Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.028687

REVIEW

Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey

Md. Shohidul Islam[1,*], Md. Arafatur Rahman[2], Mohamed Ariff Bin Ameedeen[1], Husnul Ajra[1], Zahian Binti Ismail[1] and Jasni Mohamad Zain[3]

[1]Faculty of Computing, Universiti Malaysia Pahang, Kuantan, 26600, Malaysia

[2]School of Engineering, Computing & Mathematical Sciences, University of Wolverhampton, Wolverhampton, UK

[3]Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Komplek Al-Khawarizmi, Universiti Teknologi MARA, Shah Alam, Selangor, 40450, Malaysia

*Corresponding Author: Md. Shohidul Islam. Email: msi.ice.ru@gmail.com

Received: 02 January 2023 Accepted: 15 May 2023 Published: 22 September 2023

ABSTRACT

Blockchain-enabled cybersecurity system to ensure and strengthen decentralized digital transaction is gradually gaining popularity in the digital era for various areas like finance, transportation, healthcare, education, and supply chain management. Blockchain interactions in the heterogeneous network have fascinated more attention due to the authentication of their digital application exchanges. However, the exponential development of storage space capabilities across the blockchain-based heterogeneous network has become an important issue in preventing blockchain distribution and the extension of blockchain nodes. There is the biggest challenge of data integrity and scalability, including significant computing complexity and inapplicable latency on regional network diversity, operating system diversity, bandwidth diversity, node diversity, etc., for decision-making of data transactions across blockchain-based heterogeneous networks. Data security and privacy have also become the main concerns across the heterogeneous network to build smart IoT ecosystems. To address these issues, today's researchers have explored the potential solutions of the capability of heterogeneous network devices to perform data transactions where the system stimulates their integration reliably and securely with blockchain. The key goal of this paper is to conduct a state-of-the-art and comprehensive survey on cybersecurity enhancement using blockchain in the heterogeneous network. This paper proposes a full-fledged taxonomy to identify the main obstacles, research gaps, future research directions, effective solutions, and most relevant blockchain-enabled cybersecurity systems. In addition, Blockchain based heterogeneous network framework with cybersecurity is proposed in this paper to meet the goal of maintaining optimal performance data transactions among organizations. Overall, this paper provides an in-depth description based on the critical analysis to overcome the existing work gaps for future research where it presents a potential cybersecurity design with key requirements of blockchain across a heterogeneous network.

KEYWORDS

Blockchain; cybersecurity; data transaction; diversity; heterogeneous

1 Introduction

Block-chain is a disintermediation technology that can bridge the gap between traditional and digital transactions in our world through decisions about security and complexity for decentralized applications with verifiable and universal access. Due to the growing demand for digital applications and their security without central third parties and intermediaries, the blockchain attracts tremendous attention from various sectors such as healthcare, industry, smart cities, intelligent transport systems, academia, e-governance, etc. as verification and proof of data transactions [1]. Significant advances in sustainable and intelligent data communication technology in software and hardware have been paved where it will continue to arise in the years ahead [2]. Nowadays, academicians and researchers show great interest in blockchain technology for transaction activities with smart contracts, digital signs, consensus methods, and time-stamped measures across the different types of applications where heterogeneous devices are interconnected for a secured network. However, with the rapid growth of information and communication technology, the heterogeneous network can play a significant role in the secure revolutionary future in today's world. A heterogeneous network (HetNet) delivers multi-services to interconnect different types of devices, technologies, operating systems, nodes, and protocols over wireless networks. Generally, HetNet can be used for data transactions of big data applications such as e-commerce, social network, etc., in our real world. Distributed data transaction mechanisms, including various sensing abilities and different wireless technologies, can be provided through IoT applications in our surrounding area [3]. The heterogeneity of wireless data transaction networks and their operations are being evolved through a variety of new technologies to get better user experience and quality of real-time services.

Our ways of life today are deeply intertwined with modern digital information technology, where cybersecurity leads a significant role in data exchange and cyber threat monitoring. Cybersecurity operates on technologies, processes, methods, hardware, and software through the computer network to protect sensitive information from misdirection, damage, or unauthorized access from outside. Cybersecurity mainly ensures data correctness and information safety during the data transaction over the network with confidentiality, integrity, and availability of data. Blockchain can be a critical factor in achieving the cybersecurity of modern digital data communication and network systems to enhance data security and privacy in the academia, health, government, agriculture, transportation, and industry sectors [4].

According to a report by Statista, the number of active internet users was 4.66 billion over the world, where there was 59.50% of the world population on January 2021. There were 4.32 billion internet users who only accessed from mobile devices. Besides, the number of active social media users was 4.20 billion, of which the number of active mobile social media users was 4.15 billion. Thus, data transactions across heterogeneous networks can be a major cause of concern for digital users in social media and global industries. Data transparency and sharing of any network is not only the major issue; data security and scalability is also an important concern for protecting digital content in the distributed network environment [5]. Further, Digital data is maintained and stored by network nodes in order to achieve the high efficiency of the transaction, but network node failures can lead to data transaction deviations where existing blockchain methods cannot consider the node failures. However, ensuring the management of data certification and integrity is another challenge where data transactions will be transparent among legal or illegal participants in the distributed network [6]. Any security vulnerability to an existing decentralized system where there is no central trusted controller and a group of users working through its storage space can lead to unauthorized access to multiple cloud storage [7].

As a result, stored data can be tampered with by unauthorized persons. Besides, in the cloud storage scenario, bandwidth diversity is another important challenge to researchers in exchanging data across heterogeneous network nodes. Consequently, regional network diversity is a more serious matter due to a large number of IoT components and their scalability for data transactions [8]. Similarly, the throughput and latency of data transactions in a distributed network are also a big issue due to the diversity of nodes and operating systems [9]. It is very important to manage data storage and transactions using the components of individual active operations through distributed blockchain network-based applications for the cybersecurity of all digital organizations. The basic framework of blockchain-based HetNet with cybersecurity is shown in Fig. 1. This framework is generally designed to take measures of privacy, scalability, integrity, or network heterogeneity for various resource transactions of any organization.

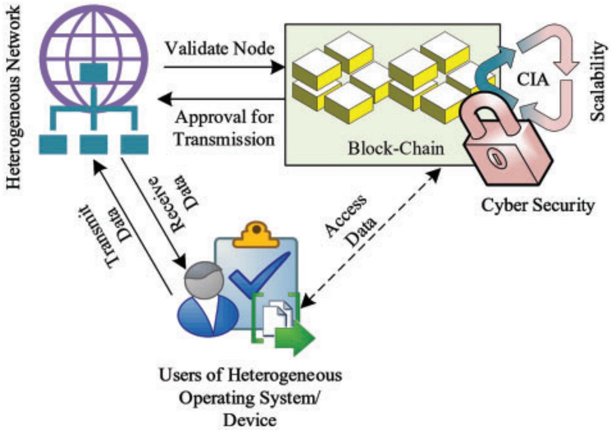

Figure 1: Basic framework of blockchain-based HetNet with cybersecurity

Taking into account the issues of existing surveys, many researchers have tried to be more involved in creating an effective framework for blockchain-based cybersecurity from multiple aspects. Although the researchers have studied in detail the existing work on three important areas, such as blockchain, cybersecurity systems, and heterogeneous networks, separately, there are limited literature surveys where the prior papers and studies in the mentioned areas have not shown their research relationship together. This survey paper is stimulated by the impressive recent developments in blockchain, cybersecurity systems, heterogeneous networks, and its future research advancement. So, to bridge such gaps, this study conducts revolutionary blockchain-based cybersecurity surveys that can be engaged in the heterogeneous network to improve its integrity, security, and effectiveness. In particular, this paper proposes a widespread review of blockchain technology in the heterogeneous network with full importance on enabling cybersecurity for high-security applications related to HetNet. The foremost contributions in this study are enumerated as follows:

1. This work assists the readers in gaining background knowledge and idea about cybersecurity, including blockchain technology for distributed networks.
2. This work presents a complete taxonomy and its modern strategies together with existing analysis and implementation of blockchain-enabled data communication technologies in HetNet for cybersecurity.

3. A comprehensive study exposes the recent technological advancements, requirements, and improvements to the operations of different portions in blockchain building cyber for various network applications.
4. This study presents a viable conceptual smart framework of the heterogeneous network that can provide blockchain-enabled cybersecurity services and their applications with real-time data transactions for overall performance and systematic improvement.
5. This study provides a wide range of open research challenges and directions for future research perspectives on blockchain-based secured cyber network opportunities by suitable indications of technological challenges and issues.

The remaining parts of this survey paper are mainly arranged through the following structure. Section 2 describes the fundamental components, concepts, and methods of blockchain-based heterogeneous network applications with cybersecurity from different aspects. Section 3 establishes a complete taxonomy and classifies the various existing approaches for blockchain building. Section 4 describes the demonstrations of a proposed framework named blockchain-enabled cybersecurity for heterogeneous networks and cross-chain mechanism in blockchain platforms for the participating organizations. Section 5 gives details of the open research issues of blockchain-associated heterogeneous networks toward cybersecurity. In the ending part, this paper is concluded in Section 6.

2 Fundamentals of Blockchain Based HetNet and Cybersecurity

2.1 Cybersecurity

Cybersecurity is a major concern in digital practice on the system and network defense from cyber-attacks that can access, modify or abolish digital data and sensitive resources. It is required to perform the model-based risk analysis and dynamic defenses [10] to address specific vulnerabilities in cybersecurity systems. Any type of cyber occurrence like as ID stealing, data breaches, cracking of security files, etc., in any organization can affect a large amount of individual data. In this case, cybersecurity can play a significant role in data privacy, and blockchain can ensure that cybersecurity overcomes internal and unauthorized access during data transactions. According to cybersecurity reports [11,12], cyber-attacks are on the rise in today's world, and ensuring the security of any organization to protect against cyber-attacks on most networks is a matter of concern. In addition, some blockchain strategies need to be developed to reduce and mark off internal security and privacy attacks which are also very important to cybersecurity in the critical digital assets of many organizations and nuclear power plants. Vulnerable cybersecurity affects the ways of personal data exchanges of companies or customers over the worldwide business network. So, it needs the execution of a blockchain-based real-time environment to control cybersecurity vulnerabilities. Thus, it is very significant to identify the factors of cybersecurity behavior [13] and to sense the intrusions through blockchain security models. Regardless, based on previous assessments, researchers need to focus deeply on cybersecurity.

2.2 Heterogeneous Network

In order to perform data transactions over the computer network, Heterogeneous Network (HetNet) incorporates various network nodes and other different computing devices [14] for the purpose of generating interconnections among them where users can access different types of customized services using significantly different operating systems and network protocols. A promising approach to the data communication paradigm can be developed to address the challenge of achieving high throughput for heterogeneous networks, and protocols [15]. The construction of HetNet can be used to enrich the quality of interconnection of different network nodes, which are arranged into hierarchical clusters and broadcast information from one type of network to another. In this system, users can utilize a number of access points across different networks in data communications. Emerging technologies of HetNet in digital data communication [16] can especially play an important role in cybersecurity. Due to the arising challenges of digital data privacy and security in resource allocation with maintaining network bandwidth scheduling, researchers need to develop a rich decentralized heterogeneous architecture. Moreover, communication protocols and their reliability and validity guarantee [17] are specifically more challenging issues in terms of HetNet operation. So, it needs to design the integration of the blockchain approach with network heterogeneity. Besides, a strong cross-disciplinary collaboration is needed to maintain a secure, efficient, and scalable data communication system across heterogeneous networks that enabled IoT. To overcome all the complexities of data transactions, specifically, it needs to focus on a rich assessment in blockchain-based HetNet systems. There is another important matter to managing the interoperability of heterogeneous distributed systems.

2.3 Adaptation of Blockchain Technology

With the adaption of blockchain technology, it is important to measure its effectiveness across heterogeneous networks to ensure the cybersecurity of decentralized applications [18]. The significant factors of adapting blockchain in a network, such as security, efficiency, scalability, or speed of data transactions, can be major challenges for reliable service delegations [19] in any organization. The adaption of blockchain technology can provide better quality services to users, save product transaction time, and make better supply chain management. Users can track all ingredients of their services in the digital heterogeneous network environment. In this case, there is a big concern about the technical complexity of blockchain-based cybersecurity systems. The adaption of blockchain technology in a distributed environment is depicted in Fig. 2.

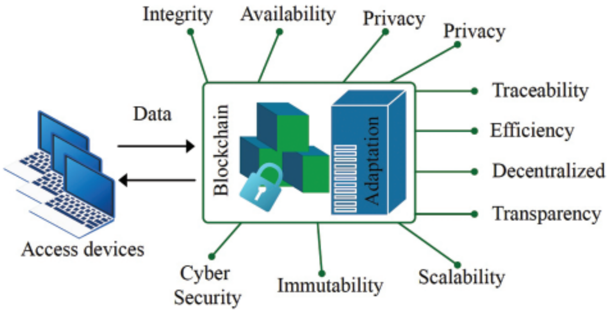

Figure 2: Adaption of blockchain technology

There is a need to develop a technical adaption of block-chin application in today's industries or companies for its data confidentiality, integrity, and availability through dynamic encryption scheme and cross-chain protocol [20] in distributed and wireless network. In order to achieve the advanced digital life factors through high-quality data transactions, such industries or organizations can consider the process of adaptation together to store the impenetrable data. However, it needs to replace the existing network systems with scalable and integrating systems for the block transactions per second in blockchain-based distributed heterogeneous network [21]. Researchers can design blockchain-based distributed networks in cybersecurity by developing user confidentiality, data transparency, traceability, authentication, immutability, safe storage with data processing, and secure data transfers without failures [22]. However, in cybersecurity, blockchain can provide robust safeguards in healthcare, transportation, crypto-currency, etc., against data tampering.

3 Taxonomy of Blockchain-Based Cybersecurity in HetNet with a Critical Review of Existing Works

Most of the existing applications of blockchain technology on heterogeneous networks represent a variety of designs that can be figured out as an important component of cybersecurity during data transactions. Owing to the blockchain-based features and functionalities upgrade, the security of scalable decentralized network-aided designs [23,24] is being developed faster for the quality of digitized transactions and making it more transparent. However, this paper introduces different approaches associated with blockchain-enabled cybersecurity to present various challenging issues using the recent existing heterogeneous network-aided technologies. To study the various mechanisms and key concepts of blockchain-based cybersecurity from recent research papers, the complete taxonomy of blockchain building is described in detail and established in Fig. 3. Based on the design, methods, consensus protocol, decentralized transactions, and operations, this taxonomy has been classified as blockchain technology, cybersecurity based on blockchain, and heterogeneous networks related to cyber. Then, other approaches have been categorized according to the perspective of state-of-the-art blockchain infrastructural design and its strongest method. Besides, in this section, the recent trends and comparative explorations in Blockchain based network applications from the security perspective of each appraised research work are shown in Tables 1 and 2. The mentioning of various traditional approaches can further support enhancing the research quality in this sector.

3.1 Cyber Attacks on Distributed Networks

The major cyber attacks and security risks that occur during data transactions or storage over the network are included below in this section of the paper. Based on affecting the protection of user data transactions and blockchain operations, cyber-attacks on distributed networks can be classified as centralization attacks, integrity attacks, hash-based attacks, network intrusion attacks, social engineering attacks, and so forth. In this case, unauthorized or illegal users target the instant of data transaction creation, block formation, mining, validation processes, key generation, user wallets, contracts, pools, and so on. Hence, it is necessary to focus on the impact of the following attacks to implement security and authenticity measures in the blockchain-based network. Cyber attacks on distributed network have been demonstrated in Fig. 4.

3.1.1 Centralization Attack

Selfish mining is a policy of the originating mining income where a group or miners carry away the block rewards, which are one of its vulnerabilities in blockchains [25]. In this policy, generated new blocks of it are not immediately released to the network and remain isolated from the standard protocol. In this situation, a selfish mining attack [26] can happen in the network at any time, and attackers undermine the integrity of the heterogeneous network for malicious purposes. In this strategy, it provides miners an increase in revenue compared to the amount of performing work in the distributed network [27], but only the corrupt miners conceal the mine blocks from others and harm the innocent miners by helping to make the distrust on the integrity of blockchain network. The selfish miners intentionally push to increase their rewards for making secret chains by withholding their personal blocks and trying to reveal them publicly, creating confusion among honest miners. At the same time, they continue to vex the fair miners and their authorities to collect more rewards. For this undesirable scenario, honest miners [28] cannot broadcast their transactions in the network.

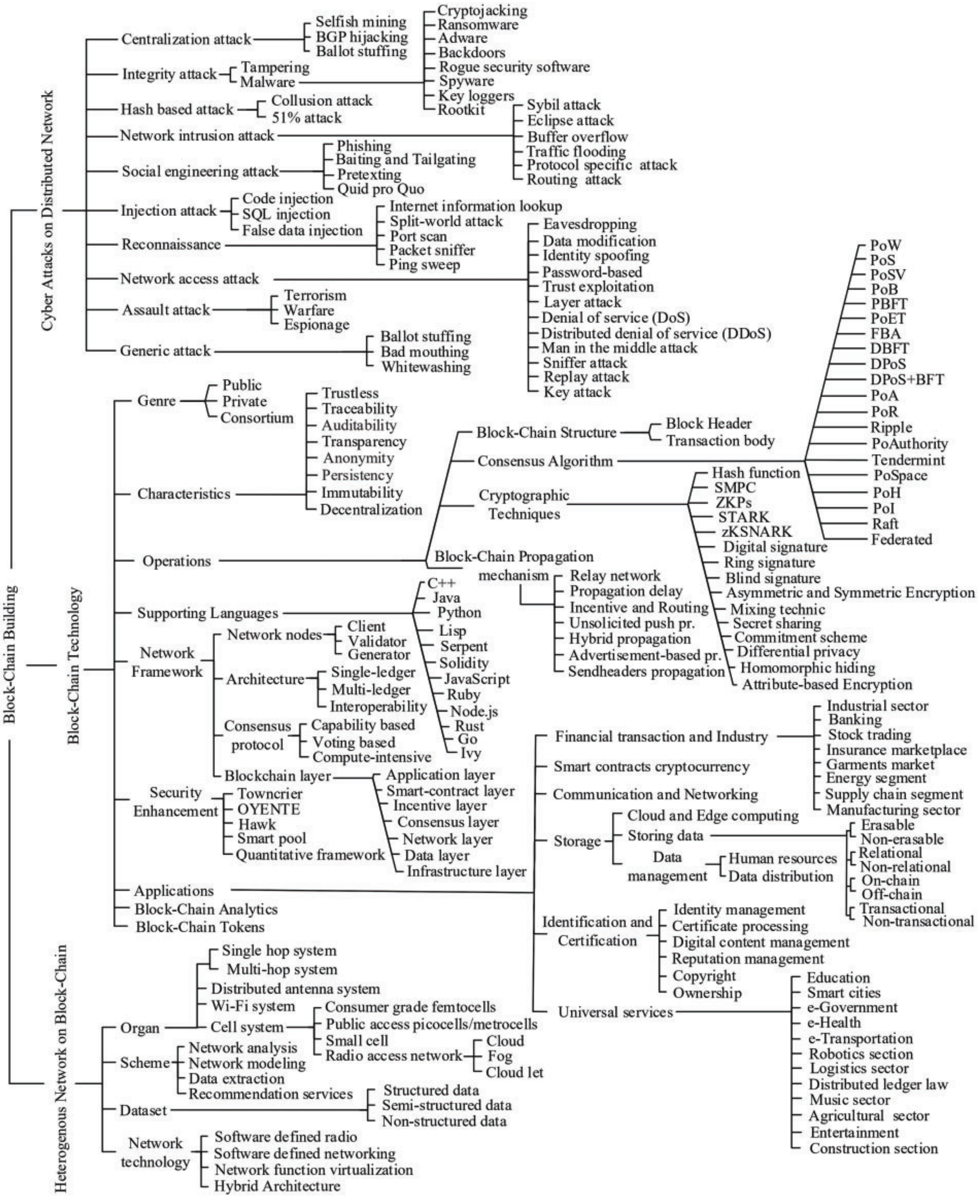

Figure 3: Taxonomy of blockchain building

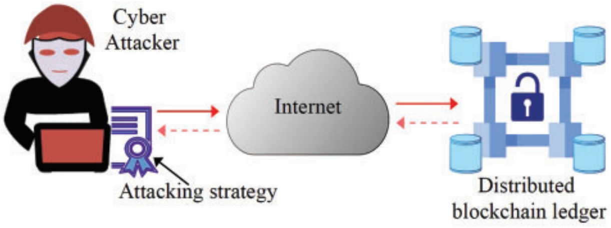

Figure 4: Cyber attacks on distributed network

Border Gateway Protocol (BGP) provides the legislation of IP-packets connectivity and transportation among autonomous systems through forwarding to their desired destination, which is known as the de-facto inter-domain routing protocol of the network [29]. The accuracy and validity of packet route announcements are not verified in BGP management [30] where multiple large-scale networks are interconnected without a traffic controller or administrating system. Due to inefficient routing management, the optimal route for data packets to travel to their targeted IP address is not determined, and data packets may take a long time to reach the desired destination or may never arrive. In this case, attackers can manipulate or hijack the BGP routing system to intercept the blockchain network traffic. For that, BGP hijacking [31] can control the distribution network operators by manipulating the network-level and node-level transactions as well as influence the distribution of mining power due to the high centralization of mining pools. The BGP hijackers [32] can steal cryptocurrency from the sufferer users by splitting or changing the network miner connections from the mining pool server. However, the attackers or spammers can apply the BGP hijacking technique in order to make deception in legitimate IPs.

In general, malicious users can execute the **Ballot stuffing** process even by evading system user monitoring or system surveillance [33]. The malicious recommenders take an attempt to boost the level of their accomplice's trust by applying their good recommendations so that they can achieve their hypocritical objectives [34]. They elected their accomplices as a forward attacker for the commit of crimes. The malicious user nodes also throw the well-behaved nodes on the blacklist for doing incidents of invisible crimes [35]. In this case, ballot-stuffing attackers [36] enlarge their reputation by their self-announcement, including positive feedback from each other and concealing the incompatible intentions to the higher authorities. In consequence, all trust models are devoted to recommendation trusts directly and indirectly, which can be easily affected by ballot-stuffing attacks [37]. The e-voting model can be faced with ballot-stuffing attacks.

3.1.2 Integrity Attack

Tampering as a cyber-attack [38] can create an insecure situation in the use case of several stages in web-based applications. Attackers can easily partially modify the parameters of various digital applications for wireless communication by stealthily evading the consciousness of users or controllers. Blockchain network nodes may experience data tampering attacks [39] during the block transactions. If offenders can steal the user's private key, they will easily make tampering with blockchain accounts as well as they will try to control all information of legitimate users [40]. Sometimes, attackers can make tempering the different software or source codes by inserting and deleting code randomly to fulfill their desired purpose like as malicious activity, copyright infringement, etc. The learning and analysis of blockchain [41] can avoid data tampering and protect the records against modification attempts. Due to the increasing prevalence of cryptocurrency, cybercriminals have turned their attention to gaining cryptocurrencies by using malware-based, or browser-based **Cryptojacking** activities [42] that is a global problem. Cryptojacking-based malware [43,44] variants slow down the computer systems which are infected to take control of various organizations, consumers, or industries so that they can speed up their activities illegally. Hackers or cyber criminals ensure their activities by sending a malicious link in the victim's emails, which by clicking on the links automatically impose crypto mining code on the victim's systems or automatically install JavaScript code in the victim's browser [45]. Also, this method utilizes the bandwidth and electricity processing capabilities of internet users on behalf of illegal attackers. Cryptojacking injection, browser extensions, or antivirus programs can afford limited protection from crypto-jacking issues or attacks.

Crypto-**ransomware** [46] is one of the most challenging threats to cybersecurity in today's world, which can damage the performance of thousands of businesses worldwide in general. The spread of ransomware is continuously evolving through different strains, and it is becoming increasingly difficult to prevent these attacks by traditional identification systems to protect our financial contents. Crypto-ransomware is a sophisticated malware program [47] where hackers install these programs on phishing websites during currency transactions to encrypt the victim data stored on computers or other devices. Ransomware obstructs users from accessing their devices or systems, and the victims suffer significant financial losses across different domains. Most of the time, ransomware mainly targets the different types of windows platforms due to the ignorance of the users and attacks these platforms [48]. Users can protect their data and system from ransomware by practicing secure computing activities and using up-to-date security software, as well as needs dynamic analysis of ransomware to save the user activities in the network.

Adware is an undesirable malware software [49] that is a major issue for cyber users. It is often referred to as advertising-supported software that is generated automatically from the internet and can infect any computer or device without the user's knowledge, although different types of advertising are not illegal online [50]. Generally, in order to instruct for automatically installing malicious code on the user system, adware induces the online users to click on the ad in the different system interface without any experience. Malicious adware [51] easily enters the system due to a pop-up ad. However, it is important to improve cybersecurity by using blockchains to protect user personal information by preventing such malware.

A malicious software program called **spyware** can use various operating system-based smartphones or computers to harm sensitive information, which may pose a threat to the users accessing their data. Spyware [52] is designed to be secretly installed on various systems to monitor user activities where spy collects these activities with browsing practices to access the user information with malicious intent. Various large organizations or firms face a kind of vulnerability in protecting their data due to such secret agent software [53]. The Israeli cyber arms firm recently installed a type of spyware called pegasus on iOS and Android phones to gather user personal information. Thus, it is necessary to develop the blockchain-based data security system against spyware and analyze the online activities of secret agents for spy detection.

Rootkits [54] are suspected to be the biggest threat and major security vulnerability in protecting user data. This malware is designed or installed in such a way that it cannot be easily detected by anti-malware software and can stop the detection methods by exploiting the vulnerabilities of system software [55]. Intruders can take control of the user system unexpectedly and modify the user security information. In fact, a rootkit [56] actively provides the special privileges of continuing to access data on a user system while hiding its malicious presence and activities where there are absolutely no chances of their identification of malicious processes. The strategy of blockchain-based user signatures can be designed to maintain data integrity against these malicious issues.

Backdoor attack is one of the serious malicious attacks on the network [57,58] that is not easily detected. The attackers implant a backdoor approach on the website servers to control the authority of the targeted websites and supervise the penetration tests, data robbery, and online movement. Backdoor attackers [59] obtain unauthorized access to the user systems through websites without the user's consciousness and collect sensitive information using GPRS gateways or WAPs. As a result, some sensitive information of targeted organization or industry moves out to criminals and easily make a fake identity that helps to drop a backdoor onto their system [60]. However, there is a needed website scanner defender with updated tools to detect and mitigate this type of malicious actors as well as to analyze the daily activities of new types of malware.

Keylogger attacks can wreak havoc on cryptocurrency users or finance management of any company, although such attacks are the oldest form of cyber threat [61]. Keylogger attackers [62] infect the user's computer using USB sticks, keyboard strokes, and system bugs while users log in to the webpages by typing in their passwords and credit card numbers. Attackers can easily recognize the keystroke patterns and log in to the user system [63]. Criminals furtively move the personal or financial records of any company or employees by applying this technique from the client side. **Rogue security software** [64] is often created by malicious programs that pose a security threat by misleading users on the client systems. This type of malicious program convinces the users by taking refuge in various tricks that the security measures of their system are vulnerable or fake malware removal tools are installed [65], which is a real concern in security and offers them to resolve. But that software is malware in itself that manipulates the users to provide money fraudulently.

3.1.3 Hash Based Attack

In the cryptographic networking system, **Collusion attack** traces the similar type generated hash values for the data transmission to the network hubs and nodes [66]. Thus the attacker uses these hash values to receive rewards through penetration. Generally, such attackers target a specific group of hubs or network nodes. To prevent this collusion attack [67], there is necessary to investigate all activities of these intruders and develop a blockchain-based sustainable mechanism. The technique of Proof of Tsar defends the hash collusion attack. As a majority attack, **51% attack** occurs on blockchain-based applications, which is one kind of vulnerability for the security of distributed networks [68]. Such attacks are carried out by a single or a group of miners and are able to control more than 50% of the hashing power of the blockchain system [69]. It can interrupt the record of the new blocks by confining the activities of other miners, although it may not completely damage digital currency or bitcoin. The successful attack depends on the network size, where an attack is possible for 51% or more on a relatively small blockchain network than on larger networks [70].

3.1.4 Network Intrusion Attack

A **Sybil attack** is a type of attack that is seen to cause confusion in peer-to-peer networks on a blockchain where any network node actively leads multiple fake identities at the same time [71]. These attackers manipulate their fake identities to make a mutual perception based on network system effectiveness. The distributed network system [72] produces undesirable reports as spam for users. Thus, system users can lose their data privacy and data security. The attackers can affect the entire network by using the Sybil attack approach. Blockchain-based peer-to-peer network security can be vulnerable due to **Eclipse attacks** [73] where the malicious network nodes use IP addresses to isolate the connections of their neighboring hunting nodes. Typically these attackers infect a single node aimed at compromising the incoming and outgoing traffics instead of the entire network [74]. It poisons the routing table to prove neighbors lie in the decentralized network. A successful Eclipse attack [75] supports an attacker for the connection monopolization attack, including the creation of a lot of node identities through exploiting the weaknesses of specific peer-to-peer selection. Thus, it is very important to explore and mitigate the associated risks of eclipse attacks, such as cyber-attacks in cryptocurrency.

A **Buffer overflow** is a programming error in web applications, and server software that creates a type of vulnerability in data security [76]. A buffer overflow attack can happen when the process of writing a program with an error in the memory block does not support sufficient memory space to address the data values. It can enhance the network load or traffic in the fixed routes and corrupt the system. When nodes in the heterogeneous network perform this type of program, the attackers affect the performance of system memory and the overall network [77]. These attacks can occur while transcribing data without testing data fit in the destination buffer. However, blockchain-based web applications or server software can be used to control buffer overflow vulnerabilities. A **Traffic Flooding attack** is a form of denial-of-service assault on the targeted web servers. This type of attack is caused by the transfer of a very large load or traffic to a system [78]. Thus, this attack can slow down the system performance and reduce the messaging activities through the exploration of TCP connection management. The traffic flooding attackers [79] flood the entire network using the route request messages among the destination nodes. The ultimate goal of flooding attackers is to consume a large amount of energy for their network bandwidth and destroy the system output completely.

Protocol specific attack is the unauthorized activity on the distributed computer networks which installed on a victim system to hijack sensitive resources by exploiting a specific programming bug, or modified feature of the protocol [80]. Typically, protocol-specific attacks occur in the network and transport layer of the OSI model based on their vulnerabilities. Protocols [81] performed in accordance with specific rules and procedures in the network can be IP, TCP, ARP, ICMP, UDP, or other application protocols in which this protocol attack effortlessly compromises the targeted protocol and harms the targeted system. **Routing attacks** arise due to route hijacking, adversary congestion, traffic route diversions, and other service attacks. These attacks may depend on data manipulation or modification to the distributed network, which increases the risk of routing violation [82]. Attackers can generate routing attacks using network partitioning and delay the attack. The partition attack is split into more than two groups in order for the attacker to supervise an autonomous transit process and hack some sensitive key points. Also, for a delay attack [83], the attackers can tamper with the internet services in order to make unauthorized delay in the propagation program and create a suspicious network by messaging that data services.

