network

MDPI

Review

A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges

Patikiri Arachchige Don Shehan Nilmantha Wijesekara * and Subodha Gunawardena

Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka; subodha@eie.ruh.ac.lk
* Correspondence: nilmantha@eie.ruh.ac.lk

Abstract: Knowledge-Defined Networking (KDN) necessarily consists of a knowledge plane for the generation of knowledge, typically using machine learning techniques, and the dissemination of knowledge, in order to make knowledge-driven intelligent network decisions. In one way, KDN can be recognized as knowledge-driven Software-Defined Networking (SDN), having additional management and knowledge planes. On the other hand, KDN encapsulates all knowledge-/intelligence-/cognition-/machine learning-driven networks, emphasizing knowledge generation (KG) and dissemination for making intelligent network decisions, unlike SDN, which emphasizes logical decoupling of the control plane. Blockchain is a technology created for secure and trustworthy decentralized transaction storage and management using a sequence of immutable and linked transactions. The decision-making trustworthiness of a KDN system is reliant on the trustworthiness of the data, knowledge, and AI model sharing. To this point, a KDN may make use of the capabilities of the blockchain system for trustworthy data, knowledge, and machine learning model sharing, as blockchain transactions prevent repudiation and are immutable, pseudo-anonymous, optionally encrypted, reliable, access-controlled, and untampered, to protect the sensitivity, integrity, and legitimacy of sharing entities. Furthermore, blockchain has been integrated with knowledge-based networks for traffic optimization, resource sharing, network administration, access control, protecting privacy, traffic filtering, anomaly or intrusion detection, network virtualization, massive data analysis, edge and cloud computing, and data center networking. Despite the fact that many academics have employed the concept of blockchain in cognitive networks to achieve various objectives, we can also identify challenges such as high energy consumption, scalability issues, difficulty processing big data, etc. that act as barriers for integrating the two concepts together. Academicians have not yet reviewed blockchain-based network solutions in diverse application categories for diverse knowledge-defined networks in general, which consider knowledge generation and dissemination using various techniques such as machine learning, fuzzy logic, and meta-heuristics. Therefore, this article fills a void in the content of the literature by first reviewing the diverse existing blockchain-based applications in diverse knowledge-based networks, analyzing and comparing the existing works, describing the advantages and difficulties of using blockchain systems in KDN, and, finally, providing propositions based on identified challenges and then presenting prospects for the future.

Keywords: blockchain; intelligence; Knowledge-Defined Networking; machine learning; Software-Defined Networking

Citation: Wijesekara, P.A.D.S.N.; Gunawardena, S. A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges. *Network* **2023**, *3*, 343–421. https://doi.org/10.3390/network3030017

Academic Editor: Christos Bouras

Received: 30 July 2023
Revised: 17 August 2023
Accepted: 25 August 2023
Published: 30 August 2023

1. Introduction

Blockchain is a distributed, immutable, and Peer-to-Peer (P2P) database composed of information secured using cryptography, which is very strong in securing transactions and ensuring the preservation of data integrity and authenticity [1]. In the early days, the blockchain concept emerged to support BitCoin for secure transactions without an intermediary [2]. There are basically two types of blockchain architectures: linear and Directed Acyclic Graph (DAG). Linear blockchain is the conventional blockchain, where

transactions form a Merkle tree and are bundled to synthesize a block containing the hash value of the previous block [3]. On the other hand, DAG blockchain is the more modern approach, bringing advantages in scalability and computation by parallelism. In a DAG blockchain, typically, single transactions exist without grouping, where each transaction validates multiple previous transactions [4]. Blockchains rely on consensus algorithms for transaction validation and creating a new block/transaction to the blockchain. The scattered elements of the blockchain network may come to an understanding of the legitimacy of the transactions or blocks using consensus processes [5]. Blockchains are further characterized by high persistence, as there is less chance for falsification or high fault recovery capability (because several nodes have copies of the same legitimate transaction or block in their possession), and high transparency, as each user has similar rights and access to the blockchain network [6]. However, blockchain cryptographic vulnerabilities still exist where an attacker can use a side channel attack to leak sensitive information. Furthermore, blockchains are well known for their high propagation delay due to the distributed consensus approach consisting of validation and transmission of transactions; thus, it is advisable to select a consensus approach after a performance analysis [7]. Moreover, they are also susceptible to decentralized refusal of service attacks, which can overwhelm the connections to the point where resources are inaccessible to authorized users [8].

To enhance the functionality of cognitive networks, it has been suggested that blockchain-based approaches be combined with AI and ML techniques. The authors in [9] argue that a smart city can achieve more sustainability with the fusion of blockchain and AI. Furthermore, AI has been proposed to deliver error-free smart contracts for blockchain 2.0, as opposed to the smart contracts developed manually by human programmers, which can contain loopholes and flaws [10]. Blockchain has the potential to be utilized in the medical field to build reliable artificially intelligent models and to display medical records using blockchain to improve service efficiency and reduce costs [11]. Furthermore, the strengths of blockchain for privacy preservation, the capacity to manage massive data amounts, and the ability to cope with the computing demands of intelligent networks have been discussed in [12]. Likewise, deep extreme machine learning has been utilized in smart home architecture along with blockchain to ensure the security goals of integrity and privacy [13]. Some researchers have integrated AI and blockchain to achieve energy-efficient and secure routing, which obviates proof-of-work consensus for control plane communication [14]. However, there are challenges in applying blockchain technology in cognitive networks, such as high energy consumption, resource management difficulties, a lack of standardization and scalability, increased latency, limited throughput, etc., as discussed in detail in this survey (in Section 6.2).

Because the controller continuously gathers network usage statistics, Software-Defined Networking (SDN) has an overall overview of the network as a whole and performs traffic manipulation more effectively than network connectivity based on conventional hardware [15]. Moreover, by isolating the primary network governing functionality from the routing components and providing logical network control centralization as opposed to ordinary networking, where the control layer is closely connected with end devices, SDN enables the programming of networks [16]. Due to the conceptual divorcing of the control layer, SDN's three layers—the data/infrastructure layer, control layer, and application layer—offer benefits of agility and network programming capability. Thus, the network's broad perspective makes it feasible to perform dynamic energy assignment, load balancing, motion governance, and other functions [17]. Additionally, network analytics gathering also makes it possible to experiment with and apply innovative protocols more affordably [18]. Additionally, the control plane is able to relate with all of the data plane's components by using a southbound interface. Services like virtual networking, cloud-based services, big data, etc. are possible thanks to SDN [19].

The three modes of control of SDN are combined, decentralized, and centralized, whereas the single controller model has complete logical and physical centralization and explicitly stated flow rules for the data plane elements [20]. Centralized control is best suited

to be deployed when there is a requirement for simplified network control, in data center networks where global optimizations are very important, when the network size is small, and when the network environment is relatively stable. This approach, however, is less extensible, has a propensity to be a source of collapse, and has an extended communication latency for the control layer [21]. The central point of malfunction and challenges with scaling observed in the single controller paradigm are successfully avoided in distributed control architecture, where the control is conceptually and/or physically dispersed among numerous synchronized controllers. Distributed control architecture is well suited for large networks having thousands of pieces of user equipment, when fault tolerance is crucial, and when low-latency local decision-making is necessary. However, because there are several controllers, distributed control models have trouble maintaining consistency and typically take longer to optimize globally [22]. On the other hand, the term "hybrid (combined) control model" refers to a combination of completely centralized control and completely distributed control, where the conceptually centralized controller may modify the control on the data plane elements from complete (completely centralized control) to null (completely distributed control), considering the network circumstances [23]. Thus, hybrid control is best suited when the size of the network is variable and the network conditions can change over time from stable to highly dynamic. Moreover, blockchain has been employed to improve different aspects of SDN. The most dominant application is the security and privacy that blockchains enable due to their immutable properties [24]. Like every paradigm, SDN has a number of difficulties. The original conceptually centralized SDN approach has a variety of problems, including that it has a single physically and conceptually centralized controller, which makes it less trustworthy due to one source of breakdown [25]. Furthermore, SDN has security risks in heavily mobile networks like automotive networks [26], and, because of the changeable network layout, routing is problematic [27,28]. Other obstacles that SDN encounters include expansion, difficulty connecting with historical networks, and the absence of a few standards for the northbound interface [29].

Data/information are utilized to create knowledge with the aid of a knowledge creation technique in Knowledge-Defined Networking (KDN), which is used in updating application policies and aids in making decisions in control and management planes [30]. As an example, through conflicts between automotive actions, the idea of KDN was employed to investigate knowledge of hazard perception [31]. Furthermore, the significance of an area's centralization has been determined via automobile mobility analysis, and nodes in this knowledge-defined vehicular network are entitled to this perception [32]. Moreover, knowledge generated using data in the management information base can be deployed to aid in decision-making regarding network monitoring and network configuration in the management plane by jointly considering application policies. For example, when the knowledge plane detects that the bandwidth consumption of the network devices is high, if there is an application policy specifying that the network bandwidth consumption must be lower than a given threshold, then the network configuration module can dynamically reconfigure network devices such that bandwidth consumption is reduced. Likewise, in the control plane, based on data collected on security events, routing protocols, QoS data, traffic statistics, etc., the knowledge plane can generate knowledge that can be used to make decisions in the control plane. For example, based on security events or behavior-based data collected, when the knowledge plane categorizes a certain set of network devices as malicious devices, the control plane can enforce the routing application policy by updating all flow tables in the network and setting flow rules such that packets are not forwarded through the malicious devices. Thus, when implementing a KDN, detection data from various forwarding devices is employed to develop insight into the general control setting [33]. The key roles of the knowledge plane in KDN are knowledge generation, knowledge compilation, and knowledge dissemination [34]. As another option, KDN has been put forth by academics as a framework for implementing artificial intelligence (AI) in SDN [35]. Knowledge-based networking, also known as the KDN paradigm, combines data

and information to create understanding by employing AI models or rule-based models, such that KDN represents knowledge-based networking in all types of networks [36]. Despite the fact that the idea of a knowledge plane was first put forward in [37] almost 20 years ago, KDN has lately attracted interest because of the challenges associated with moving directly from regular networks to KDN and current developments in artificial intelligence.

For KDN's security concerns, Machine Learning (ML) has been employed for identifying breaches [38], detecting service denial assaults [39], and identifying abnormal behavior [40]. In [41], machine learning has been used to predict control traffic to aid in controller virtualization and control channel isolation. Furthermore, researchers in the study [42] utilized deep neural networks to identify communication patterns in nearby automobiles that reduced the number of packet crashes. Moreover, in the KDN, ML has additionally been employed to classify flow [43] and packets [44], forecast connection stability [45], determine the optimum pathways using link lifetime and delay prediction [46], and perform other tasks. Artificial intelligence has been utilized for automotive networks that employ the idea of KDN to anticipate Vehicle-to-Infrastructure (V2I) connection reliability [47], identify service denial incidents [48], and locate paths based on faith [49], among other things. Additionally, knowledge for KDNs has been generated using fuzzy reasoning, meta-rules, and artificial intelligence [50]. Through network orchestration of operations chores, KDN may decrease the requirement for human involvement, save operating expenses, and boost energy savings [51]. In order to achieve the idea of an autonomous vehicular network, the KDN principle has been applied for network surveillance as a feedback control system [52]. Likewise, reinforcement learning with deep learning can potentially be applied for autonomous packet forwarding in KDNs to acquire knowledge from experience while carrying out surveillance of the network to understand how the environment interacts [53]. Additionally, a self-contained packet forwarding method that uses deep machine learning in a self-governing KDN to determine the most trustworthy pathways on request has been studied in [54]. Furthermore, an autonomous driving system utilizing graph-based neural networks that chooses the best route for responsive traffic operating and service function linking has been researched in [55], taking advantage of automation coming from knowledge development in KDN. In [56], an artificial intelligence-based approach to identifying huge striking fluxes was examined. On top of that, fifth-generation KDNs [57] have employed artificial intelligence for audiovisual traffic categorization. Machine learning—specifically, deep learning—has been extensively applied in healthcare networks for medical image analysis, etc. to generate knowledge regarding disease diagnosis with high classification performance [58]. An intelligent hybrid clinical diagnostic system using particle swarm optimization and back propagation neural networks has been utilized to detect prostate cancer using medical records with high accuracy to aid in clinical decision-making [59]. Similarly, deep convolutional neural networks have been leveraged to detect subtypes of acute lymphoblastic leukemia using blood smear images to generate knowledge regarding the disease from benign cases and determine the appropriate treatment technique [60].

The KDN idea continues to be relatively fresh, and there are not many standards or techniques for communication within the main planes [61]. In contrast to SDN, KDN features an extra administration (management) layer and a cognitive (knowledge) layer that are conceptually distinct from the operation of the control layer. The cognitive layer uses knowledge creation frameworks to analyze all the information and data gathered from the management and control layers and to create regulations and intelligence that are then provided to the application, administration, and control layers. By automatically designing flows according to an evaluation of recent data and immediate information gathered from the network, KDN has been used to enhance the efficiency of networks [62]. KDN transforms classic SDN's humanly programmed control plane operations into a self-executing, dynamic control plane that creates rules based on AI-/ML-generated understanding [63]. KDN, whose network actions are driven by AI-/ML-generated knowledge and optimiza-

tion techniques, has a higher efficiency than traditional networking, in which network device actions are explicitly defined by the network administrators, thus not being able to adapt to dynamic network conditions. In contrast to traditional networking, KDN has high automation, high scalability, high security, and a low operational cost. However, KDN is more complex due to additional layers; thus, it incurs a high implementation cost compared to traditional networking [64].

The survey in [65] explores the application of blockchain in SDN for security and protection. A similar survey presents blockchain applications in SDN for security and protection, albeit with a broader perspective and future avenues [66]. Furthermore, another review article presents the application of blockchain in SDN in both security and non-security fields and further investigates the challenges of the applications [67]. The review paper in [68] presents the fusion of blockchain and ML for 5G and beyond IoT networks. Similarly, review papers [69–71] review the blockchain and machine learning integrated frameworks for wireless sensor networks and smart grids, with an emphasis on security and privacy. Different from the previously mentioned surveys, our survey involves reviewing the application of blockchain technology in knowledge-defined networking. Knowledge-defined networking can be expressed as the artificial intelligence-/machine-learning-/knowledge-based extension of the SDN paradigm, which encapsulates all types of knowledge-driven networks such as intelligent smart grids, intelligent wireless sensor networks, intelligent Internet of Things, intelligent vehicular networks, intelligent optical networks, intelligent medical networks, etc. Therefore, compared to surveys on blockchain in generic SDN [65–67], our survey is for a special futuristic case of SDN, where knowledge is generated using machine learning/artificial intelligence/fuzzy logic/meta-heuristic techniques for blockchain applications. Moreover, compared to previous surveys [68–71], our survey has a broad perspective, having generic knowledge-driven (not only limited to machine learning, but also addressing other heuristic knowledge-generation techniques such as optimization, meta-heuristics, fuzzy logic, etc.) network applications without being bound to the security and privacy applications of a special network category of knowledge-based networks. As far as we are aware, we are the first to examine how blockchain technology is being applied in Knowledge-Defined Networking with a broad perspective, analyzing and discussing diverse network applications (not being bound to security and privacy), challenges, and opportunities in those applications in order to provide recommendations and future directions.

Figure 1 provides a visual representation of the organizational structure of this review article.

Different sections of this review article are structured in the following manner, in agreement with the organizational structure visualized in Figure 1. In Section 2, we give a summary of the blockchain technology with its architecture, consensus algorithms, framework, characteristics, security vulnerabilities, and types. Section 3 depicts a synopsis of the Knowledge-Defined Networking framework while comparing it with existing networks. Section 4 reviews existing applications of blockchain technology in knowledge-defined networks in diverse categories. Section 5 summarizes the reviewed frameworks under application categories; compares blockchain-based, knowledge-based, and network-based parameters of each framework while analyzing the performance; and analyzes the overall distribution of parameters for the survey. Section 6 examines the advantages and difficulties of integrating blockchain technology into intelligent networks. Finally, the piece of writing winds down in Section 7 by providing final thoughts, propositions, academic implications, and future prospects.

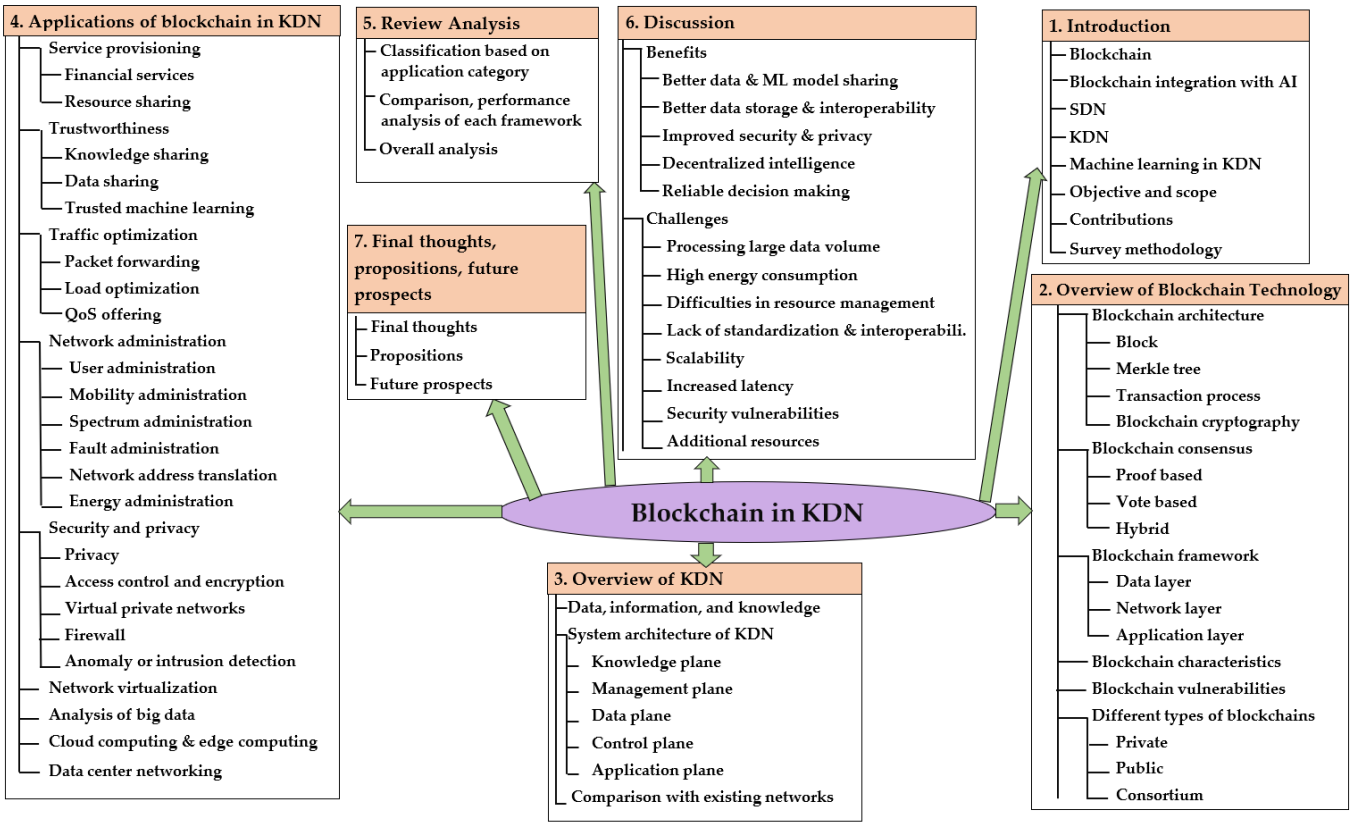


Figure 1. Hierarchical organization of the survey on application of blockchain technology in Knowledge-Defined Networking.

1.1. Objectives and Scope

The primary objective of the survey is to investigate existing blockchain-based frameworks that have been proposed for diverse applications in Knowledge-Defined Networking. Furthermore, we provide introductory education to the reader on each concept of blockchain technology and Knowledge-Defined Networking. In achieving the main objectives, we focus on all sorts of knowledge generation techniques in KDN, not being limited to machine learning, and, at the same time, not being limited to security and privacy in blockchains. Another objective is to identify and discuss the benefits and challenges of applying blockchain technology in KDN in order to derive useful propositions for the applications that future academicians can use as a guideline when applying blockchain in intelligent networking. The final objective is to analyze both qualitatively and quantitatively the reviewed blockchain-based applications in terms of different parameters.

1.2. Contributions to the Existing Literature

- As this is the first review of how blockchain technology has been applied in Knowledge-Defined Networking, this work will serve as a beneficial resource for other scholars who pursue more study in this domain;
- Survey analysis, with respect to blockchain-based parameters and intelligent networking parameters, provides insight into the distribution and statistics of existing solutions for the considered parameters;
- Advantages of and difficulties in applying blockchain in KDN are discussed while deriving recommendations to overcome the challenges.

1.3. Survey Methodology

This survey is qualitative and longitudinal in its approach and critically reviews the existing work on blockchain in Knowledge-Defined Networking published over a

period of time. Furthermore, it reviews individual aspects of blockchain technology and Knowledge-Defined Networking. Therefore, the population for this survey consists of all original research articles and web pages published on KDN, blockchain, and blockchain in KDN. However, all references within the population cannot be reviewed in a survey article. Therefore, we sampled 410 references by searching online databases with appropriate search strings and selection criteria.

We searched the MDPI article search engine, ScienceDirect, the ACM digital library, the Wiley online library, IEEE Xplore, and Google Scholar. The search strings that we used most commonly were "Blockchain" OR "Knowledge-Defined Networking" OR "Artificial intelligence-based networking" OR "Machine Learning-based networking" OR "Artificial intelligence-based Software-Defined Networking" OR "Machine Learning-based Software-Defined Networking" OR "intelligent networking" OR "intelligent Software-Defined Networking" OR "Cognitive networking" OR "blockchain in Knowledge-Defined Networking" OR "blockchain in machine learning-based Software-Defined Networking" OR "blockchain in artificial intelligence-based Software-Defined Networking" OR "blockchain in intelligent Software-Defined Networking" OR "blockchain in artificial intelligence-based networking" OR "blockchain in machine learning-based networking" OR "blockchain in cognitive networking" OR "blockchain in intelligent networking" OR "blockchain in fuzzy logic-based networking" OR "blockchain in intelligent meta-heuristic-based networking".

The selection criteria consisted of several criteria for filtering the articles. First, the reference had to be written in English, and, secondly, it had to be highly relevant to the searched string. Thirdly, priority was given to journal articles over conference presentations and pre-prints, to improve the validity of the conducted survey. However, the selection criteria did not have any bias toward publications from certain publishers, and we treated all publishers as equal. Finally, the last criterion was that a given reference should have been published in the years from 1980 to 2023.

We found out that 32 references were duplicates, so the original sample was reduced to 378. Furthermore, we used 16 research articles to refer to definitions and explanations related to different concepts presented in this survey. Moreover, later, we added 7 survey papers to the sample to compare this survey with existing surveys, increasing the total number of references to 401.

For survey qualitative analysis, we used the tabular data structure to compare existing blockchain-based applications in Knowledge-Defined Networking under various parameters such as blockchain characteristics, machine learning characteristics, network features, and performance. Additionally, we used the Microsoft Excel software package to generate graphs to analyze the survey statistics related to blockchain-based and knowledge-based networking parameters quantitatively.

This survey belongs to communication networks, so ethical considerations are not applicable.

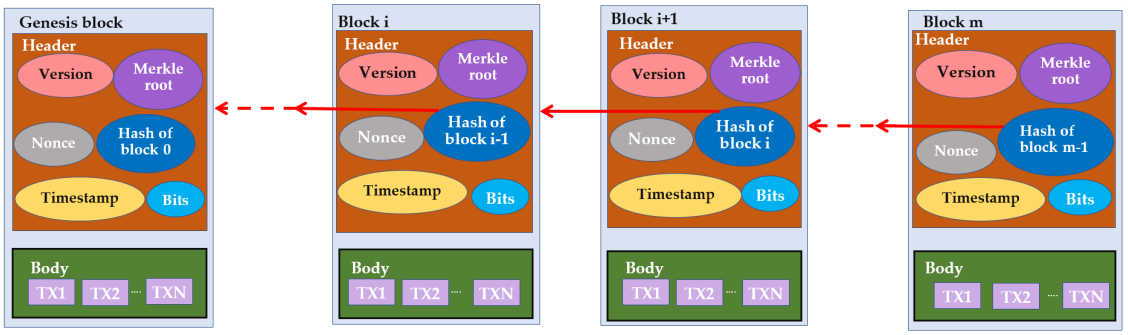
2. Overview of Blockchain Technology

2.1. Blockchain Architecture

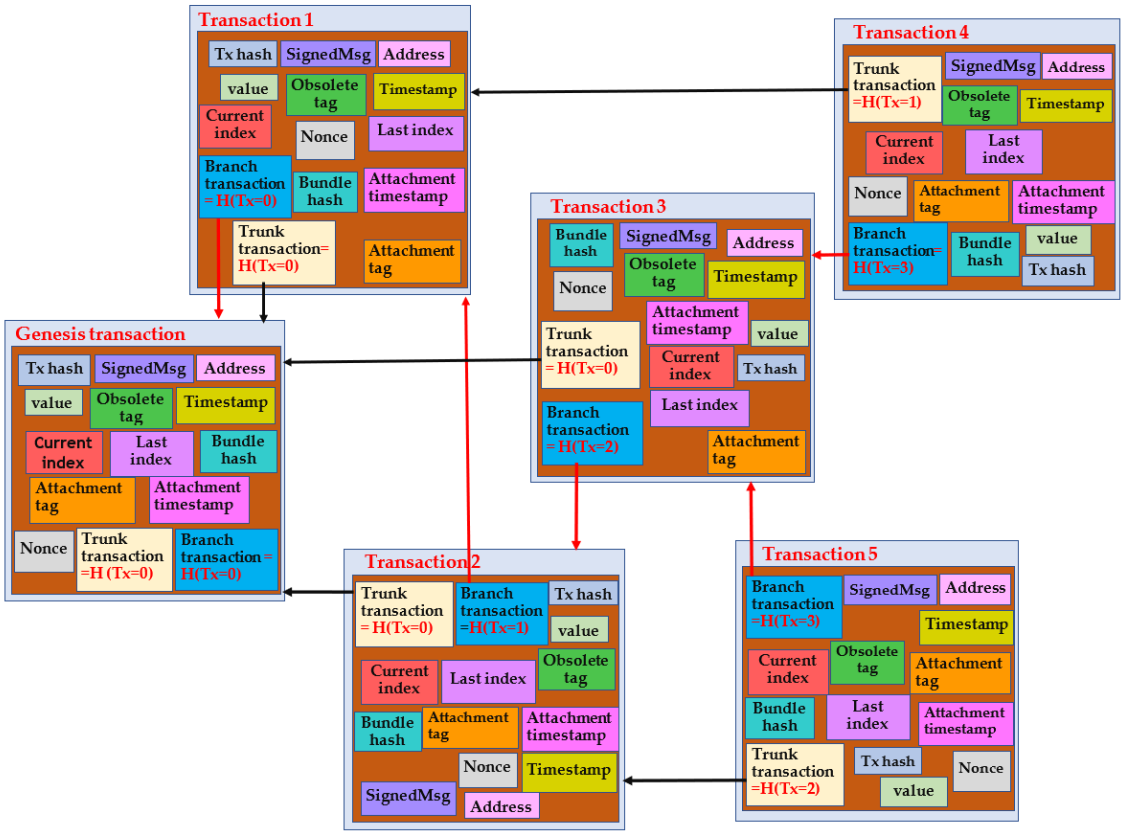
As implied by the name itself, the blockchain is a sequence (series) of block segments with transaction records in each block, like a public ledger, in which every single block, with the exception of the genesis block, remains connected to its parent block via the parent block's hash digest [72]. The term blockchain was officially introduced to the world in 2008 as a distributed ledger for Bitcoin, even though some researchers have previously proposed concepts related to blockchain such as cryptographically secured blocks, Merkle trees, etc., beginning in 1982 [2].

2.1.1. Block

The blockchains have two types of implementations: linear blockchain [3] and Directed Acyclic Graph (DAG) blockchain [4], which are graphically illustrated in Figure 2.



(**a**) Linear blockchain



(**b**) DAG blockchain (IOTA).

Figure 2. Different realizations of blockchains.

Linear Blockchain

As evident from Figure 2a, the genesis/first block is the initial block in the distributed ledger that lacks a parent block. In a linear blockchain, a block fundamentally has two components: the block body and the block header. The version, parent block hash digest, root of the Merkle tree of operations/transactions, timestamp, nonce, and bits constitute the block header [73]. The version includes the most recent iteration of the block validation specifications that may be used to verify the block's validity. The hash digest of the preceding block's header is utilized as the parent block's hash. The root of the Merkle tree is the hash digest of the base of the Merkle tree, formed by the aggregation of the hash values of operations inside the block in a hierarchical manner. The formation of a Merkle tree using operations is described in the next section. The block's moment of birth is recorded by the timestamp, while the nonce is implemented as a counter that increments for every hash computation until the desired hash is found during consensus.

Bits is an entity depicting the difficulty level of the consensus algorithm. A group of transactions/operations and a transaction/operation counter with a value indicating how many operations/transactions exist within the block constitute the block body. Note that in, a linear blockchain architecture, multiple operations/transactions constitute a block [74].

DAG Blockchain

Different from linear blockchain architecture, DAG blockchain, as shown in Figure 2b, is a DAG consisting of linked operations/transactions. The genesis transaction/operation is the very first transaction to occur on the DAG blockchain. The initial transaction in the IOTA DAG blockchain is empty. Typically, the transactions/operations are not categorized into blocks in the DAG blockchain, in contrast to a block on a linear blockchain, and instead exist as single transactions that are essentially linked and may confirm multiple previous transactions [4]. Indeed, this architecture has a transaction as a block and, thus, does not have the body and header fields found in the block of a linear blockchain. Furthermore, this architecture does not employ a Merkle tree and, therefore, does not need block miners to create and validate blocks. Hence, DAG blockchains have higher scalability and parallelism than linear blockchains [75]. IOTA tangle is one such realization of a DAG blockchain, which is a blockchain of transactions, with each transaction containing transaction hash, signed message, sender or receiver address, obsolete tag, value, timestamp, current index, last index, bundle hash, nonce, references to previous transaction data (trunk transaction hash, branch transaction hash), attachment tag, and attachment timestamp. The operation's/transaction's hash code has been designated as the transaction's hash. The transaction or operation that has been digitally signed and contains both the information regarding the transaction and the digital signature is commonly referred to as the signed message. The obsolete tag is a user-defined tag, while the value contains the amount of cryptocurrency in the transaction. The transaction's timestamp is contained in the moment at which it became connected to the tangle. The bundle's last index is the reference value for the previous transaction/operation, whereas the current index is its reference value for the most recent transaction/operation. The bundle hash contains the hash of value, last index, current index, timestamp, address, and obsolete tag. Nonce is a field used in proof-of-work consensus that is modified until a valid solution is found. References to previous transactions can be multiple, being two (trunk transaction hash and branch transaction hash) in the case of the IOTA DAG blockchain, and varying in other models of the DAG blockchain [76]. The attachment tag is a user-defined tag, while the attachment timestamp is the time elapsed since 1970 up to the point at which consensus was finished.

2.1.2. Merkle Tree

A trustworthy and immutable distributed ledger may be created using the Merkle tree idea [77]. Figure 3 illustrates the Merkle tree's structure.

Figure 3 makes it clear that the bottom of the tree is made up of a group of transactions. Note that each operation's/transaction's hash digest falls within the first tier, while subsequent upper layers are formed by computing the hash value of two components of the preceding layer. Finally, the Merkle tree root contains a single hash value representing the content of all validated transactions [78]. Note that, even if a minute change occurs for one transaction, the block's hash code is different due to the modification of the base of the Merkle tree, such that the whole blockchain is affected by a single transaction modification. Since hash functions have the characteristic that a minor alteration to the input induces an enormous modification in the output, even for very small transaction modifications, the links in the blockchain are broken.

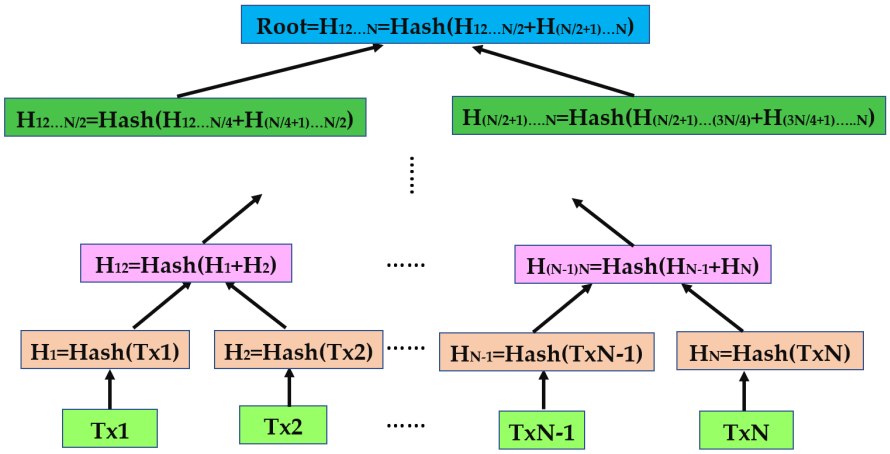


Figure 3. The structure of the Merkle tree in a block of a linear blockchain.

2.1.3. Transaction Process

Every transaction inside a given block in the blockchain should be verified so that only legitimate users perform the transactions. This is achieved with the help of digital signatures such as elliptic curve digital signatures, which use the concept of asymmetric key cryptography [79]. The digital signature signing and verification process is graphically illustrated in Figure 4.

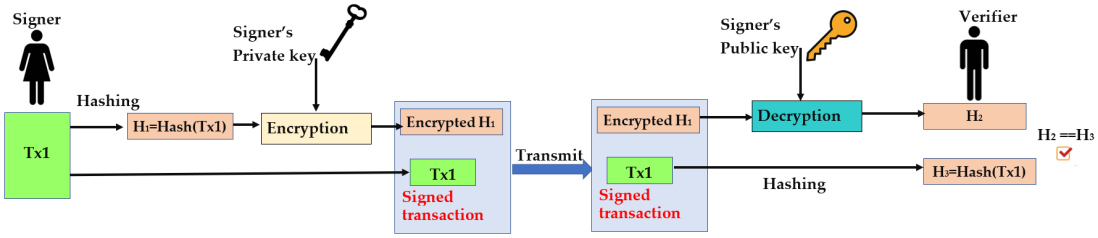


Figure 4. The signing and verification process of digital signature.

Figure 4 makes it clear that a certain user will sign a blockchain transaction using his private key so that other users may access it using the public key provided to the person who executed the transaction. While verification entails decrypting the signed content employing the public key and comparing it to the hash digest of the operation/transaction, signing entails computing the hash value and encrypting it using the private key [80]. A digital signature ensures that only legitimate (valid) users are performing transactions by verifying that the calculated hash of the recipient and the decrypted hash match. Figure 5 depicts the generic transaction process.

The technique of consensus is implemented to insert operations/transactions onto an existing blockchain. As evident from Figure 5, a transaction is initiated by a transaction request, which has been encrypted with the private key belonging to the sender and contains the sender's and recipient's addresses within the transaction itself. Then, the transaction is published to every network member, such that each user saves the signed transaction locally. The transaction is then verified by every network node by means of the public key assigned to the sender. The transactions are then gathered by a miner who is chosen based on consensus, and they are combined into a block that is put on the blockchain. The fresh block will then be broadcast throughout the network, and, before it is added to the blockchain locally by every single node, it is checked for legitimacy [5].

