strategy where attackers exploit the topological relationships among nodes to achieve network isolation. The solar eclipse attack may lead to further exploitations [93] as the attacker implements it on a node with superior computing power, leading to a disconnection of computational resources, impacting the distribution of mining rewards, and subsequently simplifying the execution of other attacks like self-mining or double spending [94].
- Issues with privacy protection: Privacy safeguards at the data layer are unable to prevent the correlation between transactions and user IP addresses during network transmission; attackers may leverage this to monitor and trace IP addresses, compromising privacy protection. The network layer offers mixing services for anonymous transactions in the digital currency realm [95]. Mixing services involve combining and outputting multiple unrelated inputs to obscure the link to transactions, thereby ensuring that outsiders cannot trace the flow of digital currency for anonymous payments [96]. There are two categories of mixing services: centralized mixers and decentralized mixers:
- Centralized mixer: Conducted by a third-party server, where the user submits transaction tokens, and after several transactions are combined, the final output is sent to the intended recipient. This approach undermines the decentralization aspects of blockchain, posing risks like third-party backdoors that could steal tokens and create a single point of failure. The TumbleBit protocol serves as an off-chain currency mixing solution requiring third-party involvement, but it only knows how to provide services without accessing transaction specifics.
- Decentralized mixer: It creates a new transaction by randomly blending several transactions and redistributing the tokens based on the initial transaction, thus enabling anonymous payments. CoinJoin is a cryptocurrency mixing technology that operates independently of protocols. Users must rely on a third party to facilitate a transaction that combines multiple inputs, although CoinJoin technology is not entirely anonymous, the third party providing the service can track the flow of mixed currency transactions.

3.2. Consensus Layer:

The consensus layer is designed to ensure that nodes share the same valid view and communication method provided by the blockchain network, focusing on the creation of a more secure, efficient, and low-energy cost consensus mechanism. A robust consensus mechanism can enhance the performance of the blockchain system, offer solid security assurances, accommodate application scenarios with sophisticated functions, and encourage the growth and expansion of blockchain technology. Nevertheless, the consensus mechanism has certain drawbacks, including incomplete security proofs, questionable security assumptions, limited scalability, inconsistent consistency, and challenges in initialization and reconstruction:

- Incomplete security proof: When modeling security, consensus mechanisms must take into account a variety of factors, yet new consensus mechanisms are continuously being developed, and some frameworks struggle to fully certify the security of these new mechanisms. Kiayias introduced a model and proof method for security in synchronous networks. Much of the research on provable security related to consensus mechanisms primarily revolves around PoW, which typically considers only a single factor. Additionally, the complex nature of network environments complicates the security analysis of consensus mechanisms.
- Questionable security assumptions: The security assessment of contemporary cryptosystems is based on computational complexity theory, but some security assumptions can be easily compromised in real-world applications. For example, Bitcoin's use of PoW can become vulnerable if a mining pool reaches 56.5% of the computational power, which can undermine the security assumptions of PoW, hindering the verification and recording of transactions and disrupting the consensus mechanism's activity.

- Inconsistent consistency: Consistency is a crucial property for evaluating the security of the consensus mechanism, but ensuring stable consistency in real-world applications is challenging. Even proof of elapsed time (PoET) and proof of luck (PoL) depend on trusted hardware to provide randomness, ensuring that network conditions do not influence the consistency of the consensus mechanism.
- Limited scalability: Scalability is a vital characteristic in the study of consensus mechanisms and is essential for the usability of blockchain. As new blocks are created, they will accumulate, but the number of transactions within each block remains constrained. The Elastico protocol represents the first consensus mechanism that employs sharding concepts on the blockchain. The legal digital currency framework RSCoin, proposed by the Bank of England, also incorporates sharding technology into its permissioned blockchain to enhance scalability. While sharding technology theoretically addresses scalability issues, it introduces complexities related to cross-chain transactions, necessitating strong security assumptions and potentially diminishing blockchain security.
- Unstable consistency: The initialization process of a blockchain is crucial for confirming the stability and reliability of the consensus mechanism, as it directly impacts the safety and dependability of the subsequent consensus mechanism operations. Currently, there are two methods for initializing a blockchain; one involves using a third party to create the genesis block. This contradicts the decentralized design principles of blockchain and is unsuitable for permissionless blockchain solutions within a P2P network; it also fails to guarantee the randomness and security of the genesis block generated by the third party, possibly affecting the formation of subsequent blocks. The alternative method is to derive it from an existing natural transition; a well-established blockchain dependent on a mature PoW-based blockchain is used to create a genesis block, which adds to the complexity of the initialization process. The vulnerabilities inherent to PoW can directly compromise the security of the genesis block as well as the creation of future blocks.
- Challenging initialization and recovery: The consensus mechanism provides blockchain with immutability and enhances its reliability, but it also complicates the process of recovery. If the security is compromised, restoring the blockchain to its state before the attack is ineffective without the intervention of trusted third parties. A hard fork [105,106] currently stands as the only viable method for reconstructing the blockchain. Nonetheless, there are numerous constraints associated with hard-fork reconstruction, and the hard-fork process may lead both parties to lose interest in these legal transactions.