3.1.5 Social Engineering Attack

Phishing is one of the fatal cyber threats in which criminals attempt to move important data by sending fake emails or using fake pages on the user network [84]. Phishing assaults by social network hacking, resource cloning, and intentional object hacking can be widespread. This type of phishing scam exposes the victim's sensitive information such as job credentials, login data, online account passwords, and credit card user information using malicious websites or emails [85]. Due to the increasing use of text messaging, audio or video messaging, email, social network pages, etc., for communication, attackers apply this malicious technique to steal data. Also, sometimes users allow valid access to sensitive data, including their own credentials, to their family members, acquaintances, or employees, which can be a dangerous reason for phishing [86]. Developers need to make a good analysis to deal with the effects of such attacks.

A **Baiting** attack is a malware-arisen social engineering attack whereby attackers tempt the users to click on the malicious based link or email by applying the strategies such as a pop-up interface for getting free stuff [87]. Baiting attacks are usually based on the user's curiosity or greediness, so attackers use unsafe computer materials, such as physical or portable electronic media as well as intriguing packaged email letters, to target a person or object [88]. When the victim enters such a device into the computer, the malware present in the device is immediately installed and activates this attack unwittingly. Another social engineering attack named **Tailgating** is mainly based on physical access techniques that are used to get access into unauthorized locations [89]. Attackers closely follow a legitimate person who has a security clearance in an unauthorized area or building where those attackers cannot enter. In this case, the attackers will seek to enter a restricted area by using a false or fake relationship between them from behind the person with legitimate access [90]. Tailgating can occur when attackers manipulate the RFID network to accomplish their malicious purposes.

Pretexting attacks can be used as a type of social engineering attack because it is based on fake and trustworthy situations [91]. In such an attack, attackers refer to users to create trust in them with their false identity to be camouflaged as a good colleague so that they can easily receive sensitive information like user passwords. Pretexting [92] is not merely used for illegal activities in the cyber world, but investigators also use it for their investigation in the legal methods to gain important information from the people. As another form of social engineering attack, the **quid-pro-quo** attack [93,94] is operated by low-level attackers who target something or the desired user in order to grab important information in exchange for some free services. Pretending to be professional engineers or technicians, they guarantee free technical assistance to the victims. The attacker waits for an opportunity and launches malware into users' systems while they gain access [95]. In this way, they grab important information from victims.

3.1.6 Injection Attack

Code injection is one type of malicious injection that exploits the illegal data processing for unauthorized access to the system [96]. An attacker injects malicious code into a vulnerable computer application. This type of attack is used to attack the poor handling of untrusted data of any system. The injecting code compromises the security and integrity of the information within the application. There are many blockchain applications that can be at risk of code injection and, in that case, data security breaches. So, some organizations may often be unable to prevent code injection risk to protect their sensitive data. Typically, code injection [97] attackers hijack any kind of vulnerable application to conduct commands unreasonably in the user's operating scheme. **SQL injection** is one of the most recurring and harmful techniques of attack for malicious purposes due to web security vulnerabilities. The malicious persons attempt to capture unauthorized access to the database server to move sensitive information. SQL injection [98] interferes with the security of entire databases and network systems that organize web applications. In this case, the attackers will be able to view and modify the data of the host web applications, for which the content of the application will constantly be changing [99]. The main effects of SQL injection contribute to violating the privacy and integrity of sensitive user information, loss of personal data authentication, to manipulation of the entire system information. **False data injection** is a class of cyber-attacks against the reading, monitoring, and measurement systems of multiple power grid sensors over a wide area of the smart grid [100]. This attack is capable of bypassing traditional malicious data identification processes by misleading the operations and control centers of such system states. By injecting false data into the software [101], the attackers send the misleading data to the inter-operative sensor network, and the security of such a network is exposed to a vulnerable situation due to making erroneous system calculations. False data injection attacks [102] are so sophisticated that they compromise with controllers on network systems to provide unreliable IoT applications with incorrect service.

3.1.7 Reconnaissance

Split-world attack [103] is a core approach to providing irrelevant log data where certain users are allowed a fake form of the log from a malicious log server. A technical attacker can get a fraudulent certificate as valid from the users. These attacks only apply if an attacker can offer different views of the log data to their desired users [104]. In such cases, although users receive various ways to share the views of the log with others, the attackers may repel users from understanding the valid evidence. That is why the victims can never know about such attacks and malicious motives. **Internet Information Lookup attack** is an activity that manipulates the user's internet information using internet tools to easily discover the IP address of any network without visually altering the physical entity [105]. Attackers can interfere with the host information of the user system by performing lookup bias and misdirection attacks on the network. They can anonymize a lookup initiator and modify host files to point out any harmful location [106]. When navigating the user hostname correctly on some sites, a certain server may persuade some clients to send to fraudulent sites where confidential and sensitive files are gathered for malicious purposes.

Port scanning is a repeatedly used process on the network to systematically scan the ports of computers, which can be performed by network patrons or assaulter [107]. Computer ports are typically applied to design network traffic in the appropriate process, so attackers attempt to scan ports on the attack victim's computer to obtain sensitive information about what packages are offered on which port. At the same time, cybercriminals send a lot of TCP data to the sufferer's computer to switch the desired port to understand the concept of the operating system and to discover the network vulnerable points [108]. They use these necessary responses to launch actual attacks on their target environment, and they hack the victim system. Some of the notable scanning processes to launch this attack are Windows scanning, TCP scanning, ACK scanning, SYN scanning, UDP scanning, etc.

Packet sniffing or sniffing attack is a type of network attack strategy that is used to illegal access the network data packets by capturing network traffic maliciously and extracting the unencrypted packets unlawfully [109]. The attackers can read and modify those unencrypted sensitive data packets. Packet sniffers in the role of hardware or software are capable of monitoring all transactions between client nodes by controlling network traffic or administration. Cybercriminals [110] can easily steal any sensitive information, such as usernames, passwords, credit card info, user messages, etc., from social or business networks through sniffing attacks. **Ping sweep** attack is one of the reconnaissance attacks that attack the client computer systems by gathering information through network search, or surveillance [111]. As a network scanning technique, the ping sweep is used to ping a range of IP addresses to know which host systems are active. With this strategy, cyber intruders transmit ping data [112] to these IP addresses and wait for a reply, as well as identify which machines are responding. After that, intruders search the network ports, such as TCP or UDP, to find out what kinds of services are accessible to which host or website at certain IP addresses. This can be an easy way for attackers to hack the target system and steal its data.

3.1.8 Network Access Attack

Eavesdropping is an unauthorized real-time attack that spreads over a network via a smart device or computer to move personal data. In this criminal tactic, the attacker codes to instantly listen to instantaneous network conversations without the knowledge of the user or the system, which are subsequently used to the detriment of the victim [113]. Eavesdropping occurs over the user's phone call, instant chat, or video conference on an unsecured network [114]. They can disclose the user's privacy. This attack creates a high privacy risk by recording sensitive personal conversations and financial and business information. **Data modification** attacks usually occur by interrupting the exchange of data that causes extensive loss to a system [115]. Attackers change, insert or revoke a part of data to prevent the message from reaching the recipients, which results in a lack of comprehension on the part of the recipients and could lead to any kind of accident at any time. Data modification attacks [116] can mainly occur when sending email, message, or text. This type of modification damages the integrity of the original information.

Spoofing technology has a significant impact on cybercriminals in carrying out malicious activities on information security. Identity spoofing or spoofing attacks [117] allow criminals to masquerade as permitted users in the systems where these criminals pretend to have legal privileges. In this technique, malicious devices or criminals masquerades themselves as other persons or objects in order to perform malicious activities [118]. Many strategies are used to build trust in the system and to distribute malicious program codes for data or currency theft. Criminals can spoof phone numbers, email addresses, websites, IP addresses, domain name servers, address resolution protocols, etc., through identity fraud. **Password-based attack** is one type of cyber-attack strategy to hack the user system. Passwords are usually required to access a system as sensitive key information to manage web-based services [119]. Attackers attempt to steal user passwords to access user or organizational services by exploiting password-related vulnerabilities. A password attack is a malicious code that observes and records the password, including the username, by using various methods criminally when logging in to a website [120]. Attackers can use password-based attacks in a variety of ways, such as through shoulder surfing, social engineering, brute force, credential stuffing, dictionary attack, hash injection, etc.

Trust exploitation-based assault is a criminal process of controlling an entire system by establishing a relationship of trust with a computer or network system [121]. Trust exploitation attackers establish a trust relationship with one of the hosts and carry out attacks on other hosts in the network by exploiting that trust. A hacker takes advantage of using existing trust relationships to attack an internal network by compromising an external system. The presence of high confidence in network management often does not guarantee data security due to misuse of trust [122]. From external hosts, hackers can use trust exploitation-based attacks to redirect traffic or ports to internal host networks. **Layer attacks** occur when different layers of the network are exposed to a large number of threats while accessing the network. These attacks are designed by a kind of malicious behavior or program in mind to fully target different layers of data transfer in the network system [123]. In this case, attackers can modify packets transmitted among the various layers of the wired or wireless networks and even block web application firewall services [124]. Moreover, a bad or malicious design of a piece of software in a software-defined network could compromise the potential security of the network, which can provide the attacker complete control over the core networking infrastructure of the layers.

Denial of service (DoS) attack is one type of cyber invasion that makes any system inaccessible to users and interrupts the activity of the desired network or system [125]. Typically, this attack is designed to often target the web servers that block the normal flow of data outside and lead to the system crash. In this case, attackers use a variety of malicious programming codes [126] that can mostly unplug Internet-connected services or systems and pose a major threat to businesses or organizations. DoS attack enables a malicious agent to dominate by flooding the network with more traffic or data by making frequent requests from multiple computers than allowing anyone else to use the targeted network. DOS attack affects the system control center by generating the correct code, and it causes huge fluctuations in the power stability of the system and its frequency; in extreme cases, the whole system collapses. **Distributed denial of service (DDoS)** [127] is another serious concern in the area of distributed or decentralized network security. These attacks need a little attempt to target the key resources to cause massive damage to the computer system or network bandwidth. DDoS attacks [128] engage a number of distributed online systems in order to operate single or multiple computing machines, and it is used to flood a target website with thousands or millions of messages by making transferring fake data packets and traffic. These attacks have the ability to make online services, host machines, or websites unavailable to the user and even crash target systems [123]. In this case, it reduces the performance of the distributed network system against the services to legitimate users.

Man in the middle attack is a conventional form of cyber-attack on the distributed network [129] where the invaders secretly change the communication between the two sides and establish an independent connection as a middle man with them separately. Meanwhile, users on both sides of the passageway think they are talking or communicating directly with each other, but they do not understand that they are being completely controlled by the attacker [130]. The malware in the middle attack as an external user often takes control of the user's network protocol and can access, study, or modify any types of confidential information without manipulating the cryptographic system. Due to the limited security measures, it looks like a regular exchange of information and is a very easy target for invaders to steal connected information.

In the context of network security, sniffing attacks are used to capture the network traffic for sensitive data theft by manipulating the use of switch-based networks. **Replay attack** is another form of security attack that maliciously replays the valid transmitted data of a user over the network [131]. In many cases, it even fraudulently delays data transmission and replays them for data theft, or access [132]. To carry out this type of attack, the attacker, as the original sender, hacks the machine at a network substation, interrupts all transmitted data sequences from the sensor, and then sends it back to misguide the receiver. As a result, the receiver deems the message from the attacker to be valid. In this case, the recipient will respond to this new request and incur a large loss. **Key attack** on cryptographic primitives is a malicious technique that attacks a cryptographic system by finding vulnerabilities in the key-related codes, ciphers, or algorithms of the management design and mathematical analysis [133]. This attack compromises any device over the wireless or wired protocols to counteract the secured data transmission [134]. Cryptographic attackers are usually aware of the relationship between different keys in order to access encryption functions with related keys.

3.1.9 Assault Attack

In the cyber world, **Terrorism** is an alliance of the unlawful use of violence and cyberspace by intimidation [135] which is a strategy to attack the targeted objects socially, ideologically, economically, or politically through computer data, programs, websites, and telecommunications activities. Attackers spread fake information about victims using different social or online channel platforms [136] virtually and physically, endangering and humiliating these victims socially, ideologically, economically, or politically. This type of terrorism is often used especially against powerless and feeble-minded civilians for illegal purposes. Digital terrorism is often used to tarnish the image of a government or a respected person. Cyberterrorism is employed to create an environment of violence and combat among sub-national groups.

Cyberwarfare is a strategy of digital attack by which any nation, state, group, or international organization secretly attempts to harm the computer and information network of another country or organization [137]. This attack is carried out to destroy various digital infrastructures and organs of the government or organization. In some cases, the attacks are operated by a non-state group to create a state security crisis. Cyberwarfare [138] can be a virtual means of attack by carrying out malicious military activities digitally to weaken a target country economically. **Cyber espionage** is a type of criminal offense that is used to obtain sensitive data or intellectual property from client computer systems without permission through illegally abused techniques [139]. By this technique, the criminals steal confidential information and knowledge from individuals, rivals, friends, groups, companies, governments, and even competitors to get personal, political, economic, war, and other benefits with malicious intent. However, in this case, those involved in cyber espionage [140] prefer to remain anonymous most of the time without revealing themselves. In some cases, a state or a nation prepares a skilled intelligence team to use espionage tactics in future cyber-wars.

3.1.10 Generic Attack

The malicious recommenders easily influence the user's belief in committing a crime through a type of generic attack named Ballot stuffing that represents a centralization attack. **Bad mouthing attack** is one type of attack generated from malicious technology where bad nodes provide unlawful recommendations to honest nodes in the network system and falsely prove the effectiveness of those good nodes to reduce reputation [141]. In this bad-mouthing attack, malicious devices secretly ruin the trust level against well-behaved nodes [142]. These bad recommenders lie about the transaction even though they receive advanced services from excellent service providers. The efficiency of the network system decreases due to the lack of customer connectivity.

A **whitewashing attack** occurs in the cyber community to serve malicious purposes where an attacker abdicates their present status and rejoins the system with a new identity, injecting a bad reputation or unfair rating by exploiting some strategic weakness [143,144]. Subsequently, they behave as an honest service holder in the system. In fact, when a new service provider joins the network, its integrity score is low due to the deficiency of performance in the system as new, although they have no ill intentions. In this case, whitewashing attackers exploit these vulnerabilities in the network. Deal with such a situation, and it is necessary to improve the properties and functionality of nodes with low integrity scores.

3.2 Block-Chain Technology

3.2.1 Genre of Blockchain

Blockchain technology works in the data access scenario when someone joins as a network node with permission or without permission. There can be three categorizations of the blockchain-based on data access. These are public blockchain, private blockchain, and federated/consortium blockchain.

Public blockchain-A public blockchain [145] conducts data transactions on an open platform for all users of different networks. It is decentralized, and no one from any network can control its activity of it. Each network user can create their own blockchain profile and then access and observe blocked data without compliance [146]. This type of technology is open to any user to read or write the blockchain data content. It is also termed a permissionless blockchain. Popular digital transactions such as Bitcoin and Ethereum are permissionless blockchains. The public blockchain network is presented in Fig. 5.

Private blockchain-A private blockchain governs the sharing and exchange of data privately among the individual networks [147]. It is a centralized invitational network and handles the data transactions to everyone in a closed platform [148]. In such a system, an institute or organization can access data in compliance with the blockchain authority. It is also called a permission blockchain. The advanced cross-industry technology of the Linux Foundation, like Hyperledger, is a strong instance of the private blockchain network. A private blockchain network is exhibited in Fig. 6.

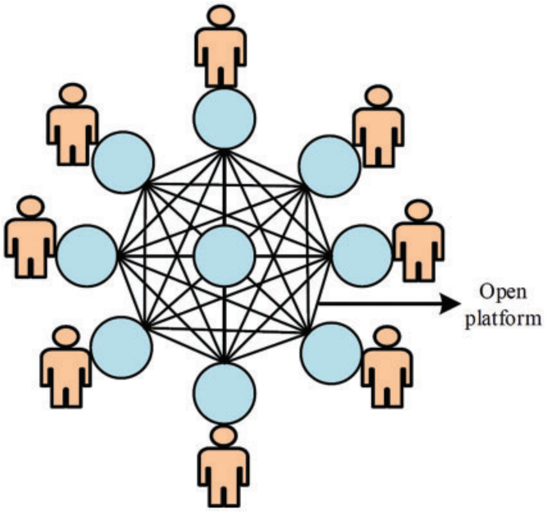

Figure 5: Public blockchain

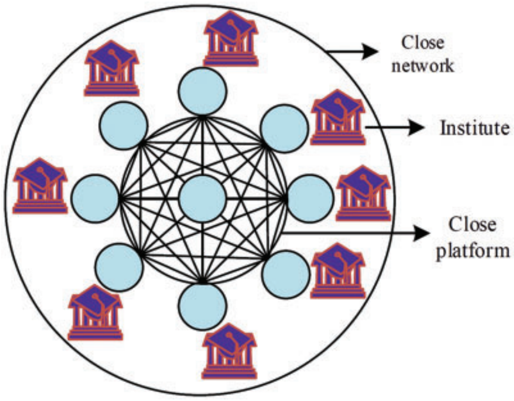

Figure 6: Private blockchain

Federated/Consortium blockchain-A federated/consortium blockchain conducts collaborative block data access and observation between multiple institutions or organizations [149]. This blockchain leads under a group administration without allowing others to participate in the data transaction process. As a decentralized nature, it handles all policies and issues within certain specific organizations like a private blockchain [150]. For example, these types of blockchain are usually placed in the banking (R3), energy (EWF), or insurance (B3i) sectors. A federated/consortium blockchain network is shown in Fig. 7.

3.2.2 Characteristics of Blockchain Technology

The significant characteristics of blockchain technology are needed to create a highly attractive and emerging network framework. Digital transaction between customer and supplier of a growing organization requires blockchain features. The characteristic aspects are described as follows:

Trustless-Blockchain is capable of constructing a reliable framework in a trustless network circumstance. Blockchain facilitates to exchange of digital data through trustless entities among trustworthy networks among trustless environments. Actually, "trustless" is conducted in blockchain technology [151] to manage the trust in a decentralized activity to the distrust entities in the blockchain network. To share or transact the digital data securely using a trustless model, the participants do not require network trust because trustless occurs in smart contracts or human interaction, but trust is the inherent strategy in the system. A trustless system [152] is the equal interaction between trust and distrust entities in the blockchain network where the blockchain framework authorizes transactions with an untrusted environment.

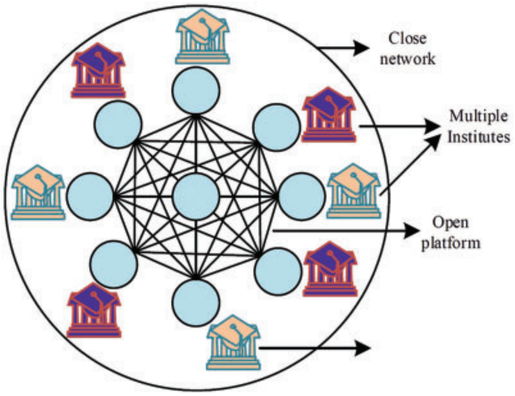

Figure 7: Federated blockchain

Traceability-The traceability of blockchain technology is the capability to trace the desired data, transaction processing, data procurement time, data path, and location to make accumulated raw elements, production, adjustment, and valuation in the blockchain network [153]. Actually, it makes to easily identify the transparent and distributed data from the ledger of the blockchain environment. It is also involved in tracking the source, attributes, certification, and quality of the data. Each and previous transaction can be safely traced back to the blockchain ledger. So, traceability [154] is a leading feature of the blockchain framework to manage and control digital assets. A traceability system is deployed on the blockchain network to disclose all these assurance activities.

Auditability-Auditability is a special and systematic feature in which auditors can verify the data integrity and correct operations for submitted data facts by communicating with nodes in the blockchain network in a confirmable and secure way [155]. Successful suitability of a blockchain network depends on auditing all data access and retrieving information related to tag transactions from the secured blockchain. Auditability is the ability to perform a comprehensive investigation of the desired blockchain evidence and representation in a state machine system for a client. Consequently, blockchain auditors [156] can manage and verify the smart contracts, validated transaction interfaces, and data integration with external data sources by accessing distributed network nodes.

Transparency-Transparency is the presence of being transparent about openness, transaction, relationship, trust, commitment, and accountability to the nodes of the blockchain network [157]. Blockchain technology provides massive transparency in where the transactions of participants are open to the functional components of the blockchain network environment in a secure and trustworthy way [158]. Every transaction process through the nodes in the blockchain network is verified, which allows transparency. So, secure transparency should be implemented in the data transaction of blockchain applications for use cases.

Anonymity-In the blockchain network, anonymity is a systematic manner for data transactions in which data users wish to provide their data to protect privacy without revealing their authentic identity [159]. Thereby, data users can allow their data to be shared anonymously. Group signature and signer identification do not publicly disclose the actual users for the convenience of anonymous storage of their particular information because the information may involve individual personal data in the blockchain network. In this way, anonymity [160] indicates the capability to exchange data among users without disclosing any personal information or transactions which are made by them with exercising the access control of the blockchain system.

Persistency-Persistency denotes a process in a blockchain environment in which the transactions are justified by trusted objects according to the consensus rules, and no changes or deletions can be made when each transaction is confirmed and occurs across network nodes for storage in blocks [161]. Thus, it does not recognize illegal transactions in order to rely on the behavior of changes and the relative allocation of related materials [162]. For that, any falsification can be easily identified due to uninterrupted transactions in a blockchain ledger. Blockchain can be performed on the state of the persistent process, and data can be easily retrieved to maintain the data transactions or workspace if the blockchain network environment is turned on.

Immutability-Immutability is one type of feature of blockchain that allows the data transactions in the distributed different network nodes, and it is not possible to modify or erase the transaction records from distributed blockchain ledger [163]. Each block of transaction in the blockchain is connected to the previous block through the cryptographic function. Consequently, for immutable blockchain ledgers, it is difficult to make a change in the content of a block because of subsequent blocks. This type of feature [164] enhances the satisfaction in the data transactions of the system and diminishes the data forgery o maintain integrity and authenticity.

Decentralization-Decentralization is the activity of data transfer or decision-making on a distributed blockchain network [165] in which all transactions have occurred with the consent of blockchain network nodes, and validity is required to store the data resources across its network. Share and control the data transactions in the blockchain, decentralization [166] consents to be non-trustful on the central entity and risks elimination of a middleman. Also, it enables all distributed network nodes to use consensus techniques to perform the blockchain. For managing the distributed ledger, a decentralized blockchain system decentralizes data generation and exchange.

3.2.3 Operations

(1) Blockchain Structure-**Blockchain structure** is the cryptographic hash pointer or back-linked list based on a bunch of blocks for data transactions in the distributed and decentralized ledger of the cyber-enabled heterogeneous network world. The blockchain structure for data transactions is presented in Fig. 8. Computer clients store the blocks of desired metadata as a general database in the blockchain, which can be accessed easily in securely with verification and identification of integrity to maintain data scalability. Blockchain [167] contains a chain of cryptographic blocks that shares and distributes the information among the nodes of a network. Consequently, blockchain consists of three main parts such as block, hash, chain, and node. A block hash encapsulates a header and a body of the data transactions that are stored in the blockchain ledger [168] via the network for later use. The hash function links among a number of blocks during the transactions. This block linking is called a chain. There are several transaction nodes in a network, where each node carries block data. A network node

finds the previous block hash after checking the arriving block header [169]. In terms of operation, the block header accommodates a number of block elements such as validate version number, hash related previous block, Merkle tree root hash, digitized timestamp, difficulty status block hash, and cryptographic nonce. Moreover, the block body [170] incorporates all transaction, data contents, and their counters to preserve the root hash of the Merkle tree. The highest amount of block transactions is controlled by the size of the block data, where the cryptographic method ensures the authenticity, confidentiality, and integrity of the scalable data transactions [171]. The block version number is used to track the blockchain protocol decisions or upgrades to ensure the accuracy of the upgrade data to abolish the outspread of poisonous software; otherwise, it cannot proceed with the validity and verification of the consensus structure.

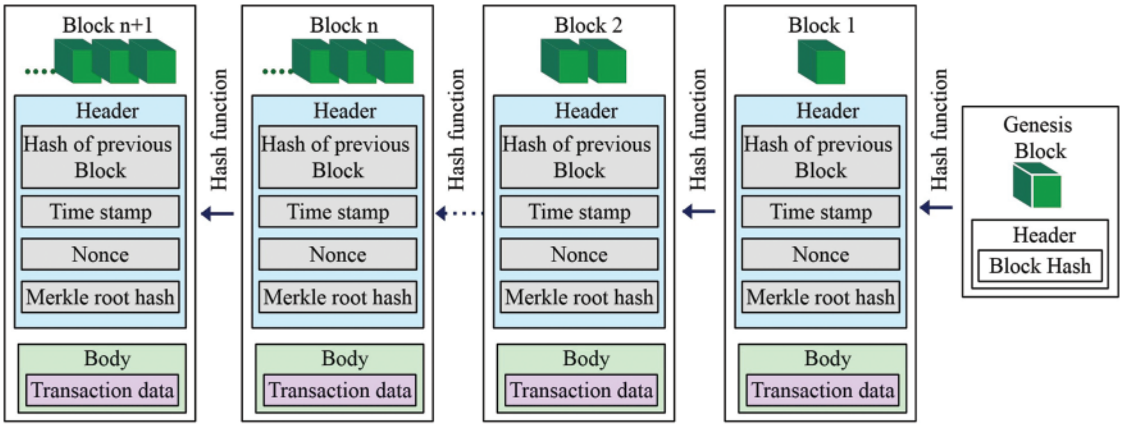

Figure 8: Blockchain structure

Hash-related previous block indicates the prior position of the active block hash in the blockchain structure. It is the main block hash [172] as the parent block hash to ensure the blockchain immutability where each block in the list of block hashes is associated with its parent block. The previous block hash is also called the genesis block hash, as the first block has no parent. Merkle tree root hash is the hash value of a complete binary tree for all transactions in the blockchain [173] where hashes with information are recorded via a root node in all nodes as parent and children node. A root hash-based Merkle tree provides scalability, integrity, and security of information in blockchain applications by optimizing storage and network capability without malicious changes [174]. When a block is generated, accessed, or altered during the blockchain network operation, a digitized timestamp is used to store system time for each digital transaction. The block difficulty target hash is used to measure the difficulty of blockchain mining for an approved target where the block difficulty estimates and adjusts hash computing power after generating a particular number of blocks to make the entire network more secure. Whereas a cryptographic nonce is an arbitrary random value for storage in a valid block transaction mining which is used to control the distributed network communication by an authentication protocol.

(2) Consensus Algorithm-In the blockchain network architecture, a **Consensus algorithm** is a hashing-based protocol that is used to allow the system machines and users to ensure effective data transmissions and their necessary agreement (consensus) among all parties of distributed environment. The consensus algorithm is the key concept for creating validated blocks in network nodes for blockchain applications. In general, this consensus method will determine how it propagates the consensus for data transactions among untrustworthy network node participants. It is also necessary

to exercise the gap between complexity, data scalability, and cost-effectiveness for the existing consensus algorithm in blockchain technology. Consensus algorithms for secure data transactions and storage in blockchain-based decentralized systems can be classified according to their features and characteristics. However, consensus algorithms and their classification can play an important role in various aspects, such as understanding the strengths and weaknesses of different algorithms, their comparison and evaluation, advanced research and development of new algorithms, effective digital communication, and so on. For data transactions in distributed blockchain applications, the consensus mechanism is exposed in Fig. 9. The following, it is summarized the different types of consensus algorithm.

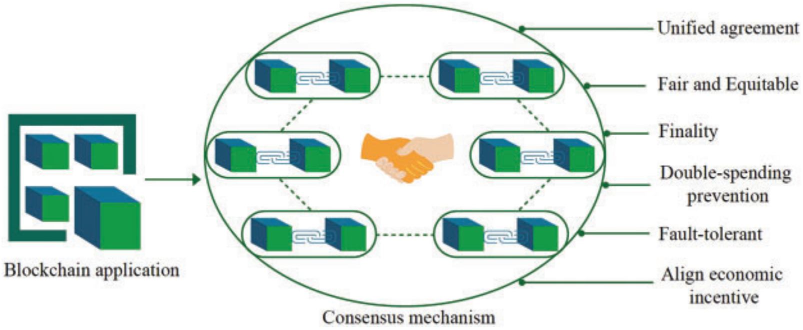

Figure 9: Consensus in blockchain structure

Proof of Work (PoW)-The most significant consensus protocol to acquire the block transaction agreement in the decentralized network is PoW. In the blockchain, PoW [175] will confirm the cryptographic block transactions and generate new blocks in the blockchain when users transmit the validated digital transaction in blocks to each other. In 1993, the concept of proof-of-work was first patronized by Cynthia Dwork and Moni Naor to deter spam and abuses of network services in computer data processing. But, in 1999, it was first established by Markus Jakobsson and Ari Juels based on several security protocols. It gained popularity when it was used as a consensus mechanism in Bitcoin blockchain by Satoshi Nakamoto in 2008. In this approach, cryptographic hash functions are used to verify data transactions and to prevent data tampering of unscrupulous participants where PoW needs a cryptic computational process on all nodes of the distributed network [176]. For publishing and recording the block transactions in the blockchain ledger from a random selection of decentralized networks via computational process, each node computes a hash value of the block header in PoW [177]. Block header carries nonce and miner in blockchain network where miners mine the blocks to accumulate in the blockchain and nonce change itself recurrently to get separate new hash values. If one network node acquires the target value with a validated block, it supplies that block to other nodes and ensures the validity of the hash value. In this case, PoW [178] needs an extensive amount of energy in these computational activities. Thus, the main activity of the PoW mechanism is to try to annihilate the cyber-attacks on the distributed networks where the data in the blockchain remains immutable.