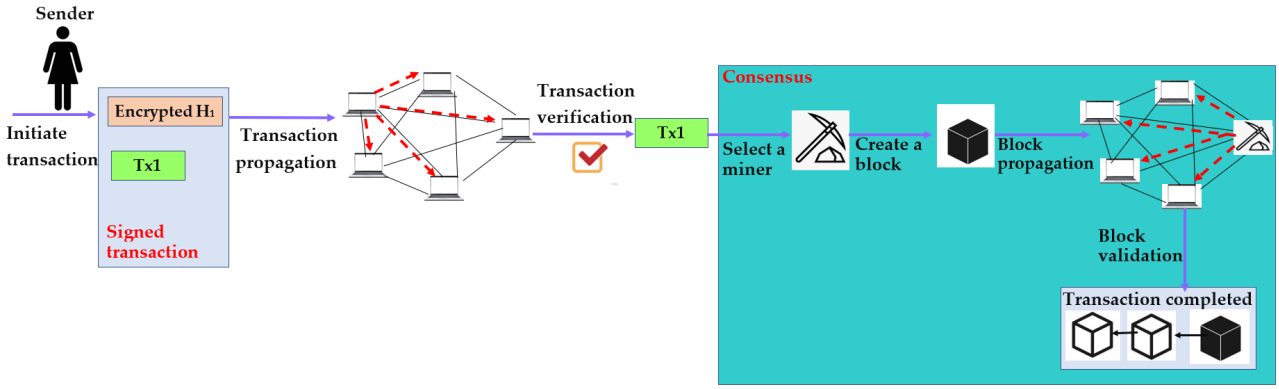


Figure 5. Generic transaction process of a blockchain.

In the existing literature, two types of transactions can be identified based on the blockchain platform: Bitcoin transactions and Ethereum transactions.

In Bitcoin transactions, the main transaction element is the transaction output that is not spent (UTXO), while the possession of some bitcoin amount is transferred from one address to another. A miner can obtain transaction fees and rewards for block creation using a Coinbase transaction [2].

Ethereum transactions, on the other hand, have the main transaction element as an account, where transactions directly update the account balance. An Ethereum transaction transfers ether and may also trigger a smart contract. Ethereum has incentives to be provided to block creators in the form of gas points to be provided for transaction fees [81].

2.1.4. Blockchain Cryptography

It is worth reviewing the cryptography used in blockchains. Blockchains use three types of cryptographic techniques, namely, hash functions, public key cryptography, and zero-knowledge proof.

A hash function converts given input data of variable size into a fixed-size hash digest. Hash functions are used inside digital signatures to compute the hash of transactions, the hash value of blocks, etc. [82]. A hash function is characterized by difficulty in estimating the input given the output of the hash function. Furthermore, they are known for fewer collisions where there is a very low possibility of producing the same hash output for two distinct inputs. Most importantly, they help to verify the integrity of data due to the characteristic that the hash digest changes significantly when the input is even slightly altered [83].

Public key cryptography is used in the digital signature for verifying the legitimacy of the operations/transactions, where a block miner or a peer validates the operation/transaction, utilizing the public key after the end user signs the transaction or operation by employing a private key [80], as discussed in the section on transactions. In addition to verifying the user of a transaction, a digital signature makes sure that the transaction is unaltered.

Zero-knowledge proofs (ZKPs) may be applied to confirm that transactions are correct without revealing the identity of those transactions, thus securing privacy and preventing sensitive information disclosure [84]. For instance, when sending cryptocurrency from a sender to a receiver, owing to the utilization of ZKPs, the blockchain does not need to know how much cryptocurrency exists in the wallet of the sender.

However, classical public key cryptographic techniques and hash functions belong to the pre-quantum computing era, and their security is challengeable in the post-quantum computing era. Post-quantum cryptography (PQC) involves efficient cryptographic techniques that are resistant to attacks from quantum computing; thus, efficient and lightweight PQC is desirable for blockchains to minimize quantum computing-based attacks [85]. Being

descendants of the family of elliptic curve cryptography, Montgomery curve (Curve448) and Edwards curve (Ed448) cryptographic techniques are deployed in digital signatures and key agreement, which can be efficiently implemented in Cortex-M4 with performance improvements and, thus, can be deployed in hybrid systems that use a mixture of classical and post-quantum cryptographic techniques [86]. Moreover, the Supersingular Isogeny Key Encapsulation (SIKE) mechanism is a post-quantum key encapsulation technique that can be implemented in the Cortex-M4 platform, yielding energy efficiency and fast computation; thus, it is suitable to be deployed in resource-constrained platforms such as blockchain-based KDNs [87]. Furthermore, Kyber is a post-quantum cryptographic technique that can be deployed for secure key exchange and is considered by the National Institute of Standards and Technology (NIST) for standardization. It has been tested on the 64-bit ARM Cortex platform, where it has resulted in faster encapsulation, decapsulation, and key generation [88]. Additionally, the Edwards curve digital signature algorithm, which has been optimized for execution time (Ed25519), is a digital signature algorithm proposed to be deployed in hybrid cryptographic systems that has been tested in a Field Programmable Gate Array (FPGA) implementation with speed improvements and improved utilization area [89]. Likewise, an optimized version of the key exchange technique known as Supersingular Isogeny Diffie–Hellman (SIDH) has been tested for achieving post-quantum security levels on 64-bit ARM processors, where the projective approach has shown better overall performance than the affine approach [90].

Fault attacks, a type of side-channel attack, can be launched by an attacker to induce a fault and analyze its effects to obtain sensitive information from the encrypted data. Thus, robust error detection mechanisms must be deployed for the cryptographic techniques that are deployed in blockchains to recover from fault attacks. WAGE is a stream cipher derived from the Welch–Gong cipher, and error detection using signatures for non-linear sub-blocks of it has been effective in a FPGA-based hardware implementation with good error coverage [91]. Furthermore, an error detection framework for the Camelia block cipher considering non-linear and linear sub-blocks, using different S-box variants, where the reliability can be fine-tuned based on requirements having high error coverage has been studied in [92]. Similarly, for the symmetric key Midori cipher, a fault diagnosis scheme for the non-linear S-box layer is presented, and simulations with injected faults show that the proposed framework is reliable [93]. Likewise, a hardware-based, lightweight signature-based error detection for block cipher QARMA for 64- and 128-bit versions that can counter both permanent and transient faults has been benchmarked in an FPGA device satisfying reliability requirements with acceptable overhead [94].

Differential Power Analysis (DPA) is a passive attack where an attacker analyzes the power traces to get an inference about the internal operation of the cryptographic algorithm. DPA can be combined with Differential Fault Analysis (DFA) by an attacker to launch a more powerful attack, so there should be robust countermeasures against such attacks. Error detection is deployed against fault analysis, while masking techniques can be deployed to counter power analysis attacks in order to protect ciphers from side channel attacks [95].

2.2. Blockchain Consensus Algorithms

Blockchains do not employ trusted third parties but rely on consensus algorithms for trustworthiness validation. Consensus procedures are mechanisms that follow a unified agreement to produce and approve fresh blocks while ensuring the consistency of ledgers at various endpoints [5]. Note that consensus approaches are deployed to develop trust inside the blockchain network, which each member of the blockchain needs to follow. Consensus may be broken down into two separate groups: vote-based and proof-based. Both of these classifications are simply explored in the subsequent paragraphs.

2.2.1. Proof Based Consensus

The element that yields convincing evidence receives the potential to introduce a fresh block to the blockchain and obtain compensation in proof-based consensus. One option, among the inaugural consensus techniques for blockchain consensus that were originally established, is Proof of Work (PoW) [96]. In PoW, a node is required to prove its trustworthiness by performing work (mining). Specifically, a hard problem to solve, such as guessing the nonce value when the hash code of the nonce and block is required to be matched with the challenge level (bits). Thus, the first node that spends computational resources to figure out the problem obtains the opportunity to insert the block after verifying and confirming every operation in the freshly created block. However, due to energy expenditure, PoW is known to be less energy efficient.

In Proof of Stake (PoS) [97], the element that shows the highest ownership of the currency becomes the winner, assuming richer nodes have a low probability of attacking the blockchain. Once per time frame, a miner is picked at random, depending on their stake, to contribute a block; thus, PoS is an energy-efficient approach compared to PoW. However, PoS has some drawbacks, such as the dominance of wealthier nodes, its attack-prone nature due to mining costs being much lower, the nothing-at-stake problem, etc.

Since both PoW and PoS have their own drawbacks, a hybrid approach combining the features of both PoW and PoS has been proposed known as Proof of Activity (PoA) [98], where a group of validators have to digitally sign a produced block for it to be considered legitimate, such that, even if there is a dominant node with a high stake, it cannot control block creation on its own. In PoA, miners first engage in PoW to create new blocks, while PoS is applied to generate subsequent blocks based on the stake. As a drawback, PoA consumes considerable time for the transition from PoW to PoS.

Proof of Space (PoSp) [99] involves nodes allocating a significant amount of storage for storing predefined data (plots). In PoSp, the node that has the highest plot space obtains the opportunity to synthesize a block. Even though PoSp uses less energy to operate compared to PoW, it can be attacked by storage pre-computing.

In Proof of Burn (PoB) [100], the miner who burns the highest amount of cryptocurrency token within a given amount of time obtains the chance to mine a new block. PoB involves miners voluntarily destroying their own cryptocurrency by sending it to a burning address, assuming that legitimate users burn more cryptocurrency. However, PoB may discourage users as it involves the permanent burning of cryptocurrency tokens.

In Proof of Authority (PoAu) [101], authority is assigned to a particular set of pre-approved validators, typically chosen based on reputation, who are allowed to verify and append fresh blocks. But PoAu has some degree of centralized authority, which reduces the distributed consensus features of the blockchain.

Proof of Elapsed Time (PoET) [102] is a novel consensus procedure in which nodes ask a trustworthy entity to wait (for an elapsed time), and the element with the shortest waiting time is given the chance to process the subsequent block. However, PoET has been known to suffer from scalability issues, and the wait time determined by execution environment may not be accessible to every node in a decentralized manner.

2.2.2. Vote Based Consensus

In vote-based consensus, messages are exchanged between the nodes, while all nodes verify the blocks together.

Practical Byzantine Fault Tolerance (PBFT) [103] is a consensus approach based on voting that can prevent crashing nodes and subverting nodes. In PBFT, one node is the leader, while the other nodes are peers. Initially, the nodes send requests for validating transactions to the peers, whereas, after passing a specific number of transactions, the leader node composes them into a block and broadcasts it to the peers in the pre-prepare phase. During the preparation phase, the peers rebroadcast the received block to verify that the received block from the leader is the same. The new block is introduced to the blockchain during the commit phase, provided every node obtains copies from over two-thirds of

all other peers. Thus, PBFT can function in the presence of 1/3 of the total nodes being malicious nodes. However, PBFT has poor scalability due to the involvement of all nodes for consensus [104].

In Delegated Byzantine Fault Tolerance (DBFT), voting determines a set of nodes that verify operations and insert a fresh block on the blockchain in a similar manner to PBFT instead of all nodes [105].

Raft is a crash–fault tolerance-based consensus approach with the assumption that more than 50% of the nodes function normally. In Raft, a given node can be a leader, follower, or candidate. Candidate nodes select a leader through a voting process. Once a leader is appointed, the leader records all transactions sent by multiple followers. When the leader receives a transaction, it broadcasts the logged transaction and the index of the previous transaction to followers. Followers synchronize with the leader on the transactions according to the transactions received from the leader. Finally, the leader verifies that all nodes have the same transactions and then assembles the transactions together, creating a block, and publishing the block out to all followers to add the block to their blockchain [106].

2.2.3. Hybrid Proof- and Vote-Based Consensus

A mixture of evidence-driven agreement and election-driven agreement has been employed in the mixed proof- and vote-based consensus technique. The best example of such a hybrid approach is Delegated Proof of Stake (DPoS) [107]. There exist two different sorts of nodes in this method: delegates and witnesses. Each node with a stake can act as a witness to vote and elect delegates, which are then used to validate blocks. However, DPoS has a tendency toward centralization of authority and high-stake nodes for controlling the blockchain [108].

2.3. Blockchain Framework

Even if a blockchain may be summarily described as a sequence of blocks, each of which is associated with the one preceding it, a blockchain framework consists of a blockchain having interactions with the network environment and applications [109]. Figure 6 represents the structure of the blockchain framework.

As evident from Figure 6, there are three tiers in a blockchain framework: the data tier, the application tier, and the network tier, which are discussed in the following subsections.

2.3.1. Data Layer

The fundamental blockchain layout is principally contained within the data tier, consisting of an immutable ledger that has blocks with transactions forming a Merkle tree in the block using cryptographic hash functions whose root hash value is stored in the headers (in the case of linear blockchains) [77]. A graph with a directed acyclic structure (tangle) functions as the data tier in the DAG blockchain, consisting of linked transactions where each transaction validates (containing the cryptographic hash value) multiple previous transactions [4].

As discussed previously, the transactions' legitimacy is secured using a digital signature [80] in the data layer, and the transactions are composed into blocks with the help of consensus in the network layer [5]. Furthermore, data stored on the blockchain can be optionally secured using asymmetric key cryptography to protect sensitive data [110].

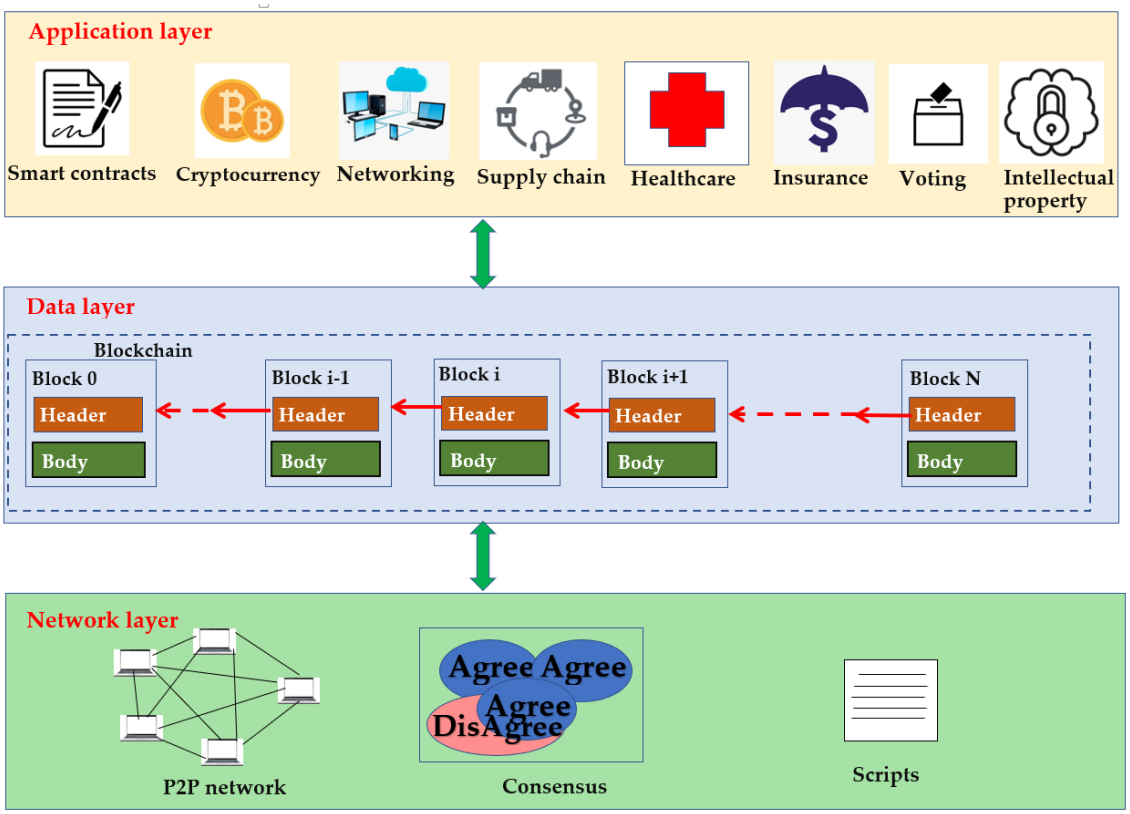


Figure 6. The structure of the blockchain framework.

2.3.2. Network Layer

The network tier acts as an interaction environment for the blockchain. A primary responsibility of the network tier is consensus, a method for shared agreement across blockchain nodes for confirming transactions and introducing fresh blocks to the blockchain [5]. This is realized with the help of P2P conversations, which give every node in a network the same importance and keep a copy of the blockchain without the need for a centralized authority. Furthermore, each node establishes decentralized connections with the other nodes to exchange data and authenticate transactions and blocks. Even if every single node in the network is equal, they can play different roles, such as leader or follower, in coming to an agreement. It is challenging to eliminate the blockchain's presence in the network since every node keeps an exact replica of it. P2P conversation is made possible in the Bitcoin ledger network by means of the Bitcoin protocol, which uses a simplified internet protocol for communication [111]. The Ethereum wire protocol is implemented in Ethereum blockchain networks to facilitate P2P conversation. It was created to allow for the deployment of smart contracts as well as the propagation of transactions and blocks [112]. Inter-Planetary File System (IPFS) is a P2P file transfer protocol that is based on content-addressable storage to enable distributed data storage in blockchain networks [113].

In a blockchain network, there is an approach for locking and unlocking scripts for access control of transactions or resources. When locking a script, a user defines a set of conditions required to unlock the script, whereas, upon reaching the conditions, another user can unlock the script to access the transaction/resource in Transaction-Based Access Control (TBAC) [114].

2.3.3. Application Layer

The application tier has a variety of purposes for which blockchain can be utilized. Cryptocurrency, smart contracts, supply chains, networking, healthcare, insurance, voting,

and intellectual property stand out as eight of the most dominant blockchain applications that are worth discussing briefly.

Cryptocurrency

The two most widely used cryptocurrencies built on blockchains are Ether and Bitcoin. Without the help of reputable centralized institutions like banks, financial transactions may be carried out securely and reliably using cryptocurrency [115]. The blockchain for Bitcoin offers a public ledger for every transaction, guaranteeing the transactions' immutability [2]. Contrarily, self-executing contracts may be created on Ethereum's blockchain, which pave the way for decentralized finance bound by contractual terms and conditions [81].

Smart Contracts

A smart/self-executing contract is a blockchain application tier implementation that specifies contractual statements of an agreement that are automatically executed when certain events occur [116]. It can be deployed on a platform based on blockchains. Once deployed, the contract is immutable due to the immutable nature of the blockchain, so its integrity can be trusted. They eliminate the requirement for an intermediary to enforce the terms and conditions of contracts, so that business contracts can be automated using smart contracts. Self-executing contracts could be deployed for restricting access to ensure that only individuals with proper authorization can use particular assets [117]. The stipulations of the smart contract are able to be employed to establish the requirements for permitting access to certain assets, such that control over the resources will be provided upon meeting the access-granting conditions. However, all transactions that are executed upon reaching some condition of the contract are written to the blockchain. Smart contracts help automate transactions strictly following contractual conditions and thus result in reduced operational costs compared to conventional contract operations. Formal methods that are mathematical approaches to modeling and testing software to make sure that it operates in the desired manner can be deployed to verify the functioning of smart contracts in order to prevent costs and security breaches that occur in the case of smart contract errors or vulnerabilities [118]. These formal models can capture user behaviors and blockchain properties in the process of smart contract verification during execution, unlike traditional approaches for smart contract verification [119].

Supply Chains

Blockchains enable data sharing in supply chains where stakeholders can track the origin and movement of products with reduced risk of unethical behavior. It is possible to keep track of operations using a dispersed blockchain and the movement of goods along the supply chain [120]. A practical illustration of supply chain management with blockchain is cold chain management [121]. A systematic literature review on blockchain applications suggests that blockchain has been extensively used in supply chain management as a business application for identifying and tracking products, sharing information among stakeholders, facilitating supply chain decisions, etc. [122].

Networking

For decentralized data sharing, network administration, and network security, blockchains have applications in networking, particularly in Internet of Things (IoT) networks and Unmanned Aerial Vehicle (UAV) networks. By assisting network intrusion detection systems, creating network security records, preventing unauthorized access, protecting data integrity, etc., blockchains may be utilized to ensure network security. To automate decision-making and enforce network regulations, smart contracts can be used. For example, TRUCON is a platform built on the blockchain for trustworthy data exchange that has traffic management capabilities for the web of automobiles, where stationary devices serve as complete nodes and moving automobiles serve as portable nodes [123]. IoTChain leverages blockchain infrastructure to offer permitted customers safe accessi-

bility to IoT assets. Multicast teams are established for these individuals on the public blockchain [124]. UASTrustChain is a trust management framework for UAV networks where observers maintain the trust score of UAVs in a secure and reliable blockchain ledger to detect abnormal behaviors [125]. Moreover, the integration of blockchain and the Internet of Things (IoT) has resulted in a new paradigm called Blockchain and the Internet of Things (BIoT), in which there are intellectual cores such as data security and privacy, applications, frameworks, etc. [126].

Healthcare

Blockchain technology has numerous applications in healthcare. One of them is applying blockchain to prevent drug counterfeiting by utilizing the power of an immutable ledger [127]. Blockchain may also be leveraged for exchanging medical information in a safe approach, protecting the integrity and exposure of sensitive medical data. With the incorporation of self-executing contracts, blockchains harness cryptography and accessibility restrictions to avoid the disclosure of confidential information. Medblock [128] and MedShare [129] are examples of frameworks that utilize the power of blockchain technology for secure medical data sharing and management.

Insurance

Blockchains can be utilized to secure many functions in the insurance domain. They can be used to store the information of policyholders and claim histories in an immutable manner, which smooth and automate the insurance claim processing while being resistant to data integrity attacks as stakeholders verify tamper-proof data [130]. Furthermore, blockchain and smart contracts can be utilized to prevent insurance fraud, as blockchains provide a framework to store insurance data in a manner that cannot be manipulated by unauthorized third parties [131]. Furthermore, blockchains can enhance the process of reinsurance and catastrophe bond issuance through the process of appropriate risk assessment by estimating asset- or human-associated losses using a risk index [132].

Voting

In addition to all the security features provided by blockchains, such as data integrity, trustworthiness, confidentiality, etc., in voting systems, blockchains facilitate the prevention of duplicate votes. PriScore is one such blockchain-based voting framework that stores ballots on the blockchain to prevent tampering while using self-tallying for calculating and verifying the election result using score voting to prove two given conditions as a challenge [133]. Blockchain-based voting is convenient as it allows secure digital voting even from remote places and provides faster result generation as vote tallying and result verification can occur in real-time. Moreover, the blockchain-based voting process is auditable, starting from voter registration until the dissemination of the election result, ensuring the trustworthiness of the voting process [134].

Intellectual Property

Blockchain can be employed to protect the intellectual property of its users by facilitating their maintenance of a proof of creation/ownership. For instance, Proof-of-Contribution (PoCo) is a consensus approach that calculates the behavior and actions of users in the blockchain based on their contribution, where the node with the highest contribution is allowed to mine the next block, which has been very effective in protecting the intellectual property of the users [135]. Consortium blockchain has been leveraged for Intellectual Property Rights (IPRs) management, thanks to the decentralized and tamper-proof nature of blockchain, where registering and enforcing IP rights can occur [136].

2.4. Blockchain Characteristics

Blockchains are distinctive in that they have characteristics in common with other blockchains, proving that they are superior to other frameworks. First off, because

blockchains are decentralized, no centralized authority has any influence over how they function [1]. Instead, blockchains rely on P2P communication for validating the transactions, which prevents drawbacks in conventional centralized governing authority architectures such as one potential site of breakdown, service costs, etc. [137]. Next, blockchains have high data integrity due to the layout in which every single block archives the base of the Merkle tree and the hash digest of the preceding block, such that even a minor modification of a transaction affects the entire blockchain [77]. All transactions on the blockchain are traceable due to the transactions storing the transaction timestamp, sender and receiver addresses, transaction funds, etc. [138]. Furthermore, due to the leveraging of digital signatures for transaction/operation verification, where the user performing the transaction signs it using the private key to ensure non-repudiation, users cannot deny that they have carried out the transaction [80]. In blockchains, every user has equal access and interaction rights with the blockchain network, which enables high transparency for users [103]. Furthermore, blockchains have a high fault recovery tendency, mainly thanks to consensus, as, in most consensus approaches, for the flawed operations to be approved and appended to the system, the errors must exist in excess of 50% of the nodes [5]. Similar to fault tolerance, the blockchains are resistant to hacking attacks, given that the hacked nodes make up a small portion of the nodes within the network and the infected nodes are unable to alter the blockchain. Consensus among the majority of good peers can overwrite the hacked nodes [139]. Blockchains have a high persistence, as each transaction should be confirmed and distributed across the blockchain network in a block, and the blocks are validated by each node such that falsification can be detected easily [140]. Blockchains have pseudonymity, which means that a given node generates a pseudonymous address to interact with the blockchain, reducing the privacy exposure to a certain level [141].

2.5. Blockchain Vulnerabilities

Despite the characteristic strengths of the blockchains discussed in the previous section, there are known vulnerabilities in blockchain. Blockchain hazards have been encapsulated into six high-level categorizations in current research, which are briefly discussed below:

- Network attacks—Attacks related to the blockchain network, such as denial of service attacks that submit more transactions than the blockchain's capacity, routing attacks, domain name service attacks, eclipse attacks, etc., fall under this category [142];
- Endpoint attacks—Endpoint attacks target endpoints (nodes) in the network of a blockchain. In the 51% vulnerability, malicious nodes, consisting of greater than 50% of the network endpoints, can manipulate the blockchain in a malicious manner, compromising the security. Another endpoint attack is the cryptojacking attack, where an attacker uses a node's computational resources to mine cryptocurrencies [143];
- Intentional misuse—Intentional misuse refers to individuals exploiting vulnerabilities in the blockchain network for personal gain. In a double-spending attack, the individuals trick the blockchain network into performing two transactions simultaneously by using the cryptocurrency sufficient for one transaction [144]. In selfish mining, miners intentionally delay the broadcasting of mined blocks to obtain a knowledge advantage over other nodes [145];
- Code vulnerabilities—Code vulnerabilities refer to the misconfiguration or poor use of software code. For example, broken access control refers to misconfiguration or poorly implemented access control such that unauthorized users may obtain access to sensitive data on the blockchain [146]. Criminal smart contracts are smart contracts implementing contractual actions to deceive or harm blockchain users in order to steal cryptocurrency, promote illegal transactions, etc. [147];
- Data exposure—This refers to sensitive data exposure and privacy leakage, which can occur when private data are stored on the blockchain with poor encryption. Furthermore, as blockchain transactions are traceable, some of an individual's activities can be identified [138];

- Human negligence—The security of the blockchain node may be misconfigured by humans due to negligence. If humans do not properly monitor the security logs, security breaches will not be identified in a timely manner [148].

2.6. Different Forms of Blockchain

There are mainly three forms of blockchain that exist in the existing literature: private blockchain, public blockchain, and consortium blockchain, which are briefly addressed in the segments that come next.

2.6.1. Private Blockchain

Private blockchains are fully centralized and permissioned for consensus. Private blockchains have lower integrity compared to public blockchains, and data access can be public or restricted. Private blockchains have high scalability and efficiency because they are controlled privately [149].

2.6.2. Public Blockchain

The public ledger is fully scattered and consent-free. Public blockchains have high integrity as all nodes participate in the consensus, so data cannot be tampered with easily, despite the public access given to data. However, public blockchains are less scalable and have low efficiency [150].

2.6.3. Consortium Blockchain

A hybrid strategy that brings together the advantages of both private and public blockchains is referred to as the consortium blockchain. Thus, it is partially centralized and permissioned for consensus. They have lower integrity compared to public blockchains, while the data access can be public or restricted. Consortium blockchains also have high scalability and efficiency as they are controlled by an organization [151].

Table 1 summarizes protocols/models/languages for achieving different functions in each plane of the blockchain framework.

Table 1. Summary of protocols/models/approaches/frameworks/examples in each plane of the blockchain framework.

Plane	Function/Purpose	Protocols/Models/Approaches/Frameworks/Examples
Network	Proof-based consensus	PoW [96], PoS [97], PoA [98], PoSp [99], PoB [100], PoAu [101], PoET [102]
	Vote-based consensus	PBFT [103], DBFT [105], Raft [106]
	Hybrid consensus	DPoS [107]
	Scripts	TBAC [114]
	P2P communication	Bitcoin protocol [111], Ethereum wire protocol [112], IPFS [113]
	Network attacks	DoS attacks, routing attacks, domain name service attacks, eclipse attacks [142]
Data	Architectures	Linear [3], Directed acyclic graph [4]
	Types	Private [149], Public [150], Consortium [151]
	Cryptography	Hashing [82], Public key cryptography [80], Zero-knowledge proofs [84], Post-quantum cryptography [87,88,90], Hybrid cryptography [86,89], fault-tolerant ciphers [91–95]
	Endpoint attacks	51% vulnerability, cryptojacking [143]
Application	Smart contracts	Contractual automation [116], access control [117]
	Cryptocurrency	Bitcoin [2], Ethereum [81]
	Supply chain	Cold chain management [121]
	Networking	TRUCON [123], IoTChain [124], UASTrustChain [125]
	Healthcare	Drug counterfeiting [127], Medblock [128], MedShare [129]
	Insurance	ClaimChain [130], Insurance fraud protection [131], Decentralized reinsurance [132]
	Voting	PriScore [133], Auditable voting [134]
	Intellectual property	IP protection [135], IP rights management [136]

3. Synopsis of KDN Paradigm

3.1. Introduction to Knowledge Concept

The most basic component is a piece of data, which is unrefined, fresh, and has a single value and a unit of measurement [152].

A structured, examined collection of fresh data is referred to as information, and it may be utilized to help make decisions [153].

Knowledge is described as the condition of comprehension (abstract content) attained by individual encounters, education, and the evaluation of gathered facts and information [154]. Thus, knowledge has a significantly stronger decision-making capacity than information because of its level of comprehension.

We now use an automobile networking instance to help explain these ideas. The three-dimensional velocity $(v1_x, v1_y, v1_z)$ is an illustration of data. The differential velocity between two automobiles is determined by analyzing the velocity data of the two automobiles at a specific time instance. Therefore, the differential velocity of two vehicles at a particular time instance $(vehicle_1, vehicle_2$, 15:05, $(dv_x, dv_y, dv_z))$ is an illustration of information. Estimating the likelihood that vehicle 1 and vehicle 2 are likely to be in an accident is, thus, an illustration of learnable knowledge that may be derived by recognizing and understanding a variety of information, like hazard alerts, sensor observations, pathfinding instructions, etc., between the two cars.

3.2. Detailed KDN Architecture

The KDN structure's detailed block schematic with interfaces, sub-layers, and data/information/ knowledge/rule/policy flows is displayed in Figure 7 [34,37,155–159].

A KDN is made up of five primary layers, as witnessed in Figure 7, while the combined (encapsulated) control layer, which is an encapsulation of the cognitive, administration, and control layers, is responsible for managing the network and making control choices based on knowledge-based inference and application guidelines [160].

3.2.1. Knowledge/Cognitive Layer

A conceptual layer called the knowledge layer is in charge of producing, combining, and distributing knowledge over a network. This layer enables network managers to see issues and address them before they arise or worsen inside the network, maximize network functionality in response to evolving demands, and take preventative measures to reduce risks. The knowledge and/or rules generated by the knowledge layer may be used to identify and fix network problems, setup the network with the least amount of user involvement, find malicious attacks or anomalies, etc. Three sub-layers make up the knowledge layer.

Employing data and information, the knowledge creation layer creates knowledge utilizing algorithmic-based or artificial intelligence techniques. The Resource-Description Framework (RDF) modeling language may be utilized for modeling the knowledge generated by the knowledge-generating layer. Resource, property, and value are the triad that RDF provides to express knowledge. Resources and values are distinguished by uniform resource identifiers, while properties show the connections between resources and values [161]. Rule-based techniques often entail the use of an algebraic framework to explain the fresh data [162] or the use of the data's internal connections [163] to produce knowledge. Simple logic or data fusion are two other pragmatic ways of producing knowledge [164].

An ontology editor is implemented in the knowledge composition layer to combine created knowledge and universal knowledge (pre-existing knowledge in the knowledge base) to create assembled knowledge, which may be utilized to build rules via integration with user intent, as shown in Figure 7. Furthermore, by employing an ontology vocabulary to designate organizational structures, groups, connections, and attributes within the fields, an ontology editor may be utilized to construct the ontology's architecture [165]. In order to provide the structure and allow for expressing and modifying knowledge using a computer-understandable format, five primary knowledge modeling languages

have been introduced for KDNs: Knowledge-Interchange Format (KIF) [166], Ontology-Inference Layer (OIL) [167], Resource-Description Framework (RDF) [161], RDF-Schema (RDFS) [168], and Web-Ontology Language (OWL) [169]. Additionally, in order to create fresh rules using a rule creator to create rules that may be utilized by other layers, the knowledge composer layer creates innovative rules by comparing the requirements of the application with the combined knowledge [64]. A rule creator is often realized as a rule-based model using a computer language like Java or Lisp [170]. The rules produced from the rule creator ought to be expressed in a universal language so that other layers can comprehend them. A specialized rule language, such as Rule-Markup Language (RuleML) [171], Rule-Interchange Format (RIF) [172], or Semantic-Web Rule Language (SWRL) [173], may perhaps be utilized to express the created rules.

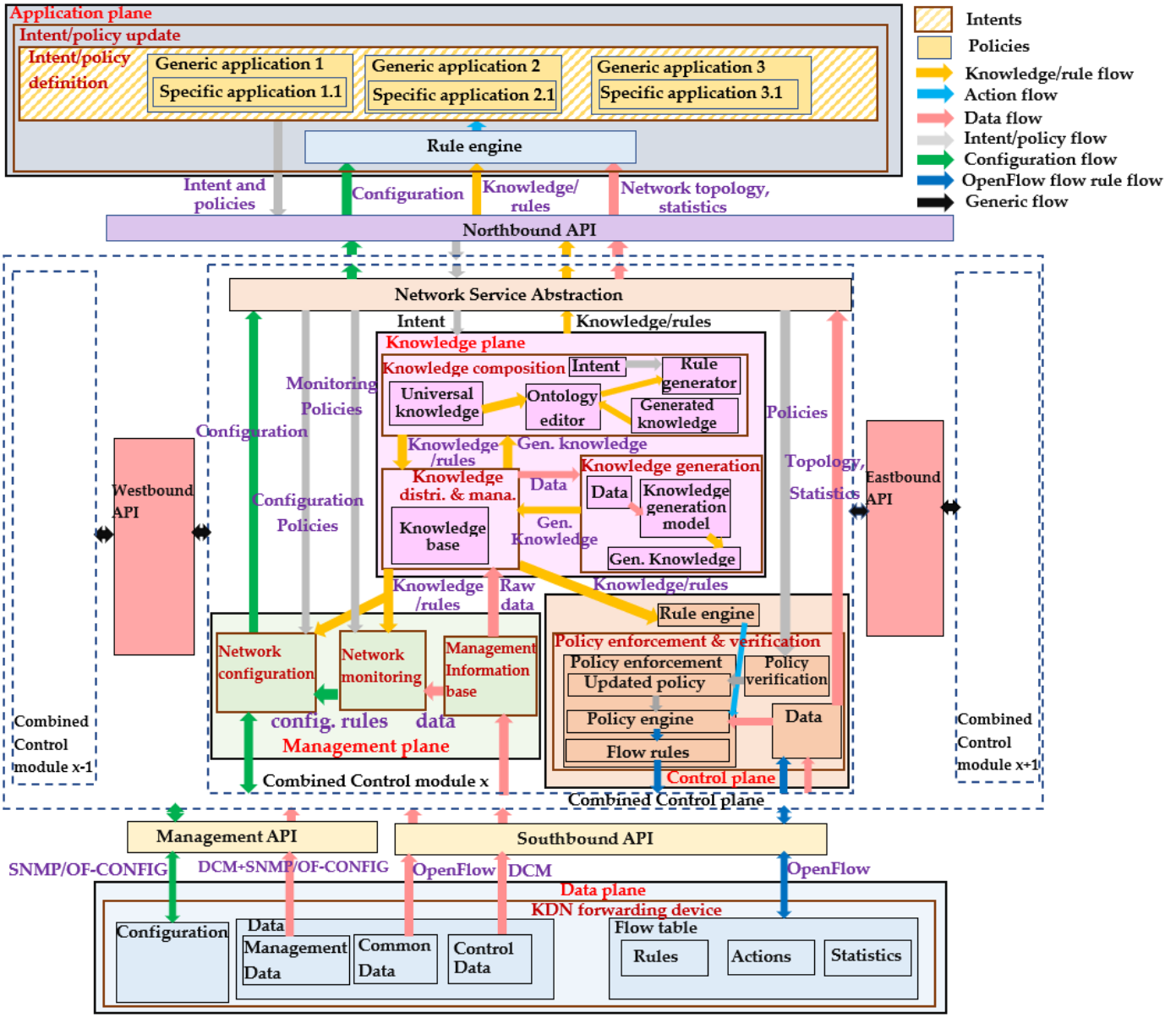


Figure 7. Detailed block schematic for the layered structure of KDN with interfaces, sub-layers, and flows.