Incentive Layer:

In a permissionless blockchain, the incentive and consensus layers are interconnected, working together to ensure the security and stability of the blockchain system. The design of the consensus mechanism will influence the choice of incentive participants and the strategy for distributing rewards; likewise, the design of the incentive mechanism is linked to the security of the consensus process and the overall stability of the blockchain. Nodes that engage in transaction validation and block creation to earn higher rewards might adopt strategies that are detrimental to maintaining the system, which could even pose security risks. Consequently, the incentive layer requires the detection of strategic behavior and the optimization of a dynamic reward system.

- The selfish mining attack: Under ideal conditions, a node should receive mining rewards proportional to its computational power in a Proof of Work (PoW) blockchain; however, in practice, certain nodes may obtain rewards exceeding their fair share, resulting in a selfish mining attack. This type of attack, proposed by Eyal in 2013, targets PoW and is challenging to identify and prevent. In theory, PoW-based permissionless blockchain systems can be vulnerable to selfish mining, which represents a significant risk to system security and the fairness of the incentive mechanism.
- Block withholding: Mining pools lower the barriers for nodes to engage in mining, enabling broader participation for reward acquisition. However, some mining pools might exploit the reward distribution strategies of their target mining pools to carry out block-withholding attacks that yield higher rewards. This can involve tasking certain miners with joining the target mining pool to generate an invalid workload, thus sharing in the target pool’s rewards while ultimately seeking greater compensation from their mining pool.
- Unsustainable problem: The incentive structures of cryptocurrencies like Bitcoin encompass block rewards and transaction fees, yet the primary income for miner nodes increasingly diminishes due to capped block rewards. As block rewards dwindle, these blockchains are forced to rely solely on transaction

fees, which raises sustainability concerns. Research by Carlsten has examined the viability of blockchains that depend exclusively on transaction fees to incentivize nodes, highlighting the difficulty of avoiding a tragedy of the commons scenario. This can lead to numerous blockchain forks, undermining the security and efficiency of the blockchain. Nevertheless, the inflation associated with continuous token issuance means that block rewards may lose their allure over time.

3.3. Layer of Contracts:

A smart contract is a digital program that executes automatically based on agreed-upon terms between a buyer and a seller, encompassing the necessary code and data designed for deployment, forming the foundation of the contract layer. Ethereum is the first open-source platform for developing smart contracts because it is accessible to everyone and facilitates digital currency transactions; any exploitation of code vulnerabilities can lead to irreversible losses.

- Vulnerable code: Ethereum employs a scripting language for creating smart contracts, making it challenging to eliminate vulnerabilities. Based on a survey of smart contracts, various types of attacks on Ethereum smart contracts include transaction-ordering (TOD) attacks, timestamp dependency attacks, DAO(decentralize autonomous organization) attacks, stack size limit attacks, immutable bugs attacks, gas-less send attacks, re-entrance attacks, and short address attacks.
- Issues with external data sources: While blockchain technology aims to provide secure payment methods without a trusted third party, smart contracts must obtain external data through reliable technology to interact with the outside world. The TLSNotary and Towncrier methods utilize the HTTPS(hypertext transfer) protocol to access external data but fail to ensure consistent and authentic data across different nodes and cannot prevent malicious alterations by the data provider's website or attacks that may lead to a single point of failure. The Auger approach requires particular users to deliver results at designated times through a penalty system yet does not offer users a way to access the system freely, limiting its practicality.
- Imperfections in formal verification: The security issues highlighted by Ethereum's EVM pose risks to the execution of smart contracts and the digital assets of users; therefore, formal verification and program analysis tools are needed to scrutinize the smart contract code and its execution. However, most available tools focus solely on detecting and verifying known vulnerabilities, underscoring the need for future research into existing anti-patterns and program analysis for real-time detection.