Proof of stake (PoS)-PoS is one type of consensus protocol that is employed in distributed blockchain networks where the concept of PoS states to validate the block transactions without depending on the mining nodes [179]. PoS can be used as an energy-saving protocol in a blockchain environment instead of PoW. The mechanism of PoS through a specific network stake operates a blockchain network to establish the validity of block transactions and create a certain amount of blocks [180]. Network nodes make a particular amount of cryptocurrency stake among node participants for the new valid block transactions. In this mechanism, the selection algorithm combines an amount of stake of the cryptocurrency, including the randomization process, and elects the network node from the nominee's pool for getting validated new blocks in proportion to the cryptocurrency association [181]. PoS was first introduced in 2011 and first used in Peercoin for cryptocurrency in 2012. Subsequently, Nxt, ShadowCoin, and black coin have been adopted with the PoS method. In the near future, PoS may be implemented on the manet. Although Ethereum currently uses PoW, it is in the active development process to exchange for a PoS system. Consequently, PoS resolves some of the vulnerabilities of PoW-based cryptocurrencies in the case of cryptographic transactions like Bitcoin. PoS [182] governs the blockchain network environment with less computational power by simplifying the validation process. PoS makes the security of blockchain network by the validated stake of validators; otherwise, if they behave in the opposite way as defendants, they will lose their network access and crypto stake.

Proof of Stake Velocity (PoSV)-The PoSV [183] is another consensus algorithm instead of PoS and PoW for securing the peer-to-peer distributed network that is used for Reddcoin transactions. This type of method was developed to make social interactions in digital transactions. PoSV [184] was established on the basis of modifications in the properties of PoS and PoW. Consequently, this approach stimulates the participation of more effective networks. The idea of PoSV method was based on velocity (activity) and stake (ownership) of cryptocurrency, which promotes better participatory economic strength.

Proof of Burn (PoB)-A consensus mechanism, PoB, intends to bootstrap the cryptocurrency from one blockchain network to another network with minimal energy expenditure where it ensures the transmission of burning coin-based blocks in an unspendable location [185]. In this way, PoB can be called an alternative distributed consensus method of Proof of Stake and Proof of Work. Unlike PoS, the process of PoB-based blockchain makes validated transactions in the blockchain network by excluding cryptos from conduction permanently, and it is engaged in the interaction of user coins transactions to secure the distributed network. PoB [186] is a sustainable and decentralized mining mechanism which employed by writing blocks of transactions in proportion to their burnt coins by permitting miners to burn crypto-currency tokens [187]. This process is set up to refrain from double-expending on decentralized networks by creating offense worthless to certain users or communities, and PoB demolishes the currencies by forwarding them to uncontrolled and unspendable addresses. Today's cryptocurrencies such as Counterparty (XCP), SlimCoin (SLM), and Factom (FCT) use the PoB mechanism.

Practical Byzantine Fault Tolerance (PBFT)-A PBFT is a workable consensus technique in blockchain networks that can ensure the system safety despite having some malicious nodes due to cryptographic hashing protocol, and verifiable digital signature [188,189]. In this case, the nodes of the blockchain network share their information with each other to consign a block to the desired chain and transmit tampered blocks. The strategy of PBFT achieves fault tolerance by the decisions of the most conscientious nodes to disregard the effects of malicious nodes without affecting the network data integrity. Besides, this consensus algorithm in blockchain inherits a number of properties from the version applied in distributed systems and works to adopt the block validity. PBFT [190] technique disclosed by Miguel Castro and Barbara Liskov in 1999 tolerates Byzantine faults for state mechanism replication. PBFT is used to approve the data transaction processes in Hyperledger technology to confirm the accuracy and consistency of the final decision by avoiding malicious decisions.

Proof of elapsed time (PoET)-A giant chip manufacturing corporation named Intel developed a blockchain network consensus algorithm named PoET in 2016 to address the performance issues of consensus protocols. This algorithm enables reliable computing in blockchain environments to be randomly applied while waiting for blocks to be created, where an individual random timer is operated on the network nodes one by one. PoET [191] is applied on a permission-based blockchain network to control the mining rights and take the efficient decision of block winners by limiting the high utilization of resources and consumption of upper energy. In this case, PoET builds a secure environment to operate a trusted algorithm and enhances transparency among the prospective participants by deciding propagated random elapsed time [192]. As a desirable consensus method and popular tool, PoET is used for a modular frame of Hyperledger Sawtooth to implement and evaluate the distributed ledger schemes [193]. A Trusted Execution Environment (TEE) of a distributed network is accomplished by the cryptographic activities of Intel's Software Guard Extensions (SGX) for allocating individual memory parts where PoET is involved in boosting the security of Intel's new CPU processors.

Federated Byzantine Agreement (FBA)-FBA is a Byzantine fault tolerance-based consensus mechanism [194] that allows the participants to engage with a blockchain network where a group of nodes verifies the block transactions in place of one node to send the information to others. FBA can build transactional robustness by achieving network data scalability, better throughput, and minimum transaction costs. Each byzantine of FBA requires a trust agreement through quorum slices for their individual blockchain [195], which can make sure consensus of the definite decisions by controlling some abusive network members. The Stellar Consensus consent was first disclosed in 2015 by David Mazières, where this approach further rectifies the FBA protocol to make blockchain networks more secure. In this case, each node in the FBA application does not need to be realized and confirmed in a timely manner and selects those participants who believe. In a decentralized network, quorum slices arise from all those decisions which are prepared by individual nodes. In consequence, the blocks are signed by these specified quorum slices and become valid for the transactions of the network participants.

Delegated Byzantine Fault Tolerance (DBFT)-Another consensus mechanism designated by DBFT is used to strengthen blockchain networks. DBFT can get at a strong consensus using all network nodes, even if there are a small number of malicious nodes. DBFT operates system functions to be faster and more centralized in transactions between participants. Besides, it enhances the efficiency of the BFT network through the approval of authorizing validated delegates of the network. According to DBFT designers [196], a large number of participants are allowed to elect the delegates by the voting technique, and then they reach an agreement among themselves. There is a finalization feature in DBFT for transactions where a block is created by incorporating the transactions, and the blocks are joined together to form a blockchain [197]. Once finalized, the blocks cannot be split, or the transaction cannot be withdrawn. In this case, new blocks will be presented for validation to elected delegates, and the created blocks will be validated. All validated block transactions will be monitored and stored on the blockchain network by them. Binance is one cryptocurrency exchange among the largest cryptocurrency exchanges, which uses the DBFT as a consensus mechanism for its chain-sharing to deal with untrustworthy participants more effectively on the blockchain. The consensus protocol, DBFT, was introduced by a promising project called blockchain-based NEO cryptocurrency [198]. However, NEO as a public blockchain is the first smart economy project in china which is known as Ethereum of China. In this approach, all transactional information is digitized by supplying smart contracts.

Delegated Proof of Stake (DPoS)-A DPoS is an advanced evolutionary concept of PoS as a consensus algorithm that operates to verify valid transactional agreements and maintain the digital democratic mechanism in the blockchain network [199]. It is noteworthy that DPoS is used to create more reliable and robust networks through validating blocks as a technology related to democratic processes which relies on an elected delegate's group in favor of all network nodes, and it allows more various user groups to join on the heterogeneous network. Unlike PoS, a different consensus approach called DPoS was first introduced in 2014 by Daniel Larimer. He implemented DPoS on a decentralized cryptocurrency system named BitShares [200]. Today, there are several blockchain-based cryptocurrency platforms, such as Ark, EOS, Steem, Cardano, and Lisk, that use the DPoS consensus mechanism. The DPoS not only selects nodes but also manages an entire election system by selecting network nodes for validating blocks in real time. So, these network nodes can be called validated block producers. Every token holder casts their votes into a staking pool to elect their delegates, and it ensures the valid transactions and optimal activities of active network nodes where elected delegates exchange themselves periodically [201]. Usually, the election system can vary depending on the individual activities of the delegates. So, the entire electoral system directly depends on the reputation and trustworthiness of delegates. Besides, the delegates can share their collected rewards among respective token holders proportionally.

Delegated Proof of Stake + Byzantine Fault Tolerance (DPoS + BFT)-The DPoS + BFT is a blockchain-based hybrid consensus protocol that generates high performance and more security by the association of two consensus methods named Delegated Proof of Stake and Byzantine Fault Tolerance [202]. In DPOS + BFT algorithm, a large number of participants can agree with a random order where blocks are produced in a predefined commitment or order. For building a new block of a node, a block must wait for its approval because it cannot define whether evil should be done or if any of its nodes are confirmed. Due to predefined block approval, the next time, a node can generate a block without waiting for confirmation. DPOS + BFT consensus protocol [203] is implemented on a blockchain platform, EOSIO, which provides the pre-commitment and block transactions to achieve greater improvements and completeness of scalability. However, DPoS + BFT restricts the block production to only block producers. In the EOSIO blockchain, all participants generate 12 blocks very quickly by 21 Block Producers to adopt a round-robin method, and 252 blocks are made in one rotation. The DPOS + BFT [204] based EOSIO is optimized by 99.999% of the block generation probability in 100% reliable nodes where it can achieve the finality for larger transactions in under a few seconds.

Proof of Activity (PoA)-A PoA process [205] is a consensus algorithm in the blockchain which is made by the incorporation of the supreme aspects of two consensus approaches named proof of work (PoW) and proof of stake (PoS). PoA is applied in the cryptocurrency-related communications of the decentralized network. In that case, the PoA [206] is an important addition to the digital currency Bitcoin or a similar digital scheme. It delivers a strong security system for all transactions in the blockchain against potential aggressive action and ensures the consensus of arriving miners. In this system, the operation of mining is conducted in the same way as the process of a PoW method. Then, as in the PoS method, PoA puts the miner's reputation into the stakes after mining a new block, and the validator nodes are operative to provide validity to the network [207]. So, it can be used to reduce the overall energy consumption and improve the secured network topology. In the distributed PoA network, the most remarkable cryptocurrency, Decred (DCR), is exploited, and PoA secures the related crypto-transaction to nodes in the Bitcoin network.

Proof of Reputation (PoR)-The PoR mechanism is a lightweight consensus model that builds the reputation of network nodes based on their digital resources, the general agreement of participations, and transaction activities [208]. This decentralizing reputation keeps the network safe where the quantity of reputation is derived from the behavior of social network members and the nature of participation. Each participant must have a significant reputation as a block signer of data transactions; otherwise, they will face major losses for cheating with the system. This is because PoR [209] is used as a validator rather than as an individual in the organizational network. In this case, when a new block is produced by the highest reputed network node, it validates that new block by voting on the basis of reputation. As a result, all validated generating new blocks of highly reputed nodes will be able to participate in the PoR consensus process, and they will gain their rewards which are shared among the node validators according to their reputation values for transactions [210]. PoR method is utilized in GoChain using network participant reputation to get a stronger and upgraded network. The node behaviors and produced block transactions influence their overall reputation value, where a good reputation of the network nodes can guarantee the integrity of reliable transaction outcomes and diminish computational power utilization.

Proof of Authority (PoAuthority)-To ensure the proper execution of consensus transactions, another alternative consensus protocol named PoAuthority [211] can be considered as a new family of the consensus algorithm Byzantine fault-tolerant (BFT). In the consensus network protocol, PoAuthority verifies the transactions to select the network nodes on the basis of reputable Byzantine nodes for making blocks. However, PoAuthority [212] enables faster transactions with relatively low computational power by identifying valid block stakes. It is a permission-based private blockchain in which all nodes have to be pre-authenticated to create their own chains for a high transaction rate. Thus, this algorithm utilizes a specified number of node validators for scalable block transactions, and network nodes are authorized to yield new blocks. Indeed, this type of protocol can work in the presence of adversaries who are half of the entire existing participants. PoAuthority [213] consensus algorithm is being designed in Ethereum, VeChain, and Microsoft Azure network to maintain their block transaction privacy. In the Ethereum ecosystem, PoAuthority was operated by clients named Aura and Clique for private network transactions to build and assemble the blocks in the chain by a set of authorized trusted nodes.

Proof of Space (PoSpace)-In a nutshell, PoSpace [214] is an interactive cryptographic technique of prover and verifier that provides an alternative consensus protocol to confirm multiple blocks in the recyclable storage space of a permissionless blockchain network. PoSpace, also known as Proof-of-capacity (PoC), is one such way to prove the capacity of storage space that provides valid transactions by utilizing an allotted size of unused disk space or memory. It solves the challenge of using disk space instead of computational operating power with the service provider's assistance. To ensure more security in the blockchain, during the usage of the consensus technique, PoSpace [215] must be bound with proof of block times to maintain consistent time. Blockchain consensus network could be under threat due to the abuse of extra capacity. Thus, it diminishes the usage of additional hardware set-up as opposed to the searching target hash of PoW. Participants of the same storage in a blockchain system can achieve more convenience using single-chain schemes on PoSpace instead of direct sharing from multi-chain schemes. The consensus protocol PoSpace [216] has been applied in Storjcoin by accomplishing two methods such as Merkle audits and pre-generated audits according to cryptographic contract. Burstcoin, SpaceMint, and Chia are recent crypto-currencies that use the consensus protocol of the PoSpace method for transactions across their entire network.

Proof of History (PoH)-The PoH in blockchain architecture is an ingenious algorithm for the sequence of computation that provides a cryptographic way to verify and encode the time itself by lightening the network load during the block processing on the nodes [217]. Thus, it can be recorded a reliable sequence of messages for transactions into a ledger using the trustless passage of time. PoH is a Verifiable Delay Function (VDF) as a high frequency where it generates an individual output by evaluating the specific moment using successive steps in the event. The Solana Network is the blockchain-based first web-scale distributed system in the world where PoH is implemented using VDF to record the permissionless passage of time [218]. In this system, network events will occur at a particular moment in time before consensus, and it will make lighter and faster the network transaction process achieve a high throughput blockchain. PoH can provide adequate defense over time against forged ledgers and long-range offensives.

Proof of Importance (PoI)-The PoI [219] is a higher standard consensus technique in blockchain platform which is first presented by NEM cryptocurrency of 'New Economic Movement' project. In crypto-technology, PoI [220] is designed to determine the transactions of network participants named network nodes where participants are qualified to efficiently perform the amounts and sizes of calculations by accumulating new data blocks in the blockchain. In this consensus approach, PoI utilizes the importance of network nodes to prescribe the validity of the new blocks and their other factors. The overall score of the network nodes treats the amount of the number of mining transactions for the priority issues of cryptocurrency projects. In particular, PoI [221] harvests the eligible blocks to evaluate the holistic metrics such as participant transaction, vested currency, and size of transactions in accordance with the contribution of overall network nodes. These metrics, called importance scores, assist in achieving better-sophisticated outcomes and rewards in the distributed network.

(3) Cryptographic Technique-The cryptographic technique is the most significant data protection strategy in the blockchain network. Various modern cryptography techniques are associated with the cybersecurity system to ensure data safety. Cryptography techniques deal with the confidentiality, integrity, and authenticity of blockchain data among communication parties.

Hash function is a remarkable cryptographic primitive technique that is used to design an arbitrary data range in a fixed-size array values [222]. This approach meets the encrypted and security requirements for the computing blockchain networks as a one-way function by collision resistance. This method converts the data into a unique string as a hash value, secret text, or message digest that will be of a certain size [223]. The most notable hash functions in decentralized blockchain networks for integrated data security of distributed ledger are SHA-256, MD5, Whirlpool, Bcrypt, etc. Thus, blockchain-based on cryptographic hashing algorithms can be associated with ennobling the integrity, immutability, and confidentiality of the digital badges or cryptocurrencies. **Secure multiparty computation** (SMPC) is a cryptographic primitive field in the blockchain network where a group of mutually mistrustful distributed parties is permitted to collectively compute their individual and confidential inputs [224]. In this case, it performs successful calculations without any damage to data privacy or safety as well as it does not compromise the appearance of active adversaries on data security and secrecy. Thus, SMPC is also named uncorrupted trusted third party for their secure data sharing among them through intelligent computation of input functions [225] where all parties can trust each other protocol to achieve appropriate output. This concept is a perfect way to deal with the problem of multiparty data sharing, which was first introduced in 1982 by Andrew Yao. SMPC [226] provides much-appreciated service privacy, correctness, fairness, and independence of inputs to receive correct outputs from a suited blockchain environment.

As a modern interactive protocol for power dealing blockchain networks, **Zero Knowledge Proof** (ZKP) is one such cryptographic method of taking place between two parties named prover and verifier, where a prover is allowed to demonstrate certain data to a verifier for assuring the authenticity without disclosing the details of secret data [227]. In this case, a verifier is not capable of proving the exposition to anyone else except by acquiring the secret data. The encryption concept of ZKP was first introduced in 1985 by Shafi Goldwasser. ZKP [228] can be interactive or non-interactive based on the interactions between prover and verifier in a distributed blockchain network. Zero-Knowledge Proofs based on the true or false statement can achieve the features like completeness, soundness, and zero-knowledge. The ZKP process is used in the blockchain method of digital currency Zcash to protect confidential transactions and privacy. Thus, ZKP can be used to enable privacy-conducting authentication in smart contracts to generate an anonymous credential transaction for digital currencies.

In the crypto sense, the **Scalable transparent argument of Knowledge** (STARK) [229] is a protocol based on the perception of scalable and transparent IOP of knowledge (STIK) for mutual authentication among provers and verifiers of the blockchain network. The features of STARK design can be Succinct verification and universally verifiable, including the ability of distinguished witness. Winterfell has been developed as a proof-of-computation method using a prover and verifier of a general-purpose STARK, which can generate computational integrity. STARK is completely resistant to possible attacks from opponents and is transparent in the case of a trusted setup. Thus, STARK is a type of cryptographic proof protocol that allows efficiently scalable transactions in the blockchain industry. For the successive improvements of the blockchain network, another new cryptographic concept is **Zero-knowledge succinct non-interactive arguments of knowledge** (zk-SNARK) that ensures data privacy. The zk-SNARK is the new ingenious appearance of zero-knowledge cryptographic proof in which certain data to prove belongs to one party which are not disclosed [230]. In the zk-SNARK, that proof is feasible by building a secret key before a data transaction among the parties. The proof length can be a few hundred bytes which can be verified in a few milliseconds through the zk-SNARK. In this case, the non-interactive part of the zk-SNARK [231] ensures that there is no interaction among complete or very limited provers and verifiers, but it provides messages from provers to verifiers. The prover can generate arguments about any wrong statements using computational power, including the knowledge of any specific witness to ensure the balanced public-key encryption. This type of protocol is used in Zcash cryptocurrency as part of a strong privacy guarantee in the blockchain. Thus, as the preferred protocol, the operations of zk-SNARK can be used in Ethereum, Bitcoin, or other cryptocurrencies.

Digital signature is one type of cryptographic mathematical method for creating data blocks in a blockchain network that ensures the authenticity of digital information or messages [232]. It is performed by a cryptographic public key for identifying digital information where a string of digits is generated for a valid proof of data authenticity without any scope of a forged signature. In the distributed blockchain network, digital signature [233] can be a promising technology to achieve nonrepudiation and strong security for decentralized ledger through identity and integrity verification. Currently, different types of algorithms are used to generate digital signatures in distributed data transmission networks, such as Elliptic Curve Digital Signature Algorithm (ECDSA) is used in Bitcoin transactions. **Ring signature** technique is an encryption technology of a specific group signature to protect privacy during the transactions in the blockchain network [234]. This encryption algorithm secretes the user identities in a group of public key rings in order to obtain anonymous data transactions where each member of a specific group has its own key. Actually, a ring signature can be employed by an anonymous signature of a high-ranker user without disclosing the signature of any officer on the document. Thus, it is not feasible to determine the user officer who generates the signature from the group. Ring signature [235] algorithm was constructed in 2001 by R. Rivest, A. Shamir, and Y. Tauman. In order to obtain data privacy and security on the blockchain network, a ring signature method can provide a very important role for anonymous data transactions in the field of election voting and digital currency.

A **Blind signature** is a cryptographic digital signature scheme that provides privacy preservation by concealing the facts of a message and sender before signing [236]. Especially, the blind signature can be utilized in the digital transaction functionality of blockchain-enabled systems. In fact, this technology retrieves messages by the ability of anonymity and authentication in a particular cryptographic way. In 1982, the foundation of the blind signature was first exposed by David Chaum during the development of the untraceable payment technique as a digital cash system. This technique chooses a blinding factor and signs a transmission message to a secret that factors in the corresponding nodes through calculating private/public key [237]. Then, it verifies the validated signature to receive the sending message. Thus a blind signature can be used to verify the eligibility and anonymity of blockchain network nodes in the digital election and e-cash system, where it can minimize the size of the signature to reduce the computation stress.

Mixing technique is a cryptographic mapping way that consists of the various feasible clauses of the identifiable crypto-transactions. A tool named mixer is designed by this technique to provide cryptocurrency-related services [238]. In this case, it sustains maximum anonymity in digital transactions such as bitcoin. Thus, it will not be possible to trace the digital transactions of the blockchain network. The mixing protocol can be decentralized or centralized based on the combination of the aspects of all user transactions in the blockchain network where there is no consistency between the original transaction and the mixed transaction [239]. When the mixing process is completed once through a combination of all user transactions, the digital transaction is transferred to the new owner's storage. The most usable mixing techniques are CoinJoin, MixCoin, CoinShuffle, etc., in which all users transfer their digital currency to each other by the anonymous mixed protocol to facilitate privacy. **Secret sharing** is a cryptographic technique for supplying shares with privacy in a distributed network. This scheme consolidates the shares to restructure the secrets after distributing a share of secrets among the participants [240]. Actually, the owner of a secret generates a set of shares that can reconstruct the secret. Consequently, the owner can commence distributing the individual shares to different parties that are not used for its own, but it can be able to reform the secret by fulfilling certain conditions. In the secret sharing scheme, a secret is divided into multiple parts named share, which is used to reform the main secret. The secret sharing technique can be the best way to store highly sensitive and significant documents for more security in blockchain networks [241]. Secret sharing can be used to handle the fairness of linguistic cryptography, key-aggregate authentication, secret image sharing, or secure multiparty cloud computing.

The **Commitment scheme** is a primitive tool in cryptographic applications which is capable of hiding the data values. This scheme allows an authorized user to specify all messages in advance to keep these hidden from others and only to disclose with ability what should be disclosed after proving the commitment [242]. As well this technique is used to bind the values which are related to commitments, and one can not interchange them by adapting to other messages due to commitment. But, at the same time, both hiding and binding do not occur in the commitment scheme. The commitment scheme [243] as a cryptographic concept can be particularly significant for secure coin flipping or computation. This concept consists of the commitment phase and the reveal phase. In the commitment phase, the message as commitment is selected and specified from the sender to the recipient. In the reveal phase, the message is revealed after proving the commitment. The commitment scheme can be used in different cryptographic applications based on blockchain.

Differential privacy is an innovative security preservation strategy in the hostile network environment which is achieved by adding random noise to a numerical data record [244] where the adversary is not allowed to learn about the targeted data from the personal user record. Even adding, modifying, or removing a single part of data within a record of this approach will not have a significant effect on the final outcome of the corresponding distribution. This type of cryptographic formation effectively maintains the privacy of statistical records in the real circumstances of cybersecurity and receives the statistical exploration of all possible aspects of user records without compromising personal data identifications. Only aggregated data can be accessed for reference, reporting, and analysis through this approach instead of the user's personal data. This could be a potential way due to adding the desired noise that different types of organizations can access their user data for statistical analysis without private identity privacy sharing in distributed blockchain network [245,246]. In general, the differential privacy method works in two processes exponential mechanism and Laplace's mechanism. By this algorithm, no adversary can realize which information are personal in the record or which is not. Thus, it can ensure vigorous privacy guarantees on the specific client and server point of the distributed network.

Homomorphic encryption is a significant encryption process with the ability to evaluate encrypted data computation without compromising the secret key access. This approach allows a distributed processing system to perform specific mathematical operations on ciphertext to resolve the privacy issues of user data with security on the base of encrypted results [247]. It does not elicit any actual content during the secure data processing but receives the encrypted results from the existing data computation. A homomorphic encryption scheme can be used to sustain sensitive data privacy and preserve it in the blockchain-based cloud, including multiparty computation [248]. In this case, to get the exact transmission, the user will only be capable of decrypting the acquired encrypted data from the cloud with its own key but will not be able to manipulate the encrypted data. Homomorphic encryption scheme [249] contains partially homomorphic, somewhat homomorphic, and fully homomorphic encryption, which is used to perform a variety of computations of encrypted data.

The essential specifications of cryptographic technologies include **Symmetric encryption and Asymmetric encryption**, which can be important to ensure the accuracy, privacy, and integrity of blockchain-based digital currencies like Ethereum and bitcoin. Symmetric key cryptography uses a single secret key in any application to encrypt or decrypt data [250]. This key may be any number, word, or string of random symbols. The same secret key is used in both data encryption and decryption between sender and recipient if they agree with each other for their data transaction [251]. Asymmetric key cryptography is a significant concept in modern cryptography to solve the difficulty of symmetric encryption by improving the distribution key. This cryptography contains a pair of keys such as a private key and a public key instead of a single shared key which is used to encrypt and decrypt the data. When a text is encrypted by a public key, the encrypted text can be just decrypted by a private key [252]. In this different case, the public key is called the encryption key, and the private key is called the decryption key. In this method, private keys are performed by creating random numbers, whereas public keys are obtained by an irreversible performance.

A promising cryptographic mechanism named **Attribute based encryption** is a concept of an encrypted access control scheme that widely appends effective data sharing access within a dynamic community of users regarding data security and privacy matters [253]. In such a method, the data is encrypted by a set of user decision attributes or policies. After encrypting different data sets, users can only decrypt the corresponding ciphertext with their own original key whose attributes or policies satisfy the system. These user attributes and policies are engaged as a public key, but the data is decrypted by a private key. Attributed-based encryption [254] was first introduced by Sahai and Waters to solve data security issues. There are two types of attribute-based encryption based on key policy and ciphertext policy. In this case, when many users try to access their data, the data separately needs to be re-encrypted with each user's public key to disable the common encryption schemes [255]. The secret key policies and ciphertext policies of the attribute-based encryption model are controlled using cryptographic logical operations to solve the ultimate security issues during data access. Thus, this technique can play a significant role in preventing adversary attacks on data sharing in the distributed network server.

(4) Blockchain Propagation Matrices-In digital cryptocurrency transactions on a blockchain network, block propagation time [256] is the measurement of time for the generating of a new block. But in this case, when a blockchain network receives extreme congestion, it makes a backlog of block

transactions and generates a delay in the propagation of data transactions. Thus, in the blockchain-based bitcoin network, the **Propagation delay** is the difference in the length of time it takes to generate a new block or a transaction in a node and receive the data to other nodes [257]. This type of delay can occur in different mines of any blockchain-designed network. The scalability and security of blockchain networks can be at massive risk due to the longer propagation delay [258]. But if the number of routing hops in the block propagation can be reduced comparatively, then the delay in propagation will also be reduced.

An **incentive mechanism** is defined as a user-motivated formal scheme of any blockchain network that provides a reward of blocks to a blockchain miner where it safely performs a successful activity by making the right decision to speed up the data transactions in the network [259]. It affects the behavior of all users who participate in the miner rewards, token registries, transactions, and prediction markets of the system by modifying the relative expenses and conveniences according to their preferences. So, the ethical design of incentives is very effective in preserving the overall miners in decentralized blockchain systems such as cryptocurrency [260]. Subsequently, a lot of ways can be developed or analyzed to achieve incentive mines of routing nodes as well as to ensure more security and stability of the blockchain network. This mechanism with a routing node can minimize the transaction and storage costs [261] during the data sharing in an efficient way with a quality guarantee on the Ethereum and bitcoin blockchain networks.

An advanced and strong **Relay scheme** plays a very effective role in measuring the data of all nodes in the blockchain network as an important operator. The relay scheme justifies the data or token transaction capability on decentralized blockchain networks to store in the intended blockchain [262]. The relay scheme of a blockchain-based decentralized digital currency is a high-rate block-relay structure with the peer nodes for miners or data exchanges. This system relays the blocks to the public bitcoin network with minimal latency between miners. This structure permits to verification of the data transactions which have occurred in other blockchains, and it relays data chain-to-chain publicly in the distributed network nodes. All the scattered nodes of the bitcoin relay network are linked to each other to make peers. In this case, it demonstrates an own peering agreement using the majority of the key mines where the agreement in one chain can be a client of the other chain. Relay schemes [263] such as BTC Relay and PeaceRelay is designed to enhance the abilities of a secure block transaction, including verification on blockchain interoperability networks.

Sendheaders propagation is the upgraded mechanism from advertisement-based propagation. In this propagation, peers of the network nodes transmit the block header messages, and blocks are expressed directly [264]. Once the other peers have received the corresponding block header information, it sends this information to that sender's peers. In this case, it is not required to transmit inv-messages to sender peers, and so, the usage of inv-messages can be excluded. In consequence, it abates the bandwidth overhead and minimizes the latency in the transmission of block header messages. **Advertisement-based propagation** is a management mechanism to propagate desired messages which are derived from the Bitcoin network. By this approach, when the relevant data of a block is conferred on the network nodes, those nodes telecast the inv message to its connected peers, which is the message utilized in cryptocurrency [265]. Thereafter, when the recipient node accepts the inv message from the sender node, it will review whether the recipient node entities have the relevant data of that block. In this case, it will not operate; otherwise, it will send its response to the entity of the sender node by taking further mentioned activities to receive the transactions [266]. In the end, after receiving the response message from the receiving node in the network, the sender node will send the complete data or content of the block to the recipient node.

At the present time, different types of **unsolicited advertisements** can be critical issues for the security of user's data transactions [267]. To relieve the deficit of transactions among the network nodes and to get data security and integrity, the unsolicited push propagation mechanism generates a significant impression on the blockchain system. Unsolicited push propagation [268] allows the miners of the blockchain network node to broadcast their blocks directly to other network nodes after mining a block where the unsolicited advertisements are not engaged in the system. Sendheaders messages or inv-messages are not needed in this mechanism for the data transmissions. Thus, in the case of data transactions, it controls the overhead bandwidth and enhances the block propagation speed more. The **hybrid propagation** mechanism is the combination of push and advertisement propagation approach in blockchain technology, which is used in some systems like Ethereum [269]. In this mechanism, a network node conducts the activities by a particular quantity of connected peers that can be presented by n. The blocks will be pushed directly to the $\sqrt{n}$ connected peers through this node [270]. At the same time, the sender node will be capable of advertising the significant hash value of the transmitted data-related block to its neighboring $n - \sqrt{n}$ connected peers.

3.2.4 Network Framework

Network Nodes-As an effective part of a decentralized blockchain, network nodes handle the data transactions of a cryptocurrency with security. The nodes can be called the network participants in a blockchain network framework for securely sharing crypto data among users. Generally, three types of blockchain network nodes, namely client node, node generator, and node validator, are very significant for the data transactions [271]. Client nodes are treated as virtual users who access a number of predefined data block transactions in the blockchain network through their specific network interface [272]. It includes a real-time authentication hash during block transactions to receive the original document. Client nodes take action on blockchain transactions by accepting the client application's confirmation. It establishes a successful network transaction with low cost and high security to solve the optimization problems of data communication [273]. The Block generator node constructs a new block transaction through an initial transaction process to maintain the consensus mechanism and broadcasts it to the neighboring network nodes. Competing with other nodes in the network, once a node can generate a new block and is able to transmit the block data, that node is the generator node [274].