The knowledge management and dissemination layer includes a repository of knowledge known as the knowledge base to store rules/knowledge and utilizes appropriate protocols/languages to enter, modify, eliminate, and share rules/knowledge [34]. Thus,

knowledge produced through knowledge creation models, combined knowledge created using ontology editors, rules created by rule creators, network data that have been gathered, and messages from the control layer make up this knowledge base in this sub-layer. Additionally, in order to analyze the rules or knowledge communicated by the knowledge dissemination sub-layer and carry out the operations, other layers must include a reasoning (rule) engine like RETE [174], Bossam [175], Jess [176], Drools [177], etc. A rule engine applies rules or draws conclusions from understanding, then decides, depending on how well the rules and knowledge were applied. Moreover, with the assistance of knowledge retrieval and modification languages like SPARQL [178] and GraphQL [179], current knowledge may be altered in accordance with new regulations, etc. Likewise, knowledge retrieval-only languages like SQWRL [180], Knowledge–Graph Query Language (KGQL) [181], and Knowledge Query-and-Manipulation Language (KQML) [182] permit advanced users to question and collect knowledge from the knowledge base regardless of prior familiarity with the knowledge base's fundamental structure. This makes it easier and more efficient for services and individuals to acquire knowledge.

3.2.2. Management/Administration/Measurement Layer

As illustrated in Figure 7, the administration layer, which runs concurrently alongside the KDN control layer, carries out the functions of data or information accumulation through the network equipment, network component monitoring, and network instrument configuration. Additionally, the management layer in KDN may be impacted from the knowledge layer in assisting with actual-time network surveillance as well as from the application layer in implementing setup guidelines, in which monitoring results can help with dynamically setting the network [155,159]. An encapsulation of network services is the network-service abstraction sub-layer that encapsulates services including load balancing, intrusion detection, fault management, etc., serves as a bridge for control and administration choice-making programs to link with control and administration layers [183]. Moreover, network data needed for network surveillance in the management layer and knowledge creation in the knowledge layer are stored and managed in the Management Information Base (MIB).

Due to its compatibility with OpenFlow-based forwarding devices, the OpenFlow management-and-CONFIGuration Protocol (OF-CONFIG), which transports data via the NETwork-CONFiguration Protocol (NETCONF), is the most frequently used network setup and management protocol [184]. Likewise, OF-CONFIG or NETCONF can be replaced with the Simple-Network-Management Protocol (SNMP), a protocol that has been developed for the surveillance and setting up of network gadgets in KDN [185]. Moreover, Complexity-Oblivious Network-Management (CONMan) [186] and Platform for Automated-Operation and Configuration-Management (PACMAN) [187] are two other alternative network management frameworks that can be utilized in KDNs. These frameworks provide the combined tasks of network surveillance and configuration as network management tasks.

There have been frameworks proposed only for the task of network surveillance. Network surveillance frameworks such as Payless [188], joint HOst-NEtwork (HONE) [189], OpenNetMon [190], and OpenSample [191] have been utilized for network surveillance by collecting traffic statistics data and QoS data.

It should be noted that the administration layer can gather facts for network setup (configuration data) and network surveillance (traffic statistics, network layout, metrics of performance, etc.) utilizing a protocol like SNMP/OF-CONFIG or a network surveillance platform. Additionally, other data can be gathered using a Data Gathering Method (DGM), like quadratic integer programming-based optimization [192], packet sampling [193], adaptive data collection [194], and sensor measurement collection [195]. Additionally, the management layer may gather a variety of data, including layout, setting up, traffic patterns, records of events, consumption of resources, indicators of performance, information from sensors, etc.

A representation language called Yet Another Next-Generation (YANG) has been employed to represent the setups and state information of network gadgets [196]. As an alternative, the Common-Information Model (CIM) is a model of data that provides a consistent method of displaying data regarding instrument functionalities and network architecture [197]. It should be noted that data inside the MIB of the administration layer can be represented using both YANG and CIM data representations.

3.2.3. Data/Infrastructure Layer

The data layer is made up of transferring components that can analyze, save, or transfer data in compliance with the traffic rules transmitted by the control layer. Furthermore, the infrastructure layer is needed to transmit the fresh facts sought by the measurement and control layers, which are used to generate insight in KDN [198]. Such knowledge-based awareness is used by the controller to make choices about network control, by the management layer to make selections about network surveillance and setting up, and by the application layer to continuously alter policies.

In comparison to switching devices in SDN, data-transfer components in KDN demand more capacities, such as throughput and computing power, owing to the greater communication load used for transmitting data to surveillance and control layers. Real switching devices, virtualized switching devices, routing devices, wireless connection points, base stations, etc. are examples of forwarding equipment [199]. While network traffic flow rules have been created by the controller, these devices are set up and observed by the measurement layer. There are several switch-transferring models that employ protocols like OpFlex [200], ForCES [201], OpenFlow [202], Protocol-Oblivious Forwarding (POF) [203], Path-Computation Element Path-Computation Client (PCEPCC) [204], OpenState [205], and others.

Network executives may adjust network layouts dynamically without altering the core network infrastructure by using simulated switches, which are software components that connect virtual computers and real network hardware. Moreover, modern virtual switches such as VMware NSX, Open vSwitch, etc. can separate data flow between several emulated machines or collections of emulated machines, allowing for the creation of network sectors and enhancing network security [206].

Circuit switching is a necessary component of fiber optic networks, and KDN switches that are a part of a fiber optic network are dependent on light circuit switching. Dedicated path switching, in contrast to connectionless switching, occurs at the infrastructure plane of the OSI concept, employing light routes to link multiple optical switches via fiber optics. On the other hand, infrastructure plane transmission in packet switching networks typically uses wired or wireless media.

3.2.4. Control Layer

The control layer, which can consist of multiple SDN controllers determined by the control model paradigm, is in charge of transmitting to the infrastructure layer forwarding rules, authorization rules, rules for prioritizing data flows based on quality of service, etc. Program guidelines and dynamic rules or perceptions derived using the knowledge layer are both used to drive control in the KDN [207], as shown in Figure 7.

The integrated control layer and application layer may communicate with one another thanks to the northbound interface, which can be implemented using an ad hoc [208], RESTful [209], intent-based [210], or language-based API [211]. On the other hand, using protocols like OpenFlow, ForCES, OpFlex, and others, the southbound interface serves as a bridge between the infrastructure layer and the control layer. It is used to transmit raw facts from the data forwarding components to the controller and to convey flow rules from the control layer to the infrastructure layer equipment [202]. Additionally, in order to have an overall perspective of the network, east–westbound interfaces like ALTO [212], Hyperflow [213], ONOS [210], Onix [214], etc. allow communication between the physically scattered controllers.

Centralized control, decentralized/distributed control, or mixed/hybrid/combined control models are all possible in KDN. NOX [208], Trema [215], Ryu [216], Meridian [217], and other controllers maintain the conceptually and physically centered controller design, but SMaRtLight [218], HyperFlow [213], ONOS [210], Onix [214], Kandoo [219], Orion [220], and other controllers retain the conceptually centralized and physically scattered architecture. On the other hand, mixed control architectures such as DevoFlow [221], Fibbing [222], HybridFlow [223], etc. incorporate a blend of completely centralized and fully scattered designs. Moreover, controllers like Distributed-SDN Controllers (DISCO) [224], D-SDN [225], Cardigan [226], etc. represent conceptually and physically scattered controller paradigms. Note that either complete or partial consistency exists among the dispersed controllers.

OpenFlow-enabled packet control provides the maximum level of control resolution. On the other hand, there are benefits to rough-grained flow control, such as decreased costs for control layer communication, that uses packets in the form of a flux of numerous packets, like traffic flows, depending on quality of service.

Reactive control approaches cause modifications to the network in response to flows or happenings. On the other hand, the controller pre-computes the switching components with a collection of rules when utilizing proactive control to manage all potential streams of traffic prior to the traffic even reaching the switches.

One of the controller's primary operations is to figure out the ideal route for data streams (path computation) and traffic optimization, which involves improving the traffic fluxes in order to boost the network's efficiency with the help of the gathered data. Additionally, the control layer may gather raw facts such as traffic information, QoS data, regulations, security incidents, protocols used for routing, etc. [227]. Moreover, by implementing a policy engine, the control layer may instruct network gadgets to perform specific tasks when specific requirements are satisfied, executing policies, as shown in Figure 7. These network guidelines are transformed into rules using a policy orchestrator (engine) by taking into account additional information, other rules, and perceptions from knowledge [228].

Network data are routed via a network service sequence using flexible/agile service chaining, where the controller selects the services to be included in the chain depending on changing network circumstances [229]. Furthermore, the controller may also flexibly build simulated networks, such as private virtual networks, and scale them depending on dynamic network requirements [230].

3.2.5. Application Layer

Application developers can use this layer as a base to convey their needs to the underpinning physical network. Additionally, it enables network managers to centrally set network settings guidelines that are better matched with general business goals and objectives (intents), with the application function being divorced from hardware, and specify network policies unique to applications. Moreover, application guidelines may be continuously modified in KDN depending on information about the network's functioning, which enhances the delivery of services [231].

The application layer separates the service function from the physical components in order to centrally define the desired intentions and regulations. Within the application layer, there are essentially two sub-layers: the objective/policy definition sub-layer and the objective/policy update sub-layer, as shown in Figure 7.

The objective/policy creation sub-layer's main function is to use network supervisors to establish guidelines and goals. Following their definition, objectives and policies can be continually modified by the objective/policy update sub-layer, utilizing the rules and knowledge-based perception obtained using the cognitive layer, the set of settings obtained from the administration layer, and the network's layout and analytics obtained using the control layer. As a result, when the network's condition changes, application principles and intentions may be dynamically changed. There are programming frameworks such as Procera [211], Nettle [232], Frenetic [233], Kinetic [234], etc. that are built on top of

common programming languages such as Python, Haskell, etc. for achieving the previously mentioned policy definition and updating tasks.

Common examples of general KDN applications include traffic optimization, network administration, and security. Moreover, the application layer uses a northbound interface and an abstraction layer of network services to interface with other layers except the data layer.

Table 2 depicts a synopsis of protocols/models/languages for achieving different functions in each layer of KDN.

Table 2. Synopsis of protocols/models/languages in each layer of KDN.

Plane	Function	Protocols/Models/Languages
Knowledge	Store knowledge	KIF [166], OIL [167], OWL [169], RDFS [168], RDF [161]
	Rule modeling and dissemination	RuleML [171], RIF [172], SWRL [173]
	Knowledge querying only	KGQL [181], KQML [182], SQWRL [180]
	Knowledge querying and modifying	SPARQL [178], GraphQL [179]
	Rule/knowledge assessment	RETE [174], Bossam [175], Jess [176], Drools [177]
Management	Network management	OF-CONFIG [184], SNMP [185], PACMAN [187], CONMan [186]
	Network monitoring	Payless [188], HONE [189], OpenNetMon [190], OpenSample [191]
	Data collection	IQP [192,235], packet sampling [193], adaptive data collection [194], sensor measurement collection [195]
	Data storage	YANG [196], CIM [197]
Data	Forwarding models	OpenFlow [202], ForCES [201], OpFlex [200], POF [203], PCE-PCC [204], OpenState [205]
Control	Northbound API	Adhoc [208], RESTful [209], intent-based [210], language-based API [211]
	East–Westbound API	ALTO [212], Hyperflow [213], ONOS [210], Onix [214]
	Southbound API	OpenFlow [202], ForCES [201], OpFlex [200], POF [203], PCE-PCC [204], OpenState [205]
	Logically and physically centralized control	NOX [208], Trema [215], Ryu [216], Meridian [217]
	Logically centralized and physically distributed control	SMaRtLight [218], HyperFlow [213], ONOS [210], Onix [214], Kandoo [219], Orion [220]
	Hybrid control	DevoFlow [221], Fibbing [222], HybridFlow [223]
	Logically and physically distributed control	DISCO [224], D-SDN [225], Cardigan [226]
Application	Policy definition and update	Procera [211], Nettle [232], Frenetic [233], Kinetic [234]

3.3. A Glimpse Comparison of KDN with Existing Networks

The first approach of networking is known to be conventional networking, which requires manually setting and controlling equipment. This networking approach has been used often since networking's inception, and it continues to be employed in contemporary communication networks. Moreover, in conventional networks, the infrastructure layer and the control layer are dispersed among network nodes and closely connected, with nodes like routers serving both control and data-handling purposes. Since every network component must be individually set, older networks are challenging to maintain and administer. This is because massive networks can become unattainable because of the time commitment and susceptible to mistakes nature of human configuration. Furthermore, in these networks, choices are made strictly in accordance with the flow rules or guidelines that network managers have established for setup and surveillance purposes.

A more modern strategy than regular networks is SDN that allows for greater versatility in network architecture by divorcing the control layer from the infrastructure layer. Network operators utilize apps to administer the network, conceptually centralizing the control layer. Due to its better adaptability and customization ability, this framework enables network executives to operate networks more rapidly and efficiently. However, SDN

does not place a strong emphasis on knowledge generation while making control choices, but the controller that is conceptually centralized utilizes network information to build an overall network picture and make judgments with the support of network application-enforced regulations. Although administration is centralized, it is not separated as a distinct layer but rather is a part of the control layer. Moreover, actions taken by the controller are determined by network application policies rather than knowledge-based inference.

KDN adds a new conceptually separated knowledge layer and divorces the administration layer from the control mechanism in the SDN paradigm. In order to supervise, set up, and control networks, it places a strong emphasis on modeling knowledge, logical thinking, and the making of decisions. In order to automate the administration of network equipment and build a smart network that can gain insight and adjust to varying circumstances, it leverages domain-oriented knowledge visualization (knowledge ontologies). Furthermore, by utilizing artificial intelligence to detect risks in an instantaneous fashion and using the knowledge layer and the control layer to reduce hazards, KDN offers even greater protection than SDN. Note that SDN programs network behavior using APIs and software controllers, but KDN automates network control and administration by additionally utilizing knowledge-based technologies like machine learning. Additionally, knowledge is generated using data gathered by network equipment and utilized to derive rules and understanding that can be provided to the control layer for use in making control choices based on perceptions in KDN. Because administration functions and control logic are conceptually separated, troubleshooting errors is significantly simpler in KDN. Moreover, by updating administration guidelines within the application layer using understanding based on knowledge gleaned from the network, network administration can potentially be automated. Because controlling is founded on network regulations as well as understanding derived from knowledge created, the control layer is both conceptually centralized and learning by itself.

4. Application of Blockchain Technology in Knowledge-Based Networks

In this phase, we explore how KDNs take advantage of blockchain. The deployment of blockchain in KDN brings intelligent, decentralized, and secure network operation and management [236]. Service provisioning, trustworthiness, traffic optimization, network administration, security and privacy, virtualization of networks, analysis of massive data, cloud computing and edge computing technology, and data center networking categories are used to group the blockchain applications in knowledge-based networks. These identified blockchain applications in intelligent networking are graphically illustrated in Figure 8 and are reviewed with respect to the existing literature in the following subsections.

4.1. Service Provisioning

4.1.1. Financial Services

With the aim of protecting users from financial loss and eradicating financial fraud, monetary transactions made by network members must be reliable and safe. In the KDN domain, in order to perform transactions securely, Deep Reinforcement Learning (DRL)-based secure transactions have been proposed to enable transaction communication with confidentiality and public divisibility [237]. Furthermore, as KDNs are often challenged due to the enormous amount of data required for generating knowledge using machine learning, through the assistance of the cryptographic technique employed in blockchains, an architecture defined as the Blockchain-Enabled Intelligent IoT Protocol (BEIIP) is offered for assuring high-level network availability and data integrity [238].

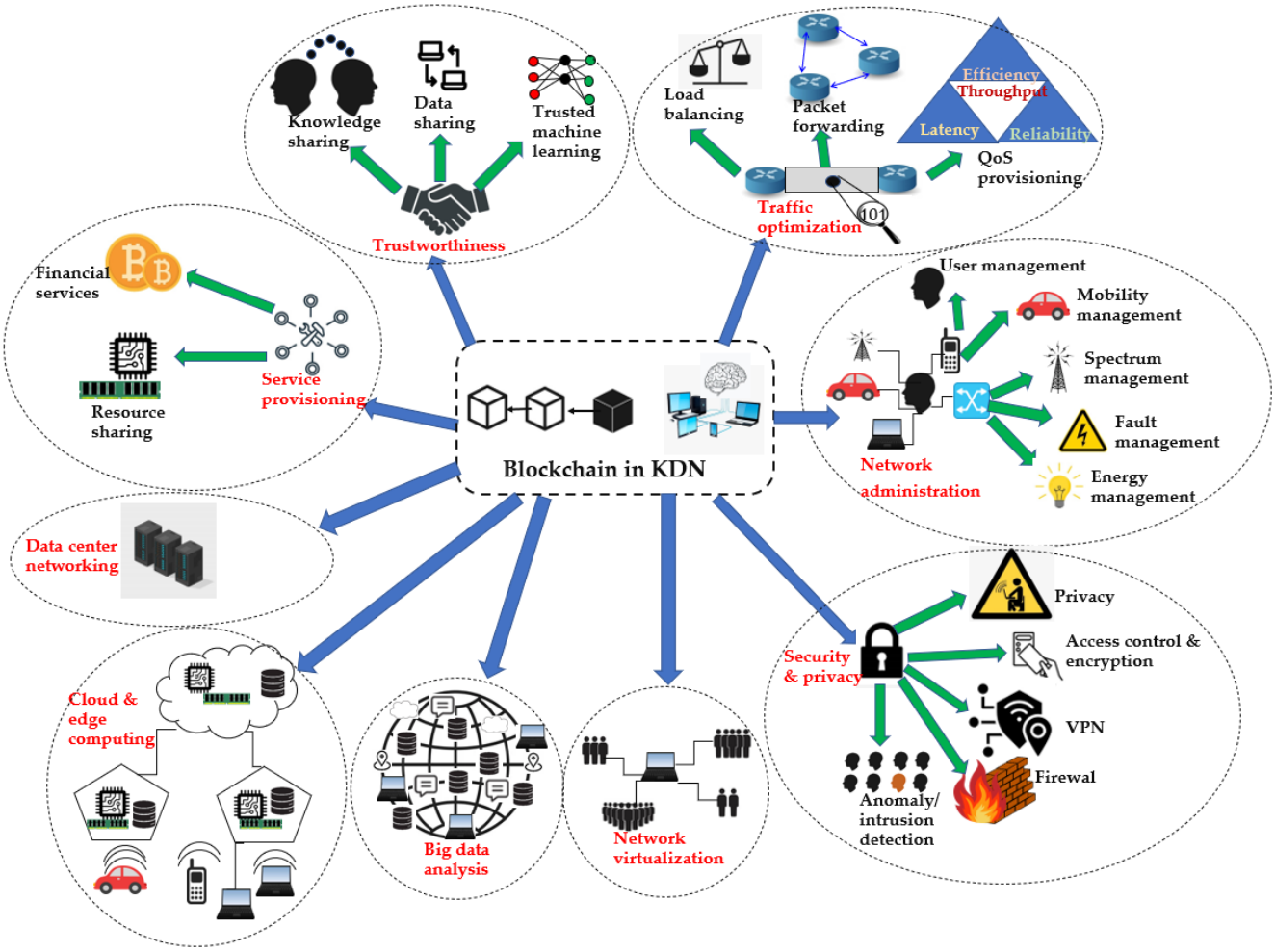


Figure 8. Graphical illustration of blockchain applications in knowledge-based intelligent networks.

4.1.2. Resource Sharing

Resource sharing is an important concept in a KDN as multiple devices/clients may rely on the same resources, such as computational and memory resources. In [239], blockchain has been utilized along with deep reinforcement learning for secure resource sharing by developing a content caching system. Furthermore, in [240], network resources are allocated and shared using artificial intelligence, network function virtualization, and consortium blockchain in a KDN with the aid of time prediction and resource allocation algorithms. Additionally, blockchain has been utilized as a bridge to record user transactions and broadcast knowledge-based terminals' resource demands in sixth-generation networks with the aid of smart contracts, and artificial intelligence has been utilized to improve pattern recognition in Dynamic Resource Sharing (DRS) [241]. Moreover, using blockchain and self-executing contracts, an end-to-end framework utilizes the permissioned nature of the blockchain, allows service level agreements to share infrastructure, and performs federated learning among different parties involved in future 6G-Internet of Vehicles (IoV) KDNs [242]. Likewise, in portable network edges with UAVs allowed, deep reinforcement learning was successfully used for flexible compute transferring and assigning resources, while blockchain has been used for protecting and improving the offloading tasks [243]. In contrast, in IIoT networks, a framework known as ManuChain for manufacturing planning and resource sharing utilizes permissioned blockchain for decentralization, while a two-level intelligence model in which the lower tier uses self-regulating cognition while the upper tier uses holistic optimization for cognition [244].

4.2. Trustworthiness

4.2.1. Knowledge Sharing

In knowledge-defined networks, knowledge sharing (dissemination) is a key component for making knowledge-driven decisions and updating application policies based on inferences from knowledge. Even though knowledge retrieval and manipulation languages such as SPARQL/SQWRL can be used for efficient knowledge dissemination, these protocols do not guarantee the trustworthiness of the knowledge. Therefore, in the recent past, there have been numerous attempts to improve the trustworthiness of knowledge sharing by employing blockchain technology.

A various medium-dispersed blockchain network named MKShareNet has been applied for the cooperative sharing of knowledge in service-minded repair choice-making [245]. Moreover, given the necessity to use computationally intensive consensus procedures like PoW, PoS, etc. due to resource constraints in network gadgets and the risk of knowledge spying, work in [246] proposes employing a user-centric blockchain for edge knowledge sharing with the aid of a speedy and low-energy-consuming proof of popularity consensus approach. Furthermore, the practice of exchanging knowledge has evolved as a collective leadership and collaborative game in the trade market that effectively reduces the malicious attacks on knowledge in an Internet of Vehicles network, where the machine learning-generated knowledge is distributed using the Hierarchical Blockchain-Enabled Federated Learning (HBEFL) framework, enabling feasible trustworthy knowledge sharing in large vehicular networks [247]. Additionally, a framework called CKShare utilizes a trustworthy blockchain network to record knowledge and its transactions, where a K-nearest neighbor-based retrieval mechanism is proposed for knowledge retrieval [248]. Likewise, for intelligent connected vehicular networks, an Asynchronous Distributed Learning (ADL) algorithm has been used for knowledge generation, while Directed Acyclic Graphs have been used to reduce the operation latency and ensure fast consensus for the blockchain, which has been used for knowledge sharing [249].

4.2.2. Data Sharing

In instances of case analysis, such as the investigation of the causes of accidents in an intelligent transportation system, untampered data are required to identify the root causes of the accidents. In these situations, the blockchain can come in handy by making data immutable so that it can be considered digital proof, whose credibility is further enhanced through the adoption of self-executing contracts to gather data in ambiguous situations [250].

According to a study by [251], a system for safe data exchange in a commercial IoT network through the KDN approach, permissioned blockchain, and Federated Learning (FL) for safeguarded device interactions, where self-executing contracts operate for seeking and modifying archives in the blockchain, has recently been developed. A similar work points out the one potential site of breakdown and DDoS attacks in the centralized KDN architecture and proposes blockchain and artificial intelligence (federated learning) for safe data exchange in fifth-generation drone networks [252]. Furthermore, blockchain is implemented on a hyper-ledger fabric platform integrated with deep learning for the sharing of data in a distributed and automatic manner, eliminating the necessity for every demand for the exchange of data to be approved by the data proprietor in an industrial healthcare KDN system known as Permissioned Blockchain Deep Learning (PBDL) [253]. Moreover, a foundation for private Medical Data Sharing (MDS) has become possible with the incorporation of collective authorization and encryption, driven by attributes for restricting access, self-executing contracts to support organization rationality, and blockchain for linking personal databases for safe data supply, where an intelligent artificial intelligence-driven IoT-based KDN is utilized to establish the sharing regulations [254]. Similarly, softwarized unmanned aerial vehicles make use of the KDN principle, which divorces components and control reasoning, while blockchain has been proposed to register, verify, and validate the communication using Proof of Concept consensus and smart

contracts, and deep learning has been utilized to generate knowledge regarding illegitimate transactions by analyzing the data [255].

Blockchains can be used in sensitive data transmission systems to perform transactions without leaking the sensitivity of the data with the aid of smart contracts [256]. In healthcare systems to share sensitive health data, a system based on self-executing contracts has been investigated for precise authentication and sharing of medical data while protecting privacy by introducing anonymity noise into federated learning, known as the Medical Privacy Blockchain (MPBC) [257]. Moreover, in order to share data among different network operators, mutual trust is developed using distributed blockchain, which implements the creation of a platform for data exchange in artificial intelligence-driven cognitive networks utilizing self-executing contracts and fine access management [258].

In order to analyze the trustworthiness of data, a fuzzy logic engine has been utilized, where IoT data gathering is carried out using blockchain while additional encryption is used to secure the data [259]. Moreover, ANFPB is a blockchain-based adaptive neuro-fuzzy-based payment for safe data exchanging in an Internet of Vehicles (IoV) network where a neuro-fuzzy system is used to evaluate rewards based on different automobile parameters while the blockchain preserves privacy [260].

4.2.3. Trusted Machine Learning

Byzantine attacks frequently target dispersed education platforms while changing model variables and combining gradients between several learners. Thus, in order to overcome the byzantine attack, a framework known as PiRATE using the sharding mechanism of blockchain has been proposed and is effective in distributed machine learning in next-generation knowledge-based networks [261].

Some have attempted Distributed Federated Learning (DFL) by making use of a blockchain-driven agreement process to train artificial intelligence models within end devices for trustworthy shared training in knowledge-defined vehicular networks [262]. Moreover, secure collaborative deep learning at the device level in IoT KDN to avoid having only one spot of malfunction, data poisoning, privacy leaks, etc., where blockchain is deployed to guarantee immutability and secrecy in deep learning, called BlockDeepNet, has been studied [263]. Additionally, in [264], blockchain has been utilized by using a voting-based consensus approach for validation and having forwarding elements that are registered and verified using zero knowledge proof to provide secure data for a deep Boltzmann machine learning model for flow analysis to detect switch anomalies. Furthermore, taking into account the tendency of ML methods learned on private data to reveal information for hostile assaults, a framework known as PriModChain has been proposed that leverages the federated machine learning secured by the Ethereum blockchain and smart contracts in intelligent knowledge-based industrial Internet of Things networks [265].

In next-generation 6G KDNs, even though they are controlled and managed centrally, scattered education is a possibility for machine learning algorithms. Therefore, in order to ensure trustworthy model training, a Blockchain-Based Distributed Deep Learning (BB-DDL) design is proposed, wherein, to validate the machine learning algorithms, bipartisan blockchain agreement is required [266]. In addition to improving trustworthiness in AI systems with the integration of blockchain, some have attempted to improve the explainability of AI outputs. Additionally, an arrangement made up of AI was recently investigated in [267], where the decision-making output relies on a decentralized agreement of various AI and comprehensible AI predictions that are carried out using blockchain.

4.3. Traffic Optimization

By maximizing the effectiveness and use of network resources, traffic optimization assures seamless traffic data flow. Packet forwarding, load optimization, and QoS delivery are the three basic categories under which traffic engineering optimization falls.

4.3.1. Packet Forwarding

In contrast to load optimization, packet forwarding (routing) includes choosing the best route for packet flow among two ends depending on a variety of variables, including the network's layout and situation, routing regulations, routing protocol, etc. Each transmitting device's routing tables must be programmed by the controller, who computes pathways using a variety of parameters. As a result, routing applications give the control plane routing strategies to employ while calculating paths.

In the distributed controller KDN paradigm, there exists an attack known as the black hole attack, where a malicious controller exchanges malicious paths with legitimate controllers and drops packets in crossing-domain path routing for the domain controlled by the malicious controller. In order to avoid the black hole attack, blockchain has been proposed, where each controller needs to upload an abstract topology to the blockchain using smart contracts to produce a true picture of the whole network, while trust is based on a reputation score [268].

A route accuracy technique is used to rectify a Genetic Algorithm-based Routing (GAR) computation that also optimizes the nodes' utilization of energy and inspects for malicious nodes in the route by using the blockchain to maintain a malicious list of nodes [269]. Moreover, another work employing blockchain to make routing information traceable and immutable and using reinforcement learning to select trusted links evaluates a trustworthy routing technique for Wireless Sensor Networks (WSNs) [270]. Furthermore, Intelligent Edge Network Routing (ENIR) has been studied in [271], which learns knowledge using deep reinforcement learning for closed-loop routing control and optimization where blockchain is utilized to share knowledge and routing optimizations. Similarly, work in [272] shows that blockchain and Compact Deep Reinforcement Learning (CDRL) can be utilized to learn a routing policy where the student model is implemented off-chain to improve transaction efficiency. In contrast, FLEA-RPL is a fuzzy logic-driven energy aware routing approach that utilizes fuzzy logic to compute routing metrics, which decreases data traffic, increases network lifetime, and scrutinizes blockchain to reduce the number of data packet transfers for industrial IoT networks [273].

4.3.2. Load Optimization

In order to improve effectiveness, increase accessibility, and shorten reaction times, traffic from the network is distributed across several pathways or pieces of network equipment through the technique of load optimization. The flexible load optimization technique is well suited to be implemented in a KDN situation due to consideration of both network conditions and application regulations for optimization.

Work in [274] further expands the blockchain system to allow Load Balancing utilizing Deep Reinforcement Learning (LB–DRL) in a ledger-based strategy for distributing loads in the blockchain network. Furthermore, reinforcement learning is used for traffic congestion prediction to balance the traffic load using an edge computing platform where transactions are secured by access control using the Hyperledger Fabric blockchain [275]. Similarly, a framework known as Blockchain-based Controller Load Balance (BCLB) has been utilized in the distributed control architecture of KDN, where blockchain is utilized as a decentralized data sharing model to provide inter-domain links and a global view for global controller load balancing, which also aids deep reinforcement learning analysis to offload load from the overloaded controllers [276].

For automotive KDNs, a multiple-stage blockchain design for multi-controller load optimization has been examined using a fuzzy approach to generate knowledge [277]. This architecture makes use of a fuzzy inference-based technique to perform actual-time adaptive reconfiguration of the blockchain in situations like changes in traffic, changes in controllers, etc. Likewise, a framework known as Intelligent Vehicular Edge Computing (IVEC) integrates the centralized control power of KDN along with the smart contract mechanisms of distributed blockchain to create a resource management controller for load balancing in IVEC that uses artificial intelligence techniques for computations [278].

4.3.3. QoS Offering

Applications can confirm when particular QoS demands are fulfilled by directing traffic in accordance with those criteria [279]. Machine Learning-based Blockchain QoS Routing (MLBQR) inside a vehicular KDN is applied to transmit many forms of traffic, including footage, tele-medicine, text, and others. QoS adherence in the realms is delivered and confirmed via the communication of trust data utilizing blockchain and self-executing contracts, while Q learning is utilized to improve the overall QoS by optimizing blockchain parameters [280]. Likewise, MLSMBQS, a machine learning-enabled blockchain framework for QoS-driven blockchain sharding optimization, which reduces privacy concerns in QoS-based OpenFlow routing with the aid of blockchain, has been studied for an IoT-based KDN [281]. Additionally, for blockchain-powered IoT KDN systems, which are regarded as autonomous systems, a QoS improvement framework has been proposed that utilizes the power of blockchain and machine learning to create secure side chains [282]. Furthermore, ATQMB is a framework that leverages blockchain and machine learning to create a QoS-aware media access control model with the aid of encryption, a distributed agreement method, and self-executing contracts with the goal of providing QoS at a reduced cost and adjusting to QoS's unpredictable character for knowledge-defined wireless networks [283]. In contrast, meta-heuristics have been used for intelligent task scheduling in a framework known as QoS-ledger, where permissionless blockchain is leveraged to preserve medical data while QoS computation is performed using an algorithm in healthcare networks [284].

4.4. Network Administration

Applications for network administration set regulations for various administrative activities that are executed on the management/administration plane, such as managing mobility and managing energy. In order to make managerial decisions for the various circumstances mentioned above, the administration layer in KDN takes into account both application regulations and actual-time network intelligence.

4.4.1. User Administration

In intelligent networks, user administration involves the management of proper interactions between network users and operators. The blockchain technology has been utilized with the help of Cryptocurrency and Game Theory (CGT) along with a spectrum sharing algorithm to intelligently administer the relationships between network users and operators [285].

4.4.2. Mobility Administration

Programs for mobility administration are employed to control how network participants and equipment travel across various network regions. By monitoring the position of the gadget in order to smoothly switch links between various network fields, such as mobile networks, wireless local area networks, automobile networks, etc., it ensures that operations are maintained while users travel across various zones.

Generic mobility management—Blockchain and Muliti-Agent Deep Reinforcement Learning (MADRL) have been suggested as a way for resource and mobility management where virtualized resource allocation is modeled as a Stackelberg game in KDNs using 5G in unmanned aerial vehicular networks [286]. Alternatively, another work uses blockchain and deep reinforcement learning for secure, optimized handover and service offloading in an ultra-dense edge computing network environment, which has shown reduced handover latency with low packet loss rates during handover [287]. Furthermore, with the use of blockchain technology and enquiry response methods, a Blockchain Integrated Network Function Management Scheme (BINFMS) is deployed for handling movement and network address translation while simultaneously obtaining the necessary mobility-related measurements [288]. Moreover, driven by existing security flaws in the distributed mobility management of hierarchical and flat distributed control architectures of ultra-dense 5G KDNs, a secure and intelligent Distributed Mobility Management (DMM) framework has

been proposed by employing blockchain and federated deep reinforcement learning, which has proven to work independently from the network layout while at the same time fulfilling distributed security needs [289].

Authentication handover—Authentication handover involves transferring authentication credentials from one network entity to another whenever a portable gadget switches between networks. Blockchain and artificial intelligence have been proposed to reduce re-authentication and repeated handover using public and private keys in IoT networks' Authentication Handover (IoTAH), which has resulted in low latency and overhead for handover [290]. Furthermore, blockchain has been utilized to create immutable ledgers, while deep learning has been used to classify users as legitimate or not by learning mobility patterns using channel state information to prevent impersonation attacks during handover authentication [291]. Moreover, by excluding re-authentication with less delay, work in [292] performs efficient authentication handover by utilizing credit-based blockchain consensus, where credit is assigned to the secondary peers upon successful involvement in consensus verified by a local service center using Reinforcement Learning with Actor Critic-based Fuzzy Neural Network (RLAC-FNN). Additionally, for knowledge-defined heterogeneous 5G IoT wireless body area networks, authentication handover by storing user credentials in the hierarchical blockchain while using a bio-signature validation authentication mechanism and by using an Artificial Electric Field Optimization (AEFO) algorithm and edge intelligent agents for handover using the State Action Reward State Action (SARSA) algorithm, considering access network constraints and matching theory, has been studied in [293]. Likewise, in [294], a secure Multi-Factor Authentication (MFA) technique for handover in industrial IoT networks has been investigated. This scheme, known as Authentication Transfer Learning Blockchain (ATLB), provides the usage of blockchain to confirm the open keys of network gadgets and log the geographical locations of individuals with the goal of protecting the key agreement system and handover procedure, along with transfer learning to improve the authentication process.

Channel scheduling—Channel scheduling is the process of allocating and organizing communication channels or time slots to transmit data among multiple devices. A framework known as Blockchain and Backscatter Aided Internet of Things (BBAIoT) collects sensor data and sends it to a blockchain network to verify, store, and process in a trusted manner, where an optimization problem is solved considering the dynamics of the primary channel for time scheduling of transmission time and backscatter time [295].