•Concerns regarding privacy protection: Both Ethereum and Hyperledger function as open-source platforms. Smart contracts engage numerous users, and the execution of transactions necessitates users to share transaction details. Similar to the data layer, cryptography serves as a technical foundation for enhancing the privacy features of smart contracts. Some applications that require high levels of confidentiality and have intricate functions present challenges in the design and coding of smart contracts. Additionally, cryptography has its constraints in real-world applications.

3.4. Application Layer:

Blockchain technology has found diverse applications in sectors such as finance, supply chain, and energy [118,119]. The application layer must embody the business functions relevant to various scenarios, and its architectural design may exhibit slight variations. This layer directly engages with users, necessitating a degree of uniformity in architectural design. Typically, the application layer comprises an API interface, cross-chain heterogeneity, and regulatory technology:

3.4.1. *Challenges in cross-chain operations:*

Given the plethora of heterogeneous blockchain applications, establishing connections between them through cross-chain technology is essential for creating a cohesive, interoperable, and reliable application network. Unlike traditional systems, decentralized blockchain achieves interoperability without relying on central nodes. The primary challenge faced by cross-chain technology is how to facilitate the linkage among decentralized blockchain platforms. Blockchain developers have been utilizing mechanisms such as notarization, sidechains or relay networks, hashed time-locked contracts (HTLC), and distributed private key management to enable interconnection among diverse blockchains.

3.4.2. *The absence of regulatory technology:*

Security incidents akin to those occurring in darknet transactions, ransomware attacks, and the theft of digital assets in Bitcoin and Ethereum have ignited significant discussions within the community concerning the insufficient oversight of blockchain platforms. Oversight technology involves the reporting, tracking, and accountability of unlawful activities to safeguard the integrity of the blockchain platform's content. However, the decentralized nature, immutability, and complexity of blockchain systems create challenges in establishing an effective oversight mechanism. As the most developed blockchain platform with the highest usage demand, Bitcoin has naturally taken the lead in exploring supervisory technology. Given that the data monitoring and analysis strategies utilized by the network typically employ a "one-size-fits-all" approach, there is a risk of compromising legitimate users who often use Bitcoin for lawful transactions; consequently, the supervisory technology used for Bitcoin is inherently unsuitable for other blockchain mining platforms.

3.4.3. *Additional attacks:*

During the development of the application layer, code vulnerabilities can arise, particularly in scenarios involving third-party platforms, increasing the risk of unauthorized exploitation. Furthermore, in a multi-party blockchain environment, an attacker may gain control over the application software or hardware within their access rights, executing a MATE attack (man-at-the-end attack) [121], breaching application layer protocol standards or industry regulations, and maliciously exposing or altering user information, thus compromising the confidentiality and integrity of data. Given these considerations, despite its numerous security shortcomings, cybersecurity professionals have numerous strategies at their disposal to address these challenges, facilitating the design of more resilient security protocols within a distributed framework. IT specialists equipped with strong analytical and technical skills are ideally suited to implement blockchain technology in the most secure way possible. Therefore, comprehending every aspect influencing blockchain security is essential.

4. Discussion

4.1. Concerns Regarding the Security of Blockchain Technology:

Blockchain presents numerous applications within the healthcare sector, assisting researchers in unraveling genetic data by facilitating secure exchanges of patient medical information, managing the pharmaceutical supply chain, and guaranteeing the secure transfer of data. The explanations highlight the principles of cryptography, immutability, and decentralization, which seem to ensure security due to cryptographic protections and the assurance that data is infrequently altered without the knowledge of other participants. Cryptographic algorithms are pivotal in the execution of the data security framework. Although blockchain is not impervious to cyber threats and fraud, it is a sophisticated emerging technology that necessitates thorough scrutiny and has faced multiple security breaches, revealing its vulnerabilities at different levels. There are various major security issues and preventive strategies related to blockchain. One notable issue is the 51% attack: the primary role of miners is to validate transaction requests and compile data, which allows them to pursue the subsequent block. A 51% attack represents one of the most significant dangers in the blockchain domain since it permits manipulation of the entire blockchain, especially during its initial phases when the number of miners is limited. To reduce this risk, it is crucial to increase the hash rate, enhance monitoring of mining pools, and avoid utilizing proof-of-work (PoW) consensus mechanisms to prevent 51% of attacks.