The block generator node takes action on successful valid transactions and ignores the illegal transactions in the network. It consolidates block identity, previous block hash, and timestamp using the personal key into the block data blockhead, then attaches the newly generated block to the end block of the chain. It transmits the block to the neighboring network nodes. Validator nodes [275] are utilized to approve the data block transactions for successful participation in the consensus process. This type of node validates the data blocks that have been transacted by the blockchain client node or user node. Each validator will record all valid and immutable block transactions in the decentralized ledger or blockchain. Thus, each selected validator node takes action on the successful transaction by participating in the blockchain network in consensus procedure with maintaining the client's or verifier's anonymity.

Architecture-Single ledger architecture is used in the data management of public, private, and hybrid blockchain networks and their permissions. This architecture can establish more desirable implementations of decentralized transactions, digital currency, and smart contracts in the blockchain environment. The single ledger architecture [276] is a peer-to-peer distributed network that allows secure and instantly desired data records for data sharing, better efficiency, functional error testing, and minimizing transaction time through real-time processing. Single ledger architecture can be applied to different application sectors of public blockchain networks where users do not need to make individual transactions and authentication in data sharing [277]. In this architecture, the participants are appointed through full nodes or mining nodes for a validated transaction to the blockchain. But, this structure for private networks is used to make a blockchain in a trusted area. In the hybrid blockchain, it occurs a confidential transaction among a part of the network participants using the public domain.

A multi-ledger architecture is a significant building design by appending cryptographic techniques which are used to develop different distributed multi-ledger applications of blockchain networks through achieving the committed more secure transactions [278]. The blockchain network operates different data blocks of the chain in multi-ledger architecture efficiently, where it allows access to the specific chains to the network nodes. It can support a hybrid blockchain to make a better throughput in the transactions by building the private network channel on the public blockchain, and clients of this structure make interaction with the system to allow peer-to-peer transactions by maintaining data privacy. A multi-ledger [279] architecture can be used to conduct a confidential and individual transaction among participants in the private blockchain network of an organization. It requires further encryption or decryption process to activate the confidential transactions of all authorized and committed peers. So, the blockchain network can synthesize data encryption/decryption processes and multi-ledger architecture to improve the access control, correctness, and confidentiality of the transactions.

Interoperability architecture [280] is a discernible design in a blockchain system to perform a distinctive and promising distributed data ledger that executes the verifiable data transaction to record information. This architecture can take a key functionality to facilitate blockchain security in the different applications using the consensus protocol where there is no required cooperation of a reliable third party for digital transactions. It is able to exchange secure data within two or more interoperable components of the heterogeneous public permissionless and consortium permission blockchain system [281]. This architecture, through interoperability, can be used to improve network security where one blockchain is connected to another blockchain publicly or privately.

Consensus protocol-The key procedure of governing affairs in the blockchain is the consensus protocol that maintains data integrity, immutability, and consistency during digital information transactions. Blockchain uses these protocols for generating valid transactions where network users participate on the basis of consensus among network nodes. In this section, it has been categorized the various consensus protocols of blockchain into three groups such as compute-intensive founded consensus protocol, non-computing capabilities founded consensus protocol, and voting founded consensus protocol [282]. Compute-intensive-based consensus protocols make high energy consumption to complete the mining process of blocks in the blockchain network. For this consensus category, different consensus algorithms are utilized in distributed blockchain networks [283]. In this system, miners mine the next new block because of the competitive approach among them and broadcast valid blocks to the network at the same time.

Miners-related network peers solve the various mathematical problems by cryptographic hashes to spend more time and energy. All network nodes preserve the block data in a blockchain where one section of the network-peer collects one block from one mine, and another section collects one block from another mine based on the network connectivity. However, the consensus protocols of this group face various sufferings, such as more energy consumption, low throughput, and less scalability during the data transactions. Capability-based consensus protocols are the algorithms of all mining processes in the blockchain system where it does not require high energy consumption for computing capability to maintain those protocols [284]. The capability of the mining process for a new block depends on a number of facts like the number of crypto-transactions, trusted networks, the amount of data storage, and their performances which are measured based on their own miners. The various consensus protocols of this category can minimize the high rate of energy consumption even though it faces some issues like network centralization, wealth dominance, and malicious activities. Another well-established category of consensus protocols is the voting-based consensus protocol which securely chooses a miner to produce a block [276]. These consensus protocols allow the network nodes to generate a new block in a chain. It operates among participating nodes for data transactions in the network through the new block validation. After that, these protocols reach an ultimate decision for their digital transactions. During the node selection operations, the voting-based consensus protocol can minimize the high energy consumption, the issues of the rich getting richer and malicious activities in the case of a failing node. Voting-based protocols can provide lower transaction throughput and better scalability compared to other group consensus protocols.

Blockchain layer-Block-chain controls the functioning of decentralized networks using a variety of cryptographic technologies for security purposes. Especially blockchain system consists of layered architecture to exchange digital data or currency. The structure of blockchain layers is shown in Fig. 10. A number of research articles compose the blockchain architecture by several layers such as the application layer, smart-contract layer, incentive layer, consensus layer, network layer, data layer, and infrastructure layer [285]. The application layer of blockchain architecture is incorporated with the various applications which interconnect data users with the blockchain network nodes. A variety of applications at this layer include user interfaces, ledger security, intellectual property, business applications, digital identity, etc., which enrich the blockchain environment. In this case, the application layer appends the capability of blockchain executions for digital data transactions in the applications of different industries or organizations. This layer can coordinate unreliable nodes, digital agreements, and cryptographic ingredients in the blockchain system for potential transactions of cryptocurrency to establish the privacy and security of user data. For the effective use cases of this layer, a specific and promising blockchain-based software development interface can be developed to exchange the data within network nodes and provide optimized management [286].

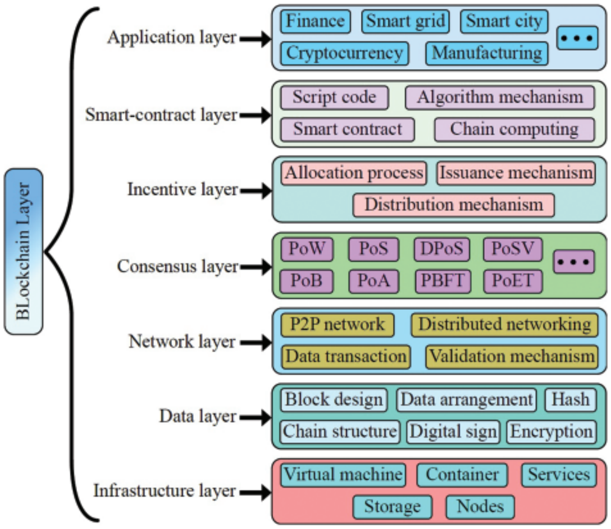

Figure 10: Blockchain layer

The Infrastructure-contract layer provides programmable instructions for secure transactions in the blockchain system. Blockchain-based programmable software must be verifiable, reliable, and secure for this layer because it utilizes different script codes and algorithms for various services and optional components with their smart contracts. This layer can correctly integrate smart contracts, chain computing, multi-signatures, data feeds, etc., within a blockchain system and another technical approach. Smart contracts are capable of storing user's digital data and transaction obligations in the blockchain using state-and-business response rules [287]. The incentive layer is capable of integrating the data transportation factors like incentive distribution, allocation process, etc., for the purpose of user interaction and secure data validation policy in the blockchain network, where it stimulates network nodes to contribute by their own hash power. This layer makes an incentive sketch using digital crypto-currency in a blockchain system where the rewards are distributed among the participants of network miners to provide transaction security.

The incentive structure [288] fairly sustains the security of the digital ledger in any permissionless blockchain environment. In this case, a minimum fee must be charged for transactions in the blockchain in order to achieve incentives from network miners. Thus, the incentive structure can be further improved to make a secure and trusted transactions environment. The consensus layer in the blockchain deals with the arrangement of the ledger within a decentralized environment to encapsulate the various consensus functions.

It makes the decision of node activities within a group of users, which attain a consensus in the network during the digital transactions by the verification of generated blocks. In this layer, the consensus algorithms are used to control fraud-related activities, verify the authenticity of the block, or ensure the fair transactions of data [289]. A number of significant consensus algorithms in the existing distributed blockchain applications are capable of ensuring the appropriate consensus within the decentralized user nodes in this layer. By this layer, the consensus techniques sustain the consistency of data transactions among all network nodes without replication or emulation. In the network layer, a blockchain system manipulates the functioning operations of a distributed network to share information with privacy and security. The network layer is basically engaged with various strategies such as peer-to-peer networks, data transactions, distributed networking, data validation, and more established procedure, which are significant for immune data interactions and distributions among users [290].

However, this layer can be designated as the perspective of data transactions through hardware in the blockchain networks. The network layer operates all activities of transactions in any public or private network using blockchain protocol-based software. By this layer, all services and resources of digital transactions are transmitted directly among the user nodes to maintain the data synchronizations in the entire network. Decentralized blockchain architecture involves a data layer where the distributed ledger is replicated on a vast scale. In a data layer [291], all network transactions are set in order to encapsulate the data encryption, hash value, and timestamped data in the blocks. This layer manages the design of the block structures, data arrangements, chain structure, secured transactions, hash functions, and data storage of the blockchain system. Consequently, this layer justifies the distinctive attributes or aspects to efficiently control various assembled data from the heterogeneous network. In the same way, it traces all confirmed hash blocks and securely verifies the integrity of existing transactions in the blockchain. The infrastructure layer is usually conducted to handle data transactions, data storage, information security, data mining and network protocol [292]. This layer specifically supports the activities of the physical and cyber infrastructure of blockchain applications. It can manage the supported functions for efficient transactions, information verifications, and infrastructure services across the decentralized network nodes.

3.2.5 Security Enhancement

Town-Crier is one type of technology that can connect as a bridge among smart agreements and existing web applications to support data integrity using interoperable Intel's Software Guard Extensions (SGX) with a trusted hardware environment [293]. This approach allows sensitive data processing to ensure privacy, reliability, and security for transactions in the network for accessing crypto-currencies and maintaining contracts. Town Crier system [294] provides high-trusted and authenticated data to adjust user credentials among HTTPS-enabled web applications and the blockchain. It performs a concise account of data named datagrams in the blockchain for secure and trusted environments through the act of retrieving web data. Town-Crier utilizes Intel Software Guard Extensions to keep safe data attestations against a lack of security or malicious operating system. The first and most suitable security exploration tool is **Oyente** which was designed to identify the potential bugs in smart contracts [295]. This kind of symbolic functional tool is used to control the loopholes policy of adversaries in Ethereum. However, it analyzes the byte-code of Ethereum-based smart contracts through the compiled EVM execution scheme, and this byte-code is stored in the blockchain. Consequently, Oyente can be an effective way to detect bugs during the byte-code storage of smart contracts in blockchain [296]. The potential security bugs such as the dependence of transaction-ordering with the timestamp, vulnerabilities, reentrancy, or mishandled exceptions can be discovered in the decentralized Ethereum system using the design of Oyente.

Hawk is a novel framework for advanced privacy-preserving and smart cryptographic contracts in the blockchain architecture. For the transactional privacy of decentralized intelligent contract systems, the hawk is used to endorse the transactional encryption in the blockchain systems where financial transaction data is not explicitly stored. It can produce a secure protocol for interconnecting with the blockchain to maintain privacy-preserving without cryptographic protocol implementation [297]. There is a hawk compiler to compile the writing programs in the intelligent contract system. This compiler produces the secure cryptographic protocol without conscious thought. The private parts of this system store the financial transaction data without involving public parts. On the hand, it writes those codes in the public part, which do not need privacy. The hawk system makes an inter-agreement with the blockchain architecture using the concepts of cryptographic primitives like ZKPs. Consequently, by avoiding explicit financial transactions from public's points of view, it can provide security and privacy to user's personal data in the blockchain.

A **smart pool** is one type of distributed pool mining concept that is designed for Ethereum and its classic networks to balance the maximum number of miners [298]. It works on the recent technology of the existing crypto-currencies to control the pool environments. The smart pool provides a good solution against making blockchain vulnerabilities for more mining pools and receives transactions, including data pool mining tasks from user nodes. The smart pool [299] clients receive the completed transactions to conduct the hashing computation of the system pooling task. These transactions or shares are performed to deploy a smart pool contract through verification, and the Ethereum client nodes accept the rewards. The advanced data structures and blueprints of the smart pool build its secure decentralized protocol where the efficient probabilistic verifications of this scheme for miners diminish the number of transactions and the expenses to conduct the pool.

A **quantitative framework** is used to make symmetry among the execution, performance, and security provision in a blockchain system by analysis which consists of a stimulator and a security model. The blockchain stimulator of this framework simulates the blockchain execution to apply the consensus protocol parameters and its blockchain-based network parameters as inputs. After the analysis of the stimulator, it achieves statistical execution performance to get the desired blockchain, where performance statistics contain block sizes and propagation times, network delays and throughput, stale block rate, etc. Markov Decision Processes-based security model in the quantitative framework [300] incorporates the security parameters and stale block rate as input components in which optimal adversarial policy and security provisions are built in the blockchain against attacks. Consequently, this framework commits the novelty of risk reduction strategies and insurance of a blockchain system against the attacks of double-spending and selfish mining.

3.2.6 Applications

The revolution of blockchain technology is very significant for anticipating the robust security of digital transactions in the current state of various applications. Based on a structured and systematic analysis, the blockchain-enabled applications are established across various domains such as financial transactions and Industry, smart contract crypto-currency, communication and networking, storage, universal services, identification, and certifications. If scalability, confidentiality, and integrity of data transactions can be ensured in blockchain applications for different sectors, blockchain will be an efficient mechanism for securing information.

Financial transaction and Industry-However, there are a number of applications for financial transactions and Industries, such as the industrial sector, banking sector, stock trading, insurance marketplace, garments market, energy segment, supply chain segment, and manufacturing sector, which are based on blockchain. By the secure recording capability and transparency of data transactions within distributed blockchain ledgers, it can establish trust in these financial fields [301]. Generally, in these domains, financial transactions can be faced with major disruptions in the traditional decentralized online medium for successful and secure transactions. Blockchain-based financial and industrial transaction technology [302] can be used in these promising sectors for the underlying new economic digital transformation and innovation. It can provide secure and more convenient services among the participants of the stock trading, insurance marketplace, energy segment, and supply chain segment. It confirms document certification, transaction reliability, and smart contract expansion when applying blockchain to the financial Industry and their transactions [303]. Banking, stock trading, insurance, energy, or manufacturing industry investigate and execute the expectations of blockchain technology to minimize transaction cost and time, including better security, confidentiality, scalability, and transparency [304]. However, blockchain technology is applied to insurance, stock market, energy, and supply chain management for performing digital transactions, general crypto-services, business operations, intangible data transactions, and smart management, including security enhancement.

Smart contracts cryptocurrency-Smart contracts can be utilized in the recent scenarios of various applications, and aspects based on blockchain for the efficient transaction processes of crypto-currencies [305]. A smart contract is a digital transaction protocol script of codes that are stored in a blockchain by automatically executing the terms of the contract. A smart contract reduces external risks without the need for a trusted party and can provide a solution for other applications beyond cryptocurrencies. It performs a trustless transaction process with the advantages of time efficiency, transparency, and cost-effectiveness in the decentralized blockchain system. Smart contract [306,307] in the effective blockchain assists any organization of various domains securely in developing and utilize the mechanism, including integrated infrastructure. The systems of smart contracts, such as Ethereum, bitcoin, etc., are used to transfer crypto-currency. Smart contracts provide higher security during the transactions among the parties in the decentralized network at lower costs.

Communication and Networking-In the communications and networking domain, blockchain technology can be applied to a variety of applications for its meticulous and high-level security in resource sharing. It provides reliable peer-to-peer data transactions to avoid possible attacks. This technology has the capability to enhance the communications industry with its better speed and security. An investigation into the latest blockchain-based communication and networking methods [308] can be conducted to create a trusted, timely and secure asset sharing scheme. Possible indicators of this scheme, such as trusted transactions, mathematical-logical modeling, cross-network participation, consensus method, cryptographic contract, auditing, and tracking, can be improved to get better performance. In the future, constructive initiatives can be expected to integrate telecommunications and satellite communication systems with blockchain for data security where a lot of various security devices are interconnected within the network against intruders [309]. The blockchain can provide resource sharing, computation, transaction verification, and data storage among the heterogeneous nodes of vehicle networks or aerial vehicle networks by ensuring data security and confidentiality.

Storage-Storage is a very important requirement in the digital transaction system to keep the data for future use or processing. Blockchain based data storage system is a data record approach in the decentralized infrastructure of any network while maintaining security and confidentiality. In recent times, blockchain has led to technological changes in the use of huge data volumes safely. For a decentralized infrastructure, data or files are stored in the computer system or cloud storage through virtual network transactions as well as multiple copies of data can be kept in any location of multiple storage. Data service providers must ensure data integrity and confidentiality in the blockchain storage. Cloud computing [310,311] is an approach to conducting a remote server network from a personal computer or local server in any location of a region to provide the processing data or resources among internet users. The blockchain-enabled cloud storage system facilitates low cost, better performance, secure access, or other services by maintaining sensitive large-scale data from remote organizations. During the storing of data and services through the decentralized network, this type of technology coordinates and integrates the user demands such as data management, security, agreement, privacy, and reliability. The edge computing [312] is a remarkable decentralized computing technology for transmitting data from storage or cloud computing infrastructure to edge servers with acquiring low latency, privacy protection, mobility, and transparent space. Hence, edge blockchain operates all edge services by offering the advantage of massive scalability over the heterogeneous network. Each edge server stores a variety of transactions in a blockchain system using a management controller, computational capability, and storage pool. The coordination of edge computing and blockchain facilitates to allocate of data resources for many applications through real-time, secure, and reliable transmission.

A blockchain-based application can play an important role in the case of erasable or non-erasable data management in accordance with personal or public data protection rules [313]. Blockchain technology detains the modification of any stored data in any block. Besides, if necessary, network users have the rights to erase their private information, or data [314] that does not comply with the rules on the immutability of blockchain systems. During the preservation of non-erasable parts containing valid block transactions in the blockchain, the erasable parts of data transactions can be deleted. Hash-based personal data can not tamper with where only personal data is stored in off-chain storage, which is also erasable if necessary. After erasing personal data, the rest hash as a non-erasable part will become permanently worthless in the blockchain system. It provides the integrity of the block without the loss of sensitive data or information.

The exploration of relational or non-relational database models makes important contributions to storing data and their different features in the blockchain network with strong security. A relational database is a mainstream tool that is used for data storage and management in business transactions [315]. The relational database is designed by Oracle Spatial, Microsoft SQL Server, or MySQL for distributed data management, resource management, or industrial process system. However, in some cases, it also faces unusual risks and challenges to big sensitive data storage protection and privacy while processing. A blockchain system named post-chain uses the relational database to maintain scalability or efficiency. Blockchain is mainly the storage of non-relational databases without some exceptional cases. Non-relational databases contain the rising unstructured data storage or big data storage, which are produced for increasing usage in our digital life on a daily basis. It involves NoSQL databases and works to store different types of data in distributed environments as well as changes it recurrently to the database. The non-relational database of recent digital applications has been designed by Hadoop ecology, HBase, Hive, or Open Source. It does not need to ensure strong transactional consistency to make a document-oriented and key-value database, but it provides performance and scalability. The main benefits of non-relational databases for blockchain systems are data flexibility, high speed, better scalability, and low cost.

It is required the record data separately for on-chain and off-chain efficiently in the decentralized blockchain-based data sharing system at the same time [316]. A standard blockchain model can ensure security and trust in both on-chain and off-chain for data collection, transactions, and storage. The on-chain storage guarantees the integrity of stored data, and the off-chain storage ensures the secrecy of stored documents. Generally, on-chain data is the transaction that is performed by the participants, and off-chain data is the privately stored information that is controlled by related participants or the local database system. In the blockchain network, normal nodes of the on-chain network encrypt the transmitted data before broadcasting it, and verification nodes operate the network power computation services. Off-chain network nodes process the storage and calculation of data by ensuring security and confidentiality.

Recently, blockchain technology has been used extensively in both transactional and non-transactional storage to protect data from any unauthorized access [317]. Non-transactional storage is a database including data references that controls the data of an organization that is not accessible or transferable using the online transaction processing system and stored in a main repository of the blockchain system. Master Data Services, which usually supports non-transactional databases, is designed to be shared across a number of applications. It maintains the immutability of non-transactional data within the blockchain network that can be associated with hash-based off-chain data [318]. Transactional storage is a database so that independent or dependent data transactions and their activities can be manipulated successfully at the same time. The transactional storage [319] will modify or extract data in a blockchain system completely; otherwise, it will have to roll back all the steps of the transaction without any change. Blockchain technology controls all communications of transactional databases in a reliable way while maintaining data integrity and confidentiality. A reliable, secure blockchain architecture needs to be developed for making data management decisions in regard to human resources, and data distribution [320]. In a blockchain-based database management system, the heterogeneous network can provide transparent, consistent, immutable, and trustless multi-party transactions in the process of human resource recording and data distribution across their nodes. A human resource-based blockchain scheme for scalable data transactions requires the adoption of multi-storage data management, smart contracts, and data leakage prevention in a public cryptocurrency environment.

Universal services-Blockchain technology has significantly influenced the different emerging applications or universal services such as education, smart cities, e-government, e-health, e-transportation, robotics, logistics, distributed ledger law, music, agriculture, entertainment, construction, and so on. The blockchain mechanism can provide transparency, reliability, auditability, privacy, and security during data record sharing through these applications. Blockchain technology can support different educational institutions [321] as a decentralized network to share and store information like as digital transcripts, certificates, the ledger of records, online programs, participations, and payments. Blockchain makes sure security and privacy of all educational documents and provides the guarantee of unchanged and authentic grades, degrees, intellectual property, and certifications. The most promising use of blockchain in education is to enhance the security and efficiency of intellectual copyright and patent. Educational institutions can have a large amount of data for students and alumni, which is a big constraint in terms of scalability, integrity, and immutability, which can be solved using blockchain technology.

There is a variety of network participants and stakeholders in the smart city [322] who exchange their data or urban services where blockchain technology helps to ensure data reliability and transparency. This system provides security and privacy for different city services by coordinating and verifying the secure transactions on the decentralized network. Blockchain significantly supports getting smart life and quality of services from all components of the city. Blockchain significantly supports getting smart life and quality of services from all sides of the city through increasing transparency and connectivity, maintaining direct communication, or verifying integrity over information. Block-chain-based e-government technology [323] securely stores information and services that are generated by a variety of data interactions or transactions among people and government organizations. Government can protect all transactional data with trust and accountability by controlling fraud, waste, and misuse using such technology. Blockchain technology can manage a vast database of a digital government which contains information of currency, payments, annual budget, land registration, digital identity, taxation, health care, vaccinations, electronic maintenance, corporate registration, voting, labor, an annual food, defense, and legal entities management. The government can provide all citizen services using blockchain-based web interfaces while maintaining data integrity and preventing all corruption.

Blockchain is the most significant technology in the field of healthcare [324] for data sharing, protected health records, medical resource monitoring, management scheduling, and interoperability of patients. This technology enhances the data security of consultations, personalized medicine, or medical personnel over the e-health networks. In blockchain healthcare systems, scientists can store and collect data on specific diseases, symptoms, and therapies for treatment to conduct clinical trials while maintaining transparency, accountability, and privacy. Blockchain maintains the security and confidentiality of information on the ingredients needed to store drugs and vaccines in the healthcare system ledger. This system can ensure transparency and integrity when exchanging data among clinics, diagnostic laboratories, or pharmacies.

Blockchain-based e-transportation system [325] enables to delivery of heterogeneous products and securely stores digital resources of logistics firms or organizations automatically or manually, and both way more efficient. To make it more efficient and profitable, agencies and firms need to further improve the administrative and order-tracking management of their transportation systems. Blockchain technology provides trustworthy and secure data through transportation networks and logistics management systems [326] to support the expected time and low cost. This technology can help to maintain all temperature-controlled products using an automatic tracking system in an efficient way without manual processing. Logistics firms or companies can implement blockchain technology to deliver goods using multiple freight vehicles by air, sea, and land. Blockchain-based smart transportation system stores all information like package name, manufacturer, model, location, etc., and ensures the coordination, connectivity, and availability between product's traceability with the consumers.

In the robotics industry, blockchain technology can play a powerful role in securing all robotics activities through data storage, and transmission [327]. As the use of robots, both public and private, is increasing day by day, it is necessary to secure the functional data of each robot in order to integrate it with many systems. So the blockchain can be utilized as a data exchanging tool within robots that perform the assigned activities or services with trustworthiness. The safe use of blockchain-based robotics is very significant for inter-robotic communication in many areas today, such as manufacturing, transportation, education, healthcare, entertainment, etc. This type of technology can make our daily life smarter and cost-effective, safer, and self-reliant. As blockchain technology is emerging as a transformative data security approach, so it can have significant impacts on the security within the Legal Industry. However, most law departments or the legal industries are heavily overwhelmed by a huge amount of paperwork, including personal and historical records, where it is time-consuming and difficult to search and preserve the desirable legislation using traditional technology. Distributed ledger law or blockchain-based legal system [328] can support lawyers in solving these issues by sustaining integrity and privacy. Lawyers can take advantage of their transactional scripted work for document simplifications and immutability using blockchain technology as well as the judiciary can ensure justice to consumers by maintaining transparency in less time with lower legal fees. Blockchain technology provides the security, integrity, transparency, and immutability for the use of all types of laws in all legal matters like as intellectual property rights, land registry, litigation and settlements, court records, legal opinions, funds transfers, etc.

Currently, blockchain is being employed in music industries [329] to eliminate major problems like copyright infringements or fake music resources. These industries are able to provide equitable royalty payments to artists. The musicians can easily record and trace music streams through transparency, security, and monitoring. Blockchain technology supports the storage of the information of artists, writers, and publishers in the shared ledger by ensuring music license during music recording. Blockchain helps any type of music company to pay directly to all the artists who contribute to the production of music and albums where there is no need for any high-priced middle-man among music companies and artists to make the communication. In the music sector, blockchain technology provides immutable recording composition, lyrics, and contents to control piracy. Blockchain technologies have a significant influence on the agricultural sector due to data trust and secure transactions over the supply chain. The purpose of the blockchain-based global agricultural industry [330] is to reduce agricultural transaction costs and increase transparency and accountability of farming. Blockchain-based agricultural system stores all farming and transactional data or information of the participants who are involved in agriculture. It continuously improves the quality of food supply chain management by providing trust among farmers and stakeholders by tracking different food sources or cultivated products. The certifications of providing information like safer food, faster traceability, quick access to shared data, test data to reduce waste, and temperature data are ensured where it maintains the efficiency, transparency, and trust from farms to groceries and ultimately the consumer.

It is very important to develop the web interface of entertainment sectors [331] for personal recreation or leisure activities so that the audience can hold attention and interest. Blockchain technology can be used to store all digitized information of virtual and real entertainment such as movie shows, video, and audio songs, online games, novels, gossip sites, and contents of historical or tourist places. This type of technology maintains data immutability and provides authentic data at low cost and less time. The construction sector is by far one of the largest and high impact industries in the world, which needs to be improved for economic growth and productivity using digital transformation. Blockchain technique as emerging technology can be conducted to build the construction sector [332] more efficiently, with maximum productivity with minimum expense, or fully automated as well as facilitates interaction between the contractor and the client. Construction data and their management information are stored within the blockchain as an immutable and digital replica which reduces the complexity and fragmentation of big projects. Blockchain-based construction system facilitates data transactions and tracking of assets like houses, vehicles, land, copyrights, patents, or intellectual property in the minimum time. This interface keeps looking at all works of construction, desired progress, material costs, regular schedule, and client payments by ensuring accountability.

Identification and Certification-Identity management system is very significant to users for their own information security. By this system and within any organization over the web interface, blockchain can provide authorization, authentication, and secure data sharing to users. The public key address is enclosed to the user's identity information, which is stored in a blockchain-based ledger to describe the actual identity [333,334]. By blockchain-based identity management, users can only ensure their identity through national identity, passports, driving licenses, user-centric identity, or student identity to any third party without disclosing the secret data. Such systems do not work for data transactions without the direct consent of the user and without confirmation of third-party details. There are some blockchain-based identity management systems such as Sovrin, MyData, ShoCard, UniquID, Cambridge Blockchain, Authenteq, etc.

In the virtual world, it is very important to provide digital assurance and security in the certification industry. Blockchain allows the certification processing system [335] to be more transparent to the users to attest capabilities and achievements of the certificate. Through this system, digital certificates for education, health, training, participation, award, experience, skill trade, software publisher, vaccination, etc., can be stored with immutability and security, which are accepted nationally and internationally by different organizations to prove the user skills. In such cases, national or international regulatory authorities can operate the blockchain network nodes, which verify and validate the digital information for certifications. However, a blockchain-based certification system can prevent the falsification of user certification data and maintain authentic information, as well as reduce the risk of losing or damaging the certificate. In recent times, it has become very important to provide the protection of digital copyright information through proper management. Blockchain technology can be utilized in digital copyright systems [336] to provide effective protection during copyright registration, confirmation, approval, storage, transfer, and search. Besides, this technology can significantly improve the traceability and availability of copyright information of different users or organizations. The blockchain-based copyright system [337] can promote the long-awaited transparency and proof of daily generated digital works, including ensuring user's accessibility to history, law, software, audio, video, games, intellectual property, paintings, sculptures, films, books, real estate, map, and technical drawings. This system can terminate any piracy or online piracy on original digital copy due to maintaining data accuracy and immutability.

Blockchain ownership systems can facilitate the security and management of data ownership to users [338] when distributed and shared publicly across the entire network. Blockchain tracks ownership of its own material and its transactions by maintaining centralized control and mitigating high transaction delays. The blockchain system can transfer the ownership of resources in a realistic way according to how our country or society operates in the ownership of resources, without any fraud and while maintaining security. This system evaluates the functions of all transactions of its own resources for business purposes and plays a significant role in information regulation, transparency, anonymity, traceability, and security. Digital content management can be developed to distribute different forms or copies of digital data to desired consumers over the network. Blockchain systems can securely store digital content in specific formats [339]. Blockchain technology ensures authenticity when distributing various copies of digital content such as video, audio, photo, visual story, text, news, advertising, quiz site, web mapping, etc., to customers. The blockchain system ensures verification, auditability, identity, and privacy during the distribution the digital content to consumers with violation tracking and content protection.

Reputation management systems using blockchain can contribute to consumer appraisal and build their trust in e-commerce, organization, and agency services [340]. This mechanism can emerge as better management of reputation in online communities. This system can generate a reputation score by the feedback of consumer ratings of different services for future interactions with different quality resources of companies which will help to make future consumer decisions. Blockchain enabled reputation management technique handles consumer opinions or reviews on online and offline services that are stored in the blockchain cloud, then these opinions are recorded in reputation-based trust schemes [341] to improve the reliability and accuracy of services. In this case, blockchain technology allows an immutable distributed ledger of reputation and identifies malicious evaluators.