Offloading—Offloading involves diverting certain tasks or data traffic from mobile devices to other entities in mobility management. An Actor–Critic-based Deep Reinforcement Learning (ACDRL) policy is used to achieve task scheduling and offloading in a 5G-based massive internet of things KDN network, while a PoAu agreement-driven blockchain is implemented to verify operations and blocks [296]. Furthermore, in a two-layer distributed vehicular network KDN architecture, consortium blockchain is used to share the network topology among multiple controllers, while the goal of Service Offloading and Migration (SOM) optimization is used to reduce the utilization of power and increase system speed, including the blockchain. Additionally, a deep reinforcement learning strategy has been employed to tackle the aforementioned optimization concern [297]. Moreover, a Computation Offloading (CO) platform that scrutinizes the decentralized control architecture of KDN to offload computation irrespective of different service providers uses blockchain to ensure unbiased and fair scheduling and offloading, while deep reinforcement learning is utilized to strengthen the transactions [298]. Alternatively, distributed blockchain has been involved in Secure Consensus and Reliable Data Offloading (SCRDO), where a resource allocation algorithm optimizes offloading and resource allocation with the aid of deep reinforcement learning [299]. Additionally, in mobile edge-cloud knowledge-defined IoT networks, blockchain has been utilized for protection from illegal offloading actions using access control, where offloading has been achieved by optimization considering offloading and consensus scheme decisions, computational resources, and channel bandwidth to cut down the amount of time and energy used while the offloading problem is solved using

a deep Q-network [300]. Similarly, blockchain is incorporated into a mixed computing framework that combines edge technology and cloud services to achieve shared agreement and resource administration by offloading data, while Markov decision-making processes and deep reinforcement learning are applied for combined conversation, calculations, and consensus issues [301].

4.4.3. Spectrum Administration

Spectrum administration involves efficiently allocating the electromagnetic spectrum for users in the wireless network to reduce interference and optimize utilization of the spectrum. In spectrum management, radio frequency spectrum is efficiently allocated and regulated for the better functioning of communication services.

As a KDN can be operated by numerous mobile network providers, a Spectrum Management Scheme (SMS) for seamless handover among numerous mobile network providers with the minimum experience of disruption and delay has been demonstrated by employing blockchain and deep reinforcement learning for spectrum management [302]. Alternatively, another work presents the spectrum administration concept for next-generation 6G mobile networks to efficiently handover spectrum dynamically among multiple network operators driven by the KDN concept to centralize network control while at the same time achieving efficient handover using blockchain and machine learning (long short-term memory)-enabled workflow [303]. Additionally, spectrum access in Cognitive Radio (CR) IoT networks is accomplished via a combination of detection of malicious users using decision tree-based machine learning, a spectrum assigning procedure, a bilateral verification mechanism, and an agreement method for the federated blockchain, created utilizing global-level controllers [304]. Furthermore, a Digital-Twin Edge Network (DITEN) spectrum assignment framework utilizes blockchain-based federated learning to strengthen security with reduced QoS signaling overhead and eliminated centralized mediators, while reinforcement learning is leveraged to allocate spectrum resources [305]. Moreover, research in [306] studies and discusses the tokenization model, distributed ledger, and consensus algorithms along with Recurrent Neural Networks (RNNs)-based AI for intelligent spectrum sharing while studying the effect of the type of smart contract for spectrum trading in next-generation intelligent networks. Likewise, a Spectrum Sharing Algorithm (SSA) has been proposed by using blockchain to authenticate users and record transactions in a secure manner using cryptography along with an Extreme Learning Machine (ELM)-based spectrum sensing approach, while detecting and blocking malicious users in cognitive radio networks [307].

4.4.4. Fault Administration

Network fault administration involves the detection of network faults and taking precautionary measures to reduce the impact of the faults.

In hybrid micro-grids, a technique for Fault Identification and Relay Protection (FIRP) was developed by combining blockchain with machine learning, where blockchain has been applied to create a layered framework for related elements and machine learning is utilized to detect defects [308]. Alternatively, in heterogeneous smart grid neighboring area networks, Privacy Reinforcement Learning with Blockchain (PRLB) is used to match anomalies in the energy to detect faults in the network [309].

4.4.5. Network Address Translation (NAT) Administration

In network address translation, Internet Protocol (IP) addresses and port numbers are mapped from one network to another. For instance, in NAT, multiple devices in a local network can share a public IP address.

Using a blockchain and an intelligent Query–Reply Mechanism (QRM), work in [288] handles secure network address translation in Knowledge-Defined Networking. Furthermore, blockchain and FL have been utilized in an Internet of Medical Things (IoMT) network to train machine learning models collaboratively, ensuring privacy, where a pair of

IoMT device addresses are used for communication, similar to network address translation in conventional networks [310].

4.4.6. Energy Administration

Using sophisticated optimization procedures along with regulations, energy administration is a critical service within a KDN that entails lowering network consumption of electricity while achieving other technological goals like low latency, high speed, high resilience to failure, etc.

In a decentralized Unmanned Aerial and Ground Vehicle (UAGV) integrated network, blockchain and federated learning are utilized for secure and accurate decentralized service provisioning, considering energy and movement constraints [311]. Alternatively, a Resource Management (RM) framework for KDN–cloud data centers by deploying blockchain for reducing energy consumption by the scheduler, along with a reinforcement learning algorithm within a smart contract to reduce more energy consumption, has been presented in [312]. Furthermore, public blockchain has been proposed for peer-to-peer communication among network devices and private blockchain has been proposed for communication between network devices and controllers for ensuring distributed trust, while consensus has been used to develop the global view from participating controllers in a Knowledge-defined Industrial IoT network. In the preceding framework, Energy Efficiency (EE) is achieved by optimizing computational resources, considering trust features, and using reinforcement learning to solve the problem [313]. Moreover, authors explain how dispersed blockchain may be implemented alongside graph convolutional long short-term memory for the commercial IoT to extract user patterns to formulate a pre-caching approach to conserve energy usage, while the blockchain-driven ledger ensures data integrity in [314]. Similarly, by integrating blockchain and artificial intelligence in networking, a framework known as Block5GIntell uses blockchain-based sharing of information and resources with the objective of lowering wireless access network-wise power usage [315].

For safe energy exchange utilizing blockchain agreements, an architecture has been developed for a Vehicular Energy Network (VEN), where vehicular communication is efficiently and securely performed using a blockchain while machine learning is utilized for calculating the minimum distance between charging stations and vehicles [316]. Furthermore, with the aid of a global knowledge-defined network controller, a framework known as DETF is an electrified automobile energy exchange platform built around the blockchain, machine learning, and self-executing contracts that validates vehicles' requests in a distributed approach, considering energy requirements [317]. Moreover, for a KDN-based Energy Internet (EI) system, blockchain has been applied for secure and privacy-protecting Distributed Energy Trading (DET), which is modeled as a Stackelberg game solved using hierarchical reinforcement learning and has yielded better performance than the traditional centralized electric energy trading model [318]. Similarly, a Secure Decentralized Energy Management (SDEM) framework, that leverages both knowledge generated using machine learning from energy consumption data and blockchain for maintaining the integrity of communication among smart-grids in an active distribution network to trade energy considering load demands in the smart grid, has been studied in [319].

4.5. Security and Privacy

Security applications can be used to set safety guidelines for authentication, encryption, traffic filtering, trespassing identification, etc. Applications assist in maintaining the authenticity, accessibility, and secrecy of network assets by enforcing policies that enable faster and more efficient threat detection and mitigation. To ensure that KDN is protected by avoiding compromises in security, KDN offers an avenue for reviewing security rules.

4.5.1. Privacy

Privacy is an important aspect of knowledge-based networking. Sensitive information must be protected in knowledge dissemination such that the intellectual properties of the users are secured while at the same time enabling smooth network functions [320].

For knowledge-based IoT smart towns, an architecture known as the Privacy-Preserving Secure Framework (PPSF) was originally put forward. It is made up of a two-tier privacy arrangement with a blockchain section that sends information privately, as well as a principal component analysis module to transform raw data and an anomaly detector using gradient boosting [321]. Additionally, anonymity-critical apps at the network's edge may guarantee that privacy is preserved by utilizing edge machine learning to evaluate information at the edge network and the Ethereum blockchain for maintaining details of users who access result analysis [322]. Furthermore, a framework for Privacy-Preserving Big Data (PPBD) transfer uses graph modeling and extracts subsets of nodes using artificial intelligence, while blockchain-based resources may be communicated with privately and secretly utilizing symmetric-based digital tokens [323]. Moreover, in Controller Area Networks (CAN) that are utilized in vehicular networks, the vehicle owners' and manufacturers' data are sensitive. Thus, in [324], a framework that protects the sensitivity of manufacturer's and owner's data for training a Federated Forest KDN Intrusion Detection System (FFIDS) by using blockchain, which stores only the hash digest of the trained machine learning algorithm and a pointer to its location, allowing individuals to provide partially trained models in a privacy-protecting manner, has been presented. In contrast, for a Smart Watering System (SWS), an integrated approach of fuzzy logic and blockchain is used, where fuzzy logic has been proposed to make intelligent watering decisions while blockchain is utilized to provide privacy for the IoT network [325]. Similarly, a framework known as FDEMATEL makes decisions based on knowledge generated using fuzzy reasoning by identifying factors for security issues where security criteria classification is realized using blockchain technology [326].

4.5.2. Authentication, Access Control, and Encryption

Techniques for access control assist in limiting network access to assets to just those individuals or equipment that are permitted. Applications can specify access restriction guidelines, which the controller translates into packet-forwarding rules to limit data based on the starting and ending addresses and interfaces. In comparison, encryption prevents unapproved individuals from accessing confidential information.

A dynamic and dispersed permissioning framework built around blockchain with attribute-driven data encryption has been utilized to successfully tokenize apps in mixed IoT areas, where tokens serve as the currency of the blockchain while reinforcement learning is utilized to optimize the security policy [327]. Furthermore, work in [328] utilizes blockchain to create regulations regarding access for IoT devices (sensors) while offering a trackable policy management system to avoid the spreading of fake rules, in which Smart Contracts (SC) are used to create standalone, unchangeable, and provable guidelines in blockchain while machine learning is utilized to detect security attacks. Alternatively, a framework called DLACB achieves access control through asymmetric encryption and a certificate-based authentication protocol, and various transfers between controllers, apps, and switching devices are added to a Private Blockchain (PB) using the method of consensus, while deep learning is utilized to authenticate users and determine the access level for a given user [329]. Moreover, Decentralized Access Control (DAC) is implemented using the Ethereum blockchain for AI-driven knowledge-generating hospital networks in order to prevent unauthorized parties from modifying sensitive health records, where all transactions are recorded in the distributed ledger [330]. Additionally, a framework known as Smart Contract Data Trading (SC-DT) provides decentralized authentication and access control for data trading between data owners and data purchasers using smart contracts, where similarity learning is used to verify the data's availability as an administrator-assistant tool for network management [331]. Similarly, another framework known as MSecureChain

employs decentralized authentication and access control and federated learning-based intrusion detection in a metaverse context for KDN smart devices, which establish trustworthy connections for communication [332]. Likewise, an evidence management system known as SIEMF for the internet of vehicles leverages deep learning to predict incident modeling while using self-executing contracts and attribute-based encryption to authorize entry and generate operations for permissioning rules in cases where granular access control has been effective due to blockchain technology [333]. Moreover, in [334], for a Knowledge-Defined Internet of Health Things Network, Support Vector Machines (SVMs) are integrated with blockchain and self-executing contracts for secure user identification, access control, and threat detection in order to transmit data to healthcare applications.

For performing authentication, authorization, and auditing in healthcare IoT networks, fuzzy logic has been used to derive knowledge on user behavior in achieving these tasks in a hyperledger blockchain framework called FBASHI [335]. Moreover, Neuro-Fuzzy (NF) machine learning and blockchain have been used in combination to provide privacy-preserving authentication, where the purpose of the neuro-fuzzy system is to recognize anomalous authentication inquiries in vehicular networks, while blockchain is used for transactions and revocations [336].

4.5.3. Virtual Private Networks (VPN)

By using a program that builds an encrypted pathway between two different networks, virtual private networks may be used to create a secure link between two separate networks via the web.

A system that enables optimizing resources while leveraging blockchain and VPN for user registration and authorization while utilizing a Variational Autoencoder (VAE)-based model to diagnose diseases in healthcare networks has been studied in [337]. Furthermore, I-Trace is a framework that uses distributed ledger technology along with machine learning to secure the infrastructure of cyber-physical networks by deploying VPNs for secure communication [338].

4.5.4. Firewall

A firewall can be recognized as a type of protection system that keeps track of and manages traffic from and to the network in accordance with established security guidelines. A program that enforces rules to limit or permit network traffic can be used as a firewall.

Blockchain security is provided by a program called ChainGuard, which filters traffic to ensure that the source of the traffic is authentic. In ChainGuard, non-legal traffic is caught by a firewall in an intelligent KDN IoT transport network, which can thereby prevent flooding attacks and offer restricting features using blockchain for authenticating nodes, while a fuzzy neural network is leveraged to diagnose malicious content, allowing traffic filtering [339]. Moreover, another blockchain-based framework (FL-FW) predicts traffic flow using federated learning, where blockchain is utilized for secure rule sharing and validation for distributed network monitoring, while blockchain consensus is realized with the help of pre-known strategies to filter malicious traffic, acting as a firewall [340]. Alternatively, fuzzy logic and blockchain have been leveraged to filter fake and anomalous data using automobile rules and behaviors in Intelligent Vehicular Networks (IVNs), acting as a firewall [341].

4.5.5. Anomaly or Intrusion Diagnosis and Suppression

Systems for detecting anomalies, attacks, and intrusions scan traffic on the network for indications of harmful behavior and take the necessary steps to avoid it. Firewalls use the technique of restricting data flow according to a preset set of regulations, which is distinct in that these systems seek indications of unusual activity or malicious attempts. Additionally, these systems either use network anomalies, behavior, or previously known patterns to uncover assaults. Behavior-driven threat detection searches for trends in operations that depart from typical conduct, whereas signature-driven detection compares data packet

flows to a repository of known threat profiles. On the other hand, anomaly detection employs statistical approaches to find strange or unanticipated traffic patterns [342].

Intrusion detection—In a distributed KDN where spectral partitioning is used for dividing the network, Support Vector Machine (SVM)-based machine learning is utilized for intrusion detection, where the Attacker List (AL) is distributed among partitioned networks, ensuring integrity using blockchains [343]. Similarly, another research work suggests using blockchain for secure data sharing for intrusion detection in networks using Deep Learning (DL) since attackers cannot modify a block in a blockchain without affecting all other blocks [344]. Likewise, the PRO-DLBIDCPS attack detection platform makes use of gated recurrent neural networks for intrusion detection. Its performance is improved by optimization, and the suggested platform's security is improved through the usage of blockchain in the digital–physical network context [345]. Furthermore, in order to provide privacy for the intrusion detection system known as the Deep Blockchain Framework (DBF), privacy-based blockchain and smart contracts are utilized, while deep neural networks based on LSTM are utilized for distributed intrusion detection [346]. Some have suggested using blockchain to store both data and machine learning models, protecting the integrity to be used in Collaborative Intrusion Detection (CID) in Unmanned Aerial Vehicular Networks where decisions are driven by knowledge [347]. Moreover, blockchain is used to establish trust and integrity, while an intrusion detection system employs the K Nearest Neighbor (KNN) machine learning algorithm to assess the likelihood of harmful activities in the network's infrastructure [348]. Additionally, a framework called DeepCoin combines a deep machine learning-inspired method to detect breaches that uses sequential neural networks to identify assaults in the blockchain-enabled power system with a blockchain-driven approach that uses brief signatures and hashing algorithms to defend against intelligent grid hacking attempts [349]. Alternatively, a Fused Realtime Sequential Deep Extreme Learning (FRSDEL) system is employed in home automation networks built on blockchain to identify breaches in knowledge-driven smart home architecture [350].

The Federated Deep Learning-based Intrusion Detection System (FED-IDS) was recently used in intelligent transportation networks for dispersed surveillance in automobile nodes at the edge, where the blockchain enables reliable training and avoids the storage of untrustworthy changes in the blockchain [351]. Similarly, a Collaborative Intrusion Detection System (CIDS) for intelligent vehicular networks has been proposed by performing federated learning using vehicles and road side units while utilizing blockchain to securely share and distribute the trained models in order for cooperative trespassing detection to provide safe interaction between each intrusion identification node [352]. In CIDS, application guidelines have been specified for employing blockchain to build trust-based conversations among identifying nodes, and the controller sends the most recent modifications to CIDS, which uses blockchain for safely distributing the signatures to the snort nodes. Moreover, a secure framework consisting of an intrusion detection system, using Random Subspace Learning and K Nearest Neighbor (RSL–KNN) to detect falsified orders and a blockchain-based integrity-ensuring system for preventing misrouting attacks, has been studied in [353]. Alternatively, when assessing a device's credibility for identifying insider assaults in cooperative attack detection using Conditional Generative Adversarial Networks (CGANs) in UAV KDN, it leverages blockchain to verify data immutability and distributed federated learning to ensure privacy and collaborative learning [354]. Furthermore, for knowledge-based SD-IoT networks, a Distributed Denial of Service (DDoS) attack recognition and suppression system has been feasible thanks to the security provided by distributed blockchain and threat detection using Artificial Neural Networks (ANNs) [355].

Driven by the uncertainty issues of deep learning techniques, an intelligent neuro-fuzzy inference system built on blockchain has been utilized to detect threats in IoT networks, where meta-heuristic algorithms have been leveraged to optimize threat detection error [356]. Similarly, an attack recognition system built using fuzzy logic and a private blockchain known as PBFL-ADS detects attacks by processing multimedia information in IoMT networks, where the purpose of the blockchain is to improve trust management

efficacy [357]. Moreover, a framework called BFT–IoMT uses fuzzy logic to detect Sybil attacks in an IoMT network where transactions are implemented on a blockchain to improve security [358].

Anomaly detection—A DAG blockchain is utilized to mitigate illegitimate packets generated due to multiple handovers in KDN. In particular, 5G users are authenticated using hash generation, where a DAG at the controller stores these hashes of users and hashes of traffic rules for verification, while authentication of dubious packets is carried out using a soft actor–critic algorithm and classification of packets is performed by a capsule neural network [359]. Alternatively, a framework known as brain–chain, which detects domain name system amplification attacks in permissioned blockchains using flow statistics collection, entropy-based disorder, and Bayes network filtering to classify illegitimate flow measurement, has been utilized [360]. Similarly, research in [361] proposes using Permissioned Blockchain-based Federated Learning for Anomaly Detection (PBFLAD), where changes to the AI framework are linked utilizing a shared ledger, allowing auditing of the machine learning models. Furthermore, in [362], IoMT Blockchain network Anomaly Detection (IoMTBC-AD) is employed to prevent insider attacks in blockchain networks utilized in IoMT by combining the network with deep learning to detect network anomalies. Moreover, Hybrid Deep Learning (HDL) making use of LSTM and convolutional neural networks for evaluating traffic flow anomalies by assisting blockchain in resolving gaps in the datasets has been studied in [363].

4.6. Virtualization of Networks

The procedure of establishing numerous conceptual networks on the foundation of actual network facilities using network splitting is known as network virtualization. This makes it possible for numerous networks to exist together while utilizing identical physical assets, where each conceptual network shows up as an independent system with unique network strategies and setups. A virtualized network enables either traffic flow level or network-specific slicing, which divides the real network into many simulated networks according to various flows [364].

To safeguard proprietors of wireless equipment from recurrent expenditure attacks, which assign the same radio frequency chunk to several simulated wireless networks, researchers have recently proposed adding apps with policies to incorporate Blockchain Technology for Network Virtualization (BTNV), where the blockchain serves to prevent recurrent expenditure attacks using reputation while machine learning is utilized to predict QoS requirements to optimally allocate wireless resources [365]. Furthermore, Deep Q Learning (DQL) is utilized in a Knowledge-Defined Vehicular Network (KDVN) to solve an optimization problem of allocating computation and networking resources for virtualizing resources by reaching consensus using a permissioned blockchain [366]. Moreover, to enable a service-focused blockchain system with network function virtualization, Distributed Ledger Technology (DLT) was initially put out as a platform for QoS-based service delivery along with decoupled management and control functions realized using smart contracts, where the consensus on the virtualization management and orchestration is modeled as an optimization problem solved through deep reinforcement learning [367].

For slicing an autonomous radio active network, a Consortium Blockchain-based Decentralized Spectrum Trading (CBDST) platform for buying and selling among spectrum providers and buyers, where the Stackleberg game framework is used for incentive maximization among the infrastructure providers, has been studied in [368]. Moreover, SliceBlock is a system designed for network slicing in sixth-generation mobile network environments utilizing KDN, where network slicing has been realized using Generative Adversarial Networks (GANs), in which a Directed Acyclic Graph-based blockchain along with a Proof-of-Space consensus algorithm is utilized for security, while Markov decision-making is used for authentication and handover [369]. Similarly, the Blockchain Network Slicing Broker (BNSB) system uses blockchain for network slicing and is an education-driven technique for allocating network resources. It allows resource vendors to fluidly

contract assets to ensure improved performance of the network services using primary and secondary interactions among users, where deep reinforcement learning is utilized for the resource allocation problem [370]. Alternatively, a framework known as Skunk enables distributed network slicing, which uses a blockchain-based bidding system for dynamic resource assignment where resource providers lease services for better performance of the services and blockchain-based federated learning is utilized to preserve data privacy [371].

A consortium blockchain that supports hyper-ledger smart contracts has been utilized for Secure Resource Trading (SRT) among mobile network operators, where a Dueling Deep Q (DDQ) network has been utilized for optimal pricing and demand policies in order to achieve Stackelberg equilibrium [372]. Likewise, in [373], a Two-Tier Resource Allocation Scheme (TTRAS) to obtain network segmentation that models trading between mobile virtual network providers and end appliances as a two-phase Stackelberg contest has been assessed. The upper tier uses federated deep reinforcement learning based on the Markov decision process for assigning assets.

4.7. Analysis of Big Data

Big data implies extraordinarily big, fast-moving, and diverse data collections that are difficult to handle or analyze using conventional data processing techniques. A framework known as BlockIoTIntelligence has utilized blockchain for big data analysis, as blockchains provide a decentralized approach for secure big data analysis with the help of artificial intelligence [374]. Furthermore, privacy-preserving Distributed Federated Learning by employing Blockchain (DFL-B) for preserving the integrity of the machine learning models and, thus, preventing model poisoning attacks has been proposed for secure massive data evaluation in networks generating massive data [375].

4.8. Cloud Computing and Edge Computing

The distribution of computer assets upon request, such as server infrastructure, memory, applications, and facilities, through the internet is identified as cloud computing. Moreover, within the cloud computing context, networking tasks can be accomplished by building cloud computing applications with guidelines for network operation virtualization and employing cloud computing equipment [376].

In the edge network of a cloud, blockchain has been deployed in an Edge Resource Scheduling Scheme (ERSS) powered by AI and motivated by cross-domain collaboration and a transaction acceptance method differentiated by credit, which has resulted in reduced edge service costs and improved service capacities [377]. Similarly, a framework for edge-network Resource Allocation (RA) by integrating edge computing nodes and IoT devices with blockchain-based policies and transactions that provide security, dependability, and flexibility, along with a smart contract mechanism to integrate DRL for assigning edge resources, has been studied in [378]. Likewise, in order to provide secure edge services, smart contracts are used to participate in these services, and machine learning is proposed to be utilized in these services to learn from data and generate knowledge [379]. Moreover, by utilizing edge computing for workload balancing, blockchain for data sharing and transactions, and machine learning for data analysis, work in [380] shows that integration of these three technologies results in lower processing times with high security. Fuzzy logic reasoning has been leveraged for Node Selection (NS) in blockchain-based edge IoT networks in order to allocate resources and make other network decisions [381].

A Blockchain-based Offloading and Scheduling System (OSS) is used in fog-cloud networks by modeling the offloading problem as a Markov problem solved using deep reinforcement learning and scheduling tasks, using blockchain for healthcare workloads in IoMT [382].

In the Distributed Security Framework (DSF) presented in [383], cloud layer and edge layer collaboration is used in Power IoT. DSF leverages blockchain and federated DRL for dynamic and secure network computation offloading, where resources are allocated flexibly and data are shared securely. Furthermore, a KDN ecosystem has brought together cloud,

edge, and IoT networks known as ChainFL, where blockchain and federated learning have been further utilized to provide secure and intelligent services for the orchestrated architecture [384]. Moreover, Consortium Blockchain and Deep Reinforcement Learning (CBDRL) are used to create a trusted service function chain orchestration for resource sharing in cloud-edge networks, where deep reinforcement learning is used to minimize orchestration cost [385]. Additionally, Blockchain Congestion Control (BCOOL) is a framework that controls messages using dispersed faith contract tactics based on the blockchain, where a multivariable linear regression-driven software-defined agreement approach is used to forecast traffic jams and machine learning for flexible service chaining in mixed cloud/edge vehicular networks [386]. Similarly, for cloud-edge collaborative computing-enabled networks, collective reinforcement learning is utilized for Intelligent Cloud-Edge Collaborative Resource Allocation (IC-ECRA) and result sharing, while blockchain is utilized for ensuring the authenticity of data sharing [387].

4.9. Networking in Data Center

Networking in a data center involves the procedure of tying together machines, archives, and other assets. To deliver capabilities with lower latency, smarter utilization of assets, and better performance, data centers are required to be built to supply facilities based on the demands of the application.

A system leverages federated learning to protect the confidentiality of contextual sensor data stored in Private Data Centers (PDCs) of smart healthcare networks, while a blockchain-based IoT cloud is utilized to ensure security [388]. Furthermore, FDC is a system for trusted data collaboration where the data is not required to be transmitted out of private data centers, while federated deep learning is utilized to make inferences from local data and train ML models, and distributed blockchain is used for secure data transmissions. Moreover, in FDC, public data centers can be employed for secure computation by multiple parties in the network [389].

5. Review Analysis

In this section, we compare and analyze the blockchain applications in Knowledge-Defined Networks.

5.1. Classification of Frameworks Based on Application Category

This subsection presents an outline of the distribution of intelligent network applications of blockchains. Table 3 summarizes applications of blockchain technology in knowledge-based networks.

Using Table 3, one can readily find any particular blockchain-based framework related to a generic application category or a specific application category. Moreover, to understand the distribution of frameworks reviewed in this research with respect to each application category, we plotted the distribution, as shown in Figure 9.

As evident from Figure 9, the highest number of blockchain frameworks exist for security and privacy applications (27.9%), followed by network administration (25.6%), trustworthiness (14.6%), traffic optimization (10.6%), cloud/edge computing (7.3%), network virtualization (6%), service provisioning (5.4%), datacenter (1.4%), and big data (1.4%). As specified in the introduction section, many researchers have focused on the security and privacy applications of blockchain. However, as evident from Figure 9, among all knowledge-defined applications, this constitutes only around one-fourth, even though it is the dominant application category. Therefore, our survey proves that there exist many other blockchain-based intelligent networking applications whose main focus is not security and privacy, but other network applications where security can be a secondary objective. Among the specific application categories, intrusion detection has the highest number of blockchain-based applications (10.6%), followed by authentication and access control (6.6%), energy administration (6%), and so on.

Table 3. Summary of intelligent network applications of blockchains.

Group	Sub-Group	Blockchain Based Frameworks
Service Provisioning	Financial services	DRL [237], BEIIP [238]
	Resource sharing	Dai et al. [239], Guo et al. [240], DRS [241], 6G-IoV [242], Mohammed et al. [243], ManuChain [244]
Trustworthiness	Knowledge sharing	MKShareNet [245], Li et al. [246], HBEFL [247], CKShare [248], Chai et.al. [249]
	Data sharing	FL [251], Feng et al. [252], PBDL [253], MDS [254], Kumar et al. [255], MPBC [257], Zhang et al. [258], fuzzy engine [259], ANFPB [260]
	Machine learning	PiRATE [261], DFL [262], BlockDeepNet [263], Singh et al. [264], PriModChain [265], BBDDL [266], explainable AI [267]
Traffic optimization	Packet forwarding	Secure routing [268], GAR [269], trusted routing [270], ENIR [271], CDRL [272], FLEA-RPL [273]
	Load optimization	LB-DRL [274], ECRL [275], BCLB [276], Fuzzy [277], IVEC [278]
	QoS offering	MLBQR [280], MLSMBQS [281], side chaining [282], ATQMB [283], QoS-ledger [284]
Network administration	User administration	CGT [285]
	Mobility (Generic)	MADRL [286], DRL [287], QRM [288], DMM [289]
	Mobility (Authentication handover)	IoTAH [290], deep learning [291], RLAC-FNN [292], AEFO [293], ATLB [294]
	Mobility (Channel scheduling)	BBAIoT [295]
	Mobility (Offloading)	ACDRL [296], SOM [297], DRL-CO [298], SCRDO [299], Edge-cloud CO [300], DCRM [301]
	Spectrum administration	SMS [302], 6GSH [303], CR-IOT [304], DITEN [305], spectrum trading [306], SSA [307]
	Fault administration	FIRP [308], PRLB [309]
	NAT administration	QRM [288], IoMT [310]
	Energy administration	UAGV [311], RM [312], EE [313], pre-caching [314], Block5GIntell [315], VEN [316], DETF [317], DET [318], SDEM [319]
Security and privacy	Privacy	PPSF [321], EAI [322], PPBD [323], FFIDS [324], SWS [325], FDEMATEL [326]
	Authentication, access control, and encryption	Dynamic AC [327], SC [328], DLACB [329], DAC [330], SC-DT [331], MSecureChain [332], SIEMF [333], SVM [334], FBASHI [335], NF-VANET [336]
	VPN	VAE [337], I-Trace [338]
	Firewall	Fuzzy NN [339], FL-FW [340], fuzzy-IVN [341]
	Intrusion detection	SVM-AL [343], DL [344], PRO-DLBIDCPS [345], DBF [346], CID [347], KNN [348], DeepCoin [349], FRSDEL [350], FED-IDS [351], CIDS [352], RSL–KNN [353], CGAN [354], ANN [355], Fuzzy-IDS [356], PBFL-ADS [357], BFT-IoMT [358]
	Anomaly detection	DAG blockchain [359], Brain-chain [360], PBFLAD [361], IoMTBC-AD [362], HDL [363]
Virtual network	— — — —	BTNV [365], DQL-KDVN [366], DLT [367], CBDST [368], SliceBlock [369], BNSB [370], Skunk [371], SRT-DDQ [372], TTRAS [373]
Big data analysis	— — — —	BlockIoTIntelligence [374], DFL-B [375]
Cloud/edge compu.	— — — —	ERSS [377], Edge-RA [378], Tian et al. [379], Shahbazi et al. [380], NS-IoT [381], OSS [382], DSF [383], ChainFL [384], CBDRL [385], BCOOL [386], IC-ECRA [387]
Data center	— — — —	PDC [388], FDC [389]

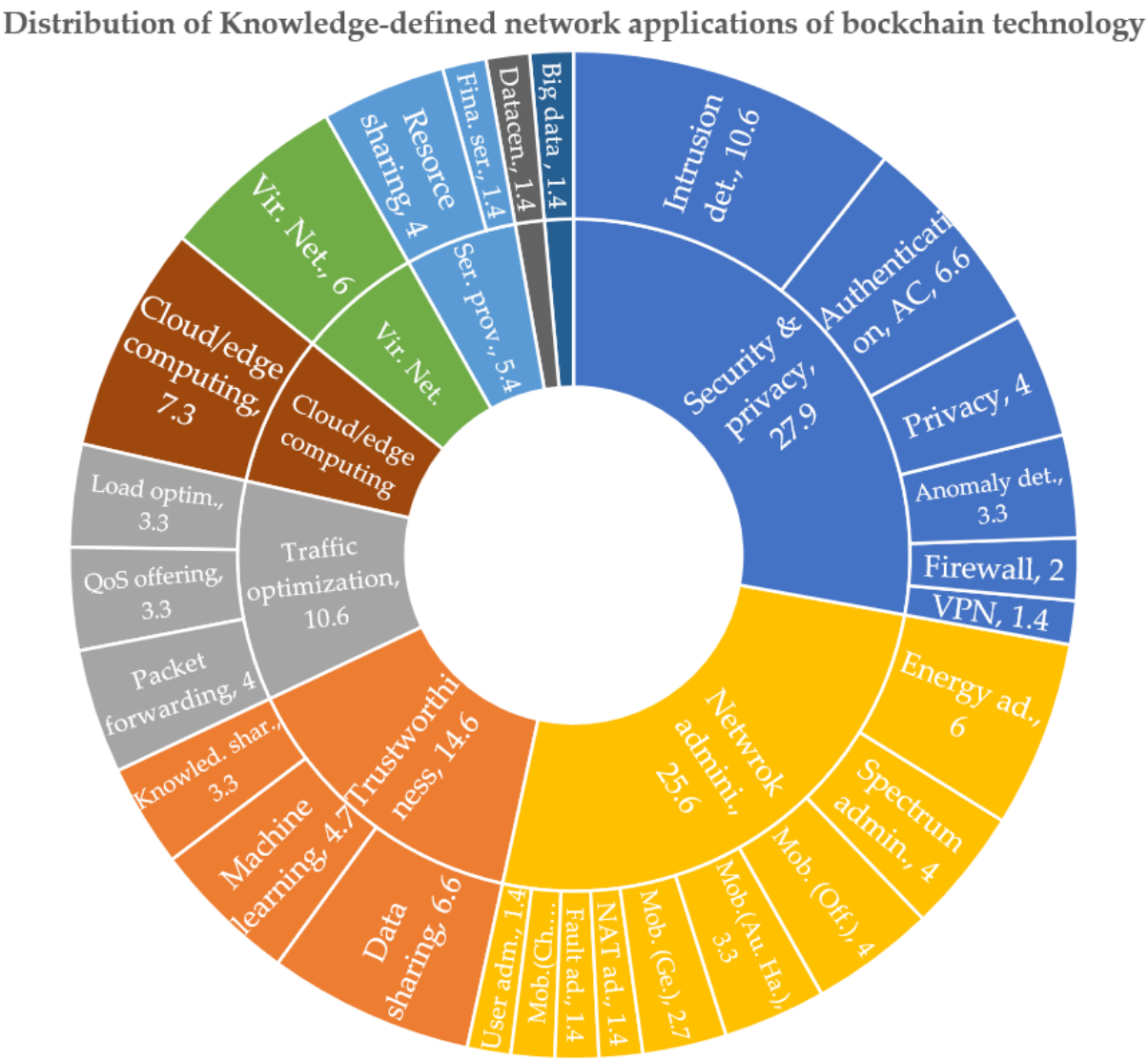


Figure 9. Distribution of blockchain-based frameworks in Knowledge-Defined Networks under various application categories.

5.2. Detailed Comparison and Performance Analysis of each Blockchain Application in Knowledge-Defined Networks

In this section, we compare each of the blockchain-based intelligent network application frameworks with each other with respect to blockchain architecture, blockchain consensus, blockchain type, knowledge generation/dissemination model, and knowledge generation or dissemination technique, while reviewing the performance of each of them.

Table 4 depicts the details of each application of blockchain technology in knowledge-based networks reviewed in Section 4.

Table 4. Detailed comparison and performance analysis of each intelligent network application of blockchains.