5. Conclusions

In this research, a detailed explanation has been presented for blockchain and security as a systematic approach. the author thorughly go through gives the discussions of architecture of blockchain with a security persepective, emerging technological and mechanism deployments with fundamental algorithms. Nowadays, with the immense use of technology, security becomes vital as a broot force. Idealogy truthness is the first entry as you show conficidentnality than as go with organizations. Scalability, interoperability, privacy and security, selfish mining, quantum resilience, and a lack of governance and standards are some of the current research and industry obstacles to implementing the Blockchain for various applications, as the paper has illustrated. There are still a lot of problems with the widespread use of blockchain applications. Blockchains will become more scalable, efficient, and durable as a result of this. Both open concerns and smart contract challenges are noted to be addressed in future research based on the survey's results. Lastly, we talked about smart contract trends for the future. Stakeholders interested in smart contract research can benefit from the information this study offers.

References

1. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161. [CrossRef
2. .Caldarelli, G.; Ellul, J. Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. Appl. Sci. 2021, 11, 1842. [CrossRef1]
3. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161. [Google Scholar]
4. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E. Bani-HaniBlockchain smart contracts: Applications, challenges, and future trends. Peer Peer Netw. Appl. 2021, 14, 2901–2925. [CrossRef]
5. M. L. Hossain, A. Abu-Siada, S. M. Muyeen, M. M. Hasan and M. M. Rahman, "Industrial IoT based condition monitoring for wind energy conversion system", CSEE J. Power Energy Syst., vol. 7, no. 3, pp. 654-664, May 2021Rupa, C.; Midhunchakkaravarthy, D.; Hasan, M.K.; Alhumyani, H.; Saeed, R.A. Industry 5.0: Ethereum blockchain technology-based DApp smart contract. Math. Biosci. Eng. 2021, 18, 7010–7027
6. M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Int. J. Surg. 2021, 88, 105906
7. Ahmad, W.; Rasool, A.; Javed; Baker, A.R.T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics 2022, 11, 16Mukherjee, P.; Pradhan, C. Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology.
8. Blockchain Technology: Applications and Challenges; Springer: Cham, Switzerland, 2021; pp. 29–49.
9. Aggarwal, S.; Kumar, N.; Alhussein, M.; Muhammad, G. Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead. IEEE Network 2021, 35, 20–29. [CrossRef]
10. Choi, T.-M.; Siqin, T. Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. Transp. Res. Part E Logist. Transp. Rev. 2022, 160, 102653. [CrossRef]
11. Kazmi, S.H.A.; Masood, A.; Nisar, K. Design and analysis of multi efficiency motors based high endurance multi rotor with central thrust. In Proceedings of the 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 13–15 October 2021; IEEE: New York, NY, USA, 2021; pp. 1–4.
12. Moke, K.C.; Low, T.J.; Khan, D. IoT Blockchain Data Veracity with Data Loss Tolerance. Appl. Sci. 2021, 11, 9978. [CrossRef]
13. Jameel, F.; Javaid, U.; Khan, W.; Aman, M.; Pervaiz, H.; Jäntti, R. Reinforcement Learning in Blockchain-Enabled IoT Networks: A Survey of Recent Advances and Open Challenges. Sustainability 2020, 12, 5161. [CrossRef]
14. Lakshmi, G., Thiyagarajan, G.: Decentralized energy to power rural homes through smart contracts and carbon credit. 2021 7th International Conference on Electrical Energy Systems (ICEES), Chennai, India, pp. 280–283 (2021)Tanwar, S. Blockchain Revolution from 1.0 to 5.0: Technological Perspective. In Blockchain Technology; Springer: Singapore, 2022;
15. pp. 43–61.
16. Kairaldeen, A.R.; Abdullah, N.F.; Abu-Samah, A.; Nordin, R. Data Integrity Time Optimization of a Blockchain IoT Smart Home Network Using Different Consensus and Hash Algorithms. Wirel. Commun. Mob. Comput. 2021, 2021, 4401809.
17. Talukdar, I.; Hassan, R.; Hossein, S.; Ahmad, K.; Qamar, F.; Ahmed, A.S. Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature. Wirel. Commun. Mob. Comput. 2021, 2021, 6693316. [CrossRef]K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," IEEE Access, vol. 8, pp. 85714-85728, 2020.Qureshi, A.; Jiménez, D.M. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. Appl. Sci. 2020, 11, 1.
18. Billy Rennekamp Aditya, Gavin. 2021. Interchain Security. https://github.com/cosmos/gaia/blob/main/docs/interchain-security.md.
19. J. Lisjak, M. Roić, H. Tomić, and S. M. Ivić, "Croatian LADM profile extension for state-owned agricultural land management," Land, vol. 10, no. 2, pp. 222, Feb. 2021.
20. Cai Y, Fragkos G, Tsiropoulou EE, Veneris A. A truth-inducing sybil-resistant decentralized blockchain oracle. In: 2020 2nd conference on blockchain research & applications for innovative networks and services (brains) IEEE.