3.2.7 Block-Chain Analytics

Different types of data analytics have been specifically established based on technical and engineering methods. Blockchain analytics [342] is one of the emerging approaches and has a major job role in data transactions in storage or cloud. So, it is essential for blockchain transactions in a heterogeneous network of organizations and institutions where data blocks are protected against illicit activities. It can help to minimize transactional crime risk to make safer and more compatible storage. Analytics on blockchain transactions [343] are morally acceptable tools to ensure the security of consumers, organizations, and their social prestige. It can be used to track the risks of transactional data offenses to restore user confidence in the data blockchain and ensure overall success. These analytics represent the blockchain-based data analyzing, clustering, and recognizing processes on decentralized networks where all the desired information will be accessible to users. Blockchain analytics [344] allows modern crypto businesses and their diversified regulation. Blockchain analytics make trust and transparency for fair and legal data transactional environments to allow modern crypto businesses and their diversified regulation. Recently, blockchain analytics tools like Chainalysis, Anchain.AI, TRM Labs, etc., are being used in the professional fields for risk management, compliance, investigation, and monitoring. Blockchain analytics helps in the transparent data transaction process, enhances efficiency, and identifies the integrity of generated data.

3.2.8 Block-Chain Tokens

Tokens have arisen to perform the assets, security, utilities, rewards, or claims in the blockchain technology as well as to represent their serviceability [345]. The ideal value of tokens, such as traceability, transferability, divisibility, and usability, can be executed digitally for the right management during data storage. Users can access all rights over existing digital or naturalistic resources from storage by executing token agreements and a set of permissions. To attain a specific and shared target individually, it approves transparent and fair transactions among the participants of the virtual market or dealings. These tokens have pertained to a part of the blockchain address and their certain behaviors. Tokens [346] can supply and stock the resources quickly and easily with low transaction costs, transparency, and trust in a blockchain-based decentralized ecosystem. However, tokens have a role in allowing access to services, fair distribution, enriching user activity, and approving owner rights in the blockchain. There are different types of intriguing tokens for their corresponding use case in blockchain, such as utility tokens, reward tokens, security tokens, investment tokens, asset tokens, donation tokens, currency tokens, etc. Specific regulatory rules and standards are followed for the creation of different tokens depending on the different features in the blockchain network system from an adjusting perception. In the blockchain-based distributed system, tokens contribute to increasing productivity, reducing corruption, controlling access costs, improve supply chain diversity.

Table 1: Recent trends in blockchain-based network applications of each appraised research work

Reference	Platform	Accessing mode	Research goals	Contributions
[347]	Blockchain based multiple cloud storage model	Multiple users	Signature verification efficiency, better bandwidth	Multi-cloud compressing storage space provider
[348]	Storage model of SACBDIBT	A number of user nodes	Store high throughput of crop breeding data	Formal analysis, Validation
[349]	Blockchain based FNC	A number of mobile users	Reduce computing power consumption and storage spaces	Time-aware computing set allocation procedure as heuristic algorithm
[350]	Blockchain driven ordered anomaly detection model	Private blockchain network	Anomaly detection, to reduce the ledger data length	Managing log data by edge intelligence design and feature extractor
[351]	Firmware over the Blockchain (FOTB) scheme	Multiple vendor nodes	Design blockchain based firmware against major cyber attacks	Performs heterogeneous IoT ecosystem and computation cost
[8]	Cloud storage optimization scheme of Blockchain	Multiple users	Increase the capability of blockchain and reserve it in the cloud storage	A multi objective optimization model in blockchain with NSGA-C
[352]	Blockchain based University Management record system	Public network nodes	To evaluate CPU utilization, loss metric, misclassification rate	A heuristic K-anonymity privacy preserving model
[353]	Blockchain based e-governance scheme	Private network	To analysis the security of e-governance services	Privacy preservation in e-government network
[9]	Lightweight blockchain storage optimized scheme	Private blockchain	Minimize communication overheads, storage cost and threshold	Improved PBFT blockchain, blockchain storage optimization
[354]	Secured cluster scheme with blockchain based SDN controllers	Public and private blockchain	To gain better throughput, lower energy consumption or delays	Security and energy efficiency mechanisms for SDN controller

(Continued)

Table 1 (continued)

Reference	Platform	Accessing mode	Research goals	Contributions
[355]	E-health network scheme based on blockchain	Committing, ordering and endorsing nodes	To detect the counterfeit medicine and find the medicines shortage	A trustworthy medicine authentication system
[356]	Secure and robust healthcare based blockchain	Multiple users in cloud	Maintain data security, Minimize execution delay	Healthcare data recording, services monitoring
[357]	Blockchain and CIDNs based combinational scheme	Three skill level network nodes	Enhance robustness of combinational scheme	Simulated and real network scheme with trust
[339]	Medical data preservation scheme	Social network nodes	Ensure protection and privacy of health records	Blockchain data record process with protocol
[358]	Blockchain based E-voting and counting scheme	E-polling IoT nodes	Security measures, correct or false authentication delay	Blockchain E-voting mechanism
[359]	Hyperledger fabric model with Distributed usage	Permissioned blockchain	To ensure trust and impose transparency	Extended access control model for business execution
[360]	Distributed cognitive manufacturing blockchain ledger	Distributes to large number of networks users	To make efficient manufacturing ledger management	Accuracy evaluation of blockchain based topic mining process
[361]	Edge computing enabled scalable blockchain network scheme	Mobile users of social Community	Minimize complex relationship, large storage, response time, propagation delay	Edge computing framework with dynamic throughput adjustment
[362]	Blockchain based smart DC Microgrid scheme	Public blockchain link	To enhance cybersecurity and detect data attack	Precise and robust detection process based on spectral energy
[363]	Secure mist computing based ITS	Global and local network nodes	Enrich security and privacy of intelligent transportation system (ITS) devices	Registration and authentication Algorithms for ITS
[364]	SDN controller scheme of distributed fog node network	A vast number of fog network nodes	Low-cost, better throughput, secure and on demand access to IoT network	Blockchain based secure distributed fog node architecture

(Continued)

Table 1 (continued)

Reference	Platform	Accessing mode	Research goals	Contributions
[365]	Blockchain based e-government system model	Permissioned blockchain network	Ensure sufficient privacy and security of decentralized data transactions	Secure and privacy preserving e-government nodes and user nodes
[366]	Blockchain based decentralized architecture of VANET	All participating nodes in VANET	Ensure security and integrity of SBMs with blockchain, vehicular identity privacy	Identity and location privacy protection UGG, IPP and LPP algorithms

Table 2: Comparative explorations from each appraised related literature

Reference	Crypto approach	Benefits	Shortcomings	Future directions
[347]	Identity based proxy aggregate signature	Reliability, integrity, availability and access efficiency of data	Only user data view from administrator side	Reduce a large amount of data and communication cost
[348]	Proxy encryption technology	Scalability, low cost, security, storage efficiency	Limitation of storage capacity	To build standalone storage framework
[349]	Cryptographic hash algorithm 256	Security and storage in fog computing system	Small scale fog node clusters (FNCs)	To implement an optimized fog computing scheme
[350]	Hash-map including raw logs	Data integrity, accuracy	Uses resource constraints and limited nodes	To evaluate the latency of blockchain based real network
[351]	PUSH and PULL update mechanism	Integrity, authentication	Limited storage capacity	Analysis to protect against other cyber attacks
[8]	Nondominated sorting genetic algorithm with clustering	Decentralization, reliability and reduce storage cost	Blockchain application for local space occupancy	To explore business blockchain models with support more peers
[352]	K-Anonymity technique	Throughput, latency	Uses publicly known data only for anonymity	Work on sensitive and non-sensitive data for further enhancement
[353]	Chameleon hashing mechanism	Data authentication, confidentiality	Limited structure with hypothetical dialog level	Work on more security defense of quantum computing

(Continued)

Table 2 (continued)

Reference	Crypto approach	Benefits	Shortcomings	Future directions
[9]	PBFT, score voting based byzantine fault tolerance	Efficient consensus service, lower recovery delay	Only store coded segments part of every block	To work on network overhead
[354]	Hashing and POW based blockchain fundamental	Secure and efficient file transfer among IoT elements	Heterogeneity and scalable limitations of IoT devices	Design a high level P4 architecture based on blockchain
[355]	PBFT technique	Data transparency, immutability, privacy	Not exclude the unauthorized medicines uses	Design the ledger-based event tracing
[356]	Attribute based Encryption	Privacy, cost efficiency in healthcare	Implements centralized healthcare services	Ensure privacy, validation and confirmation
[357]	Cryptographic hash function	Data scalability and trust, IDS	Computational power with distribution complexity	For validation and authentication across network
[339]	Elliptic curve cryptography and blockchain	Authentication, anonymity, efficient computation	More computational power and electrical energy	Design a practical medical system with scalability
[358]	Blockchain enable biometric approach	E-voting result authentication, transparency	Storage and biometric security complexity	Work on blockchain based real time e-voting database
[359]	Chaincode policy	Resource management network	Scalable network complexity	Work on extended permission model for variety of business
[360]	Sidechain based distributed consensus topic mining	Secured cognitive manufacturing services	Transparent and scalable data ledger complication	Design a data storage of scalable manufacturing ledger
[361]	SHA-256 hash with task offloading algorithm	Light-weight micro blockchain with traceability, throughput in social environment	Multiple transactions and transparent complexity	Plan on standard mobile social network
[362]	Crypto graphic hash function	Secured data exchange in the smart DC microgrid agents	Ambiguous computational time in suggested digital transactions	Design a real time smart DC microgrid controller

(Continued)

Table 2 (continued)

Reference	Crypto approach	Benefits	Shortcomings	Future directions
[363]	Blockchain based best combination hash in ITS	Scalable and distributed ITS network	Concerns about latency and throughput in 5G network	To provide rich multimedia services in ITS Network applications
[364]	2-hop blockchain technique	Provides IoT services in real-time driven computing infrastructures	Questionable data storage ability	Several energies harvesting technique over efficient communication
[365]	Decentralized crypto graphic algorithm with signature	Privacy and authentication of e-government services	Initial stages of expansion of data interoperability in public sectors	Explore and implement in a real-world environment
[366]	Hash of safety beacon messages (SBMs)	Efficient transaction and storage management in VANET	Analysis only two aspects: connectivity and average distance	Works on optimized vehicle communication system

3.3 Heterogenous Network on Blockchain

3.3.1 Organ

The single-hop and multi-hop data relay system using blockchain technology is a promising method for accessing and storing the data of node users across the heterogeneous network through improving information availability and accountability while maintaining data confidentiality and transparency. Applying single hop or multi-hop communication system [367], sensor nodes of the heterogeneous network accumulate the data from the surroundings in order to relay to the desired stations, which are used in applications of the naval academy, national defense, meteorology, agricultural economy or other organizations. In the single hop construction, packet or messages are relayed from the source to the desired station by employing a single networking design. Packet dissemination must be verifiable when a single network immediately transmits its data to the base station. Data transmission of single-hop construction is limited or within reach of a small networking area. The blockchain-based single-hop protocol can be efficient for relaying encrypted messages or packets in wireless networks through end-to-end authentication and confidentiality. Multi-hop communication system [368] is a technology that mainly supports transmitting the collected packets or data from the source node to desired destination node using two or more networking appliances through the routing protocol. This system maintains and covers a large network area for relaying the data. Blockchain technology provides verifiable multi-hop communication across the heterogeneous network in a privacy-preserving, fast, fault-tolerant, transparent, and accountable manner.

Typically, the antenna is deployed to transmit the signal of radio frequencies. A distributed antenna system is a connection of an antenna network to a universal source where data or signals of product packaging boxes and various materials are distributed over the network area using advanced technology [369]. This system can maintain security and reduce the high cost of transmitting signals through the minimal antennas on the distributed network using blockchain technology. The blockchain-based distributed antenna system can work against poor coverage inside a wide area by efficient and affordable power like repeaters. This type of system can be utilized in indoor or outdoor wireless carrier networks [370] to cover different types of services like airports, hospitals, institutes, hotels, subways, etc. It upgrades the quality of signals transmitted among the antenna components by adjusting the time variation, as well as amplifies the signals through the central controller as needed. It is very important to develop the blockchain-based antenna system to get better correspondence signals through laptops, cell phones, and workstations across the world in emerging economies. This system can help to share multiple carriers or signals to a large number of subscribers with maintaining low cost and transparency of data services in the heterogeneous network. Distributed antennas using blockchain technology can boost spectrum sensing performance and get better network throughput when transmitting signals.

Wi-Fi is a technology that allows access to data from any device through a wireless LAN network where intermediate-person or hackers can get eavesdrop on the activities of connected people by making Evil Twin. Blockchain technology can provide controlled access to approved users by regulating various security vulnerabilities in Wi-Fi network systems [371]. By applying blockchain technology to the Wi-Fi network, personal data can be safely managed, collected, stored, and fast transferred. This technology can help various companies or organizations reduce service costs for their governance and business by maintaining confidentiality and quick access to information. Blockchain can be employed in an efficient heterogeneous network design with cell technology in order to manage the handover traffic and reduce the interference and blocking probability. The properties of the heterogeneous network have established the deployment of picocells, metro-cells, femtocells, or small cells to provide better coverage and higher capacity as well as ensure the guarantees of good quality of services [372]. Picocells or metro-cells can be implemented in the public access domain, and femtocells are used in consumer-grade areas to offer low-cost network capacity expansion. Small cells are conducted to short-range access points, including low-power, for enhancing coverage and capacity. Moreover, these blockchain-based cells can facilitate traffic interaction regulation and mobility management across a heterogeneous network. Blockchain technology can be used for cloud, cloudlet, and fog radio access network services by ensuring trustworthiness, security, and reputation in information transactions [373]. To get potential benefits, better scalable solutions, and low latency, the integrating infrastructure of a blockchain-based radio access network can support sensitive and intensive IoT applications or industrial manufacturing operations by harnessing artificial intelligence capabilities. As well, this infrastructure can provide the availability of radio access, minimize traffic and limit the interference level for sharing heterogeneous network resources.

3.3.2 Scheme

Network analysis on heterogeneous networks can be performed across any online domain like as e-commerce, multi-media, social site, industrial network, and other online applications. By various advanced techniques, network analysis can be constructed from the analysis of objects or text data and their relationships across this network [374]. Network analysis typically can involve the efficacy of the clustering system, the performance of link prediction, and the evaluation of object ranking. It computes the relevance matrix of object pairs or text data using the relevant measurements based on the different meta paths. Afterthought, it stores these objects, which are constructed by efficient computing strategies. However, this analysis can supply the semantic recommendation services and different predicted rating scores under each meta path. The network model is an emerging design across heterogeneous networks based on unique features such as rich semantics, complex structures, etc. This model integrates various objects under the meta paths and associates the semantic services by creating connecting relations [375]. In the heterogeneous network, community detection (called clustering) is needed to accurately appraise the contributions of multi-typed objects, including their relationships to abstract concepts.

A scalable identification system can be designed by the exploration of all network nodes model in order to sustain network security. In this case, the network model such as star, bipartite, or arbitrary model can be more widely used over heterogeneous networks than homogenous networks to cover all data or information. The data extraction system extracts data from various data or resources of different online applications to construct a heterogeneous network [376]. The layer of this system works on data extraction and performs data exploration for better network analysis [377]. It contributes to storing the correct data, including unified format, in blockchain under the metadata paths. Data extraction schemes are more cooperative for processing data access across heterogeneous networks. The recommendation service scheme across heterogeneous networks helps to present a compatible and concise web interface where node users can locate their expected services. It ensures the quality of services for recommendation services through installing various meta paths [378]. However, the recommendation service scheme typically incorporates the semantics-based recommendation service, contents network-based recommendation service, social networks-based recommendation service, collaborative filtering-based recommendation service, and hybrid recommendation service.

3.3.3 Dataset

There is no standard dataset of widely used information or resources in heterogeneous networks due to the various data perceptions that exist in different data sources. For the importance of various object set and link set in a heterogeneous network, it is necessary to specify the meta-structure and relationships among different objects of a network. In precise, structured data, semi-structured data, and non-structure data can construct a heterogeneous network scheme [379]. Structured data typically refers to tabular data that follows the predefined data models and formats for storing in a relational database. The entity relational elements of this dataset are addressable for constructive analysis in a database with rows and columns. A heterogeneous network scheme [380] can be developed by using different-typed entities of the database and their relationships as structured data. The structured data model provides less flexibility and more interdependency in memory utilization through the minimization of data redundancy. The representation of incomplete and irregular data into database cells is semi-structure data which is not thoroughly compatible with specific dataset models over the heterogeneous network. Nonetheless, it contains elements that construct it easy to separate fields and records within the information, as well as make it easy to analyze the data properties. Semi-structure data is preserved as JSON, XML, HTML, RTF documents. Non-structure data of heterogeneous networks can be extracted from non-traditional objects and their relationships. Unstructured data [381] represents a large amount of various text data within the information service system without any database. It does not contain any predefined data structure, so it processes a variety of information in all formats, such as text, images, audio, video, etc. The processing and analysis of non-structure data across heterogeneous networks are important to the authorized users due to more storage space is required.

3.3.4 Network Technology

In the case of the heterogeneous network and communication field, software-defined radio (SDR) is an optimistic and realistic technology that handles the capabilities of the flexible and high-performance signals and routing processes [382]. This type of technology supports the transactions among the entities of a heterogeneous wireless network for the growing demand for imaging and video communication applications. It helps in the development of various modern radios by adjusting the parameters of software configuration with hardware platforms. SDR offers adaptive communication protocols by integrating heterogeneous networks for accessing any network in many domains at any time. However, the implementation of signal processing components of SDR would be beneficial for cognitive radio and heterogeneous networking environments. By identifying and analyzing the vulnerabilities for security purposes, SDR technology ensures secure transactions and enhances the frequency spectrum.

As a promising technology in distributed network infrastructure, software-defined networking (SDN) adopts a network controller and manages network configurations and their operations [383]. SDN is capable of facilitating network transactions by coordinating all optical wireless-based small cell networks and their radio frequencies. It provides network services, including operational mobility and functional cost reduction. This technology makes a programmable interface in the network as a software-defined network [384] by isolating the decisions and behavior of the network using the forwarding infrastructure controller, which means this network has been decoupled into the control and data plane. It ensures the enhancement of the security, availability, and stability of network services. The functions of various networks can operate on proprietary hardware as software in a virtual machine using network functions virtualization (NFV) technology, where NFV activates the decoupling process of network functions from hardware appliances [385]. The virtual machines in NFV technology mainly employ a hypervisor to operate the networking software and virtualize processes of network services like routing, firewalls, or load balancing. In this case, a number of virtual machines can apply on the industry-standard single server from anywhere to accomplish the distributions of secure network resources or big data. NFV [386] can help facilities reduce the network power and maintenance costs as well as optimize the network hardware space. However, it offers significant management for flexible network deployments and their operations by solving compatible issues.

The hybrid networking approach is a novel capacity-sharing network infrastructure where the functionalities of SDR, SDN and NFV can be performed to achieve all the purposes of networks [387]. The hybrid networking solution of any recognized network infrastructure can ensure the coordination of heterogeneous network protocols, equipment, and different network pattern interactions. A well-functioned hybrid network can support physical and virtual network appliances for providing an actual route of information transactions. Hybrid network architecture facilitates the improvement of data transmission, data rate enhancement, less wastage of hardware resources, and improvement of communication efficiency. However, the hybrid network model would be based on a data plane, standard configuration protocols, separated control of the network, network functions virtualization, reliability, and efficacy of the connection.

3.4 Summary of Critical Review of Existing Works

This section presents a summary of critical reviews of relevant work on blockchain-enabled various cyber networks. In this analysis, it can be observed that cyber security interactions are crucial in managing blockchain-enabled digital data transactions across decentralized networks. It can be seen that most cyber systems are using blockchain technology to trust data transactions, but cyber security is still an issue in various activities. Existing works highlight how cyber security attacks play into data manipulation techniques. Researchers are trying to analyze how blockchain technology can be used to protect management from cyber-attacks by providing security. In this case, the research community can analyze the effectiveness of specific cyber-attacks on blockchain systems using the cyber-attack concepts discussed in our study.

More research is needed on how efficiently blockchain technology can defeat or suppress the cyber-attacks mentioned in this study. Here are presented possible blockchain-based solutions for data transaction decision-making across heterogeneous blockchain-based networks. Data access control, authentication, honesty, integrity, confidentiality, etc., are discussed as secure data trust management strategies across heterogeneous networks. It summarizes the potential features and strategies of this technology to achieve trust in data management and transactions. Potential solutions for the ability of heterogeneous network devices to transact data are explored. The integration of potential solutions across heterogeneous networks with blockchain systems will reliably stimulate researchers. Consequently, we are motivated to provide a comprehensive survey of blockchain-enabled cybersecurity provisions for heterogeneous networks. Table 3 compares our survey with some recent relevant surveys, where "✓" is for "mention" and "✗" is for "not mention".

Table 3: Comparison of our survey with some recent relevant surveys

Key context	[388]	[389]	[390]	[283]	[276]	[189]	[7]	[391]	Our
Explicit the full taxonomy structure	✗	✓	✓	✗	✓	✗	✗	✓	✓
Focus on consensus mechanism	✓	✗	✓	✓	✓	✓	✓	✓	✓
Discuss potential cyber security risks	✗	✓	✗	✗	✗	✓	✓	✗	✓
Emphasis on cryptographic technique	✓	✗	✓	✗	✗	✓	✓	✓	✓
Present the propagation mechanism	✗	✗	✗	✗	✗	✗	✗	✗	✓
Promising focusses of HetNet	✗	✗	✗	✗	✗	✗	✗	✗	✓
Proposed design	✗	✗	✗	✗	✗	✗	✗	✗	✓
Focus on key issues	✗	✓	✓	✓	✓	✓	✓	✓	✓

4 Proposed Model of Blockchain-Based HetNet Application with Cybersecurity

The section of this research work proposes the secure design of a blockchain-based scalable heterogeneous network to meet the goal of maintaining optimal performance data transactions among organizations over the cyber world, which is shown in Fig. 11. The valid users can participate in any type of consensus protocol of blockchain platform to consent on each block for multipurpose and high-quality transactions. The data integrity and confidentiality of any organization can be made by this proposed model over the heterogeneous network. The heterogeneous and interoperable transactions through cross-chain technology in this model can perform data satisfaction and verifications among the users of any organization. This mentioned model can enhance user trust in data availability and correctness in the professional activities of any organizational website. The proposed model allows users to transfer secure and scalable digital resources from one blockchain to another, which is quite different in terms of data exchange from conventional websites. The necessity for secure transactions of all types of data certification or digital assets of any organization is increasing worldwide, where the mentioned blockchain-based framework can be proposed and analyzed to get scalable transaction solutions in the heterogeneous network. This web architecture can be designed for an organization to upload and store its collected data in a permanently decentralized ledger. The main transactional activities of the model can be described as follows.

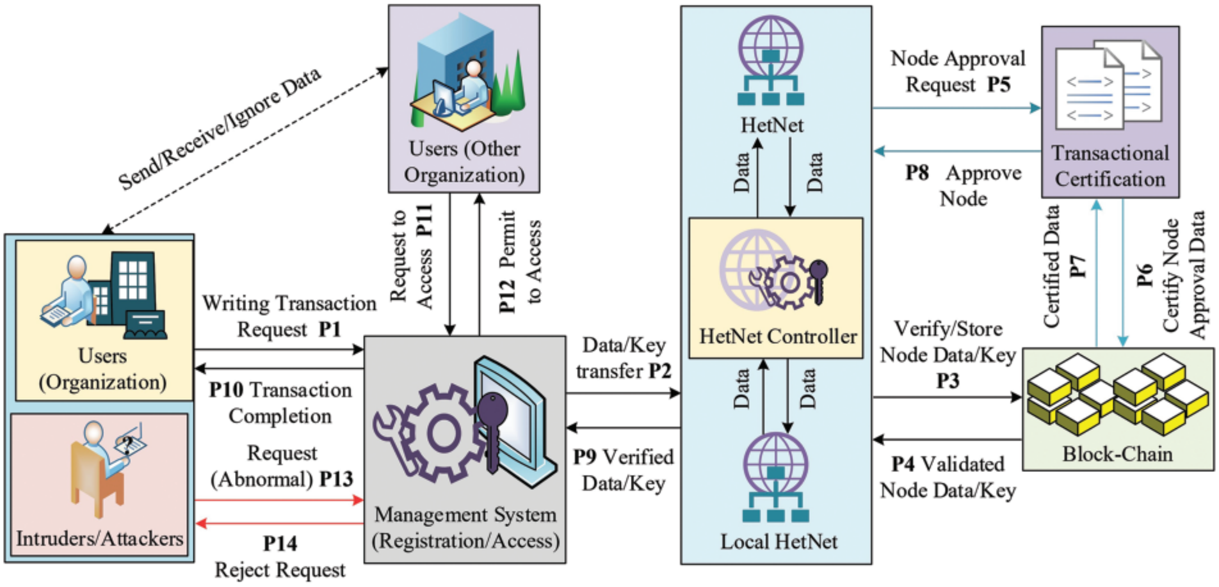

Figure 11: Proposed model of blockchain-based HetNet organization with cybersecurity

In this scheme, two or more organizations can be engaged to securely share their data when available. Firstly, a user can enter this platform to access digital resources or certified files. All activities of this architecture can be operated by two or more organizations and their users. These operations can be controlled by organizational controllers or managers. Participated organizations can securely generate and assign data keys of the user digital resources for their own users separately, but they can not produce public user data keys. The users can provide their data using the data key in the blockchain ledger or allow it to share with other organizations. However, organizational controllers can originate or modify their digital resources using the user data key within the blockchain ledger. The controllers of these participating organizations can produce a set of session keys for each of their individual transactions without sharing those resources with intruders. In this case, one organizational controller will allow sharing their resources with any other organizational controller, and the recipient organizational controller can generate a receiver data key in the blockchain, which can be used to access the data for reading or observing. But recipient organizations can not generate sender public keys, as well as they can not modify sender records.

However, users of all participating organizations can access their data resources using their own data keys, whereas a user can only key in their own data and cannot able to update any records in the blockchain ledger. In the web application, the management system module can usually allow the users to register to generate their own and identical digital accounts with their individual public keys. This module will issue a secret digital user name and user password to the user when creating an identical digital account. They can observe their authentic information on their access level using their account. At the time of each user registration, each created public key can be approved through cryptographic algorithms to sustain data integrity, and all generating account information will be stored in the blockchain ledger. This module allows the registered users of the participating organizations if would like to access or share their self-information from the blockchain through a heterogeneous network controller. It will ensure data security, availability, and scalability during the interactions among users in this system. But this module will not permit intruders to access this platform because this system will verify the user's cryptographic hash key. Another module named

HetNet Controller will specifically operate the blockchain data distribution to interconnect different types of devices, technologies, operating systems, nodes, and protocols over wireless networks. It can be used to distribute blockchain approval data among big data application-based organizations. When users of participating organization request the management system controller for data access, i.e., data upload, view, store, share from blockchain, it must be securely executed through the HetNet Controller. The secure, heterogeneous, and interoperable data storage unit of the blockchain technology-based organizational system will be designed using the cross-chain mechanism for decentralized data distributions. All transactions will be validated and certified by generating the SHA256 hash of each record where SHA256 is recurrently used to compute the data hash value in this system.

However, the two organizations can share data with each other in heterogeneous and distributed networks, which is the main purpose of this proposed model using blockchain technology. The proposed platform is mainly designed for the operations of user registration, data store, access, update, rejection, or ignore, which are presented as follows:

Operation-1 (Registration): Participating users of an organization can automatically get the username and secret key of their digital identity during the registration process. In this module, the registration process of users can be led through P1, P2, P3, P4, P5, P6, P7, P8, P9, P10.

Operation-2 (Store): After concluding registration, valid user can store their own writing data using their own digital identity through Management System and HetNet controller in the blockchain. In this case, all processes of digital data storing can be performed through P1, P2, and P3 after getting transactional data certification by using P5, P6, P7, and P8.

Operation-3 (Access): The users of the main organization can access their data. But the users of other organizations can only request to access specific data using the digital user identity of main organizations if they allow it. However, other organization users cannot be able to change the data but only view data. In this module, the access procedure can follow the P11, P2, P3, P4, P9, and P12 pathways.

Operation-4 (Rejection/Ignore): If an intruder or attacker as an organization user sends a request to the management system in disguise, then the management system will decline or ignore the request through P13, P14. In this case, the writing key of all abnormal requests will not match with the certified secret key of the specific resources.

The proposed model can be used for data transactions in any organization, be it an educational institution, health center, banking enterprise, telecommunication sector, and so forth. The proposed blockchain-based cybersecurity model can help ensure the security and integrity of data transmitted to the nodes of heterogeneous network applications in these sectors. Here can be an example of how this model works in data transactions in an organization like a health center. A health center architecture based on the blockchain can be used to collect patient data, where the data is exchanged and stored in decentralized storage through various nodes in the network. Each node or device in the decentralized network will be equipped with a unique digital signature, and transmitted health data will be encrypted. Then block data will be generated by verifying health data using a digital signature and consensus algorithm. Encrypted data will be added to the blockchain. This blockchain-based model will allow only authorized healthcare professionals to access data. Thus, a blockchain-based cybersecurity model of this type can be used to ensure the security, privacy, and tampering resistance of sensitive healthcare information.

The cross-chain technique can allow data transactions over distinct blockchain networks to increase various blockchain interactions by generating system interoperability. The cross-chain mechanism in the blockchain platform for the participating organizations is shown in Fig. 12. PoW and PBFT consensus algorithms can be used in cross-chain interactions among heterogeneous blockchain networks. For cross-chain coordination, two or more blockchains can be used to perform the protocol and transactional operations across the different participating networks. In this scheme, blockchain 1 contains the user's block data of an organization, and blockchain 2 holds the user's block data of another organization; both will be used for executing data transfer in cross-chain protocol synchronously.