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
DRL [237]	Linear	PoW	Public	ML	DRL	IoT	Offload dumping service to obtain performance up to 85%	2022
BEIIP [238]	Linear	Generic	Permissioned	ML	DL	IoT	Better compared to TORM and RouteChain	2023
Dai et al. [239]	Linear	PBFT	Consortium	ML	DRL	5G, 6G	Better convergence performance for resource management	2019
Guo et al. [240]	Linear	PoContribution	Consortium	ML	DL	IoT	Service response time increases with number of nodes	2020
DRS [241]	Linear	PoW+PoS	Public/Private	ML	DRL	6G	High throughput and profit ratio compared to Q-learning	2021
6G-IoV [242]	Linear	PoFL	Public	ML	FDL	6G-IoV	Failure rate is 5% lower with 30% malicious nodes	2022
Mohammed et al. [243]	Linear	PoW	Public	ML	DRL	UAV	No performance analysis presented	2020
ManuChain [244]	Linear	Custom-XFT	Private	Optimization	Holistic	IIoT	Improves efficiency of manufacturing planning and execution	2019
MKShareNet [245]	Linear	PoW	Consortium	MD-K ontology	Collaborative sharing	Generic	Peak throughput—1900 tps, latency—300 ms	2021
Li et al. [246]	Linear	PoP	Private	Edge KS	UCB	IoT	Low delay and latency for block generating	2020
HBEFL [247]	Hierarchical	PoL	Consortium	ML, trading market	Hierarchical FL, multiplayer game	IoV	10% more accuracy than traditional FL	2020
CKShare [248]	Linear	Generic	Public	ML	KNN	Manufacture	Gurantee confidentiality, improves ownership, avoid copyright problems	2019
Chai et al. [249]	DAG	TSA	Consortium	ML	ADL	ICV	Secure and resist malicious attacks	2021
FL [251]	Linear	PoQ	Private	ML	FL	IIoT	Good accuracy, efficiency, and security	2019
Feng et al. [252]	Linear	PoW	Public	ML	FL	5G-Drone	High efficiency for authentication and good accuracy	2021
PBDL [253]	Linear	Smart contract	Private	ML	DL (SSVAE+BiLSTM)	Industrial healthcare	Better data sharing performance compared to existing studies	2022

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
MDS [254]	Linear	Generic	Permissioned	ML	DL	IoMT	Throughput—1, overhead—600 B, low latency and packet loss rate	2023
Kumar et al. [255]	Linear	PoAuthentication	Private	ML	DL (SCSAE-ALSTM)	UAV	Good performance in detecting illegitimate transactions	2022
MPBC [257]	Linear	Committee-based	Private	ML	FL-DL	Medical	Safe and effective for sharing medical data	2021
Zhang et al. [258]	Linear	PBFT	Permissioned	ML	Generic	Generic	Secure and trustless data sharing	2018
fuzzy engine [259]	Linear	PoW	Public	Fuzzy engine	Fuzzy logic	IoT	High block reliability and data integrity	2022
ANFPB [260]	Linear	PoS	Private	ML	Neuro-fuzzy	IoV	Efficient in preserving privacy and computational costs	2021
PiRATE [261]	Linear	PBFT	Permissioned	ML	Generic	5G	More efficient than LearningChain in storage complexity and communication time	2020
DFL [262]	Linear	PBFT	Private	ML	FL	Vehicle	0.97 accuracy, good throughput, low latency, good energy efficiency	2020
BlockDeepNet [263]	Linear	PBFT	Private	ML	DL	5G-IoT	High accuracy with considerable overhead, latency	2019
Singh et al. [264]	Linear	Vote-based	Permissioned	ML	DL (Deep Boltzmann)	SD-Industrial	Scalable, better accuracy, low computation time and overhead	2020
PriModChain [265]	Linear	PoW	Public	ML	FL	IIoT	Good privacy, security, resilience, safety, and reliability	2020
BBDDL [266]	Linear	Dual-driven	Generic	ML	Distributed-DL	6G-IoE	Better accuracy and latency	2023
explainable AI [267]	Linear	Vote-based	Public	ML	Generic	Generic	Trustworthy and explainable predictions	2020
Secure routing [268]	Linear	Vote-based	Permissioned	ML	Generic	SD-IoT	High trust and secure in multi-domains	2022
GAR [269]	Linear	PoW	Public	Optimization	Genetic algorithm	SD-IoT	Optimized resource utilization for routing	2021
trusted routing [270]	Linear	PoAu	Consortium	ML	RL	WSN	Low delay even at 51% vulnerability, good throughput, energy consumption	2019

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
ENIR [271]	Linear	Generic	Permissioned	ML	DRL	IoT	Better utilization of links and low transmission delay	2023
CDRL [272]	Linear	Generic	Permissioned	ML	Compact DRL	IoT	Require only 10% of resources, good transaction efficiency	2022
FLEA-RPL [273]	Generic	Generic	Generic	Fuzzy engine	Fuzzy logic	IIoT	Improves packet delivery ratio by reducing route interruptions	2022
LB-DRL [274]	Generic	Generic	Generic	ML	DRL	Generic	Scalable and reliable load balancing	2021
ECRL [275]	Linear	Generic	Permissioned	ML	RL	Vehicle	Good accuracy and throughput, high computational time	2020
BCLB [276]	Linear	Generic	Permissioned	ML	DRL	Generic	Prevent leakage of domain info, low migration cost	2022
Fuzzy [277]	Linear	Generic	Permissioned	Fuzzy engine	Fuzzy logic	SDVN	Good throughput, low latency and computation usage	2022
IVEC [278]	Linear	PoVS	Permissioned	ML	RL	VEC	Efficiently manage unbalanced load	2021
MLBQR [280]	Linear	PoW	Generic	ML	RL (QL)	SDVN	15% low delay, 18% low energy consumption, 38% high throughput	2022
MLSMBQS [281]	Linear	PoW + EHO	Generic	ML	Generic	IoT	8.5% high throughput, 15.3% low delay, 4.9% low energy consumption, better security	2022
Side chaining [282]	Linear	DPBFT-DPOS	Generic	ML	Generic	IoT	15% high throughput and energy efficiency, High accuracy and F1-score, 10% low delay	2022
ATQMB [283]	Linear	PoS	Generic	ML	Generic	Generic	High security and traceability, moderate scalability	2022
QoS-ledger [284]	Linear	Smart contract	Public	Meta-heuristics	Genetic algorithm	Medical	Delay of 87–95 ms, 185 byte throughput, 8% duty cycle	2021
CGT [285]	Linear	Generic	Generic	Meta-heuristics	GT + SC	5G, 6G	Achieves Nash equilibrium within a short time	2019
MADRL [286]	Linear	PBFT + PoReputation	Consortium	ML	DRL	5G-UAV	Better utility optimization satisfaction for QoS	2023
DRL [287]	Linear	Generic	Generic	ML	DRL	Generic	Low computational delay and handover failure rate	2021

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
QRM [288]	Linear	Generic	Generic	Meta-heuristics	QRM	Generic	Improved latency with respect to mobility and security	2018
DMM [289]	Linear	Generic	Generic	ML	FL-DRL	5G-UDN	31.87% task execution time reduction	2020
IoTAH [290]	Generic	Generic	Generic	ML	Generic	IoT	Various smart applications in smart cities are discussed	2022
deep learning [291]	Linear	PoW	Private	ML	DL	IoT	Malicious device detection accuracy of 0.91	2021
RLAC-FNN [292]	Linear	Custom	Generic	ML	RLAC-FNN	5G	Reduce handover and consensus delay, authentication frequency	2023
AEFO [293]	Hierarchical	PoAu	Hybrid (Private + Public)	ML + Optimization	AEFO + SARSA	5G WBAN-IoT	Low delay, packet loss rate, authentication time, energy consumption	2021
ATLB [294]	Linear	Generic	Permissioned	ML	Transfer DRL	IIoT	Accurate authentication with high throughput and low latency	2021
BBAIoT [295]	Linear	PoW	Public/consortium	ML	DRL-D3QN	CRN	Better network throughput and convergence speed	2022
ACDRL [296]	Linear	PoAu	Private	ML	DRL	SD-5G-IoT	50% energy efficiency	2022
SOM [297]	Linear	PBFT	Consortium	ML	DRL	VEC	High throughput, low service execution delay and energy consumption	2021
DRL-CO [298]	Linear	Generic	Generic	ML	DRL	IoT	Low delay and consume low transmission power	2022
SCRDO [299]	Linear	Generic	Generic	ML	DRL	Medical	Lower cost than other approaches	2023
Edge-cloud CO [300]	Linear	PoW	Private	ML	DRL	IoT	High security with minimum smart contract and offloading costs	2021
DCRM [301]	Linear	PBFT	Generic	ML	DRL	Cyber-physical	Low system delay and good decision making related to self-adaptation	2021
SMS [302]	Linear	Generic	Generic	ML	DRL	CRN	Minimum experience of disruption and delay in handover	2020
6GSH [303]	Linear	Generic	Generic	ML	Deep RNN-LSTM	6G	Despite of service operators, a stabilized service quality is provided	2021

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
CR-IOT [304]	Linear	PoW	Generic	ML	Decision tree	CR-IoT	Effective in malicious user detection for secure spectrum access	2022
DITEN [305]	Linear	DPoS	Permissioned	ML	FL-RL	IoT	Data security and communication efficiency are improved	2020
Spectrum trading [306]	Linear	PoW, PoS, DPoS, PBFT	Public, Consortium	ML	RNN	6G	Good throughput and profit and low overhead	2020
SSA [307]	Linear	Generic	Generic	ML	ELM	CRN	0.68 detection rate	2022
FIRP [308]	Linear	Generic	Generic	ML	Generic	Microgrid	High power supply fault identification rate, improved relay protection success rate	2022
PRLB [309]	Linear	PoW	Private	ML	Privacy RL	Smartgrid	Better performance in outlier detection and runtime performance	2021
IoMT [310]	Linear	PoW	Generic	ML	FL	IoMT	Average accuracy around 65%	2023
UAGV [311]	Linear	Generic	Generic	ML	FL	UAV	Improved connectivity, energy enhancement, and service availability	2021
RM [312]	Linear	PoW	Public	ML	RL	Generic	Reduced cost and energy	2017
EE [313]	Linear	BFT	Permissioned	ML	DRL	IIoT	Improved energy efficiency with limited performance reduction	2020
Pre-caching [314]	Hierarchical	Custom	Private	ML	Graph Convolutional LSTM	IoT	Low energy consumption for caching	2021
Block5GIntell [315]	Linear	Modified PBFT	Consortium	ML	Generic	5G	20% decrease in energy consumption	2020
VEN [316]	Linear	Generic	Consortium	ML	KNN	VEN	Reduce charging cost and time	2022
DETF [317]	Linear	Generic	Consortium	ML	Generic	Connected EVs	Improved profitability	2019
DET [318]	Linear	Generic	Consortium	ML	Hierarchical RL	SD-EI	Total mean reward of 18%	2022
SDEM [319]	Linear	PBFT	Permissioned	ML	RNN–LSTM	Smart Grid	Low mean absolute percentage error and latency, high throughput, energy crowdsourcing	2021
PPSF [321]	Linear	PoW	Generic	ML	Gradient boosting	IoT-smart city	Intrusion detection preserving privacy, good classification performance	2021

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
EAI [322]	Linear	PoW	Private	ML	Generic	Generic	300 ms processing time, low resource consumption	2019
PPBD [323]	Linear	Generic	Generic	ML	Generic	IoT	Maintain privacy, minor computing overhead	2021
FFIDS [324]	Linear	PoW	Public	ML	FL-random forest	SDVN	Efficient memory and computation resource usage, 0.9 attack detection rate	2021
SWS [325]	Linear	Generic	Generic	Fuzzy engine	Fuzzy logic	Smart agriculture	Securely and efficiently handle watering	2019
FDEMATEL [326]	Linear	Generic	Public	Fuzzy engine	Fuzzy logic	IoT	High impact related to authentication and intrusion detection criteria	2023
Dynamic AC [327]	Linear	Generic	Generic	ML	RL	IoT	Distributed access control with efficient handling	2017
SC [328]	Linear	Generic	Permissioned	ML	Supervised ML	IIoT	Can effectively reduce different types of threats	2022
DLACB [329]	Linear	PoAu	Private	ML	DL	Generic	Correct user authentication performance, access control identifying malicious users	2023
DAC [330]	Linear	PoAu	Public	ML	Generic	Healthcare	Traceable, authorized access control	2022
SC-DT [331]	Linear	PoW	Public	ML	Similarity learning	Generic	Good confidentiality, reduce replay attacks, good integrity	2019
MSecureChain [332]	Linear	PBFT	Generic	ML	FL	Metaverse	Enhance security, scalable, prevent single point of failure	2023
SIEMF [333]	Linear	PoW	Public	ML	DL	Generic	Privacy of vehicles is preserved, low block read and retrieval times	2020
SVM [334]	Linear	PoW	Private	ML	SVM	IoHT	Trusted, low consumption, improved security	2022
FBASHI [335]	Linear	PoW	Permissioned	Fuzzy engine	Fuzzy logic	IoHT	Distributed trust, prevent single point of failure, detect malicious behavior	2022
NF-VANET [336]	Linear	Generic	Generic	ML	Neuro-fuzzy	Vehicle	91.5% accuracy, improvement in computation cost and overhead	2021

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
VAE [337]	Linear	PoW	Permissioned	ML	DL	Medical	High secrecy with good detection performance	2022
I-Trace [338]	Linear	Generic	Generic	ML	Generic	Cyber-physical	Secure infrastructure of cyber-physical networks	2021
Fuzzy NN [339]	Linear	PoW	Permissioned	ML + Fuzzy engine	Fuzzy logic + DL	SD-IoT	Fast attack detection, Accuracy of 96%, high throughput	2022
FL-FW [340]	Linear	delegated PBFT	Consortium	ML	FL	Vehicle	Prevent data poisoning attacks, flow prediction securing privacy	2021
fuzzy-IVN [341]	Linear	Generic	Generic	Fuzzy engine	Fuzzy logic	Vehicle	Detects false data and preserves reputation	2023
SVM-AL [343]	Linear	PoW	Private	ML	SVM	IoT	Accuracy, precision, F1-score close to 1	2020
DL [344]	Linear	PoW	Public	ML	DL	Generic	High accuracy in detecting attacks	2022
PRO-DLBIDCPS [345]	Linear	PoW	Private	ML	DL-RNN	Cyber-physical	Enhanced detection and security, high accuracy with low training and testing times	2022
DBF [346]	Linear	PoW	Private	ML	DL-BiLSTM	IoT	Can securely transmit data in a timely and reliably, good detection rate	2020
CID [347]	Linear	Ranking algorithm	Generic	ML	KNN, Naive Bayes, SGD	UAV	Good accuracy, precision, and detection rate, low time to train	2021
KNN [348]	Linear	Generic	Generic	ML	KNN	IIoT	Scalable, detect diverse attacks, low computational usage	2022
DeepCoin [349]	Linear	PBFT	Private	ML	DL-RNN	Smart grid	98% detection accuracy, low false alarm rate, preserve privacy	2019
FRSDEL [350]	Linear	Generic	Private	ML	FRSDEL	Smart home	Good stability and less error rate for intrusion detection	2022
FED-IDS [351]	Linear	Generic	Generic	ML	FL	Smart transportation	Efficient and credible intrusion detection	2021
CIDS [352]	Linear	PoW + PoAccuracy	Public	ML	FL	VEC	Low overhead and computational cost with collaborative privacy preserved detection	2021

Table 4. *Cont.*

Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
RSL–KNN [353]	Linear	Access rights	Permissioned	ML	RSL–KNN	SD-IIoT	96.73% accuracy, 100% detection rate	2019
CGAN [354]	Linear	Generic	Generic	ML	CGAN	UAV	Improved intrusion data detection, good generalization capability	2022
ANN [355]	Linear	Generic	Private	ML	ANN	SD-IoT	Guarantee security with improved threat detection and mitigation	2023
Fuzzy-IDS [356]	Linear	Generic	Generic	ML + Metaheuristics	Fuzzy DL + Optimization	IoT	Good threat classification performance, high throughput and low latency	2023
PBFL-ADS [357]	Linear	Generic	Private	Fuzzy engine	Fuzzy logic	IoMT	Diagnose fraudulent nodes with considerable workload, pattern identification ratio—92.1%, server utilization—40%	2022
BFT-IoMT [358]	Linear	Generic	Generic	Fuzzy engine	Fuzzy logic	IoMT	Better attack detection, low energy consumption, high packet delivery ratio and throughput	2023
DAG blockchain [359]	DAG	Generic	Generic	ML	Capsule NN	5G-SDN	Outperforms others in terms of bandwidth, delay, packet loss, and security parameters	2023
Brain-chain [360]	Linear	Generic	Permissioned	ML	Supervised ML	Generic	Fast and effective in mitigating attacks, high accuracy with low false positive rate	2020
PBFLAD [361]	Linear	Round robin	Permissioned	ML	FL	Generic	About 10% impact from blockchain to FL	2018
IoMTBC-AD [362]	Linear	Generic	Generic	ML	DL	IoMT	Detects anomalies effectively	2022
HDL [363]	Linear	Generic	Generic	ML	Hybrid DL (CNN + LSTM)	Generic	Outperform conventional SDN by 8.6% higher accuracy	2023
BTNV [365]	Linear	Vote-based	Generic	ML	Linear regression	Wireless	Minimum double spending attacks and delays when selecting radio frequency slices	2019
DQL-KDVN [366]	Linear	Custom	Permissioned	ML	Deep Q learning	SDVN	Improved throughput, require caching resources	2018
DLT [367]	Linear	Custom	Permissioned	ML	Dueling DRL	IoV	Converges with high reward	2020

Table 4. *Cont.*

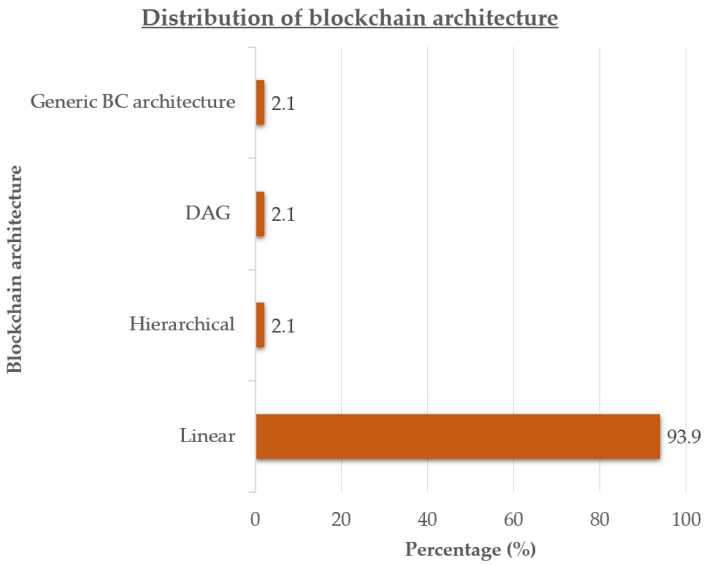
Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
CBDST [368]	Linear	PBFT	Consortium	ML	DRL	5G-RAN	Good security, utility of players are maximized	2022
SliceBlock [369]	DAG	PoSp	Generic	ML	GAN	SD-6G	Slice the network securely and energy efficiently	2022
BNSB [370]	Linear	Generic	Generic	ML	DRL	5G	Price and time delay is better, high reward	2021
Skunk [371]	Linear	Generic	Generic	ML	FL	5G, 6G	Detect attacks in the sliced network	2022
SRT-DDQ [372]	Linear	Generic	Consortium	ML	DRL	5G	12% reduction in double spending attacks, maximize player utility	2021
TTRAS [373]	Linear	Generic	Generic	ML	FL-DRL	5G	Solution converges and maximize utility under various prices	2023
BlockIoTIntelligence [374]	Linear	Generic	Permissioned	ML	Generic	IoT	High accuracy and low latency in object detection	2020
DFL-B [375]	Linear	PoW	Private	ML	FL	IoT	Efficient, preserves privacy, low packet overhead and energy consumption	2021
ERSS [377]	Linear	Credit differentiated	Consortium	ML	Generic	IIoT	Improved edge service cost and service capacities	2019
Edge-RA [378]	Linear	PoW/PoS	Private	ML	DRL	IoT	Solution convergence with low delay and task drop rate	2020
Tian et al. [379]	Linear	Generic	Generic	ML	Decision tree	IIoT	Secure and efficient, high edge service accuracy	2021
Shahbazi et al. [380]	Linear	Generic	Generic	ML	K-means	Smart manufacturing	Improves processing time of manufacturing tasks, low delay and cost of deployment	2021
NS-IoT [381]	Linear	Custom	Permissioned	Fuzzy engine	Fuzzy logic	IoT	Quick node selection, manage linguistic and numerical data	2022
OSS [382]	Linear	Custom	Hybrid (Public + Private)	ML	DRL	IoMT	Low communication and computation time for offloading and scheduling	2022
DSF [383]	Linear	Generic	Generic	ML	DRL	Power IoT	Low queing delay and consensus delay	2020

Table 4. *Cont.*

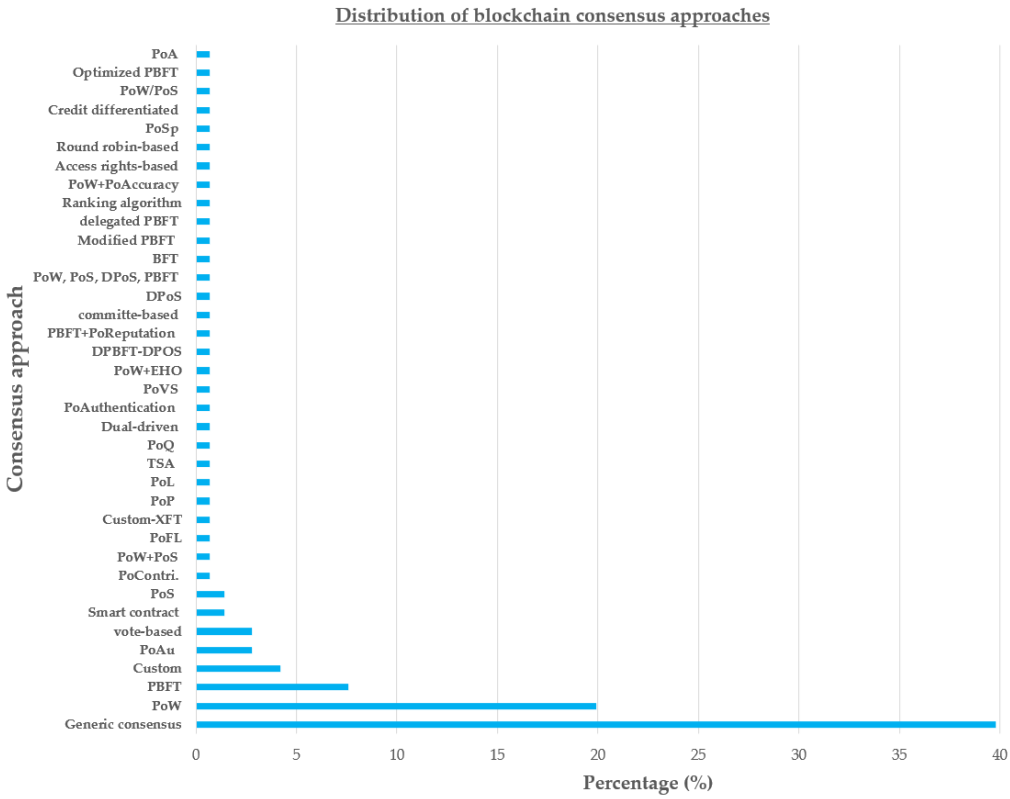
Framework	Blockchain Architecture	Blockchain Consensus	Blockchain Type	Knowledge Generation/Dissemination Model	Knowledge Generation/Dissemination Technique	Network Type	Performance	Publication Year
ChainFL [384]	Linear	Generic	Generic	ML	FL-DRL	IoT	High convergence under upload and download attacks, scalable	2021
CBDRL [385]	Linear	Optimized PBFT	Consortium	ML	DRL	IoT	15.8% and 10.1% cost saving, time saving-22% and 10% for link state routing and deep Q network placement, respectively	2019
BCOOL [386]	Linear	PoA	Generic	ML	Linear regression + K-means/random forest	Vehicle	High reliability and efficiency, accurate congestion prediction for realtime monitoring	2021
IC-ECRA [387]	Linear	Generic	Generic	ML	Collective RL	IoT	Effective in collaborative resource allocation	2022
PDC [388]	Linear	Generic	Generic	ML	FL	IoT-Datacenter	Can train ML models without sending private data	2022
FDC [389]	Linear	Generic	Generic	ML	FL	IoT-Datacenter	Converge well and have a high training accuracy compared to centralized ML	2020

5.3. Overall Analysis

Based on the parameter comparison of each blockchain-based Knowledge-Defined Networking application framework listed in Table 4, we can analyze the overall parameter distribution for the whole survey. Figure 10 provides the distribution of blockchain applications in Knowledge-Defined Networking related to blockchain, knowledge generation and dissemination, network-related characteristics, and publication year.

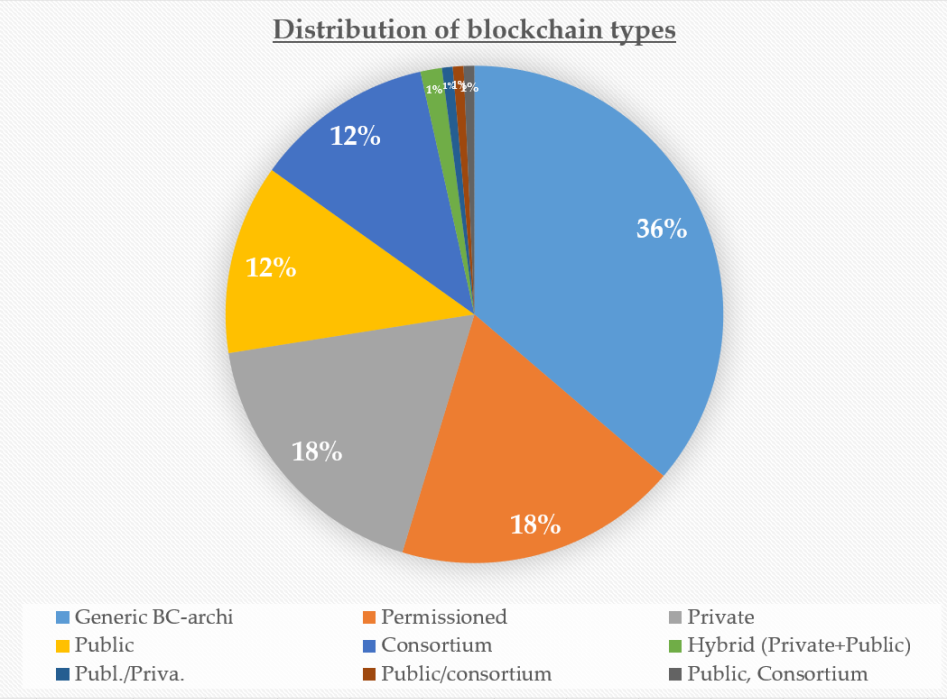


(**a**) Distribution of blockchain architecture

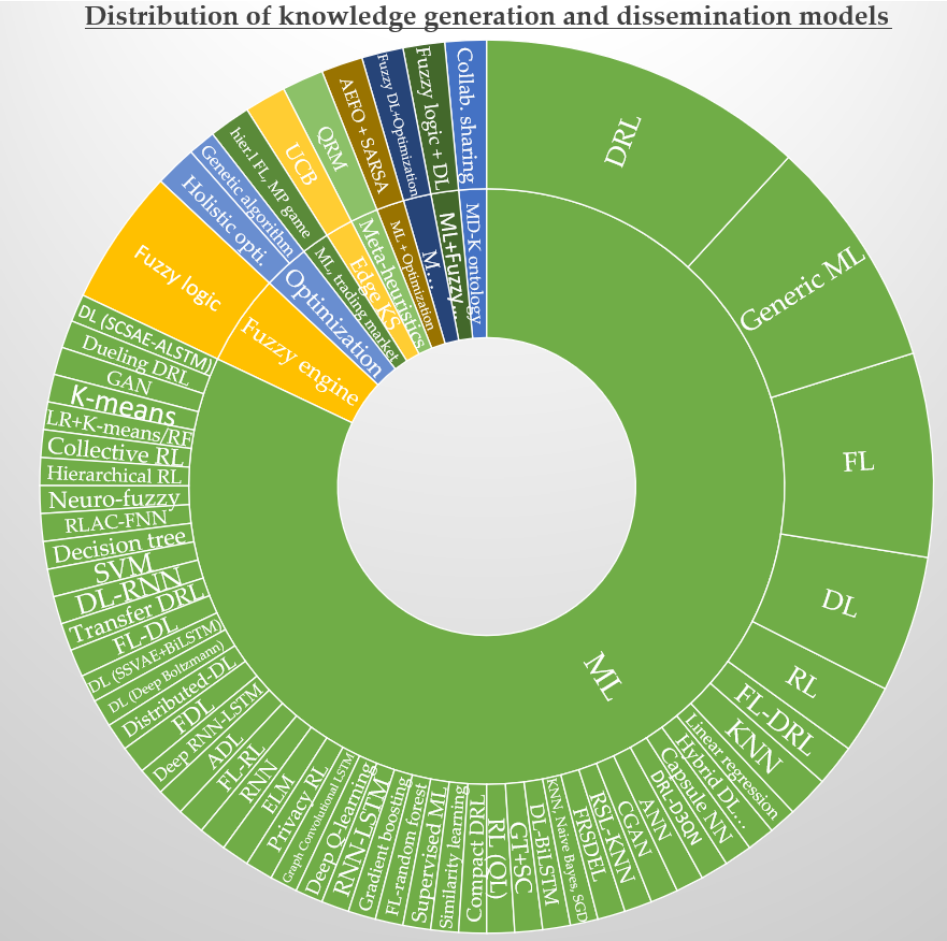


(**b**) Distribution of blockchain consensus approaches

Figure 10. *Cont.*

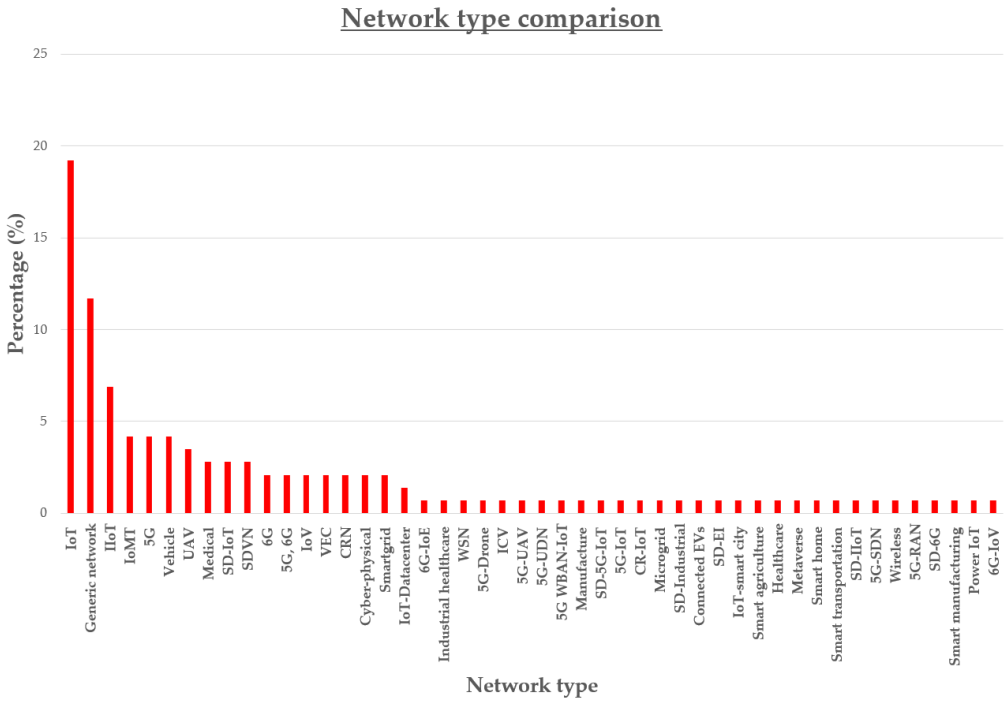


(**c**) Distribution of blockchain types

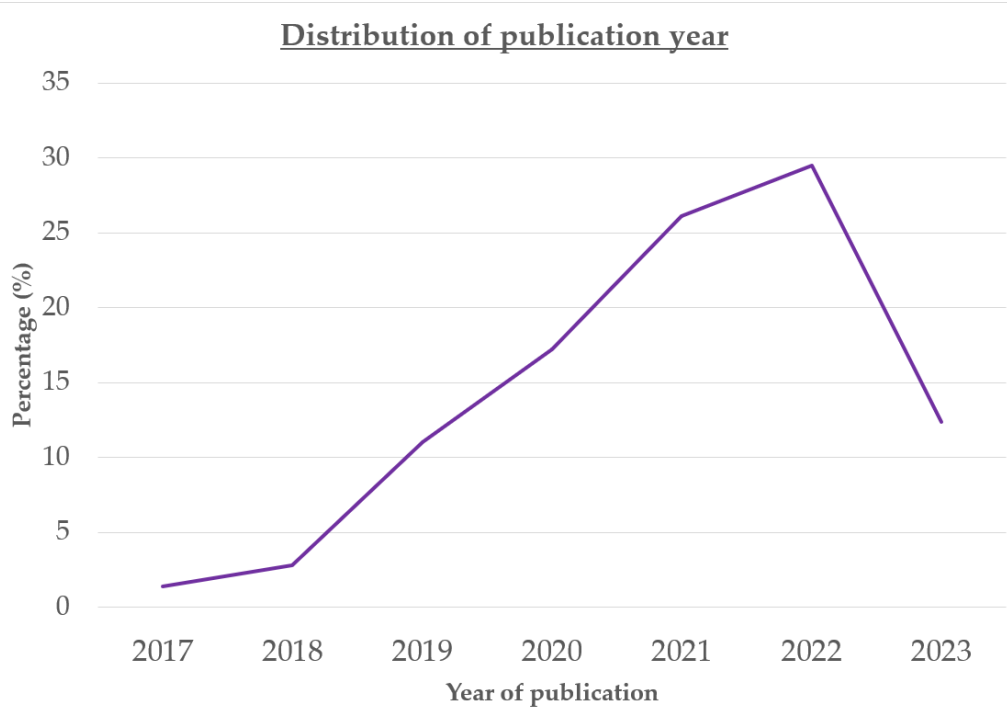


(**d**) Distribution of knowledge generation and dissemination models

Figure 10. *Cont*.



(**e**) Distribution of network type



(**f**) Distribution of publication year

Figure 10. Comparison of blockchain, knowledge generation, knowledge dissemination, network characteristics, and published year of blockchain-based Knowledge-Defined Networking applications reviewed in this survey.

As evident from Figure 10a, 93.9% of blockchain-based frameworks have been implemented using the linear blockchain architecture for Knowledge-Defined Networking applications. Only 4.2% of frameworks have been implemented using either DAG or hier-

archical blockchain architectures, while 2.1% have proposed generic frameworks without specifying the BC architecture.

When considering the consensus approaches, it is clear, according to Figure 10b, that nearly 40% of the BC-based frameworks are designed to work with any (generic) consensus approach, while the remaining 60% specify a consensus approach. PoW is the most dominant BC consensus approach used by many applications (nearly 20%), followed by PBFT, custom, PoAu, vote-based, smart contracts, and vote-based. The probability of using another consensus approach other than the one specified above is much lower (0.7%), as evident from Figure 10b.

Similar to the result on the consensus approach, most (36%) of the BC-based frameworks for knowledge-based networks are designed to support any blockchain type (generic), as evident from Figure 10c. Among the remaining 64% of frameworks that specify the blockchain type for which they are designed, permissioned (private + consortium) blockchains and private blockchains have a similar (18%) distribution of frameworks. Likewise, public and consortium blockchain distributions are also similar (12%) and significant. Note that, as evident from Figure 10c, other blockchain types such as public/private, hybrid (public + private), public/consortium, and public+consortium have the lowest probability of occurrence in Knowledge-Defined Networking applications.