Paris, France; 2020: 128-135

21. Yang, G.; Lee, K.; Lee, K.; Yoo, Y.; Lee, H.; Yoo, C. Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric. IEEE Access 2022, 10, 74902–74920.
22. GaiK. et al. Blockchain meets cloud computing: A survey IEEE Commun. Surv. Tutor. (2020).
23. Jonathan Rankin, Chris Elsden, Ian Sibbald, Alan Stevenson, Chris Speed, and John Vines. 2020. Designing artifacts and roleplay to understand decentralized identity management systems. Proceedings of the ACM on Designing Interactive Systems (2020), 1593–1606]
24. Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, et al., "A survey on metaverse: Fundamentals security and privacy," IEEE Commun. Surveys Tuts., vol. 25, no. 1, pp. 319-352, 1st Quart. 2023.]
25. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Comput. Appl. 2022, 34, 11475–11490. [CrossRef]
26. Odeh, A.; Keshta, I.; Abu Al-Haija, Q. Analysis of Blockchain in the Healthcare Sector: Application and Issues. Symmetry 2022, 14,
27. 1760. [CrossRef]
28. Tandon, A.; Dhir, A.; Islam, A.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Comput. Ind. 2020, 122, 103290. [CrossRef]
29. Sarkar, A.; Maitra, T.; Maitra, T.; Neogy, S. Blockchain in the healthcare system: Security issues, attacks and challenges. In Blockchain Technology: Applications and Challenges; Springer: Cham, Switzerland, 2021; pp. 113–133.
30. Chelladurai, U.; Pandian, S. A novel blockchain based electronic health record automation system for healthcare. J. Ambient. Intell. Humaniz. Comput. 2021, 13, 693–703. [CrossRef]
31. Fatima, N.; Agarwal, P.; Sohail, S.S. Security and privacy issues of blockchain technology in health care—A review. In ICT Analysis Applications; Springer: Singapore, 2022; pp. 193–201.
32. Denter, N.M.; Seeger, F.; Moehrle, M.G. How can Blockchain technology support patent management? A systematic literature review. Int. J. Inf. Manag. 2022, 102506
33. Azizi, N.; Akhavan, P.; Philsoophian, M.; Davison, C.; Haass, O.; Saremi, S. Exploring the Factors Affecting Sustainable Human Resource Productivity in Railway Lines. Sustainability 2022, 14, 225
34. A.M. Votto, R. Valecha, P. Najafirad, H.R. Rao Artificial Intelligence in Tactical Human Resource Management: A Systematic Literature Review International Journal of Information Management Data Insights, 1 (2) (2021), Article 100047
35. Papadopoulos P, Abramson W, Hall AJ, Pitropakis N, Buchanan WJ (2021) Privacy and trust redefined in federated machine learning. Mach Learn Knowl Extract 3(2):333–356
36. Mentzer, K., Frydenberg, M., & Yates, D. J. (2020). Teaching applications and implications of blockchain via project-based learning: A case study. Information Systems Education Journal, 18(6), 57–85.
37. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161
38. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E. Bani-HaniBlockchain smart contracts: Applications, challenges, and future trends. Peer Peer Netw. Appl. 2021, 14, 2901–2925
39. Mukherjee, P.; Pradhan, C. Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology. In Blockchain Technology: Applications and Challenges; Springer: Cham, Switzerland, 2021
40. Bécue A, Praça I, Gama J (2021) Artificial intelligence, cyber-threats and industry 4.0: challenges and opportunities. Artif Intell Rev 54(5):3849–3886
41. Alazzam H, Sharieh A, Sabri KE (2020) A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. Expert Syst Appl 148:113249
42. Di Mauro M, Galatro G, Liotta A (2020) Experimental review of neural-based approaches for network intrusion management. IEEE Trans Netw Serv Manag 17:2480–2495
43. Injadat M, Moubayed A, Nassif AB, Shami A (2020) Multi-stage optimized machine learning framework for network intrusion detection. IEEE Trans Netw Serv Manag
44. Hasan, H.R.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M.; Ellahham, S. Blockchain-Enabled Telehealth Ser-vices Using Smart Contracts. IEEE Access 2021, 9, 151944–151959. [CrossRef]
45. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. Int. J. Healthc. Manag. 2022, 15, 70–83. [CrossRef]