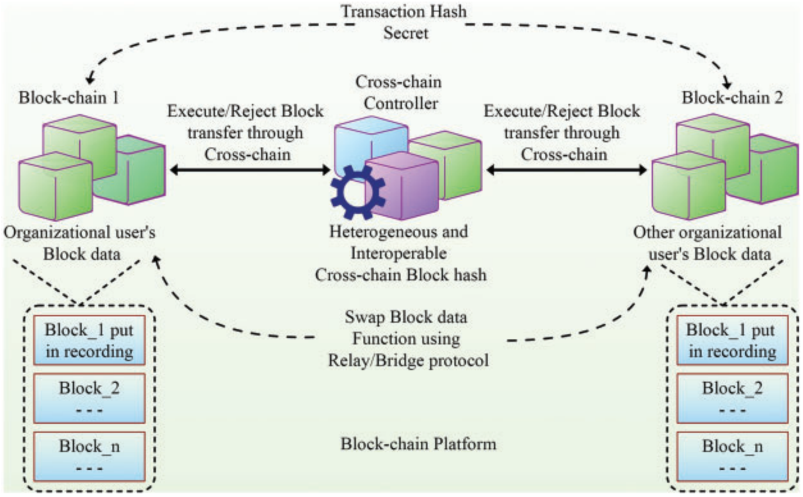
Transaction Hash
Secret
Block-chain 1
Execute/Reject Block transfer through Cross-chain
Cross-chain Controller
Execute/Reject Block transfer through Cross-chain
Block-chain 2
Organizational user's Block data
Heterogeneous and Interoperable Cross-chain Block hash
Other organizational user's Block data
Block_1 put in recording
Block_2
- - -
Block_n
- - -
Swap Block data Function using Relay/Bridge protocol
Block-chain Platform
Block_1 put in recording
Block_2
- - -
Block_n
- - -

Figure 12: Cross-chain mechanism in blockchain platform for participating organizations

During the performing of a data block swap, the user of one blockchain make a timelock contract address and generate a secret value for the calculation of the transaction hash. Then this user puts its data to the creating hashed contract address. It transmits the secret hash value and contract address to the other blockchain. However, an organization's users want to share or transmit their block data from blockchain 1 to the users of another organization in blockchain two and vice versa. In this case, any blockchain will look forward to collaborating with another blockchain. In this design, the validated block data can be swapped using relay or bridge protocol between both blockchains. One blockchain as a host will verify the block data from another visitor blockchain using a consensus algorithm in the interoperable cross-chain. The cross-chain controller will support communication between the operations of these blockchains. But, the block transfer in this process can be updated or discarded for both blockchains according to valid protocol appearance with transaction hash secret.

5 Open Research Issues

This section could play a significant role in further research to improve the existing architectures or systems across the distributed heterogeneous network using blockchain technology. However, the key issues regarding the implementation of blockchain-based cybersecurity in decentralized networks have been mentioned to further improve these systems. In order to achieve the design and implementation goals of blockchain applications, some major and critical issues may arise in terms of security, storage, network intelligence, energy with sustainability, time spent dealing, system uncertainty, standardization of transactions, and assurance of trust, which are constructed in Fig. 13. Also, the blockchain-associated network access design for addressing the identified issues is shown in Fig. 14. In this case, the solution to the identified errors in the management of relevant services of an organization introduces the principle of building a blockchain-based framework.

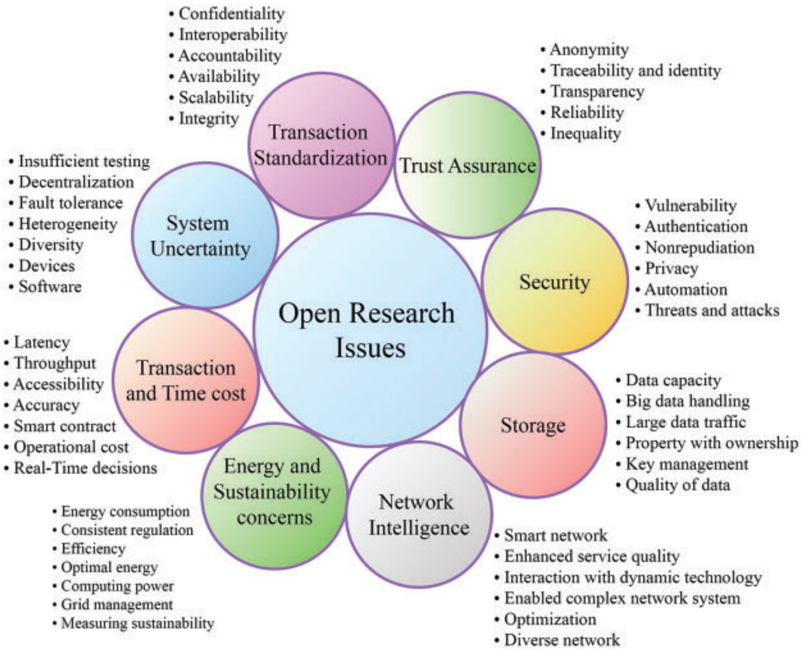

Figure 13: Open research issues of blockchain associated heterogeneous network

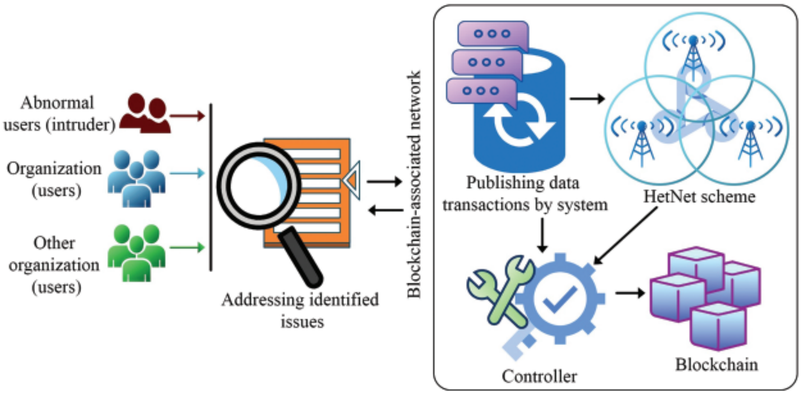
Abnormal users (intruder)
Organization (users)
Other organization (users)
Addressing identified issues
Blockchain-associated network
Publishing data transactions by system
HetNet scheme
Controller
Blockchain

Figure 14: Blockchain-associated network access design for addressing identified issues

5.1 Security

Block-chain-approved decentralized networks may be insecure due to some **vulnerabilities** or malicious bugs in the protocol device and its services [11]. If a single control system for networks, architectures, and protocols somehow crashes or fails to function, the entire system becomes inoperable, which can be a major cause of vulnerabilities. Also, the system relies on transaction-ordering, mismanagement, timestamp, or re-entry, where these issues can be identified as weak points of the system. Vulnerabilities in blockchain networks are usually caused by reliance on the algorithms of hardware, software, routing, internal services, and packet processing. After implementing a network system, it becomes difficult to detect any vulnerability, so it is necessary to verify the security vulnerabilities through proper testing methods to protect the system. Blockchain-based **authentication** schemes or protocols [371] can support management data transactions efficiently and decentralized manner across millions of network devices. Traditional authentication systems for blockchain-supported heterogeneous networks are not suitable for verifying data because all devices in those networks have to fully depend on central authorities to record and specify the identity with signature. Users face a number of difficulties in verifying the resources available in the underlying technology for digital transactions where the sender can transfer the actual resources to the right person, and the recipient can ensure that the genuine resources come from the right person.

The term **'nonrepudiation'** is a very important issue to participants in any digital organization or e-commerce transaction on the blockchain network where none of them can later refuse their data processing, transactions, or other behavior [13]. In this case, it is necessary to implement this concept with the support of blockchain technology through the proper testing method to have legal obligations or conditions to determine the origin of data in data security. Due to a large number of data transmissions to improve the quality of data transactions among participants in blockchain-based heterogeneous networks, achieving the **privacy** in the nature of data collected by network devices [22] such as user location, mobility, conversation, health status, purchase preferences, usage, data storage, etc. has raised serious concerns in contrast to service providers. When a network model is built by multiple blockchains, the interactions among the recognized or unknown participants in the chain can effectively increase privacy concerns on both sides to achieve internal and external security of the system. The decentralized nature of the networks used in blockchain technology does not allow data destruction for peer-to-peer activities, which is also a major issue for personal data privacy. Moreover, since the data collected in public blockchain ledgers is universally accessible and available to users, sensing systems of the network can continuously collect personal and sensitive data from customers, which can lead to privacy issues. So these issues of privacy need to be analyzed.

High-level **automation** needs to be implemented to control transaction agreements without the intervention of operators using blockchain due to the decentralized nature of the network system of any organization [270]. It can make any work completely flexible and reduce the workload. Automated data verification and operation, including executing contracts for the transactions of user resources using blockchain technology, requires a high level of automation. The effects of automation in terms of time and manpower need to be tested in the blockchain-based efficient infrastructure for the banking or financial sector as well as the robot industry. **Attacks, threats**, and **malicious adversaries** create many kinds of security issues in the financial industry or in the exchange of information based on blockchain infrastructure [11]. Attackers find out the bugs, inaccuracies, or defects in the various policies, improper management, and algorithms of blockchain-based applications over the distributed network in order to disrupt the distribution chain and cause irreversible damage through various malicious techniques. They occur as centralization attack, integrity attack, hash-based attack, network intrusion attack, social engineering attack, injection attack, reconnaissance, network access attack, assault attack, and generic attack in their desired network that will also cause the users to suffer. Meanwhile, the data security risks of any transactional application are mostly related to various threats such as lack of technical skills, insider abuses, social acceptance and regulations issues, insufficient facts of authorization, slow processing speeds, etc., which can be a major issue in blockchain implementation.

5.2 Storage

Specifically, blockchain-based various connected networking systems of various organizations may face issues related to data capacity, large data traffic, property with ownership, and data key management. Adding more blocks to the blockchain means that limited storage capacity-related network systems cannot store large blockchains. In this case, it can disrupt data traffic management during transactions across the network. As the size of the chain increases, more storage capacity is required in the data processing within network nodes, which makes the blockchain network unsuitable for whole data storage and data transactions [168,291]. The variability, redundant data, and key management caused by unstructured data storage can cause a lack of reliability in the core network management and data quality. For getting a decentralized, secure, and efficient digital system, further analysis of blockchain legal ownership issues is required to store proprietary information.

5.3 Network Intelligence

Addressing identified flaws in the management of smart networks, service quality, interactions with dynamic technologies, complex network systems, optimization [392], and diverse network based on the blockchain frameworks can be of significant concern. Machine learning and artificial intelligence (AI) methods [76] with blockchain technology can be applied to overcome the problems identified during the decision-making and process of actual block mining in intelligence networks. Artificial intelligence schemes can be used to maintain reliability and transparency of how information services will perform between parties involved in blockchain-based platforms. In these types of applications, complex network systems and diverse networks can be managed by improving the performance of AI-based control access systems. High-performance data transactions can be achieved by identifying and mitigating risky digital content or products on blockchain-based platforms using machine learning [393] and artificial intelligence algorithms.

Moreover, the integration of artificial intelligence [49] and blockchain into potential applications of distributed networks can be added as a direction to cyber security, where particularly graph deep learning models can be employed. Recently, graph deep learning models [394] as machine learning algorithms have indicated assurance in cybersecurity applications, particularly in the security of a decentralized network. By utilizing graph deep learning models to analyze complex graph-structured network data traffic, it may be feasible to detect and respond to threats more quickly and effectively in blockchain networks. By incorporating graph deep learning models with blockchain techniques, it can be potential to construct a decentralized and tamper-proof ledger that will securely accumulate block records and provide data of all transactions.

5.4 Energy and Sustainability

It is a big challenge to deal with the various types of identified faults of the blockchain system by practicing well about power usage, power consumption, consistent control, energy efficiency, optimal power, and computing power. A more critical issue in building an organization’s sustainable green ecosystem [186] is incorporating blockchain with green technologies that will coordinate optimal decisions in grid management and sustainability measurement. Consistent energy algorithms and models can be created to control the data transactions of blockchain applications that are related to datasets and data fields. Blockchain systems require high power to coordinate existing devices during computing and to store and transmit important information [292]. Another issue is to analyze the performance of energy profiles and energy activity functions during hash mining on the server and client side in blockchain systems. Because mining in blockchain systems requires a lot of electricity or energy to create millions and even billions of hashes per second, methods for establishing an evidence-based distribution model should be developed through experimentally searching and analyzing the direct power consumption parameters and optimal energy decisions in sensitive blockchain-based network systems. Models related to potential computing power utilization strategies can be analyzed to determine the impacts of blockchain-based cryptocurrency systems.

5.5 Transactional and Time Cost

Developing and implementing the real-time decision-making policy when routing emergency packets to their destinations in blockchain-based digital applications can be a big challenge. It is also very important to analyze the dynamic data flow management with less congestion and low latency [321]. In order to deliver the required amount of resources during the real-time operation over the distributed heterogeneous network, it is necessary to measure the effect of the change in data latency and throughput. The big issue in achieving the best solution for transferring huge amounts of data generated on a network connected by multiple devices or sensors is to increase the overall transaction time cost on both sides. To prevent unnecessary, counterfeit, manipulated, and malicious data entry into the blockchain system, various reasons for designing and setting up smart contracts need to be explored [326], as well as the next steps, need to be automatically integrated to eliminate unnecessary time delays. This type of network system requires further research to effectively suggest consensus algorithms of various parameters such as accessibility, accuracy, delay, and throughput in confirming transactions by participating nodes. In some cases, more logical and mathematical research is needed to monitor real-time data changes and operational costs in the chain of these systems to make quick and good decisions during suspicious transactions or abnormal activity.

5.6 System Uncertainty

There can be made a lot of uncertainty about a usable and realistic system in general unless some important elements, functions, approvals, and specific rules of the blockchain technology are proven or tested. Some issues arising from decentralization, diversity, heterogeneity, fault tolerance, and insufficient testing can have a major impact on creating technical uncertainty in a particular system [216]. In a decentralized blockchain framework, although there is no centralized authority or central control point, as well as transactional data, which cannot be destroyed, which makes the system secure, it does create a major issue in the privacy of personal data that needs to be properly analyzed. Designing and analyzing the interrelationships among different hardware devices, sensors, operating systems, servers, software, protocols, and scheduling algorithms, including different causal processes across a heterogeneous network, is a major challenge in the distribution of resources to users for security purposes [122]. In recent applications of blockchain-based distributed networks, the challenging issues of diversity are to address the regional network diversity, operating system diversity, bandwidth diversity, node diversity, and transactional discriminations in the digital workplace. A major concern is to develop a fault tolerance system by taking appropriate steps without correcting some errors to ensure the obtainability and consistency of any service. Blockchain systems have many insufficient testings of various important parameters or functional components where best practice is required to design, develop, and test those system applications to ensure performance and safety.

5.7 Transactional Standardization

In order to provide a service with security to users, appropriate rules and regulations need to be adapted to the standards of technical transactions that can be adjusted to the resources already available on blockchain-based heterogeneous networks. Further research is needed to develop standards and regulations related to the applicability of blockchain models to confidentiality, interoperability, scalability, integrity, availability, accountability, etc. [160,321]. In the blockchain system, it is a key issue to improve how confidentiality is achieved in order to maintain the security of specific user data while accessing and storing data. There is another concern about the interoperability with non-stop data communication in blockchain networks by working effectively and carefully along different protocols using the right instructions. Significant increases in the number and resources of users on a blockchain network can lead to scalability issues when certifying large data streams, including high broadcast traffic, and processing the redundant computational overheads. Data integrity infringement stored in the blockchain can have a profound effect on data transactions in organizations [171], which requires further research to ensure data integrity. The availability of stored data is crucially important when delivering services on a network so as not to interfere with the availability of data illegally. Accountability can be a significant way to exchange data across any decentralized network-based application to ensure transparent service among users.

5.8 Trust Assurance

In data management of blockchain networks, it is imperative to explore and improve trust assurance issues such as anonymity, traceability, identity, transparency, reliability, inequality, etc. Blockchain-based technological innovations, with adequate guarantees, should be able to provide inherent trust assurance in information distribution [33]. As data ledgers are universal in blockchain technology, ensuring complete anonymity of the user's real name or address when transacting on the network is a major issue, and open research is essential to address security concerns. The open challenge in identifying the source of any kind of fraud or correction in all network operations of various blockchain-based organizations is to implement traceability on the origin and quality of the actual donor data in the supply chain. The most obvious way to improve blockchain-enabled system management is to ensure transparency in all activities [141] where users can view their own information or history by disposing of the required transaction costs and interconnectedness issues without disclosing personal data or content when transacting in networks. In particular, establishing a user-friendly interface requires constantly exposing inconsistent and undesirable services in order to facilitate reliability in the functions of this infrastructure. Further analysis of the impact of blockchain technology in different sectors is needed to address inequalities in traditional systems.

6 Conclusion

Blockchain is currently a dynamic issue, and its development is largely continuing to be implemented in global network applications to become more mature. In the meantime, some specific functions and algorithms of blockchain operations have been enriched, and more new strategies are being designed for its implementation. Blockchain, cybersecurity, and heterogeneous network are relevant and significant technologies for the purpose of transaction security in the digital world, but it requires robust composition among them for better outcomes. This study provides a systematic review of the commonly agreed and continuously evolving algorithms, different approaches, operations, and applications related to the use and applicability of blockchain-based cybersecurity in a distributed network of different areas for secure data transactions, including technological advances, challenges, and increasing difficulties. This article has presented an overview of the various cyber attacks in a large number of industries in terms of the current context. It provides a holistic concept of different types of blockchains, characteristics, cryptographic operations, blockchain network structures, protocols, security measures, application areas, tokens, and analytics. Besides, it mentions a synopsis of the dealing methods of the heterogeneous network in blockchain technology. In this research paper, recent trends and open research issues of blockchain applications from the security perspective are highlighted. This paper proposes a blockchain-based HetNet model with cybersecurity for an organization's data transactions where a cross-chain mechanism will perform on the blockchain platform. This paper will give future research directions for researchers to develop blockchain-based applications over the distributed network.

Acknowledgement: The authors would like to acknowledge the Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA and the Ministry of Higher Education, Malaysia for the financial support through Fundamental Research Grant Scheme (FRGS) Grant No. FRGS/1/2021/ICT11/UITM/01/1. The authors would like to give thanks to the Universiti Malaysia Pahang, Malaysia, for promoting this research and providing the laboratory facility and support. The authors also extend their appreciation to the University of Wolverhampton, UK for its support.

Funding Statement: The authors would like to acknowledge the Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA and the Ministry of Higher Education, Malaysia for the financial support through Fundamental Research Grant Scheme (FRGS) Grant No. FRGS/1/2021/ICT11/UITM/01/1.

Author Contributions: The authors' contributions to the paper are as follows: study conception and design: M.S.I., M.A.R., M.A.B.A; Methodology: M.S.I., M.A.R., H.A.; original draft manuscript preparation: M.S.I., H.A.; Supervision: M.A.B.A.; Writing—Review and Editing: M.A.R., M.A.B.A., Z.B.I., J.M.Z. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Aamir, M., Qureshi, R., Khan, F. A., Huzaifa, M. (2020). Blockchain based academic records verification in smart cities. *Wireless Personal Communications, 113(3),* 1397–1406.
2. Lin, W., Yin, X., Wang, S., Khosravi, M. R. (2020). A blockchain-enabled decentralized settlement model for IoT data exchange services. *Wireless Networks, 26,* 1–15.
3. Sedighian Kashi, S. (2019). Area coverage of heterogeneous wireless sensor networks in support of internet of things demands. *Computing, 101(4),* 363–385.
4. Mendsaikhan, O., Hasegawa, H., Yamaguchi, Y., Shimada, H. (2020). Quantifying the significance and relevance of cyber-security text through textual similarity and cyber-security knowledge graph. *IEEE Access, 8,* 177041–177052.
5. Garba, A., Dwivedi, A. D., Kamal, M., Srivastava, G., Tariq, M. et al. (2021). A digital rights management system based on a scalable blockchain. *Peer-to-Peer Networking and Applications, 14(5),* 2665–2680.
6. Li, C., Xiao, J., Dai, X., Jin, H. (2021). AMVchain: Authority management mechanism on blockchain-based voting systems. *Peer-to-Peer Networking and Applications, 14(5),* 2801–2812.
7. Benisi, N. Z., Aminian, M., Javadi, B. (2020). Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications, 162,* 102656.
8. Xu, M., Feng, G., Ren, Y., Zhang, X. (2020). On cloud storage optimization of blockchain with a clustering-based genetic algorithm. *IEEE Internet of Things Journal, 7(9),* 8547–8558.
9. Li, C., Zhang, J., Yang, X., Youlong, L. (2021). Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices. *Information Processing & Management, 58(4),* 102602.

10. Zheng, Y., Li, Z., Xu, X., Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks, 8(4),* 422–435.
11. Li, Y., Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7,* 8176–8186.
12. Parn, E. A., Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management, 26(2),* 245–266.
13. Kovačević, A., Putnik, N., Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access, 8,* 125140–125148.
14. Tseng, L., Wong, L., Otoum, S., Aloqaily, M., Othman, J. B. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE Network, 34(1),* 16–23.
15. Li, R., Matsuzono, K., Asaeda, H., Fu, X. (2020). Achieving high throughput for heterogeneous networks with consecutive caching and adaptive retrieval. *IEEE Transactions on Network Science and Engineering, 7(4),* 2443–2455.
16. Passas, V., Miliotis, V., Makris, N., Korakis, T. (2020). Pricing based distributed traffic allocation for 5G heterogeneous networks. *IEEE Transactions on Vehicular Technology, 69(10),* 12111–12123.
17. AlSuwaidan, L., Almegren, N. (2020). Validating the adoption of heterogeneous Internet of Things with blockchain. *Future Internet, 12(6),* 107.
18. Sodhro, A. H., Pirbhulal, S., Muzammal, M., Luo, Z. W. (2020). Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications. *Journal of Grid Computing, 18(4),* 615–628.
19. Islam, M. S., Ameedeen, M. A. B., Rahman, M. A., Ajra, H., Ismail, Z. B. (2023). Healthcare-Chain: Blockchain-enabled decentralized trustworthy system in healthcare management industry 4.0 with cyber safeguard. *Computers, 12(2),* 46.
20. Cao, L., Song, B. (2021). Blockchain cross-chain protocol and platform research and development. *2021 International Conference on Electronics, Circuits and Information Engineering (ECIE)*, pp. 264–269. Zhengzhou, China, IEEE.
21. Tan, Y., Liu, J., Kato, N. (2020). Blockchain-based key management for heterogeneous flying ad hoc network. *IEEE Transactions on Industrial Informatics, 17(11),* 7629–7638.
22. Egala, B. S., Pradhan, A. K., Badarla, V., Mohanty, S. P. (2021). Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of medical Things with effective access control. *IEEE Internet of Things Journal, 8(14),* 11717–11731.
23. Geetha, R., Padmavathy, T., Umarani Srikanth, G. (2022). A scalable block chain framework for user identity management in a decentralized network. *Wireless Personal Communications, 123,* 3719–3736.
24. Alqahtani, A. S., Abuhasel, K. A., Alquraish, M. (2022). A novel decentralized analytical methodology for cyber physical networks attack detection. *Wireless Personal Communications, 127,* 1705–1716.
25. Kędziora, M., Kozłowski, P., Szczepanik, M., Jóźwiak, P. (2019). Analysis of blockchain selfish mining attacks. *International Conference on Information Systems Architecture and Technology*, vol. 1050, pp. 231–240. Wrocław, Poland, Springer.
26. Saad, M., Njilla, L., Kamhoua, C., Mohaisen, A. (2019). Countering selfish mining in blockchains. *2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 360–364. Honolulu, HI, USA, IEEE.
27. Nicolas, K., Wang, Y., Giakos, G. C., Wei, B., Shen, H. (2020). Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. *IEEE Access, 9,* 3838–3857.
28. Chicarino, V., Albuquerque, C., Jesus, E., Rocha, A. (2020). On the detection of selfish mining and stalker attacks in blockchain networks. *Annals of Telecommunications, 75(3),* 143–152.

29. Sun, Y., Apostolaki, M., Birge-Lee, H., Vanbever, L., Rexford, J. et al. (2021). Securing internet applications from routing attacks. *Communications of the ACM, 64(6),* 86–96.

30. Mastilak, L., Galinski, M., Helebrandt, P., Kotuliak, I., Ries, M. (2020). Enhancing border gateway protocol security using public blockchain. *Sensors, 20(16),* 4482.

31. Perwej, Y., Akhtar, N., Parwej, F. (2018). A technological perspective of blockchain security. *International Journal of Recent Scientific Research, 9(11),* 29472–29493.

32. Sentana, I., Ikram, M., Kaafar, M. A. (2021). Blockjack: Towards improved prevention of IP prefix hijacking attacks in inter-domain routing via blockchain. arXiv preprint arXiv:2107.07063.

33. Wu, X., Liang, J. (2021). A blockchain-based trust management method for Internet of Things. *Pervasive and Mobile Computing, 72(5),* 101330.

34. Anita, N., Vijayalakshmi, M. (2019). Blockchain security attack: A brief survey. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6. Kanpur, India, IEEE.

35. Waleed, M., Latif, R., Yakubu, B. M., Khan, M. I., Latif, S. (2021). T-smart: Trust model for blockchain based smart marketplace. *Journal of Theoretical and Applied Electronic Commerce Research, 16(6),* 2405–2423.

36. Amiri-Zarandi, M., Dara, R. A., Fraser, E. (2022). LBTM: A lightweight blockchain-based trust management system for social Internet of Things. *The Journal of Supercomputing, 78(6),* 1–19.

37. Baloglu, S., Bursuc, S., Mauw, S., Pang, J. (2021). Provably improving election verifiability in belenios. *Electronic Voting: 6th International Joint Conference*, vol. 12900, pp. 1–16. Virtual Event, Springer.

38. Iwendi, C., Jalil, Z., Javed, A. R., Reddy, T., Kaluri, R. et al. (2020). KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks. *IEEE Access, 8,* 72650–72660.

39. Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., Coble, J. (2019). Multilayer data-driven cyber attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics, 15(7),* 4362–4369.

40. Nesarani, A., Ramar, R., Pandian, S. (2020). An efficient approach for rice prediction from authenticated block chain node using machine learning technique. *Environmental Technology & Innovation, 20,* 101064.

41. Li, X., Wei, L., Wang, L., Ma, Y., Zhang, C. et al. (2022). A blockchain-based privacy-preserving authentication system for ensuring multimedia content integrity. *International Journal of Intelligent Systems, 37(5),* 3050–3071.

42. Tekiner, E., Acar, A., Uluagac, A. S., Kirda, E., Selcuk, A. A. (2021). SOK: Cryptojacking malware. *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 120–139. Vienna, Austria, IEEE.

43. Meland, P. H., Johansen, B. H., Sindre, G. (2019). An experimental analysis of cryptojacking attacks. *Nordic Conference on Secure IT Systems*, vol. 11875, pp. 155–170. Aalborg, Denmark, Springer.

44. Zimba, A., Wang, Z., Mulenga, M. (2019). Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks. *Journal of Organizational Computing and Electronic Commerce, 29(1),* 40–59.

45. Petrov, I., Invernizzi, L., Bursztein, E. (2020). Coinpolice: Detecting hidden cryptojacking attacks with neural networks. arXiv preprint arXiv:2006.10861.

46. Zimba, A., Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *European Journal for Security Research, 4(1),* 3–31.

47. Almashhadani, A. O., Kaiiali, M., Sezer, S., OâKane, P. (2019). A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE Access, 7,* 47053–47067.

48. Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H. et al. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments, 5(2),* 67–89.

49. Abdiyeva-Aliyeva, G., Hematyar, M., Bakan, S. (2021). Development of system for detection and prevention of cyber attacks using artificial intelligence methods. *2021 2nd Global Conference for Advancement in Technology (GCAT)*, pp. 1–5. Bangalore, India, IEEE.

50. Reuben, J., Ware, N. (2019). Approach to handling cyber security risks in supply chain of defence sector. *Industrial Engineering Journal, 12(7),* 1–12.

51. Arul, E., Punidha, A. (2020). Firmware attack detection on gadgets using Kohonen's self organizing feature maps (KSOFM). *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 21–26. Tirunelveli, India, IEEE.

52. Badih, H., Alagrash, Y., Rrushi, J. (2020). A blockchain and defensive deception co-design for webcam spyware detection. *2020 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 593–600. Calgary, AB, Canada, IEEE.

53. Gupta, S., Thakur, P., Biswas, K., Kumar, S., Singh, A. P. (2021). Developing a blockchain-based and distributed database-oriented multi-malware detection engine. *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, vol. 919, pp. 249–275. Warsaw, Poland, Springer.

54. Li, Y. G., Chung, Y. C., Hwang, K., Li, Y. J. (2020). Virtual wall: Filtering rootkit attacks to protect linux kernel functions. *IEEE Transactions on Computers, 70(10),* 1640–1653.

55. Nadim, M., Akopian, D., Lee, W. (2021). A review on learning-based detection approaches of the kernel-level rootkit. *2021 International Conference on Engineering and Emerging Technologies (ICEET)*, pp. 1–6. Istanbul, Turkey, IEEE.

56. Geetha Ramani, R., Suresh Kumar, S. (2021). Nonvolatile kernel rootkit detection using cross-view clean boot in cloud computing. *Concurrency and Computation: Practice and Experience, 33(3),* e5239.

57. Lv, Z. H., Yan, H. B., Mei, R. (2018). Automatic and accurate detection of Webshell based on convolutional neural network. *China Cyber Security Annual Conference*, vol. 970, pp. 73–85. Beijing, China, Springer.

58. Roy, D. G., Das, P., De, D., Buyya, R. (2019). QoS-aware secure transaction framework for internet of things using blockchain mechanism. *Journal of Network and Computer Applications, 144(2),* 59–78.

59. Desai, H. B., Ozdayi, M. S., Kantarcioglu, M. (2021). BlockFLA: Accountable federated learning via hybrid blockchain architecture. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, pp. 101–112. Virtual Event, USA.

60. Hashemi, S., Zarei, M. (2021). Internet of Things backdoors: Resource management issues, security challenges, and detection methods. *Transactions on Emerging Telecommunications Technologies, 32(2),* e4142.

61. Rahaman, N., Rubel, S., Marouf, A. A. (2022). Keylogger threat to the android mobile banking applications. *Computer Networks and Inventive Communication Technologies*, vol. 75, pp. 163–174. Singapore, Springer.

62. Farhin, F., Kaiser, M. S., Mahmud, M. (2020). Towards secured service provisioning for the internet of healthcare things. *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)*, pp. 1–6. Tashkent, Uzbekistan, IEEE.

63. Reyes, A. R. L., Festijo, E. D., Medina, R. P. (2019). Enhanced multi-factor out-of-band authentication EN route to securing SMS-based OTP ariel. *International Journal of Engineering and Technology Innovation, 9(2),* 145.

64. Keshavarzi, M., Ghaffary, H. R. (2020). I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review, 36(11),* 100233.

65. Mercenit, C., Rios, J. C., Liu, Y., Wang, J., Yuan, J. et al. (2019). Analysis of rogue access points using SDR. *2019 IEEE International Conference on Industrial Internet (ICII)*, pp. 50–55. Orlando, FL, USA, IEEE.