Figure 10d is a hierarchical sunburst chart showing the distribution of knowledge generation dissemination models and techniques for blockchain-based intelligent networking application frameworks reviewed in this research. It is crystal clear from this chart that the most dominant knowledge generation model in BC-based frameworks is machine learning, as it has the highest distribution percentage of 85%. The second most dominant knowledge generation/dissemination model has been the fuzzy engine, followed by optimization, ML with trading market, edge knowledge sharing, meta-heuristics, ML with optimization, ML with meta-heuristics, and the MD-K ontology. These models (except ML) usually have one or a few specific knowledge generation/dissemination techniques. For instance, as depicted in Figure 10d, the fuzzy engine model has the fuzzy logic technique, the optimization model has holistic optimization and genetic algorithms, etc. Note that fuzzy logic and optimization stand out as the most dominant non-ML-based knowledge generation techniques. On the other hand, ML has a vast variety of knowledge generation techniques, as depicted in Figure 10d. The most dominant ML techniques, in order, are DRL, generic ML, FL, DL, RL, and FL-DRL. Note that generic ML refers to frameworks that do not specify the ML technique and are designed to support any ML technique. Thus, it can be concluded that most (54%) existing blockchain-based intelligent networking applications are designed with reinforcement learning, deep learning, federated learning, or a combination of these three approaches. However, note that the percentage of all other specific ML techniques is also significant (31%), so a considerable number of frameworks use other specific ML techniques such as KNN, SVM, linear regression, naive Bayes, similarity learning, gradient boosting, decision trees, neuro-fuzzy, K-means, GAN, etc.

Now let us observe the distribution of intelligent network types among the blockchain-based frameworks reviewed in Section 4. It is very evident from Figure 10e that the most dominant network category has been IoT, having a percentage distribution of 19.2%. The next highest percentage of 11.7% is held by frameworks that are designed for generic intelligent networks, followed by IIoT, IoMT, 5G, vehicle, UAV, medical, SD-IoT, SDVN, 6G, 5G and 6G, etc., as depicted in Figure 10e.

When looking at the variation in the percentage of BC-based intelligent networking application frameworks against publication year, shown in Figure 10f, it is clear that the literature began to evolve starting in 2017. Note that, as specified in the survey methodology in Section 1.3, our population contains all frameworks published from 1980 to 2023. However, we could not find any publications having Knowledge-Defined Networking applications based on blockchains from 1980 to 2016. As seen from Figure 10f, the number of publications per year has increased approximately linearly in the years from 2017 to 2022. However, at the time of this survey, only half of 2023 has passed, so the number of publi-

cations in 2023 is lower than in 2022. Therefore, we can expect more knowledge-defined blockchain applications in the near future as well, according to the trend in the graph, as this field is still evolving.

6. Discussion

As reviewed, blockchain has been utilized to improve many applications in Knowledge-Defined Networking. The advantages and difficulties of integrating the blockchain with cognitive knowledge-based networks merit discussion.

6.1. Benefits

Due to the integration of blockchain in KDN, many advantages are achieved, like better data, knowledge, and AI model sharing; better data storage and data interoperability; improved security and privacy; decentralized intelligence; reliable decision-making; enhanced automation; better resource sharing; better network management; etc. These benefits are explored hereafter.

6.1.1. Better Data and Machine Learning Model Sharing

In the logically and physically centralized architecture of KDN, a centralized entity involves collecting a large dataset from multiple nodes and training just one artificial intelligence agent. However, the collection of such data is difficult due to bandwidth constraints, large overhead and costs in communication, and difficulty in aggregating heterogeneous data. Alternatively, in the distributed control architecture of KDN, machine learning model training is distributed, which is more compatible with decentralized blockchain technology. Thus, data can be shared on a blockchain for training ML agents. Furthermore, the trained ML models can also be shared using the blockchain. The use of collaborative federated learning using blockchain to protect the immutability of ML prototypes and thwart model contamination assaults is clear through frameworks like DBF-B [375]. Thus, the data employed for ML model training can be guaranteed to originate from legitimate users thanks to the digital signature verification, and as every piece of data inserted into the blockchain is verified using cryptographic hash functions, the data cannot be tampered with by third parties. Furthermore, blockchains can enable automatic data cleansing using consensus and smart contracts to automatically identify erroneous data, thus improving the accuracy of the data. Thus, blockchain enables accurate and trustworthy machine learning and model sharing.

6.1.2. Better Data Storage and Data Interoperability

In blockchains, data are added to a block by the miner, and that block is distributed among blockchain nodes in the network. As a result, data are stored as clones across the blockchain system, increasing data storage trustworthiness. This avoids the problem of centrally managed storage's sole source of malfunction, where the data are lost in the event of damage or loss of centralized data storage. In addition, the blockchain's self-executing contracts have the capacity to reduce the amount of time and expense associated with labeling and pre-processing data. Smart contracts can be configured to define rules such that data are automatically categorized and processed beforehand on the blockchain without the need for human participation.

When it comes to data interoperability, a KDN network that employs numerous virtual network slices may be used to transmit data using cross-blockchain technology, which has the capacity to exchange information among various blockchain networks.

6.1.3. High Security and Privacy

Sixth-Generation (6G) networks embrace AI and machine learning for service delivery, so they inherit properties from the KDN paradigm. Due to the massive amount of data, which results in enormous processing and analysis using ML for knowledge generation, these networks are vulnerable to contamination by attackers. Recent works have demon-

strated how KDNs, such as 6G networks, can leverage blockchain technology integrated with AI to improve the security concerns existing in intelligent networks [390]. As centralized machine learning is vulnerable to attacks, decentralized machine learning with the aid of blockchain technology has improved security in contrast to the centralized approach, as the sole spot of attack is prevented using the distributed approach. Furthermore, sensitive data on the blockchain can be cryptographically encrypted, and access control can be implemented with the aid of smart contracts to prevent unauthorized people from accessing sensitive data. Thus, blockchain secures the privacy of stored data by partitioning data based on identity and access control rights. Furthermore, blockchain prevents malicious nodes from contributing to the data pool thanks to consensus approaches such as voting-based consensus, where consensus from the majority of the nodes is required to validate transactions. As blockchain transactions are traceable, malicious data-tampering attempts can be readily identified and given negative rewards or isolated to protect the intelligent network. Blockchains reduce privacy exposure by utilizing pseudonymous addresses for nodes; however, they cannot guarantee full privacy since blockchain transactions are traceable. Zero-knowledge proofs can be incorporated into the blockchain for privacy-preserving data and machine learning model transfer, and anonymous authentication. In addition, the traceability of transactions enables KDN systems to trace the origin of the data and knowledge as well as confirm the validity and immutability of the data.

6.1.4. Decentralized Intelligence

In centralized intelligent systems, a centralized agent is in charge of gathering information from every node in the network and creating a centralized entity that can create global knowledge. However, the centralized intelligence architecture is less scalable and consumes more networking resources than the distributed knowledge generation approach. Furthermore, centralized intelligence is prone to sole spot of breakdown and security attacks. As an alternative, in distributed intelligence systems, many advantages such as low latency, low power consumption, etc. are realized due to the distributed approach. However, if decentralized machine learning is applied without a secure mechanism for privacy protection, users privacy can be leaked, as proven by existing studies [391]. This is where blockchains can come in handy by enabling decentralized machine learning and ensuring privacy is preserved. By utilizing blockchain, ML models can be trained, knowledge can be generated locally, and knowledge can also be shared securely using blockchain, such that a centralized authority in a KDN can aggregate the distributed knowledge in the blockchain for making global-level decisions. First, machine learning models can be trained in a secure and trustworthy manner by using legitimate and verified data stored on the blockchain. Then, trained machine learning models and model parameters can also be exchanged securely in the Knowledge-Defined Network thanks to the immutable and verifiable ledger technology. This promotes collaborative knowledge generation and network optimization, which can enhance the performance of Knowledge-Defined Networks. In order to generate a secure, optimized global model of intelligence, decentralized knowledge agents (controllers) can audit the blockchain of knowledge or machine learning models for poisoning attacks.

6.1.5. Reliable Decision Making

ML models usually involve a black box model where the inputs of the ML model are trained to map to desired outputs. However, these black box models cannot be held accountable for their decisions, and it is difficult to interpret the decisions taken by such machine learning models. The drawbacks of the black box model can be eliminated by using explainable machine learning. However, explainable machine learning alone may not be sufficient to understand how an ML model makes decisions. Thus, there should be effective mechanisms for reviewing and auditing decisions made by machine learning models. Blockchain can aid in storing the data and decisions taken by the machine learning model, making sure that those transactions are immutable, as blockchains do not allow

tampering with transactions. Therefore, the recorded processes of the machine learning agents can be audited by authorized nodes. By auditing, if any machine learning model does not make decisions in the desired manner, the reason for that can be understood by inspecting the blockchain records, and the fault can be rectified, leading to trustworthy decision-making in Knowledge-Defined Networking. Thus, blockchains provide a secure platform for sharing machine learning models decisions, knowledge, and processes among intelligent agents so that they can be reviewed by experts to ensure that decisions are made in the appropriate manner.

6.1.6. Boosted Automation

One of the objectives of transferring from the SDN paradigm to the KDN paradigm is to enhance the automation of the network. KDN systems need to have a high level of automation where network decisions are taken with the aid of application guidelines and real-time network knowledge. Typically, machine learning data pre-processing and labeling for machine learning model training are performed manually by humans. If this manual approach is used in a KDN, it can hinder the efficiency of the KDN system. Data pre-processing, cleaning, and labeling tasks can be decentralized and automated by utilizing smart contracts on blockchains. Smart contracts provide a means for task automation by defining contractual terms upon meeting certain criteria or events.

6.1.7. Better Resource Sharing

In a complex network like a knowledge-defined network, network resources should be efficiently and securely shared among legitimate network users. In order to achieve that task autonomously, smart contracts and blockchain can be utilized. For instance, in order to share edge network resources, a smart contract can be created containing service level agreements to share resources among multiple parties while securing access control policies [242]. Furthermore, resources can be traded among multiple network operators, leveraging the blockchain system and self-executing contracts to facilitate better resource trading and sharing in a multi-operator network environment [372]. Furthermore, the cost of resource usage can be efficiently paid using incentives, as blockchains offer incentive mechanisms.

6.1.8. Better Network Administration

Network administration in a KDN scenario involves the management of diverse aspects such as users, mobility, spectrum, faults, energy, etc. As reviewed in Section 4, blockchain and cryptocurrency can be utilized together for intelligent user management [285]. Blockchains can be further utilized for secure and efficient handover in wireless communication network environments through full forward key separation [286]. Furthermore, the integration of blockchain has prevented re-authentication and repeated handover, resulting in low latency and overhead for handover [290]. Blockchain has been utilized for secure consensus and reliable resource offloading, where resources are offloaded appropriately based on consensus [299]. Blockchain consensus may also be incorporated into smart power networks for safe energy transactions [316]. Blockchain can be used along with machine learning to detect anomalies and identify network faults in a privacy-preserving manner [309].

6.2. Challenges

Application of blockchain technology in intelligent knowledge-based networks also brings in a set of challenges such as difficulty in processing big data, high energy consumption due to blockchain, resource management difficulties, lack of standardization and interoperability, low scalability, increased latency and limited throughput, security vulnerabilities in blockchain, additional resource demand, etc. The next segments examine these negatives.

6.2.1. Processing of Large Volumes of Data

Knowledge-based networks gather vast amounts of data, also referred to as big/massive data, for making inferences for network decisions. This enormous amount of data may be safely and trustworthily preserved inside the blockchain through the adoption of blockchain technology, protecting data from unauthorized modification and deletion. This information may be prepared to be used in ML model learning or making inferences from already trained models. Due to their capability to acquire knowledge from vast volumes of data through hierarchical learning, deep learning models are typically employed to learn from or make inferences from massive data. Processing large volumes of raw data can be a significant challenge, as raw data can be heterogeneous and originate from different sources. Even if self-executing contracts are deployed for automating the data preliminary processing, categorizing, and labeling, users may have a challenge in defining conditions and statements in the smart contracts for the diverse data that big data represent. Furthermore, it is challenging to process large datasets using knowledge generation models due to the high computational demand required to process them. Dispersed storage of big amounts of data is likewise difficult on blockchain, as there can be issues with how to provide incentives for users to share the data.

6.2.2. High Energy Consumption

Even though blockchain can provide benefits such as efficient data, knowledge, and machine learning model and parameter sharing, improved security, and privacy thanks to its characteristic features of data integrity, access control, non-repudiation, etc., additional energy will have to be sacrificed to achieve these benefits from blockchain. In fact, early consensus approaches such as PoW waste computational resources in order to prove that a given node is worthy of adding a block to the blockchain. However, there are less energy-consuming alternative consensus approaches, such as PoS, but, still, the overall blockchain process demands additional energy consumption. Thus, transaction and block creation, distribution, validation, and storage cause the expense of network energy in terms of processing, storage, and communication bandwidth, which can be considered a challenge in integrating blockchain systems for knowledge-based networks.

6.2.3. Difficulties in Resource Management

It has been challenging in blockchain networks to achieve efficient resource allocation and management of resources such as computational, storage, and communication. Consensus protocols should consider how to allocate these resources optimally during mining. However, efficient resource allocation during consensus has not been effectively studied in the existing literature. It is difficult to determine how to distribute the optimal resources needed for every network endpoint to operate the blockchain in a constrained capacity ecosystem like a knowledge-defined network. Furthermore, different users on the network may have different QoS requirements. Thus, it is challenging to provide access control for the resources using blockchain and to train machine learning models to cater to different users' QoS requirements while guaranteeing security and privacy.

6.2.4. Lack of Standardization and Interoperability of Blockchains

In a KDN, the network receives communication services from a number of operators, such as mobile phone companies and telecommunications companies, who have various commercial objectives. These parties and network users may have contradicting business objectives. Due to tjos, blockchain implementation platforms from different parties may be different from each other. A lack of uniformity exists when it comes to using a blockchain system that satisfies the requirements of all parties involved in the network at once. Thus, blockchain implementation among different users or among heterogeneous networks such as optical networks, wireless networks, wired networks, etc. can be different, and, thus, there is an issue with the interoperability of these different blockchain networks. For instance, the consensus algorithm used in one blockchain network can be different from

another blockchain network, so two blockchain networks become non-interoperable. Due to the difficulty of interoperability, data, knowledge, machine learning models, etc. will be difficult to exchange among these blockchain networks, reducing the efficiency and accuracy of decisions made by the KDN.

6.2.5. Scalability of Blockchain

It is widely understood that, because consensus requires the participation of all network endpoints, permissionless public ledgers are less scalable. However, this scalability issue can be reduced by employing a private or consortium blockchain along with a KDN. However, still, with the increase in users, tokens, investors, etc., it is challenging to maintain a large blockchain with the increase in network size. This raises issues regarding data size in blocks, Peer-to-Peer verification response time, high consensus time, the demand for high computational resources, etc. For instance, achieving consensus in a very large network demands both high computational and storage requirements. However, researchers have shown efficient blockchain consensus approaches such as Fetch [392], which combines blockchain with DAG, machine learning, resource lanes, and sharding to parallelize transactions to reduce consensus complexity and improve scalability. Sensor-Chain is another scalable lightwork blockchain framework for IoT mobile devices that operates by consuming fewer resources compared to traditional blockchains to improve scalability [393]. Furthermore, DAG blockchains have shown more scalability than linear blockchains due to their parallel processing capability and ability to handle multiple transactions simultaneously. However, these systems have drawbacks on their own, like the learning of ML algorithms in different resource lanes, etc.

6.2.6. Increased Latency and Limited Throughput

A higher network delay is a drawback of integrating the blockchain into KDN. Reducing the block capacity too much and increasing the block size of blockchains too much can result in higher propagation delays. Introducing a new block to the digital ledger requires starting a transaction procedure, and it must be propagated in the network, be verified using the digital signature, and then undergo a consensus process that involves mining, block creation, block propagation, and block validation steps. Therefore, due to the distributed approach to adding blocks to the blockchain, the latency introduced to the system cannot be prevented. When there are many transactions pending verification and addition to the blockchain, the processing time of these transactions will be high. Researchers have introduced sharding and pruning as solutions for reducing the delay in processing transactions on the blockchain [394]. However, even with such approaches, it is difficult to prevent the additional delay caused by the use of blockchains for intelligent networking. In fact, this delay increases with the increment in network size and may negatively affect delay-critical applications in KDN such as autonomous driving, remote surgery, etc.

Since both Bitcoin and Ethereum have a transaction throughput of under 100 transactions per second, blockchains are renowned for having poor transaction throughput [395]. Increasing the block size boosts throughput. However, increasing the block size causes an additional requirement for storage resources, such that nodes with limited storage resources are negatively affected. Therefore, in intelligent knowledge-based networks, applications that require low latency and high throughput can be negatively affected due to the combination of blockchain technology if the real-time network data reach the machine learning models through a blockchain network. However, recent research has proposed high-throughput blockchains such as Conflux [396], which has a tree graph-based ledger structure capable of processing concurrent blocks to achieve fast consensus and has a transaction throughput of 3480 transactions per second. Thus, these types of blockchains employing a DAG-based structure have shown high transaction throughput due to the parallel computation capability of transactions. Therefore, low-latency techniques such as sharding

and fast-throughput DAG-based blockchain frameworks such as Conflux are recommended when applying blockchain technology in time-critical knowledge-based networks.

6.2.7. Security Vulnerabilities of Blockchain

Even though blockchain transactions are immutable, pseudonymous, reliable, etc., they have been known for security vulnerabilities such as network attacks, endpoint attacks, intentional misuse, code vulnerabilities, data exposure, and human negligence. Thus, even though blockchain is applied to KDNs to improve their security and privacy, blockchain itself is vulnerable to the above attacks. Thus, it is challenging to maintain the security of a KDN even after applying blockchain for trustworthy data, knowledge, and machine learning model sharing. There should be secondary precautionary measures undertaken to mitigate the above vulnerabilities of blockchain. For example, ML may be utilized to detect attacks such as DDoS attack vulnerabilities, routing attacks, domain name service attacks, etc.; strong encryption may be used to prevent data exposure; and AI and trained human experts may be used to detect code vulnerabilities in blockchain. Thus, network operators and users may have to invest more resources in hardware, software, and human resources to mitigate the vulnerabilities, which is an additional burden when applying blockchain to intelligent networking systems.

6.2.8. Requirement of Extra Resources

Blockchain-based solutions are well known for their additional resource consumption, specifically computational, storage, and communication resources. An intelligent network like a KDN already spends additional resources on the knowledge plane to implement knowledge generation models, ontology editors, rule generators, knowledge bases, rule engines, etc. Due to the integration of blockchain, the additional resources required are even higher, as blockchains need storage for storing the transactions, where each validated transaction is essentially replicated in each node, and need computational power to compute hashes, sign and verify using digital signatures, achieve distributed consensus, implement smart contracts for automatic access control and contractual function implementation, etc. In terms of communication resources, blockchains consume bandwidth from both end users and network operators for broadcasting transactions and blocks in the P2P network. However, some academicians have attempted to propose resource-efficient blockchain-based solutions for knowledge-producing networks such as KDN by carefully assessing their reliability against security aims [13]. Thus, resource-efficient blockchain systems must be selected to reduce the burden of additional resources that are used in a distributed blockchain.

7. Final Thoughts, Propositions, and Prospects for the Future

This review article first provides overviews of blockchain technology and the concept of Knowledge-Defined Networking. Blockchain, being a distributed, immutable, and transparent ledger, has been integrated with artificial intelligence in knowledge-based networks to improve diverse high-level networking functions such as network administration, traffic optimization, service provisioning, security and privacy, etc. These existing blockchain-based applications in knowledge-based networks were reviewed, and this survey proves that blockchain has been successfully applied in diverse network applications. Finally, we critically discussed the benefits and challenges of implementing blockchain systems in knowledge-based networks.

This research adds a thorough analysis to the body of knowledge already available on the deployment of the blockchain system in Knowledge-Defined Networking. As we have identified generic and specific blockchain applications, it will be very helpful for future researchers to readily identify blockchain applications in KDN with reference to existing literature. This can open avenues for academicians to further investigate blockchain applications in new areas by obtaining insight into fields where blockchain has already

been applied. Furthermore, researchers can formulate innovative ideas to overcome the challenges of applying blockchain to intelligent networks.

The following propositions can be recommended when applying blockchain to Knowledge-Defined Networking:

- In blockchain systems integrated with KDN, as the handling and processing of big data were identified as challenges, alternative techniques for improving the handling and processing of big data in blockchain are recommended. These include sharding [394], compression, fragmentation of data, parallel processing [4], and using off-chain storage of data while storing metadata in the blockchain for verification [397];
- Blockchain systems consume excess energy, causing an additional burden on knowledge-based networking systems. Therefore, it is recommended to use an energy-efficient consensus approach such as PoS [97], DPoS [107], PBFT [103], etc.;
- As resource management is challenging in blockchain systems, it is recommended to use appropriate optimization [398] techniques to optimize resource management for efficient performance of tasks such as consensus;
- To promote interoperability between KDN systems that may utilize different blockchain frameworks, blockchain interoperability frameworks such as PIEChain [399], Interchain [400], etc. are recommended;
- It is advised to use a directed acyclic network to build blockchain with the aim of increasing its capacity for a growth-based approach having parallel processing capability [4]. Furthermore, lightweight and low-energy-consuming blockchain frameworks such as Sensor-Chain [393] can be utilized in KDN systems to improve scalability. Not only that, but off-chain storage [397] is also recommended to improve scalability;
- With the goal of reducing the extra latency imposed by blockchains, which makes the operation of the KDN system challenging, sharding and pruning [394] techniques are recommended;
- As conventional linear blockchains are well known for low transaction throughput, if such blockchains are employed in a KDN, it can limit the performance of the KDN system. Therefore, to obtain maximum performance from the KDN, high-throughput blockchain frameworks such as Conflux [396], which are based on the DAG blockchain, are recommended;
- To overcome the known security vulnerabilities of blockchain, different techniques can be recommended. First, in order to mitigate security attacks such as DDoS attack detection, ML algorithms can be utilized [401]. For preventing privacy exposure in sensitive data, strong encryption such as post-quantum cryptography with robust error detection and masking techniques is recommended, while to detect code vulnerabilities, the employment of AI and human experts is recommended;
- As blockchains cause additional resource expenditure in KDN systems, it is recommended to utilize intelligent networking with resource-efficient blockchain systems [13].

Firstly, this research's scope is limited to reviewing blockchain-based frameworks in Knowledge-Defined Networking domains. However, all types of networking applications of blockchain-based frameworks within Knowledge-Defined Networking domains with all forms of knowledge generation models are reviewed in this research. Finally, being a review article, this research does not explicitly propose and validate a blockchain-based framework for Knowledge-Defined Networking. However, this research proposes recommendations for a blockchain-based framework applied to Knowledge-Defined Networking, based on the challenges identified by surveying many existing, validated original research papers.

Blockchains can revolutionize the knowledge creation approach in KDN systems. In conventional KDN, knowledge is generated by a centralized authority. By integrating blockchain, knowledge can be created and disseminated in a dispersed and trustworthy way, allowing collaboration. Self-executing contracts can be utilized to automate network processes such as network management, access control, etc. Future research may include efficient and cost-effective techniques for intellectual property management, licensing, au-

thentication, etc. of intellectual property transactions within Knowledge-Defined Networks. Furthermore, future research may investigate how existing resources in KDN systems, such as machine learning frameworks that serve different network functions, may be leveraged to enhance the effectiveness of the underlying blockchain framework in order to make the two approaches more interoperable. Moreover, future research on blockchains deployed in KDNs may involve investigating efficient consensus approaches, cryptographic techniques, and optimization techniques. Additionally, quantum computing may be employed to improve the performance of both knowledge generation in KDN and computations related to blockchains for better performance of blockchain-based KDN frameworks.

Author Contributions: Conceptualization—P.A.D.S.N.W.; software—P.A.D.S.N.W.; validation—P.A.D.S.N.W.; formal analysis—P.A.D.S.N.W.; investigation—P.A.D.S.N.W.; resources—P.A.D.S.N.W.; writing original draft preparation—P.A.D.S.N.W.; writing review and editing—S.G.; visualization—P.A.D.S.N.W. and S.G.; supervision—S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research is part of a research project that principal and corresponding author Patikiri Arachchige Don Shehan Nilmantha Wijesekara is pursuing for a degree from the University of Ruhuna.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kim, S. Blockchain for a trust network among intelligent vehicles. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 43–68.
2. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability* **2017**, *9*, 2214. [CrossRef]
3. Park, J.; Park, K. A lightweight blockchain scheme for a secure smart dust IoT environment. *Appl. Sci.* **2020**, *10*, 8925. [CrossRef]
4. Lee, S.W.; Sim, K.B. Design and hardware implementation of a simplified DAG-based blockchain and new AES-CBC algorithm for IoT security. *Electronics* **2021**, *10*, 1127. [CrossRef]
5. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain consensus: An overview of alternative protocols. *Symmetry* **2021**, *13*, 1363. [CrossRef]
6. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
7. Yang, G.; Lee, K.; Lee, K.; Yoo, Y.; Lee, H.; Yoo, C. Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric. *IEEE Access* **2022**, *10*, 74902–74920. [CrossRef]
8. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
9. Singh, J.; Sajid, M.; Gupta, S.K.; Haidri, R.A. Artificial Intelligence and Blockchain Technologies for Smart City. In *Intelligent Green Technologies for Sustainable Smart Cities*; John Wiley & Sons: Hoboken, NJ, USA, 2022; pp. 317–330.
10. Marwala, T.; Xing, B. Blockchain and artificial intelligence. *arXiv* **2018**, arXiv:1802.04451.
11. Tagde, P.; Tagde, S.; Bhattacharya, T.; Tagde, P.; Chopra, H.; Akter, R.; Kaushik, D.; Rahman, M.H. Blockchain and artificial intelligence technology in e-Health. *Environ. Sci. Pollut. Res.* **2021**, *28*, 52810–52831. [CrossRef]
12. Fu, Y.; Li, C.; Yu, F.R.; Luan, T.H.; Zhao, P.; Liu, S. A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet Things J.* **2022**, *10*, 3587–3610. [CrossRef]
13. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A machine learning approach for blockchain-based smart home networks security. *IEEE Netw.* **2020**, *35*, 223–229. [CrossRef]
14. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283. [CrossRef]
15. Mishra, S.; AlShehri, M.A.R. Software defined networking: Research issues, challenges and opportunities. *Indian J. Sci. Technol.* **2017**, *10*, 1–9. [CrossRef]
16. Haji, S.H.; Zeebaree, S.R.; Saeed, R.H.; Ameen, S.Y.; Shukur, H.M.; Omar, N.; Sadeeq, M.A.; Ageed, Z.S.; Ibrahim, I.M.; Yasin, H.M. Comparison of software defined networking with traditional networking. *Asian J. Res. Comput. Sci.* **2021**, *9*, 1–18. [CrossRef]

17. Bhatia, J.; Modi, Y.; Tanwar, S.; Bhavsar, M. Software defined vehicular networks: A comprehensive review. *Int. J. Commun. Syst.* **2019**, *32*, e4005. [CrossRef]
18. Zhu, M.; Cai, Z.P.; Xu, M.; Cao, J.N. Software-defined vehicular networks: Opportunities and challenges. In *Energy Science and Applied Technology*; CRC Press: Boca Raton, FL, USA, 2015; pp. 247–251.
19. Nunes, B.A.A.; Mendonca, M.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
20. Islam, M.M.; Khan, M.T.R.; Saad, M.M.; Kim, D. Software-defined vehicular network (SDVN): A survey on architecture and routing. *J. Syst. Archit.* **2021**, *114*, 101961. [CrossRef]
21. Adbeb, T.; Wu, D.; Ibrar, M. Software-defined networking (SDN) based VANET architecture: Mitigation of traffic congestion. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 706–714. [CrossRef]
22. Liu, K.; Xu, X.; Chen, M.; Liu, B.; Wu, L.; Lee, V.C. A hierarchical architecture for the future internet of vehicles. *IEEE Commun. Mag.* **2019**, *57*, 41–47. [CrossRef]
23. Toufga, S.; Abdellatif, S.; Assouane, H.T.; Owezarski, P.; Villemur, T. Towards dynamic controller placement in software defined vehicular networks. *Sensors* **2020**, *20*, 1701. [CrossRef]
24. Tselios, C.; Politis, I.; Kotsopoulos, S. Enhancing SDN security for IoT-related deployments through blockchain. In Proceedings of the 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, Germany, 6–8 November 2017; pp. 303–308.
25. Fonseca, P.C.; Mota, E.S. A survey on fault management in software-defined networks. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2284–2321. [CrossRef]
26. Akhunzada, A.; Khan, M.K. Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues. *IEEE Commun. Mag.* **2017**, *55*, 110–118. [CrossRef]
27. Zhao, L.; Li, J.; Al-Dubai, A.; Zomaya, A.Y.; Min, G.; Hawbani, A. Routing schemes in software-defined vehicular networks: Design, open issues and challenges. *IEEE Intell. Transp. Syst. Mag.* **2020**, *13*, 217–226. [CrossRef]
28. Quan, W.; Cheng, N.; Qin, M.; Zhang, H.; Chan, H.A.; Shen, X. Adaptive transmission control for software defined vehicular networks. *IEEE Wirel. Commun. Lett.* **2018**, *8*, 653–656. [CrossRef]
29. Nisar, K.; Jimson, E.R.; Hijazi, M.H.A.; Welch, I.; Hassan, R.; Aman, A.H.M.; Sodhro, A.H.; Pirbhulal, S.; Khan, S. A survey on the architecture, application, and security of software defined networking: Challenges and open issues. *Internet Things* **2020**, *12*, 100289. [CrossRef]
30. Deveaux, D.; Higuchi, T.; Uçar, S.; Härri, J.; Altintas, O. A definition and framework for vehicular knowledge networking: An application of knowledge-centric networking. *IEEE Veh. Technol. Mag.* **2021**, *16*, 57–67. [CrossRef]
31. Ucar, S.; Higuchi, T.; Wang, C.H.; Deveaux, D.; Härri, J.; Altintas, O. Vehicular knowledge networking and application to risk reasoning. In Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, New York, NY, USA, 11–14 October 2020; pp. 351–356.
32. Ucar, S.; Higuchi, T.; Wang, C.H.; Deveaux, D.; Altintas, O.; Härri, J. Vehicular Knowledge Networking and Mobility-Aware Smart Knowledge Placement. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 593–598.
33. Ruta, M.; Scioscia, F.; Gramegna, F.; Ieva, S.; Di Sciascio, E.; De Vera, R.P. A knowledge fusion approach for context awareness in vehicular networks. *IEEE Internet Things J.* **2018**, *5*, 2407–2419. [CrossRef]
34. Wu, D.; Li, Z.; Wang, J.; Zheng, Y.; Li, M.; Huang, Q. Vision and challenges for knowledge centric networking. *IEEE Wirel. Commun.* **2019**, *6*, 117–123. [CrossRef]
35. Liu, J.; Xu, Q. Machine learning in software defined network. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 1114–1120.
36. Wijesekara, P.A.D.S.N. An Accurate Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka. *Res. Sq.* 2021, *Preprint*. [CrossRef]
37. Clark, D.D.; Partridge, C.; Ramming, J.C.; Wroclawski, J.T. A knowledge plane for the internet. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany, 5–29 August 2003; pp. 3–10.
38. Alzahrani, A.O.; Alenazi, M.J. Designing a network intrusion detection system based on machine learning for software defined networks. *Future Internet* **2021**, *13*, 111. [CrossRef]
39. Polat, H.; Polat, O.; Cetin, A. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability* **2020**, *12*, 1035. [CrossRef]
40. Dey, S.K.; Rahman, M.M. Effects of machine learning approach in flow-based anomaly detection on software-defined networking. *Symmetry* **2019**, *12*, 7 [CrossRef]
41. Yoo, Y.; Yang, G.; Shin, C.; Lee, J.; Yoo, C. Control Channel Isolation in SDN Virtualization: A Machine Learning Approach. In Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Bangalore, India, 1–4 May 2023; pp. 273–285.
42. Khan, M.I.; Aubet, F.X.; Pahl, M.O.; Härri, J. Deep learning-aided resource orchestration for vehicular safety communication. In Proceedings of the 2019 Wireless Days (WD), Manchester, UK, 24–26 April 2019; pp. 1–8.