46. X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems", Future Generation Computer Systems, vol. 107, pp. 841-853, 2020..
47. M. Shahbaz et al. Probing the factors influencing cloud computing adoption in healthcare organizations: a three-way interaction model Technol. Soc. (2022)D. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey
48. Abdali, T.-A.N.; Hassan, R.; Aman, A.M.; Nguyen, Q.N. Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues. IEEE Access 2021, 9, 75961–75980. [CrossRef]
49. Khalil, A.M.U.; Lai, D.T.C.; King, O.S. Cluster analysis for identifying obesity subgroups in health and nutitional status survey data. Asia-Pac. J. Inf. Technol. Multimed. (APJITM) 2021, 10, 146–169.
50. T. F. Stafford and H. Treiblmaier, "Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records", IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1340-1362, Nov. 2020[CrossRef
51. D. Chen et al., "MAGLeak: A learning-based side-channel attack for password recognition with multiple sensors in IIoT environment", IEEE Trans. Ind. Informat., vol. 18, no. 1, pp. 467-476, Jan. 2022..
52.
53. K. Sethi, A. Pradhan and P. Bera, "Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation", J. Inf. Security Appl., vol. 51, Apr. 2020.]
54. S. Banerjee et al., "Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment", J. Inf. Security Appl., vol. 53, Aug. 2020]
55. S. Gaudin, W. Raza, J. Skordis, A. Soucat, K. Stenberg and A. Alwan, "Using costing to facilitate policy making towards universal health coverage: Findings and recommendations from country-level experiences", BMJ Global Health, vol. 8, no. 1, Jan. 2023]
56. D. Li, L. Huang, B. Ye, F. Wan, A. Madden and X. Liang, "FSRM-STS: Cross-dataset pedestrian retrieval based on a four-stage retrieval model with Selection–Translation–Selection", Future Gener. Comput. Syst., vol. 107, pp. 601-619, 2020.]
57. Caruccio L et al (2022) A decision-support framework for data anonymization with application to machine learning processes. Inf Sci 613:1–32
58. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161.
59. Ghazal, T.M.; Hasan, M.K.; Alshurideh, M.T.; Alzoubi, H.M.; Ahmad, M.; Akbar, S.S.; Al Kurdi, B.; Akour, I.A. IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review. Future Internet 2021, 13, 218. [CrossRef]
60. Agrawal T.K., Kumar V., Pal R., Wang L., Chen Y. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry Computers & Industrial Engineering, 154 (2021), Article 107130.
61. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. Electronics 2020, 9, 94. [CrossRef]
62. S. Madhavan et al., "Use of electronic health records to support a public health response to the COVID-19 pandemic in the United States: A perspective from 15 academic medical centers", J. Amer. Med. Inform. Assoc., vol. 28, no. 2, pp. 393-401, 2021.
63.
64. Malik H., Farooq M. S., Khelifi A., Abid A., Nasir Qureshi J. and Hussain M., “A Comparison of Transfer Learning Performance Versus Health Experts in Disease Diagnosis From Medical Imaging,” in IEEE Access, vol. 8, pp. 139367–139386, 2020 [CrossRef]
65. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. J. Food Qual. 2021, 2021, 7608296. [CrossRef]
66. Naresh, V.S.; Pericherla, S.S.; Murty, P.S.R.; Sivaranjani, R. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions. Comput. Syst. Sci. Eng. 2020, 35, 411–421. [CrossRef]
67. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security aspects of blockchain technology intended for industrial applications. Electronics 2021, 10, 951. [CrossRef]
68. Kamruzzaman, M.M.; Yan, B.; Sarker MN, I.; Alruwaili, O.; Wu, M.; Alrashdi, I. Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities. J. Healthc. Eng. 2022, 2022, 9957888. [CrossRef] [PubMed]
69. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. Int. J. Intell. Netw. 2021, 2, 130–139. [CrossRef]

70. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and smart healthcare security: A survey. Procedia Comput. Sci. 2020, 175, 615–620. [CrossRef]
71. Lin, S.Y.; Zhang, L.; Li, J.; Ji, L.L.; Sun, Y. A survey of application research based on blockchain smart contract. Wirel. Netw. 2022,
72. 28, 635–690. [CrossRef]
73. Liu, J.; Zhao, J.; Huang, H.; Xu, G. A novel logistics data privacy protection method based on blockchain. Multimed. Tools Appl.
74. 2022, 81, 23867–23887. [CrossRef]
75. Ramzan, S.; Aqdus, A.; Ravi, V.; Koundal, D.; Amin, R.; Al Ghamdi, M.A. Healthcare applications using blockchain technology: Motivations and challenges. IEEE Trans. Eng. Manag. 2022, 1, 1–17. [CrossRef]
76.
77. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. IEEE Access 2021, 9, 37397–37409. [CrossRef]
78. Bai, T.; Hu, Y.; He, J.; Fan, H.; An, Z. Health-zkIDM: A Healthcare Identity System Based on Fabric Blockchain and Zero- Knowledge Proof. Sensors 2022, 22, 7716. [CrossRef]
79. Vyas, S.; Shabaz, M.; Pandit, P.; Parvathy, L.R.; Ofori, I. Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture. J. Food Qual. 2022, 2022, 4228448. [CrossRef]
80. Li, D.; Deng, L.; Cai, Z.; Souri, A. Blockchain as a service models in the Internet of Things management: Systematic review. Trans. Emerg. Telecommun. Technol. 2022, 33, e4139. [CrossRef]
81. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Jolfaei, A.; Islam, A.N. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. J. Parallel Distrib. Comput. 2023, 172, 69–83. [CrossRef]
82. Abu-Elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-Alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. Int. J. Med. Inform. 2020, 142, 104246. [CrossRef]
83. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161.
84. UmaMaheswaran, S.K.; Prasad, G.; Omarov, B.; Abdul-Zahra, D.S.; Vashistha, P.; Pant, B.; Kaliyaperumal, K. Major Challenges and Future Approaches in the Employment of Blockchain and Machine Learning Techniques in the Health and Medicine. Secur. Commun. Netw. 2022, 2022, 5944919. [CrossRef]
85. Mecozzi, R.; Perrone, G.; Anelli, D.; Saitto, N.; Paggi, E.; Mancini, D. Blockchain-related identity and access management challenges: (de) centralized digital identities regulation. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; IEEE: New York, NY, USA, 2022; pp. 443–448.
86. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161
87. Shah, A.A.; Piro, G.; Grieco, L.A.; Boggia, G. A review of forwarding strategies in transport software-defined networks. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.
88.
89. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 2020, 8, 21091–21116
90.
91. Wang, Z.; Jin, H.; Dai, W.; Choo, K.-K.R.; Zou, D. Ethereum smart contract security research: Survey and future research opportunities. Front. Comput. Sci. 2020, 15, 1–18. [CrossRef
92.
93. Aruna, M.G.; Hasan, M.K.; Islam, S.; Mohan, K.G.; Sharan, P.; Hassan, R. Cloud to cloud data migration using self sovereign identity for 5G and beyond. Clust. Comput. 2021, 25, 2317–2331. [CrossRef
94.
95. MIslam, R.; Rahman, M.; Mahmud, M.; Rahman, M.; Mohamad, M.H.S. A Review on blockchain security issues and challenges. In Proceedings of the 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 7 August 2021; IEEE: New York, NY, USA, 2021; pp. 227–232.