66. Noh, S., Kim, D., Cai, Z., Rhee, K. H. (2021). A novel user collusion-resistant decentralized multiauthority attribute-based encryption scheme using the deposit on a blockchain. *Wireless Communications and Mobile Computing, 2021(1999),* 1–15.

67. Thakur, S., Breslin, J. G. (2020). Collusion attack from hubs in the blockchain offline channel network. *Mathematical Research for Blockchain Economy*, pp. 31–44. Santorini, Greece, Springer.

68. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. *IEEE Access, 9,* 140549–140564.

69. Sayeed, S., Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9(9),* 1788.

70. Shrestha, R., Nam, S. Y. (2019). Regional blockchain for vehicular networks to prevent 51% attacks. *IEEE Access, 7,* 95033–95045.

71. Arifeen, M., Al Mamun, A., Ahmed, T., Kaiser, M. S., Mahmud, M. et al. (2021). A blockchain-based scheme for Sybil attack detection in underwater wireless sensor networks. *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*, vol. 1309, pp. 467–476. Singapore, Springer.

72. Kedziora, M., Kozlowski, P., Jozwiak, P. (2020). Security of blockchain distributed ledger consensus mechanism in context of the Sybil attack. *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, vol. 12144, pp. 407–418. Kitakyushu, Japan, Springer.

73. Alangot, B., Reijsbergen, D., Venugopalan, S., Szalachowski, P., Yeo, K. S. (2021). Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains. *IEEE Transactions on Network and Service Management, 18(2),* 1659–1672.

74. Marcus, Y., Heilman, E., Goldberg, S. (2018). Low-resource eclipse attacks on Ethereum's peer-to-peer network. *Cryptology ePrint Archive, 236,* 1–15.

75. Xu, G., Guo, B., Su, C., Zheng, X., Liang, K. et al. (2020). Am I eclipsed? A smart detector of eclipse attacks for Ethereum. *Computers & Security, 88,* 101604.

76. Mohanta, B. K., Jena, D., Satapathy, U., Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things, 11(8),* 100227.

77. Mirsky, Y., Golomb, T., Elovici, Y. (2020). Lightweight collaborative anomaly detection for the IoT using blockchain. *Journal of Parallel and Distributed Computing, 145(1),* 75–97.

78. Rasool, R., Wang, H., Ashraf, U., Ahmed, K., Anwar, Z. et al. (2020). A survey of link flooding attacks in software defined network ecosystems. *Journal of Network and Computer Applications, 172(4),* 102803.

79. Lakshmi, H., Anand, S., Sinha, S. (2019). Flooding attack in wireless sensor network-analysis and prevention. *International Journal of Engineering and Advanced Technology, 8(5),* 1792–1796.

80. Alkadi, R., Alnuaimi, N., Yeun, C. Y., Shoufan, A. (2022). Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues. *IEEE Access, 10,* 14463–14479.

81. Abdelatif, H., Abdelhakim, S. H., Mustapha, S. (2021). A tractable probabilistic approach to analyze Sybil attacks in sharding-based blockchain protocols. arXiv preprint arXiv:2104.07215.

82. Sahay, R., Geethakumari, G., Mitra, B. (2020). A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Computing, 102(11),* 2445–2470.

83. Ran, C., Yan, S., Huang, L., Zhang, L. (2021). An improved AODV routing security algorithm based on blockchain technology in ad hoc network. *EURASIP Journal on Wireless Communications and Networking, 2021(1),* 1–16.

84. Saxena, R., Gayathri, E. (2022). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. *Materials Today: Proceedings, 51,* 682–689.

85. Chen, W., Guo, X., Chen, Z., Zheng, Z., Lu, Y. (2020). Phishing scam detection on Ethereum: Towards financial security for blockchain ecosystem. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20)*, pp. 4506–4512. Yokohama.

86. Andryukhin, A. (2019). Phishing attacks and preventions in blockchain based projects. *2019 International Conference on Engineering Technologies and Computer Science (EnT)*, pp. 15–19. Moscow, Russia, IEEE.

87. Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., Ray, S. (2021). Social engineering attacks: Recent advances and challenges. *International Conference on Human-Computer Interaction*, vol. 12788, pp. 417–431. Virtual Event, Springer.

88. Aldawood, H., Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications, 177(30),* 1–11.

89. Subbalakshmi, C., Pareek, P. K., Sayal, R. (2022). A study on social engineering attacks in cybersecurity. *Innovations in Computer Science and Engineering*, vol. 385, pp. 59–71. Singapore, Springer.

90. Mezhuyev, V., Sadat, S. N., Rahman, M. A., Refat, N., Asyhari, A. T. (2019). Evaluation of the likelihood of friend request acceptance in online social networks. *IEEE Access, 7,* 75318–75329.

91. Weber, K., Schütz, A. E., Fertig, T., Müller, N. H. (2020). Exploiting the human factor: Social engineering attacks on cryptocurrency users. *International Conference on Human-Computer Interaction*, vol. 12206, pp. 650–668. Copenhagen, Denmark, Springer.

92. Parthy, P. P., Rajendran, G. (2019). Identification and prevention of social engineering attacks on an enterprise. *2019 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–5. Chennai, India, IEEE.

93. Conteh, N. Y., Sword, D. A. D. (2021). The dynamics of social engineering and cybercrime in the digital age. *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*, pp. 144–149. Pennsylvania, IGI Global.

94. Alghenaim, M. F., Bakar, N. A. A., Yusoff, R. C. M., Hassan, N. H., Sallehudin, H. (2021). Employee awareness model to enhance awareness of social engineering threats in the Saudi public sector. *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, pp. 1–6. Taiz, Yemen, IEEE.

95. Rege, A., Nguyen, T., Bleiman, R. (2020). A social engineering awareness and training workshop for stem students and practitioners. *2020 IEEE Integrated STEM Education Conference (ISEC)*, pp. 1–6. Princeton, NJ, USA, IEEE.

96. Thang, N. M. (2020). Improving efficiency of web application firewall to detect code injection attacks with random forest method and analysis attributes HTTP request. *Programming and Computer Software, 46(5),* 351–361.

97. Abaimov, S., Bianchi, G. (2019). CODDLE: Code-injection detection with deep learning. *IEEE Access, 7,* 128617–128627.

98. Gowtham, M., Pramod, H. (2021). Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems. *IEEE Transactions on Reliability, 71(2),* 1057–1074.

99. Li, Q., Wang, F., Wang, J., Li, W. (2019). LSTM-based SQL injection detection method for intelligent transportation system. *IEEE Transactions on Vehicular Technology, 68(5),* 4182–4191.

100. Zhang, T. Y., Ye, D. (2020). False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach. *Automatica, 120(1),* 109117.

101. Ahmed, M., Pathan, A. S. K. (2020). False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling, 8(1),* 1–14.

102. Shi, H., Xie, L., Peng, L. (2021). Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method. *Computers & Electrical Engineering, 91(1),* 107058.

103. Khan, S., Zhang, Z., Zhu, L., Rahim, M. A., Ahmad, S. et al. (2020). SCM: Secure and accountable TLS certificate management. *International Journal of Communication Systems, 33(15),* e4503.

104. Chen, J., Zhan, Z., He, K., Du, R., Wang, D. et al. (2021). XAuth: Efficient privacy-preserving cross-domain authentication. *IEEE Transactions on Dependable and Secure Computing, 19(5),* 3301–3311.

105. Boychenko, O. V., Gavrikov, I. V. (2021). Assessing password protection effectiveness using Markov processes. *CEUR Workshop Proceedings*, vol. 2914, pp. 284–290. Yalta, Crimea.

106. Pecori, R., Veltri, L. (2018). A balanced trust-based method to counter Sybil and Spartacus attacks in chord. *Security and Communication Networks, 2018(3),* 1–16.

107. Tang, F., Kawamoto, Y., Kato, N., Yano, K., Suzuki, Y. (2019). Probe delay based adaptive port scanning for IoT devices with private IP address behind NAT. *IEEE Network, 34(2),* 195–201.

108. Ernawati, T., Fachrozi, M., Syaputri, D. (2019). Analysis of intrusion detection system performance for the port scan attack detector, portsentry, and suricata. *IOP Conference Series: Materials Science and Engineering*, vol. 662. Bristol, UK, IOP Publishing.

109. Liu, X., Zeng, Q., Du, X., Valluru, S. L., Fu, C. et al. (2021). SniffMislead: Non-intrusive privacy protection against wireless packet sniffers in smart homes. *24th International Symposium on Research in Attacks, Intrusions and Defenses*, pp. 33–47. San Sebastian, Spain.

110. Gautam, Y., Gautam, B. P., Sato, K. (2020). Experimental security analysis of SDN network by using packet sniffing and spoofing technique on POX and RYU controller. *2020 International Conference on Networking and Network Applications (NaNA)*, pp. 394–399. Haikou City, China, IEEE.

111. Yu, J., Ye, X., Li, H. (2022). A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Future Generation Computer Systems, 129(3),* 399–406.

112. Thu Hien, D. T., Do Hoang, H., Pham, V. H. (2021). Empirical study on reconnaissance attacks in SDN-aware network for evaluating cyber deception. *2021 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pp. 1–6. Hanoi, Vietnam, IEEE.

113. Yahiatene, Y., Rachedi, A., Riahla, M. A., Menacer, D. E., Nait-Abdesselam, F. (2019). A blockchain based framework to secure vehicular social networks. *Transactions on Emerging Telecommunications Technologies, 30(8),* e3650.

114. Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal, 8(2),* 881–888.

115. Maw, A., Adepu, S., Mathur, A. (2019). ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive and Mobile Computing, 59,* 101048.

116. Ismail, L., Materwala, H., Zeadally, S. (2019). Lightweight blockchain for healthcare. *IEEE Access, 7,* 149935–149951.

117. Liu, Y., Wang, J., Niu, S., Song, H. (2020). Deep learning enabled reliable identity verification and spoofing detection. *International Conference on Wireless Algorithms, Systems, and Applications*, vol. 12384, pp. 333–345. Qingdao, China, Springer.

118. Gunduz, M. Z., Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks, 169(11),* 107094.

119. Stodt, J., Schönle, D., Reich, C., Ghovanlooy Ghajar, F., Welte, D. et al. (2021). Security audit of a blockchain-based industrial application platform. *Algorithms, 14(4),* 121.

120. Rahman, M. A., Mezhuyev, V., Bhuiyan, M. Z. A., Sadat, S. N., Zakaria, S. A. B. et al. (2018). Reliable decision making of accepting friend request on online social networks. *IEEE Access, 6,* 9484–9491.

121. Al-Hasnawi, A. (2021). TSCO: Trust-based secure and cooperative opportunistic resource utilization networks. *Journal of Physics: Conference Series, 1879(2),* 22094.

122. Braeken, A., Liyanage, M., Kanhere, S. S., Dixit, S. (2020). Blockchain and cyberphysical systems. *Computer, 53(9),* 31–35.

123. Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, M., Almotairi, K. et al. (2021). Distributed denial of service (DDOS) mitigation using blockchain—A comprehensive insight. *Symmetry, 13(2),* 227.

124. Pathak, S., Jhawar, A., Sharma, M., Kohli, A. (2022). Improvised security of IoT through blockchain. *Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022*. SSRN 4027047. https://ssrn.com/abstract=4027047

125. Li, Y., Zhang, P., Ma, L. (2019). Denial of service attack and defense method on load frequency control system. *Journal of the Franklin Institute, 356(15),* 8625–8645.

126. Sayad Haghighi, M., Farivar, F., Jolfaei, A., Tadayon, M. H. (2020). Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack. *The Journal of Supercomputing, 76(4),* 3063–3085.

127. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R. (2021). A distributed framework for detecting DDoS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing. *Transactions on Emerging Telecommunications Technologies, 32(6),* e4112.

128. Salim, M. M., Rathore, S., Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: A survey. *The Journal of Supercomputing, 76(7),* 5320–5363.

129. Ahmad, F., Kurugollu, F., Adnane, A., Hussain, R., Hussain, F. (2020). MARINE: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal, 7(4),* 3310–3322.

130. Choi, J., Ahn, B., Bere, G., Ahmad, S., Mantooth, H. A. et al. (2021). Blockchain-based man-in-the middle (MITM) attack detection for photovoltaic systems. *2021 IEEE Design Methodologies Conference (DMC)*, pp. 1–6. Bath, UK, IEEE.

131. Sidorov, M., Ong, M. T., Sridharan, R. V., Nakamura, J., Ohmura, R. et al. (2019). Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access, 7,* 7273–7285.

132. Hu, B., Zhou, C., Tian, Y. C., Qin, Y., Junping, X. (2019). A collaborative intrusion detection approach using blockchain for multimicrogrid systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8),* 1720–1730.

133. Hou, Y., Xiong, H., Huang, X., Kumari, S. (2021). Certificate-based parallel key-insulated aggregate signature against fully chosen key attacks for industrial internet of things. *IEEE Internet of Things Journal, 8(11),* 8935–8948.

134. Chang, J., Wang, H., Wang, F., Zhang, A., Ji, Y. (2020). RKA security for identity-based signature scheme. *IEEE Access, 8,* 17833–17841.

135. Amiram, D., Jørgensen, B. N., Rabetti, D. (2020). Coins for bombs: Increased transparency of the global financial system-evidence from terrorist attacks financing detection in blockchain-based currencies. *Working Paper*. https://doi.org/10.2139/ssrn.3616207

136. Rahman, M. A., Sadat, S. N., Asyhari, A. T., Refat, N., Kabir, M. N. et al. (2019). A secure and sustainable framework to mitigate hazardous activities in online social networks. *IEEE Transactions on Sustainable Computing, 6(1),* 30–42.

137. Zhu, L., Majumdar, S., Ekenna, C. (2021). An invisible warfare with the internet of battlefield things: A literature review. *Human Behavior and Emerging Technologies, 3(2),* 255–260.

138. Zarrin, J., Wen Phang, H., Babu Saheer, L., Zarrin, B. (2021). Blockchain for decentralization of internet: Prospects, trends, and challenges. *Cluster Computing, 24(4),* 2841–2866.

139. Caporale, G. M., Kang, W. Y., Spagnolo, F., Spagnolo, N. (2021). Cyber-attacks, spillovers and contagion in the cryptocurrency markets. *Journal of International Financial Markets, Institutions and Money, 74(5),* 101298.

140. Alkaeed, M., Soliman, M. M., Khan, K. M., Elfouly, T. M. (2020). Distributed framework via blockchain smart contracts for smart grid systems against cyber-attacks. *2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, pp. 100–105. Shah Alam, Malaysia, IEEE.

141. Shala, B., Trick, U., Lehmann, A., Ghita, B., Shiaeles, S. (2020). Blockchain and trust for secure, end-user-based and decentralized IoT service provision. *IEEE Access, 8,* 119961–119979.

142. Sibai, R. E., Challita, K., Abdo, J. B., Demerjian, J. (2021). The impact of blockchain on cybersecurity management. *Advances in Cybersecurity Management*, pp. 117–138. Gewerbestrasse, Switzerland, Springer.

143. Makhdoom, I., Tofigh, F., Zhou, I., Abolhasan, M., Lipman, J. (2020). PLEDGE: An IoT-oriented proof-of-honesty based blockchain consensus protocol. *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, pp. 54–64. Sydney, NSW, Australia, IEEE.

144. Brotsis, S., Limniotis, K., Bendiab, G., Kolokotronis, N., Shiaeles, S. (2021). On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Computer Networks, 191(1),* 108005.

145. Moustapha, B. (2020). The effect of propagation delay on the dynamic evolution of the bitcoin blockchain. *Digital Communications and Networks, 6(2),* 157–166.

146. Rawal, B. S., Manogaran, G., Hamdi, M. (2021). Multi-tier stack of block chain with proxy re-encryption method scheme on the internet of things platform. *ACM Transactions on Internet Technology (TOIT), 22(2),* 1–20.

147. Peng, C., Wu, C., Gao, L., Zhang, J., Alvin Yau, K. L. et al. (2020). Blockchain for vehicular internet of things: Recent advances and open issues. *Sensors, 20(18),* 5079.

148. Miraz, M. H., Ali, M. (2018). Blockchain enabled enhanced IoT ecosystem security. *International Conference for Emerging Technologies in Computing*, pp. 38–46. London, UK, Springer.

149. Zheng, P., Xu, Q., Zheng, Z., Zhou, Z., Yan, Y. et al. (2021). Meepo: Sharded consortium blockchain. *2021 IEEE 37th International Conference on Data Engineering (ICDE)*, pp. 1847–1852. Chania, Greece, IEEE.

150. Dujak, D., Sajter, D. (2019). Blockchain applications in supply chain. *SMART Supply Network*, pp. 21–46. Gewerbestrasse, Switzerland, Springer.

151. Pandey, P., Litoriya, R. (2021). Promoting trustless computation through blockchain technology. *National Academy Science Letters, 44(3),* 225–231.

152. Zhang, Z., Huang, L., Tang, R., Peng, T., Guo, L. et al. (2020). Industrial blockchain of things: A solution for trustless industrial data sharing and beyond. *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, pp. 1187–1192. Hong Kong, China, IEEE.

153. Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X. et al. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction, 111,* 103063.

154. Zhang, Z., Yuan, Z., Ni, G., Lin, H., Lu, Y. (2020). The quality traceability system for prefabricated buildings using blockchain: An integrated framework. *Frontiers of Engineering Management, 7(4),* 528–546.

155. Farooq, M. S., Khan, M., Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. *Computers & Electrical Engineering, 83,* 106588.

156. Huang, H., Sun, X., Xiao, F., Zhu, P., Wang, W. (2021). Blockchain-based E-health system for auditable EHRS manipulation in cloud environments. *Journal of Parallel and Distributed Computing, 148,* 46–57.

157. Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing, 63,* 101896.

158. Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I. et al. (2020). Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts. *BMC Medical Research Methodology, 20(1),* 1–17.

159. Zhang, Z., Li, W., Liu, H., Liu, J. (2020). A refined analysis of Zcash anonymity. *IEEE Access, 8,* 31845–31853.

160. Huang, K., Zhang, X., Mu, Y., Rezaeibagha, F., Du, X. (2021). Scalable and redactable blockchain with update and anonymity. *Information Sciences, 546(15),* 25–41.

161. Viriyasitavat, W., Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration, 13(2),* 32–39.

162. Schär, F. (2020). Blockchain forks: A formal classification framework and persistency analysis. *The Singapore Economic Review, 65,* 1–11.

163. Casino, F., Politou, E., Alepis, E., Patsakis, C. (2019). Immutability and decentralized storage: An analysis of emerging threats. *IEEE Access, 8,* 4737–4744.

164. Chopra, U. K., Rathore, A. K., Pandey, R. (2020). Rendering blockchain immutability in chatserver: A node .js approach. In: *Decision analytics applications in industry*, pp. 147–155. Singapore, Springer.

165. Liu, Y., Ke, J., Xu, Q., Jiang, H., Wang, H. (2019). Decentralization is vulnerable under the gap game. *IEEE Access, 7,* 90999–91008.

166. Isaja, M., Soldatos, J. (2018). Distributed ledger technology for decentralization of manufacturing processes. *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 696–701. St. Petersburg, Russia, IEEE.

167. Liu, Z., Li, Z. (2020). A blockchain-based framework of cross-border E-commerce supply chain. *International Journal of Information Management, 52(10),* 102059.

168. Zhu, Z., Qi, G., Zheng, M., Sun, J., Chai, Y. (2020). Blockchain based consensus checking in decentralized cloud storage. *Simulation Modelling Practice and Theory, 102(8),* 101987.

169. Dwivedi, S. K., Amin, R., Vollala, S. (2020). Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications, 54(23),* 102554.

170. Nosouhi, M. R., Yu, S., Zhou, W., Grobler, M., Keshtiar, H. (2020). Blockchain for secure location verification. *Journal of Parallel and Distributed Computing, 136,* 40–51.

171. Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems, 102(3),* 902–911.

172. Vladyko, A., Spirkina, A., Elagin, V., Belozertsev, I., Aptrieva, E. (2020). Blockchain models to improve the service security on board communications. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1–6. Moscow, Russia, IEEE.

173. Asaf, K., Rehman, R. A., Kim, B. S. (2020). Blockchain technology in named data networks: A detailed survey. *Journal of Network and Computer Applications, 171(2),* 102840.

174. Liang, Y. C. (2020). Blockchain for dynamic spectrum management. *Dynamic Spectrum Management*, pp. 121–146. Singapore, Springer.

175. Malakhov, I., Marin, A., Rossi, S., Smuseva, D. (2021). On the use of proof-of-work in permissioned blockchains: Security and fairness. *IEEE Access, 10,* 1305–1316.

176. Qu, Q., Xu, R., Chen, Y., Blasch, E., Aved, A. (2021). Enable fair proof-of-work (PoW) consensus for blockchains in IoT by miner twins (MinT). *Future Internet, 13(11),* 291.

177. Feng, Z., Luo, Q. (2020). Evaluating memory-hard proof-of-work algorithms on three processors. *Proceedings of the VLDB Endowment, 13(6),* 898–911.

178. Chin, Z. H., Yap, T. T. V., Tan, I. K. (2020). On the trade-offs of proof-of-work algorithms in blockchains. *Computational Science and Technology*, pp. 575–584. Kota Kinabalu, Malaysia, Springer.

179. Gaži, P., Kiayias, A., Zindros, D. (2019). Proof-of-stake sidechains. *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 139–156. San Francisco, CA, USA, IEEE.

180. Saad, M., Qin, Z., Ren, K., Nyang, D., Mohaisen, D. (2021). e-PoS: Making proof-of-stake decentralized and fair. *IEEE Transactions on Parallel and Distributed Systems, 32(8),* 1961–1973.

181. Yang, J., Paudel, A., Gooi, H. B., Nguyen, H. D. (2021). A proof-of-stake public blockchain based pricing scheme for peer-to-peer energy trading. *Applied Energy, 298(4),* 117154.

182. Deuber, D., Döttling, N., Magri, B., Malavolta, G., Thyagarajan, S. A. K. (2020). Minting mechanism for proof of stake blockchains. *International Conference on Applied Cryptography and Network Security*, pp. 315–334. Rome, Italy, Springer.

183. Katal, A., Sethi, V., Lamba, S. (2021). Blockchain consensus algorithms: Study and challenges. *Blockchain Applications in IoT Ecosystem*, pp. 45–64. Gewerbestrasse, Switzerland, Springer.

184. Sudha Sadasivam, G. (2021). A critical review on using blockchain technology in education domain. *Blockchain Technology for IoT Applications*, vol. 16276, pp. 85–117. Singapore, Springer.

185. Rebello, G. A. F., Camilo, G. F., Guimarães, L. C., de Souza, L. A. C., Thomaz, G. A. et al. (2021). A security and performance analysis of proof-based consensus protocols. *Annals of Telecommunications, 77,* 517–537.

186. Bada, A. O., Damianou, A., Angelopoulos, C. M., Katos, V. (2021). Towards a green blockchain: A review of consensus mechanisms and their energy consumption. *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 503–511. Pafos, Cyprus, IEEE.

187. Chauhan, A., Rishabh, Lokesh, N. S., Mittal, P. (2022). A deep dive into blockchain consensus protocols. *Smart Trends in Computing and Communications*, pp. 571–581. Singapore, Springer.

188. Wang, X., Jia, W. L., Chai, J. (2018). The research on the incentive method of consortium blockchain based on practical byzantine fault tolerant. *2018 11th International Symposium on Computational Intelligence and Design (ISCID)*, vol. 2, pp. 154–156. Hangzhou, China, IEEE.

189. Bhushan, B., Sinha, P., Sagayam, K. M., Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering, 90(9),* 106897.

190. Yu, G., Wu, B., Niu, X. (2020). Improved blockchain consensus mechanism based on PBFT algorithm. *2020 2nd International Conference on Advances in Computer Technology, Information Science and Communications (CTISC)*, pp. 14–21. Suzhou, China, IEEE.

191. Aggarwal, S., Kumar, N. (2021). Cryptographic consensus mechanisms. *Advances in Computers, 121,* 211–226.

192. Aleshi, A., Seker, R., Babiceanu, R. F. (2019). Blockchain model for enhancing aircraft maintenance records security. *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–7. Woburn, MA, USA, IEEE.

193. Aslam, T., Maqbool, A., Akhtar, M., Mirza, A., Khan, M. A. et al. (2022). Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. *Computers, Materials & Continua, 70(1),* 1089–1109. https://doi.org/10.32604/cmc.2022.019416

194. Hattab, S., Taha Alyaseen, I. F. (2019). Consensus algorithms blockchain: A comparative study. *International Journal on Perceptive and Cognitive Computing, 5(2),* 66–71.

195. Kim, M., Kwon, Y., Kim, Y. (2019). Is stellar as secure as you think? *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 377–385. Stockholm, Sweden, IEEE.

196. Suliyanti, W. N., Salman, M., Sari, R. F. (2021). Evaluation of an actor model-based consensus algorithm on NEO blockchain. *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 60–64. Sydney, Australia, IEEE.

197. Coelho, I. M., Coelho, V. N., Araujo, R. P., Yong Qiang, W., Rhodes, B. D. (2020). Challenges of PBFT-inspired consensus for blockchain and enhancements over NEO dBFT. *Future Internet, 12(8),* 129.

198. Wang, Q., Yu, J., Peng, Z., Bui, V. C., Chen, S. et al. (2020). Security analysis on DBFT protocol of NEO. *International Conference on Financial Cryptography and Data Security*, pp. 20–31. Kota Kinabalu, Malaysia, Springer.

199. Wang, Q., Xu, M., Li, X., Qian, H. (2020). Revisiting the fairness and randomness of delegated proof of stake consensus algorithm. *2020 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pp. 305–312. Exeter, UK, IEEE.

200. Hu, Q., Yan, B., Han, Y., Yu, J. (2021). An improved delegated proof of stake consensus algorithm. *Procedia Computer Science, 187(9),* 341–346.

201. Majumdar, M. A., Monim, M., Shahriyer, M. M. (2020). Blockchain based land registry with delegated proof of stake (DPoS) consensus in Bangladesh. *2020 IEEE Region 10 Symposium (TENSYMP)*, pp. 1756–1759. Dhaka, Bangladesh, IEEE.

202. Zhang, J., Tian, R., Cao, Y., Yuan, X., Yu, Z. et al. (2021). A hybrid model for central bank digital currency based on blockchain. *IEEE Access, 9,* 53589–53601.

203. Lee, D., Lee, D. H. (2019). Push and pull: Manipulating a production schedule and maximizing rewards on the EOSIO blockchain. *Proceedings of the Third ACM Workshop on Blockchains, Cryptocurrencies and Contracts*, pp. 11–21. Auckland, New Zealand.

204. Rebello, G. A. F., Camilo, G. F., Guimaraes, L., de Souza, L. A. C., Duarte, O. (2020). Security and performance analysis of quorum-based blockchain consensus protocols. *2022 6th Cyber Security in Networking Conference (CSNet)*, Rio de Janeiro, Brazil.

205. Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K. et al. (2020). An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends. *IEEE Access, 8,* 103994–104015.

206. Bardinova, Y., Zhidanov, K., Bezzateev, S., Komarov, M., Ometov, A. (2020). Measurements of mobile blockchain execution impact on smartphone battery. *Data, 5(3),* 66.

207. Kaur, A., Nayyar, A., Singh, P. (2020). Blockchain: A path to the future. *Cryptocurrencies and Blockchain Technology Applications,* 25–42.

208. Kleinrock, L., Ostrovsky, R., Zikas, V. (2020). Proof-of-reputation blockchain with nakamoto fall back. *International Conference on Cryptology in India*, pp. 16–38. Bangalore, India, Springer.

209. Chai, H., Leng, S., Zhang, K., Mao, S. (2019). Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. *IEEE Access, 7,* 175744–175757.

210. Aluko, O., Kolonin, A. et al. (2021). Studying the applicability of proof of reputation (PoR) as an alternative consensus mechanism for distributed ledger systems. *CS & IT Conference Proceedings*, vol. 11, no. 8. Copenhagen, Denmark.

211. Alrubei, S., Ball, E., Rigelsford, J. (2021). Securing IoT-blockchain applications through honesty-based distributed proof of authority consensus algorithm. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1–7. Dublin, Ireland, IEEE.

212. Toyoda, K., Machi, K., Ohtake, Y., Zhang, A. N. (2020). Function-level bottleneck analysis of private proof-of-authority ethereum blockchain. *IEEE Access, 8,* 141611–141621.

213. Samuel, C. N., Glock, S., Verdier, F., Guitton-Ouhamou, P. (2021). Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–5. Sydney, Australia, IEEE.

214. Andrey, A., Petr, C. (2019). Review of existing consensus algorithms blockchain. *2019 International Conference "Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)*, IEEE.

215. Dong, Z., Lee, Y. C., Zomaya, A. Y. (2019). Proofware: Proof of useful work blockchain consensus protocol for decentralized applications. arXiv preprint arXiv:1903.09276.

216. Falcone, S., Zhang, J., Cameron, A., Abdel-Rahman, A. (2019). Blockchain design for an embedded system. *Ledger, 4,* 7–16.

217. Yakovenko, A. (2018). Solana: A new architecture for a high performance blockchain v0.8.13. *Whitepaper*.

218. Bou Abdo, J., El Sibai, R., Demerjian, J. (2021). Permissionless proof-of-reputation-X: A hybrid reputation-based consensus algorithm for permissionless blockchains. *Transactions on Emerging Telecommunications Technologies, 32(1),* e4148.

219. Zhang, P., Schmidt, D. C., White, J., Dubey, A. (2019). Consensus mechanisms and information security technologies. *Advances in Computers, 115(6–10),* 181–209.

220. Sharma, K., Jain, D. (2019). Consensus algorithms in blockchain technology: A survey. *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7. Kanpur, India, IEEE.

221. Hazari, S. S., Mahmoud, Q. H. (2019). Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technology Letters, 2(3),* e100.

222. Pranav, P., Dutta, S., Chakraborty, S. (2021). An involution function-based symmetric stream cipher. *Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems*, vol. 673, pp. 61–68. Ranchi, India, Springer.

223. Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D. et al. (2020). An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems. *Sensors, 20(5),* 1521.

224. Halevi, S., Hazay, C., Polychroniadou, A., Venkitasubramaniam, M. (2021). Round-optimal secure multiparty computation. *Journal of Cryptology, 34(3),* 1–63.

225. Guan, Z., Zhou, X., Liu, P., Wu, L., Yang, W. (2021). A blockchain based dual side privacy preserving multi party computation scheme for edge enabled smart grid. *IEEE Internet of Things Journal, 9(16),* 14287–14299.

226. Zhou, J., Feng, Y., Wang, Z., Guo, D. (2021). Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors, 21(4),* 1540.

227. Pop, C. D., Antal, M., Cioara, T., Anghel, I., Salomie, I. (2020). Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. *Sensors, 20(19),* 5678.