43. Mohammed, A.R.; Mohammed, S.A.; Shirmohammadi, S. Machine learning and deep learning based traffic classification and prediction in software defined networking. In Proceedings of the 2019 IEEE International Symposium on Measurements & Networking (M&N), Catania, Italy, 8–10 July 2019; pp. 1–6.
44. Indira, B.; Valarmathi, K.; Devaraj, D. An approach to enhance packet classification performance of software-defined network using deep learning. *Soft Comput.* **2019**, *23*, 8609–8619. [CrossRef]
45. Wijesekara, P.A.D.S.N.; Sudheera, K.L.K.; Sandamali, G.G.N.; Chong, P.H.J. Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks. In Proceedings of the 20th Academic Sessions, Matara, Sri Lanka, 7 June 2023; p. 60.
46. Wijesekara, P.A.D.S.N.; Gunawardena, S. A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks. *Telecom* **2023**, *4*, 393–458. [CrossRef]
47. Toufga, S.; Abdellatif, S.; Owezarski, P.; Villemur, T.; Relizani, D. Effective prediction of V2I link lifetime and vehicle's next cell for software defined vehicular networks: A machine learning approach. In Proceedings of the 2019 IEEE Vehicular Networking Conference (VNC), Los Angeles, NV, USA, 4–6 December 2019; pp. 1–8.
48. Amari, H.; Louati, W.; Khoukhi, L.; Belguith, L.H. Securing software-defined vehicular network architecture against ddos attack. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 653–656.
49. Zhang, D.; Yu, F.R.; Yang, R. A machine learning approach for software-defined vehicular ad hoc networks with trust management. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–6
50. Latah, M.; Toker, L. Artificial intelligence enabled software-defined networking: A comprehensive overview. *IET Netw.* **2019**, *8*, 79–99.
51. Lu, W.; Liang, L.; Kong, B.; Li, B.; Zhu, Z. AI-assisted knowledge-defined network orchestration for energy-efficient data center networks. *IEEE Commun. Mag.* **2020**, *58*, 86–92. [CrossRef]
52. Hyun, J.; Van Tu N.; Hong, J.W.K. Towards knowledge-defined networking using in-band network telemetry. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; pp. 1–7.
53. Hu, Y.; Li, Z.; Lan, J.; Wu, J.; Yao, L. EARS: Intelligence-driven experiential network architecture for automatic routing in software-defined networking. *China Commun.* **2020**, *17*, 149–162. [CrossRef]
54. Gosh, S.; El Boudani, B.; Dagiuklas, T.; Iqbal, M. SO-KDN: A Self-Organised Knowledge Defined Networks Architecture for Reliable Routing. In Proceedings of the 4th International Conference on Information Science and Systems, Edinburgh, UK, 17–19 March 2021; pp. 160–166.
55. Rafiq, A.; Rehman, S.; Young, R.; Song, W.C.; Khan, M.A.; Kadry, S.; Srivastava, G. Knowledge defined networks on the edge for service function chaining and reactive traffic steering. *Clust. Comput.* **2023**, *26*, 613–634. [CrossRef]
56. Duque-Torres, A.; Amezquita-Suárez, F.; Caicedo Rendon, O.M.; Ordóñez, A.; Campo, W.Y. An approach based on knowledge-defined networking for identifying heavy-hitter flows in data center networks. *Appl. Sci.* **2019**, *9*, 4808. [CrossRef]
57. Herrera, L.M.C.; Torres, A.D.; Munoz, W.Y.C. An approach based on knowledge-defined networking for identifying video streaming flows in 5G networks. *IEEE Lat. Am. Trans.* **2021**, *19*, 1737–1744. [CrossRef]
58. Gheisari, M.; Ebrahimzadeh, F.; Rahimi, M.; Moazzamigodarzi, M.; Liu, Y.; Dutta Pramanik, P.K.; Heravi, M.A.; Mehbodniya, A.; Ghaderzadeh, M.; Feylizadeh, M.R.; et al. Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey. *CAAI Trans. Intell. Technol.* **2023**, 1–26. [CrossRef]
59. Sadoughi, F.; Ghaderzadeh, M.; Solimany, M.; Fein, R. An intelligent system based on back propagation neural network and particle swarm optimization for detection of prostate cancer from benign hyperplasia of prostate. *J. Health Med. Informat* **2014**, *5*, 1000158.
60. Ghaderzadeh, M.; Aria, M.; Hosseini, A.; Asadi, F.; Bashash, D.; Abolghasemi, H. A fast and efficient CNN model for B-ALL diagnosis and its subtypes classification using peripheral blood smear images. *Int. J. Intell. Syst.* **2022**, *37*, 5113–5133. [CrossRef]
61. Li, Y.; Su, X.; Ding, A.Y.; Lindgren, A.; Liu, X.; Prehofer, C.; Riekki, J.; Rahmani, R.; Tarkoma, S.; Hui, P. Enhancing the internet of things with knowledge-driven software-defined networking technology: Future perspectives. *Sensors* **2020**, *20*, 3459. [CrossRef]
62. Mestres, A.; Rodriguez-Natal, A.; Carner, J.; Barlet-Ros, P.; Alarcón, E.; Solé, M.; Muntés-Mulero, V.; Meyer, D.; Barkai, S.; Hibbett, M.J.; et al. Knowledge-defined networking. *ACM SIGCOMM Comput. Commun. Rev.* **2017**, *47*, 2–10. [CrossRef]
63. Yao, H.; Mai, T.; Xu, X.; Zhang, P.; Li, M.; Liu, Y. NetworkAI: An intelligent network architecture for self-learning control strategies in software defined networks. *IEEE Internet Things J.* **2018**, *5*, 4319–4327. [CrossRef]
64. Wijesekara, P.A.D.S.N.; Gunawardena, S. A Comprehensive Survey on Knowledge-Defined Networking. *Telecom* **2023**, *4*, 477–596.
65. Alharbi, T. Deployment of blockchain technology in software defined networks: A survey. *IEEE Access* **2020**, *8*, 9146–9156. [CrossRef]
66. Rahman, A.; Montieri, A.; Kundu, D.; Karim, M.R.; Islam, M.J.; Umme, S.; Nascita, A.; Pescapé, A. On the integration of blockchain and sdn: Overview, applications, and future perspectives. *J. Netw. Syst. Manag.* **2022**, *30*, 73.
67. Nam Nguyen, H.; Anh Tran, H.; Fowler, S.; Souihi, S. A survey of Blockchain technologies applied to software-defined networking: Research challenges and solutions. *IET Wirel. Sens. Syst.* **2021**, *11*, 233–247.
68. Miglani, A.; Kumar, N. Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review. *Comput. Commun.* **2021**, *178*, 37–63. [CrossRef]

69. Ismail, S.; Dawoud, D.W.; Reza, H. Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. *Future Internet* **2023**, *15*, 200. [CrossRef]
70. Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and machine° learning for future smart grids: A review. *Energies* **2023**, *16*, 528. [CrossRef]
71. Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H. Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. *Future Internet* **2023**, *15*, 83. [CrossRef]
72. Krichen, M.; Ammi, M.; Mihoub, A.; Almutiq, M. Blockchain for modern applications: A survey. *Sensors* **2022**, *22*, 5274. [CrossRef]
73. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
74. Ismail, L.; Materwala, H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
75. Son, B.; Lee, J.; Jang, H. A scalable IoT protocol via an efficient DAG-based distributed ledger consensus. *Sustainability* **2020**, *12*, 1529. [CrossRef]
76. Hellani, H.; Sliman, L.; Samhat, A.E.; Exposito, E. Computing resource allocation scheme for DAG-based IOTA nodes. *Sensors* **2021**, *21*, 4703. [CrossRef]
77. Gayoso Martinez, V.; Hernández-Álvarez, L.; Hernandez Encinas, L. Analysis of the cryptographic tools for blockchain and bitcoin. *Mathematics* **2020**, *8*, 131. [CrossRef]
78. Castellon, C.; Roy, S.; Kreidl, P.; Dutta, A.; Bölöni, L. Energy efficient merkle trees for blockchains. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021; pp. 1093–1099.
79. Ngabo, D.; Wang, D.; Iwendi, C.; Anajemba, J.H.; Ajao, L.A.; Biamba, C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics* **2021**, *10*, 2110. [CrossRef]
80. Fang, W.; Chen, W.; Zhang, W.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 56. [CrossRef]
81. Nawaz, A.; Peña Queralta, J.; Guan, J.; Awais, M.; Gia, T.N.; Bashir, A.K.; Kan, H.; Westerlund, T. Edge computing to secure iot data ownership and trade with the ethereum blockchain. *Sensors* **2020**, *20*, 3965. [CrossRef] [PubMed]
82. Khanal, Y.P.; Alsadoon, A.; Shahzad, K.; Al-Khalil, A.B.; Prasad, P.W.; Rehman, S.U.; Islam, R. Utilizing blockchain for iot privacy through enhanced ECIES with secure hash function. *Future Internet* **2022**, *14*, 77. [CrossRef]
83. Seok, B.; Park, J.; Park, J.H. A lightweight hash-based blockchain architecture for industrial IoT. *Appl. Sci.* **2019**, *9*, 3740. [CrossRef]
84. Pop, C.D.; Antal, M.; Cioara, T.; Anghel, I.; Salomie, I. Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. *Sensors* **2020**, *20*, 5678. [CrossRef] [PubMed]
85. Gupta, S.; Gupta, K.K.; Shukla, P.K.; Shrivas, M.K. Blockchain-based voting system powered by post-quantum cryptography (BBVSP-pqc). In Proceedings of the 2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 1–3 March 2022; pp. 1–8.
86. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M.; Beshaj, L. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. In Proceedings of the International Conference on Information Security and Cryptology, Seoul, Republic of Korea, 30 November 2022–2 December 2022; pp. 292–314.
87. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M. Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. *IEEE Trans. Circuits Syst. I: Regul. Pap.* **2021**, *68*, 4129–4141. [CrossRef]
88. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In Proceedings of the International Conference on Security and Privacy in Communication Systems, virtual event, 6–9 September 2021; pp. 424–440.
89. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. Cryptographic accelerators for digital signature based on Ed25519. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 1297–1305. [CrossRef]
90. Jalali, A.; Azarderakhsh, R.; Kermani, M.M.; Jao, D. Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 902–912. [CrossRef]
91. Kaur, J.; Sarker, A.; Kermani, M.M.; Azarderakhsh, R. Hardware Constructions for Error Detection in Lightweight Welch-Gong (WG)-Oriented Streamcipher WAGE Benchmarked on FPGA. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1208–1215. [CrossRef]
92. Kermani, M.M.; Azarderakhsh, R.; Xie, J. Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes. In Proceedings of the 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, Taiwan, 19–20 December 2016; pp. 1–6.
93. Aghaie, A.; Kermani, M.M.; Azarderakhsh, R. Fault diagnosis schemes for low-energy block cipher Midori benchmarked on FPGA. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2016**, *25*, 1528–1536. [CrossRef]
94. Kaur, J.; Kermani, M.M.; Azarderakhsh, R. Hardware constructions for lightweight cryptographic block cipher QARMA with error detection mechanisms. *IEEE Trans. Emerg. Top. Comput.* **2020**, *10*, 514–519. [CrossRef]
95. Kermani, M.M.; Azarderakhsh, R. Lightweight hardware architectures for fault diagnosis schemes of efficiently-maskable cryptographic substitution boxes. In Proceedings of the 2016 IEEE International Conference on Electronics, Circuits and Systems (ICECS), Monte Carlo, Monaco, 11–14 December 2016; pp. 764–767.

96. Sapra, N.; Shaikh, I.; Dash, A. Impact of proof of work (PoW)-Based blockchain applications on the environment: A systematic review and research agenda. *J. Risk Financ. Manag.* **2023**, *16*, 218. [CrossRef]
97. Karpinski, M.; Kovalchuk, L.; Kochan, R.; Oliynykov, R.; Rodinko, M.; Wieclaw, L. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. *Sensors* **2021**, *21*, 6408. [CrossRef] [PubMed]
98. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Perform. Eval. Rev.* **2014**, *42*, 34–37. [CrossRef]
99. Park, S.; Kwon, A.; Fuchsbauer, G.; Gaži, P.; Alwen, J.; Pietrzak, K. Spacemint: A cryptocurrency based on proofs of space. In Proceedings of the Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, 26 February–2 March 2018; pp. 480–499.
100. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-burn. In Proceedings of the Financial Cryptography and Data Security: 24th International Conference, FC, Kota Kinabalu, Malaysia, 10–14 February 2020; pp. 523–540.
101. Manolache, M.A.; Manolache, S.; Tapus, N. Decision making using the blockchain proof of authority consensus. *Procedia Comput. Sci.* **2022**, *199*, 580–588. [CrossRef]
102. Chen, L.; Xu, L.; Shah, N.; Gao, Z.; Lu, Y.; Shi, W. On security analysis of proof-of-elapsed-time (poet). In Proceedings of the Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, 5–8 November 2017; pp. 282–297.
103. Feng, L.; Zhang, H.; Chen, Y.; Lou, L. Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. *Appl. Sci.* **2018**, *8*, 1919. [CrossRef]
104. Ma, F.Q.; Li, Q.L.; Liu, Y.H.; Chang, Y.X. Stochastic performance modeling for practical byzantine fault tolerance consensus in the blockchain. *Peer-to-Peer Netw. Appl.* **2022**, *15*, 2516–2528. [CrossRef]
105. Zhan, Y.; Wang, B.; Lu, R.; Yu, Y. DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains. *Inf. Sci.* **2021**, *559*, 8–21. [CrossRef]
106. Huang, D.; Ma, X.; Zhang, S. Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 172–181. [CrossRef]
107. Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2022**, *15*, 4. [CrossRef]
108. Saad, S.M.S.; Radzi, R.Z.R.M. Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *Int. J. Innov. Comput.* **2020**, *10*, 27–32. [CrossRef]
109. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July 2018–2 August 2018; pp. 1–11.
110. Rahulamathavan, Y.; Phan, R.C.W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.
111. Deshpande, V.; Badis, H.; George, L. BTCmap: Mapping bitcoin peer-to-peer network topology. In Proceedings of the 2018 IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), Toulouse, France, 26–28 September 2018; pp. 1–6.
112. Gao, Y.; Shi, J.; Wang, X.; Tan, Q.; Zhao, C.; Yin, Z. Topology measurement and analysis on ethereum p2p network. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June–3 July 2019; pp. 1–7.
113. Kumar, R.; Tripathi, R. Blockchain-based framework for data storage in peer-to-peer scheme using interplanetary file system. In *Handbook of Research on Blockchain Technology*; Academic Press: Cambridge, MA, USA, 2020; pp. 35–59.
114. Zhu, Y.; Qin, Y.; Gan, G.; Shuai, Y.; Chu, W.C.C. TBAC: Transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 1, pp. 535–544.
115. Hashemi Joo, M.; Nishikawa, Y.; Dandapani, K. Cryptocurrency, a successful application of blockchain technology. *Manag. Financ.* **2020**, *46*, 715–733. [CrossRef]
116. Taherdoost, H. Smart Contracts in Blockchain Technology: A Critical Review. *Information* **2023**, *14*, 117. [CrossRef]
117. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Appl. Sci.* **2020**, *10*, 488. [CrossRef]
118. Krichen, M.; Lahami, M.; Al–Haija, Q.A. Formal methods for the verification of smart contracts: A review. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8.
119. Abdellatif, T.; Brousmiche, K.L. Formal verification of smart contracts based on users and blockchain behaviors models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
120. Litke, A.; Anagnostopoulos, D.; Varvarigou, T. Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. *Logistics* **2019**, *3*, 5. [CrossRef]
121. Bamakan, S.M.H.; Moghaddam, S.G.; Manshadi, S.D. Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. *J. Clean. Prod.* **2021**, *302*, 127021. [CrossRef]

122. Srivastava, P.R.; Zhang, J.Z.; Eachempati, P. Blockchain technology and its applications in agriculture and supply chain management: A retrospective overview and analysis. *Enterp. Inf. Syst.* **2023**, *17*, 1995783. [CrossRef]
123. Yuan, M.; Xu, Y.; Zhang, C.; Tan, Y.; Wang, Y.; Ren, J.; Zhang, Y. TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 3489–3500. [CrossRef]
124. Alphand, O.; Amoretti, M.; Claeys, T.; Dall'Asta, S.; Duda, A.; Ferrari, G.; Rousseau, F.; Tourancheau, B.; Veltri, L.; Zanichelli, F. IoTChain: A blockchain security architecture for the Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
125. Keshavarz, M.; Gharib, M.; Afghah, F.; Ashdown, J.D. UASTrustChain: A decentralized blockchain-based trust monitoring framework for autonomous unmanned aerial systems. *IEEE Access* **2020**, *8*, 226074–226088. [CrossRef]
126. Tsang, Y.P.; Wu, C.H.; Ip, W.H.; Shiau, W.L. Exploring the intellectual cores of the blockchain–Internet of Things (BIoT). *J. Enterp. Inf. Manag.* **2021**, *34*, 1287–1317. [CrossRef]
127. Sahoo, M.; Singhar, S.S.; Sahoo, S.S. A blockchain based model to eliminate drug counterfeiting. In Proceedings of the Machine Learning and Information Processing: Proceedings of ICMLIP 2019, Pune, India, 27–28 December 2019; pp. 213–222.
128. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef] [PubMed]
129. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
130. Bhamidipati, N.R.; Vakkavanthula, V.; Stafford, G.; Dahir, M.; Neupane, R.; Bonnah, E.; Wang, S.; Murthy, J.V.R.; Hoque, K.A.; Calyam, P. Claimchain: Secure blockchain platform for handling insurance claims processing. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; pp. 55–64.
131. Roriz, R.; Pereira, J.L. Avoiding insurance fraud: A blockchain-based solution for the vehicle sector. *Procedia Comput. Sci.* **2019**, *164*, 211–218. [CrossRef]
132. Johnson, O. Decentralized Reinsurance: Funding blockchain-based parametric bushfire insurance. In Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), virtual event, 2–5 May 2022; pp. 1–3.
133. Yang, Y.; Guan, Z.; Wan, Z.; Weng, J.; Pang, H.H.; Deng, R.H. Priscore: Blockchain-based self-tallying election system supporting score voting. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4705–4720. [CrossRef]
134. Pawlak, M.; Guziur, J.; Poniszewska-Marańda, A. Voting process with blockchain technology: Auditable blockchain voting system. In Proceedings of the Advances in Intelligent Networking and Collaborative Systems: The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018), Bratislava, Slovakia, 5–7 September 2018; pp. 233–244.
135. Song, H.; Zhu, N.; Xue, R.; He, J.; Zhang, K.; Wang, J. Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Inf. Process. Manag.* **2021**, *58*, 102507. [CrossRef]
136. Rambhia, V.; Mehta, V.; Mehta, R.; Shah, R.; Patel, D. Intellectual Property Rights Management Using Blockchain. In Proceedings of the Information and Communication Technology for Competitive Strategies (ICTCS 2020): Intelligent Strategies for ICT, Jaipur, India, 11–12 December 2020; pp. 545–552.
137. Li, Z.; Barenji, A.V.; Huang, G.Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robot. Comput. Integr. Manuf.* **2018**, *54*, 133–144. [CrossRef]
138. Yu, K.; Tan, L.; Aloqaily, M.; Yang, H.; Jararweh, Y. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7669–7678. [CrossRef]
139. Xu, J.J. Are blockchains immune to all malicious attacks? *Financ. Innov.* **2016**, *2*, 1–9. [CrossRef]
140. Ramachandran, G.S.; Wright, K.L.; Zheng, L.; Navaney, P.; Naveed, M.; Krishnamachari, B.; Dhaliwal, J. Trinity: A byzantine fault-tolerant distributed publish-subscribe system with immutable blockchain-based persistence. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; pp. 227–235.
141. Kanza, Y.; Safra, E. Cryptotransport: Blockchain-powered ride hailing while preserving privacy, pseudonymity and trust. In Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Seattle, WA, USA, 6–9 November 2018; pp. 540–543.
142. Aggarwal, S.; Kumar, N. Attacks on blockchain. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 399–410.
143. Coppolino, L.; D'Antonio, S.; Mazzeo, G.; Romano, L.; Campegiani, P. Facing the Blockchain Endpoint Vulnerability, an SGX-based Solution for Secure eHealth Auditing. In Proceedings of the ITASEC, virtual event, 7–9 April 2021; pp. 298–308.
144. Jang, J.; Lee, H.N. Profitable double-spending attacks. *Appl. Sci.* **2020**, *10*, 8477. [CrossRef]
145. Bai, Q.; Zhou, X.; Wang, X.; Xu, Y.; Wang, X.; Kong, Q. A deep dive into blockchain selfish mining. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
146. Poston, H. Mapping the OWASP top ten to blockchain. *Procedia Comput. Sci.* **2020**, *177*, 613–617. [CrossRef]
147. Juels, A.; Kosba, A.; Shi, E. The ring of gyges: Investigating the future of criminal smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 24–28 October 2016; pp. 283–295.
148. Ruf, P.; Stodt, J.; Reich, C. Security threats of a blockchain-based platform for industry ecosystems in the cloud. In Proceedings of the 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, UK, 29–30 July 2021; pp. 192–199.

149. Pahlajani, S.; Kshirsagar, A.; Pachghare, V. Survey on private blockchain consensus algorithms. In Proceedings of the 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 25–26 April 2019; pp. 1–6.
150. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **2021**, *182*, 103035. [CrossRef]
151. Jidong, L.; Xueqiang, L.; Yang, J.; Guolin, L. Consensus Mechanisms of Consortium Blockchain: A Survey. *Data Anal. Knowl. Discov.* **2021**, *5*, 56–65.
152. Herath, H.M.D.P.M.; Weraniyagoda, W.A.S.A.; Rajapaksha, R.T.M.; Wijesekara, P.A.D.S.N.; Sudheera, K.L.K.; Chong, P.H.J. Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies. *Sensors* **2022**, *22*, 6966. [CrossRef]
153. Wijesekara, P.A.D.S.N. Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving. *Open Transp. J.* **2022**, *16*, e187444782208191. [CrossRef]
154. Zins, C. Conceptual approaches for defining data, information, and knowledge. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *58*, 479–493. [CrossRef]
155. Sieber, C.; Blenk, A.; Basta, A.; Hock, D.; Kellerer, W. Towards a programmable management plane for SDN and legacy networks. In Proceedings of the 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, Republic of Korea, 6–10 June 2016; pp. 319–327
156. Sezer, S.; Scott-Hayward, S.; Chouhan, P.K.; Fraser, B.; Lake, D.; Finnegan, J.; Viljoen, N.; Miller, M.; Rao, N. Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Commun. Mag.* **2013**, *51*, 36–43. [CrossRef]
157. da Costa Cordeiro, W.L.; Marques, J.A.; Gaspary, L.P. Data plane programmability beyond openflow: Opportunities and challenges for network and service operations and management. *J. Netw. Syst. Manag.* **2017**, *25*, 784–818. [CrossRef]
158. Li, T.; Chen, J.; Fu, H. Application scenarios based on SDN: An overview. *J. Phys. Conf. Ser.* **2019**, *1187*, 052067. [CrossRef]
159. Trammell, B.; Casas, P.; Rossi, D.; Bär, A.; Houidi, Z.B.; Leontiadis, I.; Szemethy, T.; Mellia, M. mPlane: An intelligent measurement plane for the internet. *IEEE Commun. Mag.* **2014**, *52*, 148–156. [CrossRef]
160. David, L.; Keeney, J.; O'Sullivan, D.; Guo, S. Towards a managed extensible control plane for knowledge-based networking. In Proceedings of the Large Scale Management of Distributed Systems: 17th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, DSOM, Dublin, Ireland, 23–25 October 2006; pp. 98–111.
161. Jevsikova, T.; Berniukevičius, A.; Kurilovas, E. Application of resource description framework to personalise learning: Systematic review and methodology. *Inform. Educ.* **2017**, *16*, 61–82. [CrossRef]
162. Wijesekara, P.A.D.S.N.; Wang, Y.K. A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka. *COVID* **2022**, *2*, 793–826. [CrossRef]
163. Wijesekara, P.A.D.S.N. A study in University of Ruhuna for investigating prevalence, risk factors and remedies for psychiatric illnesses among students. *Sci. Rep.* **2022**, *12*, 12763. [CrossRef]
164. Seneviratne, C.; Wijesekara, P.A.D.S.N.; Leung, H. Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks. *Sensors* **2020**, *20*, 567. [CrossRef] [PubMed]
165. Tudorache, T.; Nyulas, C.; Noy, N.F.; Musen, M.A. WebProtégé: A collaborative ontology editor and knowledge acquisition tool for the web. *Semant. Web* **2013**, *4*, 89–99. [CrossRef]
166. Hayes, P.; Menzel, C. A semantics for the knowledge interchange format. In Proceedings of the IJCAI 2001 Workshop on the IEEE Standard Upper Ontology, Seattle, WA, USA, 4–6 August 2001; Volume 145, p. 145.
167. Fensel, D.; Van Harmelen, F.; Horrocks, I.; McGuinness, D.L.; Patel-Schneider, P.F. OIL: An ontology infrastructure for the semantic web. *IEEE Intell. Syst.* **2001**, *16*, 38–45. [CrossRef]
168. McBride, B. The resource description framework (RDF) and its vocabulary description language RDFS. In *Handbook on Ontologies*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 51–65.
169. Antoniou, G.; Harmelen, F.V. Web ontology language: Owl. In *Handbook on Ontologies*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 91–110.
170. Jarvis, M.P.; Goss, N.-J.; Neil, T.H. Applying machine learning techniques to rule generation in intelligent tutoring systems. In Proceedings of the Intelligent Tutoring Systems: 7th International Conference, ITS 2004, Maceió, Alagoas, Brazil, 30 August–3 September 2004; pp. 541–553.
171. Boley, H.; Tabet, S.; Wagner, G. Design rationale for RuleML: A markup language for semantic web rules. In Proceedings of the SWWS, Stanford, CA, USA, 30 July–1 August 2001; Volume 1, pp. 381–401.
172. Kifer, M. Rule interchange format: The framework. In Proceedings of the Web Reasoning and Rule Systems: Second International Conference, RR 2008, Karlsruhe, Germany, 31 October–1 November 2008; pp. 1–11.
173. Horrocks, I.; Patel-Schneider, P.F.; Boley, H.; Tabet, S.; Grosof, B.; Dean, M. SWRL: A semantic web rule language combining OWL and RuleML. *W3C Memb. Submiss.* **2004**, *21*, 1–31.
174. Liu, D.; Gu, T.; Xue, J.P. Rule engine based on improvement rete algorithm. In Proceedings of the 2010 International Conference on Apperceiving Computing and Intelligence Analysis Proceeding, Chengdu, China, 17–19 December 2010; pp. 346–349.
175. Jang, M.; Sohn, J.C. Bossam: An extended rule engine for OWL inferencing. In *Rules and Rule Markup Languages for the Semantic Web: Third International Workshop, RuleML 2004, Hiroshima, Japan, 8 November 2004*; Proceedings 3; Springer: Berlin/Heidelberg, Germany, 2004; pp. 128–138.

176. Friedman-Hill, E. Jess, the rule engine for the java platform. Available online: http://alvarestech.com/temp/fuzzyjess/Jess60/Jess70b7/docs/index.html (accessed on 6 June 2023).
177. Proctor, M. Drools: A rule engine for complex event processing. In *Applications of Graph Transformations with Industrial Relevance: 4th International Symposium, AGTIVE 2011, Budapest, Hungary, 4–7 October 2011*; Revised Selected and Invited Papers 4; Springer: Berlin/Heidelberg, Germany, 2011; p. 2.
178. Barbieri, D.F.; Braga, D.; Ceri, S.; VALLE, E.D.; Grossniklaus, M. C-SPARQL: A continuous query language for RDF data streams. *Int. J. Semant. Comput.* **2010**, *4*, 3–25. [CrossRef]
179. Taelman, R.; Vander Sande, M.; Verborgh, R. GraphQL-LD: Linked data querying with GraphQL. In Proceedings of the ISWC2018, 17th International Semantic Web Conference, Monterey, CA, USA, 8–12 October 2018; pp. 1–4.
180. O'Connor, M.J.; Das, A.K. SQWRL: A query language for OWL. In Proceedings of the OWLED, Chantilly, VA, USA, 23–24 October 2009; Volume 529, pp. 1–8.
181. Liu, P.; Wang, X.; Fu, Q.; Yang, Y.; Li, Y.F.; Zhang, Q. KGVQL: A knowledge graph visual query language with bidirectional transformations. *Knowl.-Based Syst.* **2022**, *250*, 108870. [CrossRef]
182. Finin, T.; McKay, D.P.; Fritzson, R.; McEntire, R. KQML: An information and knowledge exchange protocol. In *Knowledge Building and Knowledge Sharing*; IOS Press: Amsterdam, The Netherlands, 1994.
183. Sieber, C.; Blenk, A.; Hock, D.; Scheib, M.; Höhn, T.; Köhler, S.; Kellerer, W. Network configuration with quality of service abstractions for SDN and legacy networks. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 1135–1136.
184. Narisetty, R.; Dane, L.; Malishevskiy, A.; Gurkan, D.; Bailey, S.; Narayan, S.; Mysore, S. OpenFlow configuration protocol: Implementation for the of management plane. In Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop, Salt Lake, UT, USA, 20–22 March 2013; pp. 66–67.
185. Safrianti, E.; Sari, L.O.; Sari, N.A. Real-Time Network Device Monitoring System with Simple Network Management Protocol (SNMP) Model. In Proceedings of the 2021 3rd International Conference on Research and Academic Community Services (ICRACOS), Surabaya, Indonesia, 9–10 October 2021; pp. 122–127.
186. Ballani, H.; Francis, P. Conman: A step towards network manageability. *ACM SIGCOMM Comput. Commun. Rev.* **2007**, *37*, 205–216. [CrossRef]
187. Chen, X.; Mao, Z.M.; Van der Merwe, J. PACMAN: A platform for automated and controlled network operations and configuration management. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, Rome, Italy, 1–4 December 2009; pp. 277–288.
188. Chowdhury, S.R.; Bari, M.F.; Ahmed, R.; Boutaba, R. Payless: A low cost network monitoring framework for software defined networks. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–9.
189. Sun, P.; Yu, M.; Freedman, M.J.; Rexford, J.; Walker, D. Hone: Joint host-network traffic management in software-defined networks. *J. Netw. Syst. Manag.* **2015**, *23*, 374–399. [CrossRef]
190. Van Adrichem, N.L.; Doerr, C.; Kuipers, F.A. Opennetmon: Network monitoring in openflow software-defined networks. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–8.
191. Suh, J.; Kwon, T.T.; Dixon, C.; Felter, W.; Carter, J. Opensample: A low-latency, sampling-based measurement platform for commodity sdn. In Proceedings of the 2014 IEEE 34th International Conference on Distributed Computing Systems, Madrid, Spain, 30 June–3 July 2014; pp. 228–237.
192. Wijesekara, P.A.D.S.N.; Sudheera, K.L.K.; Sandamali, G.G.N.; Chong, P.H.J. An Optimization Framework for Data Collection in Software Defined Vehicular Networks. *Sensors* **2023**, *23*, 1600. [CrossRef] [PubMed]
193. Wette, P.; Karl, H. Which flows are hiding behind my wildcard rule? adding packet sampling to OpenFlow. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 12–16 August 2013; pp. 541–542.
194. Zhou, D.; Yan, Z.; Liu, G.; Atiquzzaman, M. An adaptive network data collection system in sdn. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *6*, 562–574. [CrossRef]
195. Liao, W.H.; Kuai, S.C. An energy-efficient sdn-based data collection strategy for wireless sensor networks. In Proceedings of the 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2), Kanazawa, Japan, 22–25 November 2017; pp. 91–97.
196. Bjorklund, M. YANG-a data modeling language for the network configuration protocol (NETCONF). Available online: https://www.rfc-editor.org/rfc/rfc6020 (accessed on 5 June 2023)
197. Uslar, M.; Specht, M.; Rohjans, S.; Trefke, J.; González, J.M. *The Common Information Model CIM: IEC 61968/61970 and 62325-A Practical Introduction to the CIM*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012.
198. Atutxa, A.; Franco, D.; Sasiain, J.; Astorga, J.; Jacob, E. Achieving low latency communications in smart industrial networks with programmable data planes. *Sensors* **2021**, *21*, 5199. [CrossRef] [PubMed]
199. Wijesekara, P.A.D.S.N.; Sangeeth, W.M.A.K.; Perera, H.S.C.; Jayasundere, N.D. Underwater Acoustic Digital Communication Channel for an UROV. In Proceedings of the 5th Annual Research Symposium (ARS2018), Hapugala, Sri Lanka, 4 January 2018; p. E17.
200. Paliwal, M.; Shrimankar, D.; Tembhurne, O. Controllers in SDN: A review report. *IEEE Access* **2018**, *6*, 36256–36270. [CrossRef]

201. Haleplidis, E.; Salim, J.H.; Halpern, J.M.; Hares, S.; Pentikousis, K.; Ogawa, K.; Wang, W.; Denazis, S.; Koufopavlou, O. Network programmability with ForCES. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1423–1440. [CrossRef]
202. Shalimov, A.; Zuikov, D.; Zimarina, D.; Pashkov, V.; Smeliansky, R. Advanced study of SDN/OpenFlow controllers. In Proceedings of the 9th Central & Eastern European Software Engineering Conference in Russia, Moscow, Russia, 24–25 October 2013; pp. 1–6.
203. Li, S.; Hu, D.; Fang, W.; Ma, S.; Chen, C.; Huang, H.; Zhu, Z. Protocol oblivious forwarding (POF): Software-defined networking with enhanced programmability. *IEEE Netw.* **2017**, *31*, 58–66. [CrossRef]
204. Eadala, S.Y.; Nagarajan, V. A review on deployment architectures of path computation element using software defined networking paradigm. *Indian J. Sci. Technol.* **2016**, *9*, 1–10. [CrossRef]
205. Bianchi, G.; Bonola, M.; Capone, A.; Cascone, C. Openstate: Programming platform-independent stateful openflow applications inside the switch. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 44–51. [CrossRef]
206. Ijari, P. Comparison between Cisco ACI and VMWARE NSX. *IOSR J. Comput. Eng. (IOSR-JCE)* **2017**, *19*, 70–72. [CrossRef]
207. Hasan, K.; Ahmed, K.; Biswas, K.; Islam, M.S.; Kayes, A.S.M.; Islam, S.R. Control plane optimisation for an SDN-based WBAN framework to support healthcare applications. *Sensors* **2020**, *20*, 4200. [CrossRef] [PubMed]
208. Gude, N.; Koponen, T.; Pettit, J.; Pfaff, B.; Casado, M.; McKeown, N.; Shenker, S. NOX: Towards an operating system for networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 105–110. [CrossRef]
209. Rowshanrad, S.; Abdi, V.; Keshtgari, M. Performance evaluation of SDN controllers: Floodlight and OpenDaylight. *IIUM Eng. J.* **2016**, *17*, 47–57. [CrossRef]
210. Sanvito, D.; Moro, D.; Gulli, M.; Filippini, I.; Capone, A.; Campanella, A. ONOS Intent Monitor and Reroute service: Enabling plug&play routing logic. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 272–276.
211. Voellmy, A.; Kim, H.; Feamster, N. Procera: A language for high-level reactive network control. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 13 August 2012; pp. 43–48.
212. Rotsos, C.; King, D.; Farshad, A.; Bird, J.; Fawcett, L.; Georgalas, N.; Gunkel, M.; Shiomoto, K.; Wang, A.; Mauthe, A.; et al. Network service orchestration standardization: A technology survey. *Comput. Stand. Interfaces* **2017**, *54*, 203–215. [CrossRef]
213. Bannour, F.; Souihi, S.; Mellouk, A. Distributed SDN control: Survey, taxonomy, and challenges. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 333–354. [CrossRef]
214. Koponen, T.; Casado, M.; Gude, N.; Stribling, J.; Poutievski, L.; Zhu, M.; Ramanathan, R.; Iwata, Y.; Inoue, H.; Hama, T.; et al. Onix: A distributed control platform for large-scale production networks. In Proceedings of the OSDI, Vancouver, BC, Canada, 4–6 October 2010; Volume 10, p. 6.
215. Vahlenkamp, M.; Schneider, F.; Kutscher, D.; Seedorf, J. Enabling information centric networking in IP networks using SDN. In Proceedings of the 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November 2013; pp. 1–6.
216. Sheikh, M.N.A.; Halder, M. SDN-Based approach to evaluate the best controller: Internal controller NOX and external controllers POX, ONOS, RYU. *Glob. J. Comput. Sci. Technol.* **2019**, *19*, 21–32. [CrossRef]
217. Banikazemi, M.; Olshefski, D.; Shaikh, A.; Tracey, J.; Wang, G. Meridian: An SDN platform for cloud network services. *IEEE Commun. Mag.* **2013**, *51*, 120–127. [CrossRef]
218. Botelho, F.; Bessani, A.; Ramos, F.M.; Ferreira, P. On the design of practical fault-tolerant SDN controllers. In Proceedings of the 2014 Third EUROPEAN Workshop on Software Defined Networks, Budapest, Hungary, 1–3 September 2014; pp. 73–78.
219. Hassas Yeganeh, S.; Ganjali, Y. Kandoo: A framework for efficient and scalable offloading of control applications. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 13 August 2012; pp. 19–24.
220. Fu, Y.; Bi, J.; Gao, K.; Chen, Z.; Wu, J.; Hao, B. Orion: A hybrid hierarchical control plane of software-defined networking for large-scale networks. In Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols, Raleigh, NC, USA, 21–24 October 2014; pp. 569–576.
221. Curtis, A.R.; Mogul, J.C.; Tourrilhes, J.; Yalagandula, P.; Sharma, P.; Banerjee, S. DevoFlow: Scaling flow management for high-performance networks. In Proceedings of the ACM SIGCOMM 2011 Conference, Toronto, ON, Canada, 15–19 August 2011; pp. 254–265.
222. Vissicchio, S.; Vanbever, L.; Rexford, J. Sweet little lies: Fake topologies for flexible routing. In Proceedings of the ACM Workshop on Hot Topics in Networks, Los Angeles, CA, USA, 27–28 October 2014; pp. 1–7.
223. Huang, S.; Zhao, J.; Wang, X. HybridFlow: A lightweight control plane for hybrid SDN in enterprise networks. In Proceedings of the 2016 IEEE/ACM 24th International Symposium on Quality of Service (IWQoS), Beijing, China, 20–21 June 2016; pp. 1–2.
224. Phemius, K.; Bouet, M.; Leguay, J. DISCO: Distributed SDN controllers in a multi-domain environment. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–2.
225. Santos, M.A.; Nunes, B.A.; Obraczka, K.; Turletti, T.; De Oliveira, B.T.; Margi, C.B. Decentralizing SDN's control plane. In Proceedings of the 39th Annual IEEE Conference on Local Computer Networks, Edmonton, AB, Canada, 8–11 September 2014; pp. 402–405.
226. Stringer, J.; Pemberton, D.; Fu, Q.; Lorier, C.; Nelson, R.; Bailey, J.; Corrêa, C.N.; Rothenberg, C.E. Cardigan: SDN distributed routing fabric going live at an Internet exchange. In Proceedings of the 2014 IEEE Symposium on Computers and Communications (ISCC), Funchal, Portugal, 23–26 June 2014; pp. 1–7.