96. Ahmed, M.M.; Hasan, M.K.; Shafiq, M.; Qays, O.; Gadekallu, T.R.; Nebhen, J.; Islam, S. A peer-to-peer blockchain based interconnected power system. Energy Rep. 2021, 7, 7890–7905. [CrossRef
97. Schär, F. Blockchain forks: A formal classification framework and persistency analysis. Singap. Econ. Rev. 2020, 101712, 1–11.
98. [CrossRef]
99. Yiu, C. An Overview of Forks and Coordination in Blockchain Development. arXiv 2021, arXiv:2102.10006.
100. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. Wirel. Pers. Commun. 2023, 1. [CrossRef]
101. Badruddoja, S.; Dantu, R.; He, Y.; Upadhayay, K.; Thompson, M. Making smart contracts smarter. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, NSW, Australia, 3–6 May 2021; IEEE: New York, NY, USA, 2021; pp. 1–3.
102. Al-E'mari S, Anbar M, Sanjalawe Y, Manickam S, Hasbullah I (2022) Intrusion detection systems using blockchain technology: a review, issues and challenges. Comput Syst Sci Eng 40(1)
103. Ladleif, J.; Weber, I.; Weske, M. External data monitoring using oracles in blockchain-based process execution. In Proceedings of the International Conference on Business Process Management, Rome, Italy, 6–10 September 2020; Springer: Cham, Switzerland, 2020; pp. 67–81.
104. Zhu Y, Zhang X, Ju ZY, Wang C (2020) A study of blockchain technology development and military application prospects. J Phys: Conf Ser 1507
105. Khalil, A.I.; Rahman, M.S. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. Appl. Sci.2022, 12, 11039
106. Ellul, J.; Galea, J.; Ganado, M.; Mccarthy, S.; Pace, G.J. Regulating blockchain, DLT and smart contracts: A technology regulator's perspective. In ERA Forum; Springer: Berlin/Heidelberg, Germany, 2020; Volume 21, pp. 209–220
107. Sun, W.; Fang, H.; Zheng, S.; Qian, Q. Blockchain and homomorphic encryption for digital copyright protection. In Proceedings of the 2020 IEEE Intl Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020; IEEE: New York, NY, USA, 2020; pp. 754–761.
108. Singh, S.; Hosen, A.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access 2021, 9, 13938–13959. [CrossRef
109. Guo, H.; Yu, X. A survey on blockchain technology and its security. Blockchain Res. Appl. 2022, 3, 100067. [CrossRef]
110. Hussain, H.A.; Mansor, Z.; Shukur, Z. Comprehensive Survey and Research Directions on Blockchain Iot Access Control. Int. J. Adv. Comput. Sci. Appl. 2021, 12, 2021. [CrossRef
111. Kashyap, S.; Bhushan, B.; Kumar, A.; Nand, P. Quantum blockchain approach for security enhancement in cyberworld. In
112. Multimedia Technologies in the Internet of Things Environment; Springer: Singapore, 2022; Volume 3, pp. 1–22
113. Bhushan, B.; Sinha, P.; Sagayam, K.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Comput. Electr. Eng. 2021, 90, 106897. [CrossRef
114. J. H. Cheon et al., "Introduction to homomorphic encryption and schemes" in Protecting Privacy Through Homomorphic Encryption, Cham, Switzerland:Springer, pp. 3-28, 2021
115. Sarma KV, Harmon S, Sanford T, Roth HR, Xu Z, Tetreault J, et al. Federated learning improves site performance in multicenter deep learning without data sharing. J Am Med Inform Assoc 2021 Jun 12;28(6):1259–64. doi: 10.1093/jamia/ocaa341
116. Barger, Y. Manevich, H. Meir and Y. Tock, "A byzantine fault-tolerant consensus library for hyperledger fabric", 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-9, 2021.
117. Jena, S.K., Barik, R.C., Priyadarshini, R.: A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. Internet Things, p. 101111, (2024)
118. Zhigang C, Gang H, Mengce Z, Xinxia S, Liqun C (2021) Bibliometrics of machine learning research using homomorphic encryption. Mathematics 9:2792, 11
119. Zhang, L.; Xu, J.; Vijayakumar, P.; Sharma, P.K.; Ghosh, U. Homomorphic Encryption-based Privacy-preserving Federated Learning in IoT-enabled Healthcare System. IEEE Trans. Netw. Sci. Eng. 2023, 10, 2864–2880

120. He Z, Zhang J, Yuan X, Zhang Y. Integrating somatic mutations for breast cancer survival prediction using machine learning methods. Front Genet. 2021; 11:1853

121. Yang, W., Dai, X., Xiao, J., Jin, H.: LDV: a lightweight DAG-based blockchain for vehicular social networks. IEEE Trans. Veh. Technol. 69, 5749–5759 (2020)

122. Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula and Z. Cai, "A survey on blockchain systems: Attacks defenses and privacy preservation", High-Confidence Comput., vol. 2, no. 2, pp. 100048, Jun. 2022

123. Workman, M. D., Luévanos, J. A., & Mai, B. (2021). A study of cybersecurity education using a present-test-practice-assess model. IEEE Transactions on Education, 65(1), 40–45

124. K. W. Kong et al., "Sphygmopalpation using tactile robotic fingers reveals fundamental arterial pulse patterns", IEEE Access, vol. 10, pp. 12252-12261, 2022

125. Jafar, U.; Aziz, M.A.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors 2022, 22, 7585.

126. Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. Wirel. Netw. 2021, 27, 55–90

127. B. Singh and S. Kumar, "Permission blockchain network based central bank digital currency", Proc. IEEE 4th Int. Conf. Comput. Power Commun. Technol. (GUCON), pp. 1-6, Sep. 2021.

128. HashimF. et al. Sharding for scalable blockchain networks SN Comput. Sci. (2022)

129. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. IEEE Trans. Ind. Inform.

130. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.

131. Grishin, D., Raisaro, J. L., Troncoso-Pastoriza, J. R., Obbad, K., Quinn, K., Misbach, M., ... & Hubaux, J. P. (2021). Citizen-centered, auditable and privacy-preserving population genomics. Nature Computational Science, 1(3), 192-198.

132. Yang, L., Tian, M., Xin, D., Cheng, Q., & Zheng, J. (2024). AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning. arXiv preprint arXiv:2402.17191.

133. Mao, W., & Wang, F. (2012). New advances in intelligence and security informatics. Academic Press.