228. Malik, S., Dedeoglu, V., Kanhere, S., Jurdak, R. (2021). Privchain: Provenance and privacy preservation in blockchain enabled supply chains. arXiv preprint arXiv:2104.13964.

229. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive, 2018(46),* 1–83.

230. Westerkamp, M., Eberhardt, J. (2020). zkRelay: Facilitating sidechains using zkSNARK-based chain relays. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 378–386. Genoa, Italy, IEEE.

231. Kim, J., Lee, J., Oh, H. (2020). Simulation-extractable zk-SNARK with a single verification. *IEEE Access, 8,* 156569–156581.

232. Yusup, M., Cahvadi, D., Febriyanto, E., Mardiana, Budiarty, F. (2020). The impact of socio-economic in digital signature using blockchain application. *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–6. Pangkal, Indonesia, IEEE.

233. Alzubi, J. A. (2021). Blockchain-based lamport merkle digital signature: Authentication tool in IoT healthcare. *Computer Communications, 170(1),* 200–208.

234. Li, X., Mei, Y., Gong, J., Xiang, F., Sun, Z. (2020). A blockchain privacy protection scheme based on ring signature. *IEEE Access, 8,* 76765–76772.

235. Kugusheva, A., Yanovich, Y. (2019). Ring signature-based voting on blockchain. *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, pp. 70–75. Xi'an, China.

236. Li, C., Tian, Y., Chen, X., Li, J. (2021). An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. *Information Sciences, 546(2),* 253–264.

237. Xiao, L., Han, D., Meng, X., Liang, W., Li, K. C. (2020). A secure framework for data sharing in private blockchain-based WBANs. *IEEE Access, 8,* 153956–153968.

238. Ghesmati, S., Fdhila, W., Weippl, E. (2021). Bitcoin privacy—A survey on mixing techniques. *Technical Report*.

239. Hassan, M. U., Rehmani, M. H., Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems, 97(4),* 512–529.

240. Xiong, F., Xiao, R., Ren, W., Zheng, R., Jiang, J. (2019). A key protection scheme based on secret sharing for blockchain-based construction supply chain system. *IEEE Access, 7,* 126773–126786.

241. Cha, J., Singh, S. K., Kim, T. W., Park, J. H. (2021). Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications, 57(2),* 102686.

242. Esgin, M. F., Zhao, R. K., Steinfeld, R., Liu, J. K., Liu, D. (2019). MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 567–584. London, UK.

243. Zhang, Y., Deng, R. H., Liu, X., Zheng, D. (2018). Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Information Sciences, 462(4),* 262–277.

244. Zhao, Y., Zhao, J., Kang, J., Zhang, Z., Niyato, D. et al. (2021). A blockchain-based approach for saving and tracking differential-privacy cost. *IEEE Internet of Things Journal, 8(11),* 8865–8882.

245. Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K. et al. (2021). Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Transactions on Industrial Informatics, 18(6),* 4049–4058.

246. Islam, M., Rehmani, M. H., Chen, J. (2021). Differential privacy-based permissioned blockchain for private data sharing in industrial IoT. *International Conference on Broadband Communications, Networks and Systems*, vol. 413, pp. 77–91. Virtual Event, Springer.

247. Liang, W., Zhang, D., Lei, X., Tang, M., Li, K. C. et al. (2020). Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection. *IEEE Transactions on Emerging Topics in Computing, 9(3),* 1410–1420.

248. Yan, X., Wu, Q., Sun, Y. (2020). A homomorphic encryption and privacy protection method based on blockchain and edge computing. *Wireless Communications and Mobile Computing, 2020(3),* 1–9.

249. Loukil, F., Ghedira-Guegan, C., Boukadi, K., Benharkat, A. N. (2021). Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption. *Sensors, 21(7),* 2452.

250. Tse, D., Huang, K., Cai, B., Liang, K. (2018). Robust password-keeping system using block-chain technology. *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 1221–1225. Bangkok, Thailand, IEEE.

251. Wei, Y., Lv, S., Guo, X., Liu, Z., Huang, Y. et al. (2019). FSSE: Forward secure searchable encryption with keyed-block chains. *Information Sciences, 500,* 113–126.

252. Wang, Z. C., Wu, X. Y., Yu, W. J., Liu, J. L., Zhao, H. L. et al. (2019). Medical information storage model based on block chain. *2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, pp. 39–44. Shanghai, China, IEEE.

253. Zheng, H., Shao, J., Wei, G. (2020). Attribute-based encryption with outsourced decryption in blockchain. *Peer-to-Peer Networking and Applications, 13(5),* 1643–1655.

254. Dang, N. T., Tran, H. M., Nguyen, S. V., Maleszka, M., Le, H. D. (2021). Sharing secured data on peer-to-peer applications using attribute-based encryption. *Journal of Information and Telecommunication, 5(4),* 440–459.

255. Zuo, Y., Kang, Z., Xu, J., Chen, Z. (2021). BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *International Journal of Distributed Sensor Networks, 17(3).*

256. Shahsavari, Y., Zhang, K., Talhi, C. (2019). Performance modeling and analysis of the bitcoin inventory protocol. *2019 IEEE International Conference on Decentralized Applications and Infrastructures*, pp. 79–88. Newark, CA, USA, IEEE.

257. Liwei, T., Yu, S. (2021). Research summary of blockchain fragmentation propagation mechanism based on Merkel tree. *Journal of Physics: Conference Series, 1914,* 12010.

258. Shahsavari, Y., Zhang, K., Talhi, C. (2020). A theoretical model for block propagation analysis in bitcoin network. *IEEE Transactions on Engineering Management, 69(4),* 1459–1476.

259. Chang, Z., Guo, W., Guo, X., Zhou, Z., Ristaniemi, T. (2020). Incentive mechanism for edge computing-based blockchain. *IEEE Transactions on Industrial Informatics, 16(11),* 7105–7114.

260. Xuan, S., Zheng, L., Chung, I., Wang, W., Man, D. et al. (2020). An incentive mechanism for data sharing based on blockchain with smart contracts. *Computers & Electrical Engineering, 83(1),* 106587.

261. Ersoy, O., Ren, Z., Erkin, Z., Lagendijk, R. L. (2018). Transaction propagation on permissionless blockchains: Incentive and routing mechanisms. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 20–30. Zug, Switzerland, IEEE.

262. Frauenthaler, P., Sigwart, M., Spanring, C., Schulte, S. (2020). Testimonium: A cost-efficient blockchain relay. arXiv preprint arXiv:2002.12837.

263. Otsuki, K., Banno, R., Shudo, K. (2020). Quantitatively analyzing relay networks in bitcoin. *2020 IEEE International Conference on Blockchain*, pp. 214–220. Rhodes, Greece, IEEE.

264. Ghosh, A., Gupta, S., Dua, A., Kumar, N. (2020). Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications, 163(1),* 102635.

265. Hu, Q., Xu, M., Wang, S., Guo, S. (2020). Sync or fork: Node-level synchronization analysis of blockchain. *International Conference on Wireless Algorithms, Systems, and Applications*, vol. 12384, pp. 170–181. Qingdao, China, Springer.

266. Wang, K., Kim, H. S. (2019). Fastchain: Scaling blockchain system with informed neighbor selection. *2019 IEEE International Conference on Blockchain*, pp. 376–383. Atlanta, GA, USA, IEEE.

267. Saghafi, F., Pakyari, M., Rezaei, M. (2019). Prioritizing capabilities of blockchain technology in telecommunication for promoting customer satisfaction. *16th International Conference on Information Technology-New Generations (ITNG 2019)*, vol. 800, pp. 499–503. Virtual Event, Springer.

268. Zhang, H., Lao, L., Shu, C., Xiao, B. (2021). Analysis of the communication traffic model for permissioned blockchain based on proof-of-work. *ICC 2021-IEEE International Conference on Communications*, pp. 1–6. Montreal, QC, Canada, IEEE.

269. Renieri, M. (2020). *Ethereum smart contracts optimization (Ph.D. Thesis)*. University of Camerino, Italy.

270. Zuo, Y., Qi, Z. (2021). A blockchain-based IoT framework for oil field remote monitoring and control. *IEEE Access, 10,* 2497–2514.

271. Pandey, M., Sharma, N. (2022). Blockchain architecture and policy for transforming healthcare industry. *Transformation in Healthcare with Emerging Technologies*, pp. 45–61. New York, Chapman and Hall/CRC.

272. Guerra, J. A., Guerrero, J. I., García, S., Domínguez-Cid, S., Larios, D. F. et al. (2022). Design and evaluation of a heterogeneous lightweight blockchain-based marketplace. *Sensors, 22(3),* 1131.

273. Paavolainen, S., Carr, C. (2020). Security properties of light clients on the ethereum blockchain. *IEEE Access, 8,* 124339–124358.

274. Qu, J. (2022). Blockchain in medical informatics. *Journal of Industrial Information Integration, 25(4),* 100258.

275. Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., Yi, X. (2019). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure*, pp. 97–105. Auckland, New Zealand.

276. Ismail, L., Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry, 11(10),* 1198.

277. Crepaldi, M. (2020). International exchange of financial information on distributed ledgers: Outlook and design blueprint. *Blockchain and Distributed Ledger Technology Use Cases*, pp. 95–111. Gewerbestrasse, Switzerland, Springer.

278. Moni, M., Melo, W., Peters, D., Machado, R. (2021). When measurements meet blockchain: On behalf of an inter-NMI network. *Sensors, 21(5),* 1564.

279. Kim, S. K. A. (2022). Multi-layered blockchain governance game. *Axioms, 11(1),* 27.

280. Bellavista, P., Esposito, C., Foschini, L., Giannelli, C., Mazzocca, N. et al. (2021). Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing. *Sensors, 21(15),* 4955.

281. Koens, T., Poll, E. (2019). Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing, 59(3),* 101079.

282. Fourati, M., Najeh, B., Idriss, A. (2021). Blockchain towards secure UAV-based systems. *Enabling Blockchain Technology for Secure Networking and Communications*, pp. 149–174. IGI Global.

283. Salimitari, M., Chatterjee, M., Fallah, Y. P. (2020). A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet of Things, 11(5),* 100212.

284. Bodkhe, U., Mehta, D., Tanwar, S., Bhattacharya, P., Singh, P. K. et al. (2020). A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access, 8,* 54371–54401.

285. Alharby, M., van Moorsel, A. (2020). BlockSim: An extensible simulation tool for blockchain systems. *Frontiers in Blockchain, 3,* 28.

286. Pavithran, D., Al-Karaki, J. N., Shaalan, K. (2021). Edge-based blockchain architecture for event-driven IoT using hierarchical identity based encryption. *Information Processing & Management, 58(3),* 102528.

287. Li, Z., Zhong, R. Y., Tian, Z. G., Dai, H. N., Barenji, A. V. et al. (2021). Industrial blockchain: A state-of-the-art survey. *Robotics and Computer-Integrated Manufacturing, 70(1),* 102124.

288. Majeed, U., Khan, L. U., Yaqoob, I., Kazmi, S. A., Salah, K. et al. (2021). Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *Journal of Network and Computer Applications, 181(9),* 103007.

289. Yang, F., Shi, Y., Wu, Q., Li, F., Zhou, W. et al. (2019). The survey on intellectual property based on blockchain technology. *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pp. 743–748. Taipei, Taiwan, IEEE.

290. Neudecker, T., Hartenstein, H. (2018). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials, 21(1),* 838–857.

291. Jia, D. Y., Xin, J. C., Wang, Z. Q., Lei, H., Wang, G. R. (2021). SE-chain: A scalable storage and efficient retrieval model for blockchain. *Journal of Computer Science and Technology, 36(3),* 693–706.

292. Silva, F. C., Ahmed, A., Martínez, J. M., Kim, Y. C. (2019). Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots. *Energies, 12(24),* 4814.

293. Lo, S. K., Xu, X., Staples, M., Yao, L. (2020). Reliability analysis for blockchain oracles. *Computers & Electrical Engineering, 83(4),* 106582.

294. Woo, S., Song, J., Park, S. (2020). A distributed oracle using intel SGX for blockchain-based IoT applications. *Sensors, 20(9),* 2725.

295. Fartitchou, M., El Makkaoui, K., Kannouf, N., El Allali, Z. (2020). Security on blockchain technology. *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–7. Marrakech, Morocco, IEEE.

296. Sayeed, S., Marco-Gisbert, H., Caira, T. (2020). Smart contract: Attacks and protections. *IEEE Access, 8,* 24416–24427.

297. Bünz, B., Agrawal, S., Zamani, M., Boneh, D. (2020). Zether: Towards privacy in a smart contract world. *International Conference on Financial Cryptography and Data Security*, pp. 423–443. Kota Kinabalu, Malaysia, Springer.

298. Dana Troutman, N., Laszka, A. (2021). Poolparty: Efficient blockchain-agnostic decentralized mining pool. *2021 The 3rd International Conference on Blockchain Technology*, pp. 20–27. Shanghai, China.

299. Gupta, N. (2020). Security and privacy issues of blockchain technology. In: *Advanced applications of blockchain technology*, vol. 60, pp. 207–226. Singapore, Springer.

300. Liu, X., Zhao, G., Wang, X., Lin, Y., Zhou, Z. et al. (2019). MDP-based quantitative analysis framework for proof of authority. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 227–236. Guilin, China, IEEE.

301. Gao, W., Su, C. (2020). Analysis on block chain financial transaction under artificial neural network of deep learning. *Journal of Computational and Applied Mathematics, 380(22),* 112991.

302. Wu, B., Duan, T. (2019). The application of blockchain technology in financial markets. *Journal of Physics: Conference Series, 1176,* 42094.

303. Zhang, D. (2020). The innovation research of contract farming financing mode under the block chain technology. *Journal of Cleaner Production, 270(4),* 122194.

304. Abou Jaoude, J., Saade, R. G. (2019). Blockchain applications-usage in different domains. *IEEE Access, 7,* 45360–45381.

305. Ullah, F., Al-Turjman, F. (2021). A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Computing and Applications, 35(7),* 5033–5054.

306. Leduc, G., Kubler, S., Georges, J. P. (2021). Innovative blockchain-based farming marketplace and smart contract performance evaluation. *Journal of Cleaner Production, 306(S1),* 127055.

307. Das, D., Banerjee, S., Biswas, U. (2021). A secure vehicle theft detection framework using blockchain and smart contract. *Peer-to-Peer Networking and Applications, 14(2),* 672–686.

308. Rathee, G., Sharma, A., Kumar, R., Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks, 94(2),* 101933.

309. Rawat, D. B., Doku, R., Adebayo, A., Bajracharya, C., Kamhoua, C. (2020). Blockchain enabled named data networking for secure vehicle-to-everything communications. *IEEE Network, 34(5),* 185–189.

310. Gong, J., Navimipour, N. J. (2021). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Cluster Computing, 25(1),* 383–400.

311. Murthy, C. V. B., Shri, M. L., Kadry, S., Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. *IEEE Access, 8,* 205190–205205.

312. Al-Rakhami, M. S., Gumaei, A., Rahman, S., Mizanur, M., Al-Amri, A. (2021). Decentralized blockchain-based model for edge computing. arXiv preprint arXiv:2106.15050.

313. Sarode, R. P., Poudel, M., Shrestha, S., Bhalla, S. (2021). Blockchain for committing peer-to-peer transactions using distributed ledger technologies. *International Journal of Computational Science and Engineering, 24(3),* 215–227.

314. Li, X., Chen, T., Luo, X., Yu, J. (2020). Characterizing erasable accounts in ethereum. *International Conference on Information Security*, pp. 352–371. Bali, Indonesia, Springer.

315. Lian, J., Wang, S., Xie, Y. (2021). TDRB: An efficient tamper-proof detection middleware for relational database based on blockchain technology. *IEEE Access, 9,* 66707–66722.

316. Liu, C., Guo, H., Xu, M., Wang, S., Yu, D. et al. (2022). Extending on-chain trust to off-chain—trustworthy blockchain data collection using trusted execution environment (TEE). *IEEE Transactions on Computers, 71(12),* 3268–3280.

317. Saleh, S., Shayor, F. (2020). High-level design and rapid implementation of a clinical and non-clinical blockchain-based data sharing platform for COVID-19 containment. *Frontiers in Blockchain, 3,* 51.

318. Sunil Kumar, K., Jain, K., Subramanian, N. (2021). A data privacy approach using Shamirâs secret scheme in permissioned blockchain. In: *Computer networks and inventive communication technologies*, vol. 58, pp. 875–883. Singapore: Springer.

319. Ruan, P., Loghin, D., Ta, Q. T., Zhang, M., Chen, G. et al. (2020). A transactional perspective on execute-order-validate blockchains. *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data*, pp. 543–557.

320. Kim, T. H., Kumar, G., Saha, R., Rai, M. K., Buchanan, W. J. et al. (2020). A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect. *IEEE Access, 8,* 96455–96467.

321. Rahman, M. A., Abuludin, M. S., Yuan, L. X., Islam, M. S., Asyhari, A. T. (2021). Educhain: CIA-compliant blockchain for intelligent cyber defense of microservices in education industry 4.0. *IEEE Transactions on Industrial Informatics, 18(3),* 1930–1938.

322. Sharma, P. K., Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems, 86(1),* 650–655.

323. Khan, S. N., Shael, M., Majdalawieh, M. (2019). Blockchain technology as a support infrastructure in E-government evolution at Dubai economic department. *Proceedings of the 2019 International Electronics Communication Conference*, pp. 124–130. Okinawa, Japan.

324. Biswas, S., Sharif, K., Li, F., Mohanty, S. (2020). Blockchain for E-health-care systems: Easier said than done. *Computer, 53(7),* 57–67.

325. Xu, L., Yang, Y., Chu, X. (2021). Research on the influence mechanism of block chain on the credit of transportation capacity supply chain finance. *Mathematical Problems in Engineering, 2021(1),* 1–11.

326. Humayun, M., Jhanjhi, N., Hamid, B., Ahmed, G. (2020). Emerging smart logistics and transportation using IoT and blockchain. *IEEE Internet of Things Magazine, 3(2),* 58–62.

327. Alsamhi, S. H., Lee, B. (2020). Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics. *IEEE Access, 9,* 44173–44197.

328. Dolenc, D., Turk, J., Pustišek, M. (2020). Distributed ledger technologies for IoT and business dApps. *2020 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom)*, pp. 1–8. Graz, Austria, IEEE.

329. Zeng, Y. (2020). Digital music resource copyright management mechanism based on blockchain. *2020 3rd International Conference on Smart BlockChain (SmartBlock)*, pp. 158–162. Zhengzhou, China, IEEE.

330. Borah, M. D., Naik, V. B., Patgiri, R., Bhargav, A., Phukan, B. et al. (2020). Supply chain management in agriculture using blockchain and IoT. *Advanced Applications of Blockchain Technology*, vol. 60, pp. 227–242. Singapore, Springer.

331. Chou, H. C. (2021). A blockchain-based framework proposal for online entertainment ecosystem. *2021 IEEE Region 10 Symposium (TENSYMP)*, pp. 1–5. Jeju, Korea, IEEE.

332. Li, C. Z., Chen, Z., Xue, F., Kong, X. T., Xiao, B. et al. (2021). A blockchain-and IoT-based smart product-service system for the sustainability of prefabricated housing construction. *Journal of Cleaner Production, 286(7),* 125391.

333. Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N. et al. (2021). Health-ID: A blockchain-based decentralized identity management for remote healthcare. *Healthcare, 9(6),* 172.

334. El Haddouti, S., El Kettani, M. D. E. C. (2019). Analysis of identity management systems using blockchain technology. *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, pp. 1–7. Rabat, Morocco, IEEE.

335. Karamachoski, J., Marina, N., Taskov, P. (2020). Blockchain-based application for certification management. *Tehnički Glasnik, 14(4),* 488–492.

336. Jing, N., Liu, Q., Sugumaran, V. (2021). A blockchain-based code copyright management system. *Information Processing & Management, 58(3),* 102518.

337. García, R., Gil, R. (2019). Social media copyright management using semantic web and blockchain. *Proceedings of the 21st International Conference on Information Integration and Web-Based Applications & Services*, pp. 339–343. Munich Germany.

338. Koirala, R. C., Dahal, K., Matalonga, S. (2019). Supply chain using smart contract: A blockchain enabled model with traceability and ownership management. *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 538–544. Noida, India, IEEE.

339. Lee, N. Y., Yang, J., Kim, C. S. (2021). Blockchain-based smart propertization of digital content for intellectual rights protection. *Electronics, 10(12),* 1387.

340. Lee, Y., Lee, K. M., Lee, S. H. (2020). Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. *Peer-to-Peer Networking and Applications, 13(2),* 671–683.

341. Iqbal, S., Malik, A. W., Rahman, A. U., Noor, R. M. (2020). Blockchain-based reputation management for task offloading in micro-level vehicular fog network. *IEEE Access, 8,* 52968–52980.

342. Akcora, C. G., Dixon, M. F., Gel, Y. R., Kantarcioglu, M. (2018). Blockchain data analytics. *Intelligent Informatics, 4,* 6.

343. McGinn, D., McIlwraith, D., Guo, Y. (2018). Towards open data blockchain analytics: A bitcoin perspective. *Royal Society Open Science, 5(8),* 180298.

344. Xu, Q., Aung, K. M. M., Zhu, Y., Yong, K. L. (2018). A blockchain-based storage system for data analytics in the internet of things. *New Advances in the Internet of Things*, vol. 715, pp. 119–138. Gewerbestrasse, Switzerland, Springer.

345. Kranz, J., Nagel, E., Yoo, Y. (2019). Blockchain token sale. *Business & Information Systems Engineering, 61(6),* 745–753.

346. Westerkamp, M., Victor, F., Küpper, A. (2020). Tracing manufacturing processes using blockchain-based token compositions. *Digital Communications and Networks, 6(2),* 167–176.

347. Ren, Y., Leng, Y., Qi, J., Sharma, P. K., Wang, J. et al. (2021). Multiple cloud storage mechanism based on blockchain in smart homes. *Future Generation Computer Systems, 115(3),* 304–313.

348. Zhang, Q., Han, Y. Y., Su, Z. B., Fang, J. L., Liu, Z. Q. et al. (2020). A storage architecture for high-throughput crop breeding data based on improved blockchain technology. *Computers and Electronics in Agriculture, 173(18),* 105395.

349. Wu, D., Ansari, N. (2020). A cooperative computing strategy for blockchain-secured fog computing. *IEEE Internet of Things Journal, 7(7),* 6603–6609.

350. Xie, X., Fang, Y., Jian, Z., Lu, Y., Li, T. et al. (2020). Blockchain-driven anomaly detection framework on edge intelligence. *CCF Transactions on Networking, 3(3),* 171–192.

351. Yohan, A., Lo, N. W. (2020). FOTB: A secure blockchain-based firmware update framework for IoT environment. *International Journal of Information Security, 19(3),* 257–278.

352. Sowmiya, B., Poovammal, E. (2021). A heuristic K-anonymity based privacy preserving for student management hyperledger fabric blockchain. *Wireless Personal Communications, 127,* 1359–1376.

353. Kumar, R., Bhalaji, N. (2021). Blockchain based Chameleon hashing technique for privacy preservation in E-governance system. *Wireless Personal Communications, 117(2),* 987–1006.

354. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., Choo, K. K. R. (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Transactions on Services Computing, 13(4),* 625–638.

355. Pandey, P., Litoriya, R. (2021). Securing E-health networks from counterfeit medicine penetration using blockchain. *Wireless Personal Communications, 117(1),* 7–25.

356. Mubarakali, A. (2020). Healthcare services monitoring in cloud using secure and robust healthcare-based blockchain (SRHB) approach. *Mobile Networks and Applications, 25(4),* 1330–1337.

357. Meng, W., Li, W., Yang, L. T., Li, P. (2020). Enhancing challenge-based collaborative intrusion detection networks against insider attacks using blockchain. *International Journal of Information Security, 19(3),* 279–290.

358. Krishnamurthy, R., Rathee, G., Jaglan, N. (2020). An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. *Wireless Networks, 26(4),* 2391–2402.

359. Khan, M. Y., Zuhairi, M. F., Ali, T., Alghamdi, T., Marmolejo-Saucedo, J. A. (2020). An extended access control model for permissioned blockchain frameworks. *Wireless Networks, 26(7),* 4943–4954.

360. Chung, K., Yoo, H., Choe, D., Jung, H. (2019). Blockchain network based topic mining process for cognitive manufacturing. *Wireless Personal Communications, 105(2),* 583–597.

361. Chu, C. H. (2021). Task offloading based on deep learning for blockchain in mobile edge computing. *Wireless Networks, 27(1),* 117–127.

362. Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P. et al. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. *IEEE Access, 9,* 29429–29440.

363. Sharma, P. K., Park, J. H. (2020). Blockchain-based secure mist computing network architecture for intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems, 22(8),* 5168–5177.

364. Sharma, P. K., Chen, M. Y., Park, J. H. (2017). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access, 6,* 115–124.

365. Elisa, N., Yang, L., Chao, F., Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless Networks, 29,* 1005–1015.

366. Li, H., Pei, L., Liao, D., Sun, G., Xu, D. (2019). Blockchain meets VANET: An architecture for identity and location privacy protection in VANET. *Peer-to-Peer Networking and Applications, 12(5),* 1178–1193. https://doi.org/10.1007/s12083-019-00786-4

367. Xu, M., Zhao, F., Zou, Y., Liu, C., Cheng, X. et al. (2022). BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR. *IEEE Transactions on Mobile Computing, 9743876,* 1–18.

368. Bader, L., Pennekamp, J., Matzutt, R., Hedderich, D., Kowalski, M. et al. (2021). Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability. *Information Processing & Management, 58(3),* 102529.

369. Moerman, A., Van Kerrebrouck, J., Caytan, O., de Paula, I. L., Bogaert, L. et al. (2022). Beyond 5G without obstacles: mmWaveover-fiber distributed antenna systems. *IEEE Communications Magazine, 60(1),* 27–33.

370. Rahmadika, S., Firdaus, M., Jang, S., Rhee, K. H. (2021). Blockchain-enabled 5G edge networks and beyond: An intelligent cross-silo federated learning approach. *Security and Communication Networks, 2021(11),* 1–14.

371. Jiang, X., Liu, M., Yang, C., Liu, Y., Wang, R. et al. (2019). A blockchain-based authentication protocol for WLAN mesh security access. *Computers, Materials & Continua, 58(1),* 45–59. https://doi.org/10.32604/cmc.2019.03863

372. Okon, A. A., Sholiyi, O. S., Elmirghani, J. M., Munasighe, K. (2021). Blockchain for spectrum management in 6G networks. *Wireless Blockchain: Principles, Technologies and Applications*. https://doi.org/10.1002/9781119790839.ch6

373. Lazreg, A. B., Arbia, A. B., Youssef, H. (2020). Cloudlet-cloud network communication based on blockchain technology. *2020 International Conference on Information Networking (ICOIN)*, pp. 164–169. Barcelona, Spain, IEEE.

374. Girón, A., Rivera, E., Gómez, G. (2022). Measurement of the spectral efficiency of a heterogeneous network architecture of the NG-PON type for a quasilinear propagation regime. *Entropy, 24(4),* 481.

375. Oloomi, F., Masoumi, R., Karimipour, K., Hosseiny, A., Jafari, G. R. (2021). Competitive balance theory: Modeling conflict of interest in a heterogeneous network. *Physical Review E, 103(2),* 22307.

376. Wang, J., Liang, Y., Gao, L., Pi, Z., Yang, X. et al. (2020). Heterogeneous data feature extraction technology based on long-short term memory. *2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS)*, pp. 141–144. Dalian, China, IEEE.
377. Kulkarni, A., Ramanathan, C. (2022). CDEF: Conceptual data extraction framework for heterogeneous data. *2022 14th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 329–331. Bangalore, India, IEEE.
378. Xie, F., Chen, L., Lin, D., Zheng, Z., Lin, X. (2019). Personalized service recommendation with mashup group preference in heterogeneous information network. *IEEE Access, 7,* 16155–16167.
379. Anadiotis, A. C., Balalau, O., Conceicao, C., Galhardas, H., Haddad, M. Y. et al. (2022). Graph integration of structured, semistructured and unstructured data for data journalism. *Information Systems, 104(13),* 101846.
380. Qin, D., Zheng, G., Liu, L., Li, L., Wang, X. et al. (2020). Construction of knowledge graph of multi-source heterogeneous distribution network systems. *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, pp. 162–166. Harbin, China, IEEE.
381. Peng, R. (2021). Analysis of computer information processing technology based on unstructured data. *2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, pp. 1222–1225. Dalian, China, IEEE.
382. Papa, A., Durner, R., Goshi, E., Goratti, L., Rasheed, T. et al. (2021). MARC: On modeling and analysis of software-defined radio access network controllers. *IEEE Transactions on Network and Service Management, 18(4),* 4602–4615.
383. Meng, W., Li, W., Zhou, J. (2021). Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. *Information Fusion, 70(1),* 60–71.
384. Alshaer, H., Haas, H. (2020). Software-defined networking-enabled heterogeneous wireless networks and applications convergence. *IEEE Access, 8,* 66672–66692.
385. Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J., Duarte, O. C. M. (2019). BSec-NFVO: A blockchain-based security for network function virtualization orchestration. *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6. Shanghai, China, IEEE.
386. Maksymyuk, T., Andrushchak, V., Dumych, S., Shubyn, B., Gabriel, B. et al. (2020). Blockchain-based network functions virtualization for 5G network slicing. *Acta Electrotechnica et Informatica, 20(4),* 54–59.
387. Kafetzis, D., Vassilaras, S., Vardoulias, G., Koutsopoulos, I. (2022). Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions. *IEEE Access, 10,* 9989–10014.
388. Rajasekaran, A. S., Azees, M., Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments, 52(12),* 102039.
389. Hassan, M. U., Rehmani, M. H., Chen, J. (2022). Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 25(1),* 289–318.
390. Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W. et al. (2022). A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Communications Surveys & Tutorials, 24(1),* 88–122.
391. Johar, S., Ahmad, N., Asher, W., Cruickshank, H., Durrani, A. (2021). Research and applied perspective to blockchain technology: A comprehensive survey. *Applied Sciences, 11(14),* 6252.
392. Wei, W., Rahman, M. A., Kurniawan, I. F., Asyhari, A. T., Sadat, S. N. et al. (2019). Immune genetic algorithm optimization and integration of logistics network terminal resources. *2019 Third IEEE International Conference on Robotic Computing (IRC)*, pp. 435–436. Naples, Italy, IEEE.

393. Rahman, M. A., Zaman, N., Asyhari, A. T., Sadat, S. N., Pillai, P. et al. (2021). SPY-BOT: Machine learning-enabled post filtering for social network-integrated industrial Internet of Things. *Ad Hoc Networks, 121(4),* 102588.

394. Jiang, W. (2022). Graph-based deep learning for communication networks: A survey. *Computer Communications, 185(1),* 40–54.