227. Zhu, M.; Cao, J.; Pang, D.; He, Z.; Xu, M. SDN-based routing for efficient message propagation in VANET. In *Wireless Algorithms, Systems, and Applications: 10th International Conference 2015, WASA 2015, Qufu, China, 10–12 August 2015*; Proceedings 10; Springer International Publishing: Cham, Switzerland, 2015; pp. 788–797.
228. Moghaddam, F.F.; Wieder, P.; Yahyapour, R. Policy Engine as a Service (PEaaS): An approach to a reliable policy management framework in cloud computing environments. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 137–144
229. Chen, Y.J.; Wang, L.C.; Lin, F.Y.; Lin, B.S.P. Deterministic quality of service guarantee for dynamic service chaining in software defined networking. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 991–1002. [CrossRef]
230. Yang, G.; Jin, H.; Kang, M.; Moon, G.J.; Yoo, C. Network monitoring for SDN virtual networks. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications, virtual event, 6–9 July 2020; pp. 1261–1270.
231. Ahvar, E.; Ahvar, S.; Raza, S.M.; Manuel Sanchez Vilchez, J.; Lee, G.M. Next generation of SDN in cloud-fog for 5G and beyond-enabled applications: Opportunities and challenges. *Network* **2021**, *1*, 28–49. [CrossRef]
232. Voellmy, A.; Agarwal, A.; Hudak, P. *Nettle: Functional Reactive Programming for Openflow Networks*; Yale University Computer Science: New Haven, CT, USA, 2010.
233. Foster, N.; Freedman, M.J.; Harrison, R.; Rexford, J.; Meola, M.L.; Walker, D. Frenetic: A high-level language for OpenFlow networks. In Proceedings of the Workshop on Programmable Routers for Extensible Services of Tomorrow, Philadelphia, PA, USA, 30 November 2010; pp. 1–6.
234. Kim, H.; Reich, J.; Gupta, A.; Shahbaz, M.; Feamster, N.; Clark, R. Kinetic: Verifiable dynamic network control. In Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15), Oakland, CA, USA, 4–6 May 2015; pp. 59–72.
235. Wijesekara, P.A.D.S.N.; Sudheera, K.L.K.; Sandamali, G.G.N.; Chong, P.H.J. Data Gathering Optimization in Hybrid Software Defined Vehicular Networks. In Proceedings of the 20th Academic Sessions, Matara, Sri Lanka, 7 June 2023; p. 59.
236. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Bashir, A.K.; Tariq, U.; Yu, D.; Vasilakos, A.V. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. *IEEE Transactions on Intelligent Transportation Systems* **2021**, *23*, 683–700. [CrossRef]
237. Alam, T. Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things. *Wirel. Pers. Commun.* **2022**, *126*, 995–1011. [CrossRef]
238. Saba, T.; Haseeb, K.; Rehman, A.; Jeon, G. Blockchain-Enabled Intelligent IoT Protocol for High-Performance and Secured Big Financial Data Transaction. *IEEE Trans. Comput. Soc. Syst.* **2023**. [CrossRef]
239. Dai, Y.; Xu, D.; Maharjan, S.; Chen, Z.; He, Q.; Zhang, Y. Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Netw.* **2019**, *33*, 10–17. [CrossRef]
240. Guo, S.; Qi, Y.; Yu, P.; Xu, S.; Qi, F. When network operation meets blockchain: An artificial-intelligence-driven customization service for trusted virtual resources of IoT. *IEEE Netw.* **2020**, *34*, 46–53. [CrossRef]
241. Hu, S.; Liang, Y.C.; Xiong, Z.; Niyato, D. Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond. *IEEE Wirel. Commun.* **2021**, *28*, 145–151. [CrossRef]
242. Ayaz, F.; Sheng, Z.; Tian, D.; Nekovee, M.; Saeed, N. Blockchain-empowered AI for 6G-enabled Internet of Vehicles. *Electronics* **2022**, *11*, 3339. [CrossRef]
243. Mohammed, A.; Nahom, H.; Tewodros, A.; Habtamu, Y.; Hayelom, G. Deep reinforcement learning for computation offloading and resource allocation in blockchain-based multi-UAV-enabled mobile edge computing. In Proceedings of the 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 18–20 December 2020; pp. 295–299.
244. Leng, J.; Yan, D.; Liu, Q.; Xu, K.; Zhao, J.L.; Shi, R.; Wei, L.; Zhang, D.; Chen, X. ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 182–192. [CrossRef]
245. Chang, F.; Zhou, G.; Zhang, C.; Ding, K.; Cheng, W.; Chang, F. A maintenance decision-making oriented collaborative cross-organization knowledge sharing blockchain network for complex multi-component systems. *J. Clean. Prod.* **2021**, *282*, 124541. [CrossRef]
246. Li, G.; Dong, M.; Yang, L.T.; Ota, K.; Wu, J.; Li, J. Preserving edge knowledge sharing among IoT services: A blockchain-based approach. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 653–665. [CrossRef]
247. Chai, H.; Leng, S.; Chen, Y.; Zhang, K. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3975–3986. [CrossRef]
248. Li, Z.; Liu, X.; Wang, W.M.; Vatankhah Barenji, A.; Huang, G.Q. CKshare: Secured cloud-based knowledge-sharing blockchain for injection mold redesign. *Enterp. Inf. Syst.* **2019**, *13*, 1–33. [CrossRef]
249. Chai, H.; Leng, S.; Wu, F.; He, J. Secure and Efficient Blockchain-Based Knowledge Sharing for Intelligent Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 14620–14631. [CrossRef]
250. Balasubramaniam, A.; Gul, M.J.J.; Menon, V.G.; Paul, A. Blockchain for intelligent transport system. *IETE Tech. Rev.* **2021**, *38*, 438–449. [CrossRef]
251. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]

252. Feng, C.; Liu, B.; Yu, K.; Goudos, S.K.; Wan, S. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3582–3592. [CrossRef]
253. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.N.; Shorfuzzaman, M. Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073. [CrossRef]
254. Li, C.; Huang, Y.; Wu, Y.; Wang, X.; Tian, Y.; Wu, R.; Qu, F.; Wang, Z. Intelligent data sharing strategy supported by artificial intelligence and blockchain technology: Based on medical data. *Ann. Oper. Res.* **2023**, 1–25. [CrossRef]
255. Kumar, P.; Kumar, R.; Kumar, A.; Franklin, A.A.; Jolfaei, A. Blockchain and deep learning empowered secure data sharing framework for softwarized uavs. In Proceedings of the 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Republic of Korea, 16–20 May 2022; pp. 770–775.
256. Su, X.; Ullah, I.; Wang, M.; Choi, C. Blockchain-based system and methods for sensitive data transactions. *IEEE Consum. Electron. Mag.* **2021**. [CrossRef]
257. Zhang, H.; Li, G.; Zhang, Y.; Gai, K.; Qiu, M. Blockchain-based privacy-preserving medical data sharing scheme using federated learning. In Proceedings of the Knowledge Science, Engineering and Management: 14th International Conference, KSEM 2021, Tokyo, Japan, 14–16 August 2021; pp. 634–646.
258. Zhang, G.; Li, T.; Li, Y.; Hui, P.; Jin, D. Blockchain-based data sharing system for ai-powered network operations. *J. Commun. Inf. Netw.* **2018**, *3*, 1–8. [CrossRef]
259. Anita, N.; Vijayalakshmi, M.; and Shalinie, S.M. A Lightweight Scalable and Secure Blockchain Based IoT Using Fuzzy Logic. *Wirel. Pers. Commun.* **2022**, *125*, 2129–2146. [CrossRef]
260. Alam, I.; Kumar, S.; Kumar, M.; Kashyap, P.K. Blockchain Based Intelligent Incentive Enabled Information Sharing Scheme in Future Generation IoV Networks. *Res. Squ.* 2021, *Preprint*. [CrossRef]
261. Zhou, S.; Huang, H.; Chen, W.; Zhou, P.; Zheng, Z.; Guo, S. Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks. *IEEE Netw.* **2020**, *34*, 84–91. [CrossRef]
262. Otoum, S.; Al Ridhawi, I.; Mouftah, H.T. Blockchain-supported federated learning for trustworthy vehicular networks. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
263. Rathore, S.; Pan, Y.; Park, J.H. BlockDeepNet: A blockchain-based secure deep learning for IoT network. *Sustainability* **2019**, *11*, 3974. [CrossRef]
264. Singh, M.; Aujla, G.S.; Singh, A.; Kumar, N.; Garg, S. Deep-learning-based blockchain framework for secure software-defined industrial networks. *IEEE Trans. Ind. Inform.* **2020**, *17*, 606–616. [CrossRef]
265. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A trustworthy privacy preserving framework for machine learning in industrial IoT systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6092–6102. [CrossRef]
266. Ma, Z.; Yuan, X.; Liang, K.; Feng, J.; Zhu, L.; Zhang, D.; Yu, F.R. Blockchain-escorted distributed deep learning with collaborative model aggregation towards 6G networks. *Future Gener. Comput. Syst.* **2023**, *141*, 555–566. [CrossRef]
267. Nassar, M.; Salah, K.; ur Rehman, M.H.; Svetinovic, D. Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2020**, *10*, e1340. [CrossRef]
268. Zeng, Z.; Zhang, X.; Xia, Z. Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5693962. [CrossRef]
269. Abbas, S.; Javaid, N.; Almogren, A.; Gulfam, S.M.; Ahmed, A.; Radwan, A. Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. *IEEE Access* **2021**, *9*, 139739–139754. [CrossRef]
270. Yang, J.; He, S.; Xu, Y.; Chen, L.; Ren, J. A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors* **2019**, *19*, 970. [CrossRef]
271. Guo, Y.; Wang, Y.; Qian, Q. Intelligent edge network routing architecture with blockchain for the IoT. *China Commun.* **2023**. [CrossRef]
272. Li, Z.; Su, W.; Xu, M.; Yu, R.; Niyato, D.; Xie, S. Compact Learning Model for Dynamic Off-Chain Routing in Blockchain-Based IoT. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3615–3630. [CrossRef]
273. Mehbodniya, A.; Webber, J.L.; Rani, R.; Ahmad, S.S.; Wattar, I.; Ali, L.; Nuagah, S.J. Energy-aware routing protocol with fuzzy logic in industrial internet of things with blockchain technology. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 7665931. [CrossRef]
274. Kim, H.Y.; Lee, J.H. A load balancing scheme based on deep learning in blockchain network. In Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2021; pp. 1821–1823.
275. Tiba, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Karimipour, H.; Choo, K.K.R. Secure blockchain-based traffic load balancing using edge computing and reinforcement learning. In *Blockchain Cybersecurity, Trust and Privacy*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 99–128.
276. She, H.; Zhu, X.; Guo, Y.; Cao, H.; Garg, S.; Kaddoum, G. BCLB: Blockchain-based Controller Load Balance for Safe and Reliable Resource Optimization. In Proceedings of the 2022 IEEE Globecom Workshops (GC Wkshps), Rio de Janeiro, Brazil, 4–8 December 2022; pp. 668–673.
277. Alouache, L.; Sylla, T.; Mendiboure, L.; Aniss, H. A Fuzzy approach for load balancing in Blockchain-based Software Defined Vehicular Networks. In Proceedings of the 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Thessaloniki, Greece, 10–12 October 2022; pp. 235–242.

278. Islam, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. Blockchain-enabled intelligent vehicular edge computing. *IEEE Netw.* **2021**, *35*, 125–131. [CrossRef]
279. Al-Jawad, A.; Comşa, I.S.; Shah, P.; Gemikonakli, O.; Trestian, R. An innovative reinforcement learning-based framework for quality of service provisioning over multimedia-based sdn environments. *IEEE Trans. Broadcast.* **2021**, *67*, 851–867. [CrossRef]
280. Choudhary, S.; Dorle, S. A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc network s using machine learning-based blockchain routing. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6993. [CrossRef]
281. Agrawal, S.; Kumar, S. MLSMBQS: Design of a machine learning based split & merge blockchain model for QoS-aware secure IoT deployments. *Int. J. Image Graph. Signal Process* **2022**, *14*, 58–71.
282. Vairagade, R.S.; SH, B. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4433. [CrossRef]
283. Lanjewar, A.; Kumar, S.; Malik, L. ATQMB: Design of an augmented trust enabled QoS aware MAC model with intelligent blockchain sharding. In Proceedings of the 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 29–30 April 2022; pp. 1–6.
284. Khan, A.A.; Shaikh, Z.A.; Baitenova, L.; Mutaliyeva, L.; Moiseev, N.; Mikhaylov, A.; Laghari, A.A.; Idris, S.A.; Alshazly, H. QoS-ledger: Smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. *Electronics* **2021**, *10*, 3083. [CrossRef]
285. Maksymyuk, T.; Gazda, J.; Han, L.; Jo, M. Blockchain-based intelligent network management for 5G and beyond. In Proceedings of the 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2–6 July 2019; pp. 36–39.
286. Seid, A.M.; Erbad, A.; Abishu, H.N.; Albaseer, A.; Abdallah, M.; Guizani, M. Blockchain-Empowered Resource Allocation in Multi-UAV-Enabled 5G-RAN: A Multi-agent Deep Reinforcement Learning Approach. *IEEE Trans. Cogn. Commun. Netw.* **2023**, *9*, 991–1011. [CrossRef]
287. Zhang, H.; Wang, R.; Sun, W.; Zhao, H. Mobility management for blockchain-based ultra-dense edge computing: A deep reinforcement learning approach. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 7346–7359. [CrossRef]
288. Jung, Y.; Peradilla, M.; Agulto, R. Blockchain-based NAT management for smart mobility. In Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 12–14 December 2018; pp. 495–500.
289. Yu, S.; Chen, X.; Zhou, Z.; Gong, X.; Wu, D. When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network. *IEEE Internet Things J.* **2020**, *8*, 2238–2251. [CrossRef]
290. Ahmed, I.; Zhang, Y.; Jeon, G.; Lin, W.; Khosravi, M.R.; Qi, L. A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city. *Int. J. Intell. Syst.* **2022**, *37*, 6493–6507. [CrossRef]
291. Salim, M.M.; Shanmuganathan, V.; Loia, V.; Park, J.H. Deep learning enabled secure IoT handover authentication for blockchain networks. *Hum. Cent. Comput. Inf. Sci.* **2021**, *11*, 21.
292. Manjaragi, S.V.; Saboji, S.V. Fast user authentication in 5G heterogeneous networks using RLAC-FNN and blockchain technology for handoff delay reduction. *Wirel. Netw.* **2023**, 1–19. [CrossRef]
293. Sharmila, A.H.; Jaisankar, N. Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. *Comput. Netw.* **2021**, *200*, 108508.
294. Wang, X.; Garg, S.; Lin, H.; Piran, M.J.; Hu, J.; Hossain, M.S. Enabling secure authentication in industrial iot with transfer learning empowered blockchain. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7725–7733. [CrossRef]
295. Luong, N.C.; Anh, T.T.; Xiong, Z.; Niyato, D.; Kim, D.I. Joint time scheduling and transaction fee selection in blockchain-based RF-powered backscatter cognitive radio network. *Comput. Netw.* **2022**, *214*, 109135. [CrossRef]
296. Sellami, B.; Hakiri, A.; Yahia, S.B. Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network. *Future Gener. Comput. Syst.* **2022**, *137*, 363–379. [CrossRef]
297. Ren, Y.; Chen, X.; Guo, S.; Guo, S.; Xiong, A. Blockchain-based VEC network trust management: A DRL algorithm for vehicular service offloading and migration. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8148–8160. [CrossRef]
298. Alam, T.; Ullah, A.; Benaida, M. Deep reinforcement learning approach for computation offloading in blockchain-enabled communications systems. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 9959–9972. [CrossRef]
299. He, Q.; Feng, Z.; Fang, H.; Wang, X.; Zhao, L.; Yao, Y.; Yu, K. A Blockchain-Based Scheme for Secure Data Offloading in Healthcare With Deep Reinforcement Learning. *IEEE/ACM Trans. Netw.* **2023**. [CrossRef]
300. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Secure computation offloading in blockchain based IoT networks with deep reinforcement learning. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 3192–3208. [CrossRef]
301. Wang, D.; Zhao, N.; Song, B.; Lin, P.; Yu, F.R. Resource management for secure computation offloading in softwarized cyber–physical systems. *IEEE Internet Things J.* **2021**, *8*, 9294–9304. [CrossRef]
302. Liang, Y.C. *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence*; Springer Nature: Berlin/Heidelberg, Germany, 2020; p. 166.
303. Maksymyuk, T.; Gazda, J.; Liyanage, M.; Han, L.; Shubyn, B.; Strykhaliuk, B.; Yaremko, O.; Jo, M.; Dohler, M. Ai-enabled blockchain framework for dynamic spectrum management in multi-operator 6g networks. In *Future Intent-Based Networking: On*

the QoS Robust and Energy Efficient Heterogeneous Software Defined Networks; Springer International Publishing: Cham, Switzerland, 2021; pp. 322–338.
304. Miah, M.S.; Hossain, M.S.; Armada, A.G. Machine Learning-based Malicious Users Detection in Blockchain-Enabled CR-IoT Network for Secured Spectrum Access. In Proceedings of the 2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Bilbao, Spain, 15–17 June 2022; pp. 1–6.
305. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet Things J.* **2020**, *8*, 2276–2288. [CrossRef]
306. Maksymyuk, T.; Gazda, J.; Volosin, M.; Bugar, G.; Horvath, D.; Klymash, M.; Dohler, M. Blockchain-empowered framework for decentralized network management in 6G. *IEEE Commun. Mag.* **2020**, *58*, 86–92. [CrossRef]
307. Rajesh Babu, C.; Amutha, B. Blockchain and extreme learning machine based spectrum management in cognitive radio networks. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4174. [CrossRef]
308. Liu, Y.; Gu, Y.; Yang, D.; Wang, J. Fault identification and relay protection of hybrid microgrid using blockchain and machine learning. *IETE J. Res.* **2022**, 1–11. [CrossRef]
309. Belhadi, A.; Djenouri, Y.; Srivastava, G.; Jolfaei, A.; Lin, J.C.W. Privacy reinforcement learning for faults detection in the smart grid. *Ad Hoc Netw.* **2021**, *119*, 102541. [CrossRef]
310. Calo, J.; Lo, B. IoT Federated Blockchain Learning at the Edge. *arXiv* **2023**, arXiv:2304.03006.
311. Aloqaily, M.; Al Ridhawi, I.; Guizani, M. Energy-aware blockchain and federated learning-supported vehicular networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 22641–22652. [CrossRef]
312. Xu, C.; Wang, K.; Guo, M. Intelligent resource management in blockchain-based cloud datacenters. *IEEE Cloud Comput.* **2017**, *4*, 50–59. [CrossRef]
313. Luo, J.; Chen, Q.; Yu, F.R.; Tang, L. Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning. *IEEE Internet Things J.* **2020**, *7*, 5466–5480. [CrossRef]
314. Chen, G.; Wu, J.; Yang, W.; Bashir, A.K.; Li, G.; Hammoudeh, M. Leveraging graph convolutional-LSTM for energy-efficient caching in blockchain-based green IoT. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1154–1164. [CrossRef]
315. El Azzaoui, A.; Singh, S.K.; Pan, Y.; Park, J.H. Block5GIntell: Blockchain for AI-enabled 5G networks. *IEEE Access* **2020**, *8*, 145918–145935. [CrossRef]
316. Ashfaq, T.; Khalid, M.I.; Ali, G.; Affendi, M.E.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Yahaya, A.S.; Khalid, R.; Mateen, A. An efficient and secure energy trading approach with machine learning technique and consortium blockchain. *Sensors* **2022**, *22*, 7263. [CrossRef] [PubMed]
317. Said, D. A decentralized electricity trading framework (DETF) for connected EVs: A blockchain and machine learning for profit margin optimization. *IEEE Trans. Ind. Inform.* **2020**, *17*, 6594–6602. [CrossRef]
318. Cao, Y.; Ren, X.; Qiu, C.; Wang, X. Hierarchical reinforcement learning for blockchain-assisted software defined industrial energy market. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6100–6108. [CrossRef]
319. Jamil, F.; Iqbal, N.; Ahmad, S.; Kim, D. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
320. Hossain, M.S.; Rahman, M.H.; Rahman, M.S.; Hosen, A.S.; Seo, C.; Cho, G.H. Intellectual property theft protection in IoT based precision agriculture using SDN. *Electronics* **2021**, *10*, 1987. [CrossRef]
321. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2326–2341. [CrossRef]
322. Nawaz, A.; Gia, T.N.; Queralta, J.P.; Westerlund, T. Edge AI and blockchain for privacy-critical and data-sensitive applications. In Proceedings of the 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu, Nepal, 4–6 November 2019; pp. 1–2.
323. Elhoseny, M.; Haseeb, K.; Shah, A.A.; Ahmad, I.; Jan, Z.; Alghamdi, M.I. IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: An application for healthcare using blockchain. *Energies* **2021**, *14*, 5364. [CrossRef]
324. Aliyu, I.; Feliciano, M.C.; Van Engelenburg, S.; Kim, D.O.; Lim, C.G. A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system. *IEEE Access* **2021**, *9*, 102593–102608. [CrossRef]
325. Munir, M.S.; Bajwa, I.S.; Cheema, S.M. An intelligent and secure smart watering system using fuzzy logic and blockchain. *Comput. Electr. Eng.* **2019**, *77*, 109–119. [CrossRef]
326. Kamalov, F.; Gheisari, M.; Liu, Y.; Feylizadeh, M.R.; Moussa, S. Critical Controlling for the Network Security and Privacy Based on Blockchain Technology: A Fuzzy DEMATEL Approach. *Sustainability* **2023**, *15*, 10068. [CrossRef]
327. Outchakoucht, A.; Hamza, E.S.; Leroy, J.P. Dynamic access control policy based on blockchain and machine learning for the internet of things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 417–424. [CrossRef]
328. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing. *Appl. Sci.* **2022**, *12*, 4641. [CrossRef]
329. Akbarfam, A.J.; Barazandeh, S.; Maleki, H.; Gupta, D. DLACB: Deep Learning Based Access Control Using Blockchain. *arXiv* **2023**, arXiv:2303.14758.

330. Rana, S.K.; Rana, S.K.; Nisar, K.; Ag Ibrahim, A.A.; Rana, A.K.; Goyal, N.; Chawla, P. Blockchain technology and Artificial Intelligence based decentralized access control model to enable secure interoperability for healthcare. *Sustainability* **2022**, *14*, 9471. [CrossRef]
331. Xiong, W.; Xiong, L. Smart contract based data trading mode using blockchain and machine learning. *IEEE Access* **2019**, *7*, 102331–102344. [CrossRef]
332. Truong, V.; Le, L.B. Security for the Metaverse: Blockchain and Machine Learning Techniques for Intrusion Detection. *TechrXiv* **2023**, *Preprint*. [CrossRef]
333. Philip, A.O.; Saravanaguru, R.K. Secure incident & evidence management framework (SIEMF) for internet of vehicles using deep learning and blockchain. *Open Comput. Sci.* **2020**, *10*, 408–421.
334. Gaur, R.; Prakash, S.; Kumar, S.; Abhishek, K.; Msahli, M.; Wahid, A. A Machine-Learning–Blockchain-Based Authentication Using Smart Contracts for an IoHT System. *Sensors* **2022**, *22*, 9074. [CrossRef] [PubMed]
335. Zulkifl, Z.; Khan, F.; Tahir, S.; Afzal, M.; Iqbal, W.; Rehman, A.; Saeed, S.; Almuhaideb, A.M. FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access* **2022**, *10*, 15644–15656. [CrossRef]
336. Ogundoyin, S.O.; Kamil, I.A. An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. *Veh. Commun.* **2021**, 31, 100384. [CrossRef]
337. Sammeta, N.; and Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* **2022**, *8*, 625–640. [CrossRef]
338. Cristina, C.; Moro, E.P.; Maple, C.; Epiphaniou, G. I-Trace: Protecting cyber-physical infrastructure through enhanced gateways, DLT and machine learning. In Proceedings of the Competitive Advantage in the Digital Economy (CADE 2021), Online, 2–3 June 2021.
339. Finogeev, A.; Deev, M.; Parygin, D.; Finogeev, A. Intelligent SDN Architecture with Fuzzy Neural Network and Blockchain for Monitoring Critical Events. *Appl. Artif. Intell.* **2022**, *36*, 2145634. [CrossRef]
340. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Gener. Comput. Syst.* **2021**, *117*, 328–337. [CrossRef]
341. Rahman, Z.; Yi, X.; Khalil, I.; Anwar, A.; Pal, S. Blockchain-Based and Fuzzy Logic-Enabled False Data Discovery for the Intelligent Autonomous Vehicular System. In Proceedings of the Third International Symposium on Advanced Security on Software and Systems, Melbourne, Australia, 10–14 July 2023; pp. 1–11.
342. Wijesekara, P.A.D.S.N. Prevalence, Risk Factors and Remedies for Psychiatric Illnesses among Students in Higher Education: A Comprehensive Study in University of Ruhuna. *Res. Sq.* 2022, *Preprint*. [CrossRef]
343. Cheema, M.A.; Qureshi, H.K.; Chrysostomou, C.; Lestas, M. Utilizing blockchain for distributed machine learning based intrusion detection in internet of things. In Proceedings of the 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, 25–27 May 2020; pp. 429–435.
344. Saveetha, D.; Maragatham, G. Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognit. Lett.* **2022**, *153*, 24–28. [CrossRef]
345. Mansour, R.F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. *Sci. Rep.* **2022**, *12*, 12937. [CrossRef] [PubMed]
346. Alkadi, O.; Moustafa, N.; Turnbull, B.; Choo, K.K.R. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet Things J.* **2020**, *8*, 9463–9472. [CrossRef]
347. Khan, A.A.; Khan, M.M.; Khan, K.M.; Arshad, J.; Ahmad, F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Comput. Netw.* **2021**, *196*, 108217. [CrossRef]
348. Vargas, H.; Lozano-Garzon, C.; Montoya, G.A.; Donoso, Y. Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. *Electronics* **2021**, *10*, 2662. [CrossRef]
349. Ferrag, M.A.; Maglaras, L. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1285–1297. [CrossRef]
350. Farooq, M.S.; Khan, S.; Rehman, A.; Abbas, S.; Khan, M.A.; Hwang, S.O. Blockchain-Based Smart Home Networks Security Empowered with Fused Machine Learning. *Sensors* **2022**, *22*, 4522. [CrossRef]
351. Abdel-Basset, M.; Moustafa, N.; Hawash, H.; Razzak, I.; Sallam, K.M.; Elkomy, O.M. Federated intrusion detection in blockchain-based smart transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 2523–2537. [CrossRef]
352. Liu, H.; Zhang, S.; Zhang, P.; Zhou, X.; Shao, X.; Pu, G.; Zhang, Y. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6073–6084. [CrossRef]
353. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119. [CrossRef]
354. He, X.; Chen, Q.; Tang, L.; Wang, W.; Liu, T. Cgan-based collaborative intrusion detection for uav networks: A blockchain-empowered distributed federated learning approach. *IEEE Internet Things J.* **2022**, *10*, 120–132. [CrossRef]
355. Jmal, R.; Ghabri, W.; Guesmi, R.; Alshammari, B.M.; Alshammari, A.S.; Alsaif, H. Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks. *Appl. Sci.* **2023**, *13*, 4953. [CrossRef]
356. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. *Comput. Ind.* **2023**, *144*, 103801. [CrossRef]

357. Ghazal, T.M.; Hasan, M.K.; Abdallah, S.N.H.; Abubakkar, K.A. Secure IoMT pattern recognition and exploitation for multimedia information processing using private blockchain and fuzzy logic. *Trans. Asian Low-Resour. Lang. Inf. Process.* **2022**. [CrossRef]
358. Ali, S.E.; Tariq, N.; Khan, F.A.; Ashraf, M.; Abdul, W.; Saleem, K. BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things. *Sensors* **2023**, *23*, 4265. [CrossRef] [PubMed]
359. Abdulqadder, I.H.; Zou, D.; Aziz, I.T. The DAG blockchain: A secure edge assisted honeypot for attack detection and multi-controller based load balancing in SDN 5G. *Future Gener. Comput. Syst.* **2023**, *141*, 339–354. [CrossRef]
360. Abou El Houda, Z.; Hafid, A.; Khoukhi, L. Brainchain-a machine learning approach for protecting blockchain applications using sdn. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), virtual event, 7–11 June 2020; pp. 1–6.
361. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained anomaly detection models for federated learning: An intrusion detection case study. *Appl. Sci.* **2018**, *8*, 2663. [CrossRef]
362. Wang, J.; Jin, H.; Chen, J.; Tan, J.; Zhong, K. Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network. *Inf. Sci.* **2022**, *617*, 133–149. [CrossRef]
363. Alkhamisi, A.; Katib, I.; Buhari, S.M. Blockchain-Assisted Hybrid Deep Learning-Based Secure Mechanism for Software Defined Networks. In Proceedings of the 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 6–8 January 2023; pp. 1–8.
364. Yang, G.; Shin, C.; Yoo, Y.; Yoo, C. A case for SDN-based network virtualization. In Proceedings of the 2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Houston, TX, USA, 3–5 November 2021; pp. 1–8.
365. Adhikari, A.; Rawat, D.B.; Song, M. Wireless network virtualization by leveraging blockchain technology and machine learning. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15–17 May 2019; pp. 61–66.
366. Qiu, C.; Yu, F.R.; Xu, F.; Yao, H.; Zhao, C. Blockchain-based distributed software-defined vehicular networks via deep q-learning. In Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Montreal, QC, Canada, 28 October–2 November 2018; pp. 8–14.
367. Fu, X.; Yu, F.R.; Wang, J.; Qi, Q.; Liao, J. Performance optimization for blockchain-enabled distributed network function virtualization management and orchestration. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6670–6679. [CrossRef]
368. Boateng, G.O.; Sun, G.; Mensah, D.A.; Doe, D.M.; Ou, R.; Liu, G. Consortium blockchain-based spectrum trading for network slicing in 5G RAN: A multi-agent deep reinforcement learning approach. *IEEE Trans. Mob. Comput.* **2022**. [CrossRef]
369. Abdulqadder, I.H.; Zhou, S. SliceBlock: Context-aware authentication handover and secure network slicing using DAG-blockchain in edge-assisted SDN/NFV-6G environment. *IEEE Internet Things J.* **2022**, *9*, 18079–18097. [CrossRef]
370. Gong, Y.; Sun, S.; Wei, Y.; Song, M. Deep reinforcement learning for edge computing resource allocation in blockchain network slicing broker framework. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), virtual event, 25 April–19 May 2021; pp. 1–6.
371. Bandara, E.; Liang, X.; Shetty, S.; Mukkamala, R.; Rahman, A.; Keong, N.W. Skunk—A blockchain and zero trust security enabled federated learning platform for 5G/6G network slicing. In Proceedings of the 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), virtual event, 20–23 September 2022; pp. 109–117.
372. Boateng, G.O.; Ayepah-Mensah, D.; Doe, D.M.; Mohammed, A.; Sun, G.; Liu, G. Blockchain-enabled resource trading and deep reinforcement learning-based autonomous RAN slicing in 5G. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 216–227. [CrossRef]
373. Ou, R.; Sun, G.; Ayepah-Mensah, D.; Boateng, G.O.; Liu, G. Two-Tier Resource Allocation for Multi-Tenant Network Slicing: A Federated Deep Reinforcement Learning Approach. *IEEE Internet Things J.* **2023**. [CrossRef]
374. Singh, S.K.; Rathore, S.; Park, J.H. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
375. Unal, D.; Hammoudeh, M.; Khan, M.A.; Abuarqoub, A.; Epiphaniou, G.; Hamila, R. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. *Comput. Secur.* **2021**, *109*, 102393. [CrossRef]
376. Lv, Z.; Xiu, W. Interaction of edge-cloud computing based on SDN and NFV for next generation IoT. *IEEE Internet Things J.* **2019**, *7*, 5706–5712. [CrossRef]
377. Zhang, K.; Zhu, Y.; Maharjan, S.; Zhang, Y. Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things. *IEEE Netw.* **2019**, *33*, 12–19. [CrossRef]
378. He, Y.; Wang, Y.; Qiu, C.; Lin, Q.; Li, J.; Ming, Z. Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach. *IEEE Internet Things J.* **2020**, *8*, 2226–2237. [CrossRef]
379. Tian, Y.; Li, T.; Xiong, J.; Bhuiyan, M.Z.A.; Ma, J.; Peng, C. A blockchain-based machine learning framework for edge services in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1918–1929. [CrossRef]
380. Shahbazi, Z.; Byun, Y.C. Improving transactional data system based on an edge computing–blockchain–machine learning integrated framework. *Processes* **2021**, *9*, 92. [CrossRef]
381. Gardas, B.B.; Heidari, A.; Navimipour, N.J.; Unal, M. A fuzzy-based method for objects selection in blockchain-enabled edge-IoT platforms using a hybrid multi-criteria decision-making model. *Appl. Sci.* **2022**, *12*, 8906. [CrossRef]
382. Lakhan, A.; Mohammed, M.A.; Kozlov, S.; Rodrigues, J.J. Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. *Trans. Emerg. Telecommun. Technol.* **2021**, e4363. [CrossRef]

383. Zhang, S.; Wang, Z.; Zhou, Z.; Wang, Y.; Zhang, H.; Zhang, G.; Ding, H.; Mumtaz, S.; Guizani, M. Blockchain and federated deep reinforcement learning based secure cloud-edge-end collaboration in power IoT. *IEEE Wirel. Commun.* **2022**, *29*, 84–91. [CrossRef]
384. Qu, G.; Cui, N.; Wu, H.; Li, R.; Ding, Y. ChainFL: A simulation platform for joint federated learning and blockchain in edge/cloud computing environments. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3572–3581. [CrossRef]
385. Guo, S.; Dai, Y.; Xu, S.; Qiu, X.; Qi, F. Trusted cloud-edge network resource management: DRL-driven service function chain orchestration for IoT. *IEEE Internet Things J.* **2019**, *7*, 6010–6022. [CrossRef]
386. Maaroufi, S.; Pierre, S. BCOOL: A novel blockchain congestion control architecture using dynamic service function chaining and machine learning for next generation vehicular networks. *IEEE Access* **2021**, *9*, 53096–53122. [CrossRef]
387. Li, M.; Pei, P.; Yu, F.R.; Si, P.; Li, Y.; Sun, E.; Zhang, Y. Cloud–Edge Collaborative Resource Allocation for Blockchain-Enabled Internet of Things: A Collective Reinforcement Learning Approach. *IEEE Internet Things J.* **2022**, *9*, 23115–23129. [CrossRef]
388. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
389. Yin, B.; Yin, H.; Wu, Y.; Jiang, Z. FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 6348–6359. [CrossRef]
390. Li, W.; Su, Z.; Li, R.; Zhang, K.; Wang, Y. Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Netw.* **2020**, *34*, 31–37. [CrossRef]
391. Hitaj, B.; Ateniese, G.; Perez-Cruz, F. Deep models under the GAN: Information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 603–618.
392. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C. Blockchain and machine learning for communications and networking systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
393. Shahid, A.R.; Niki, P.; Corey, S.; Rain, K. Sensor-chain: A lightweight scalable blockchain framework for internet of things. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1154–1161.
394. Zhang, P.; Guo, W.; Liu, Z.; Zhou, M.; Huang, B.; Sedraoui, K. Optimized Blockchain Sharding Model Based on Node Trust and Allocation. *IEEE Trans. Netw. Serv. Manag.* **2023**. [CrossRef]
395. Spain, M.; Foley, S.; Gramoli, V. The impact of ethereum throughput and fees on transaction latency during icos. In Proceedings of the International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019), Paris, France, 6–7 May 2019; pp. 9:1–9:15.
396. Li, C.; Li, P.; Zhou, D.; Yang, Z.; Wu, M.; Yang, G.; Xu, W.; Long, F.; Yao, A.C.C. A decentralized blockchain with high throughput and fast confirmation. In Proceedings of the 2020 USENIX Annual Technical Conference (USENIXATC 20), virtual event, 15–17 July 2020; pp. 515–528.
397. Xu, C.; Zhang, C.; Xu, J.; Pei, J. Slimchain: Scaling blockchain transactions through off-chain storage and parallel processing. *Proc. Vldb Endow.* **2021**, *14*, 2314–2326. [CrossRef]
398. Yang, L.; Li, M.; Si, P.; Yang, R.; Sun, E.; Zhang, Y. Energy-efficient resource allocation for blockchain-enabled industrial Internet of Things with deep reinforcement learning. *IEEE Internet Things J.* **2020**, *8*, 2318–2329. [CrossRef]
399. Reijsbergen, D.; Maw, A.; Zhang, J.; Dinh, T.T.A.; Datta, A. PIEChain–A Practical Blockchain Interoperability Framework. *arXiv* **2023**, arXiv:2306.09735.
400. Ding, D.; Duan, T.; Jia, L.; Li, K.; Li, Z.; Sun, Y. Interchain: A framework to support blockchain interoperability. In Proceedings of the Second Asia-Pacific Workshop on Networking, Beijing, China, 1–3 August 2018.
401. Baek, U.J.; Ji, S.H.; Park, J.T.; Lee, M.S.; Park, J.S.; Kim, M.S. DDoS attack detection on bitcoin ecosystem using deep-learning. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.