IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 September 2023, accepted 18 September 2023, date of publication 25 September 2023,
date of current version 3 October 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3319083*

SURVEY

# Qualitative Survey on Artificial Intelligence Integrated Blockchain Approach for 6G and Beyond

**VIVEK PATHAK [1], RAHUL JASHVANTBHAI PANDYA [1], (Senior Member, IEEE), VIMAL BHATIA [2,3,4], (Senior Member, IEEE), AND ONEL ALCARAZ LOPEZ [5], (Member, IEEE)**

[1] Indian Institute of Technology Dharwad, Karnataka, Dharwad 580011, India
[2] Indian Institute of Technology Indore, Madhya Pradesh, Indore 453552, India
[3] Faculty of Informatics and Management, University of Hradec Kralove, 50003 Hradec Kralove, Czech Republic
[4] School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China
[5] Centre for Wireless Communications (CWC), University of Oulu, 90570 Oulu, Finland

Corresponding author: Rahul Jashvantbhai Pandya (rpandya@iitdh.ac.in)

This work was supported by the Science and Engineering Research Board (SERB), Indian Institute of Technology Dharwad, India, under Grant EEQ/2020/000047.

**ABSTRACT** Utilizing the 0.1 to 10 THz spectrum in the next-generation wireless communication networks holds potential for futuristic applications. However, managing resources to accommodate numerous devices raises privacy and security concerns. Further, technology proliferation entwines devices, infrastructure complexity, and resources. Indeed, the transition from 5G (fifth-generation) to 6G (sixth-generation) signifies a progression towards high-speed data rates, minimal latency, and seamless integration of artificial intelligence, enabling ground-breaking applications and services. However, it complicates network management, privacy, resource allocation, and data processing. Notably, integrating Blockchain Technology (BCT) and Machine Learning (ML) is a promising solution, enhancing security, decentralization, trust in ML decisions, and efficient data sharing. This survey thoroughly reviews the integrated ML and BCT, showcasing their collaborative enhancement of network security, decentralization, trust in ML decisions, immutability, and efficient model sharing. Furthermore, we also delve into various distinctive topics, such as BCT-enabled spectrum refarming, rate splitting multiple access, 6G radar-based communication, reconfigurable intelligent surfaces, visible light communication, and integrated sensing and communication. Moreover, it also explores the integration of ML and BCT in novel 6G communication technologies, including molecular, holographic, and semantic communication. Finally, critical open issues, challenges, solutions, and futuristic scope are identified for forthcoming researchers.

**INDEX TERMS** Terahertz (THz) communication, artificial intelligence (AI), machine learning (ML), blockchain technology (BCT), resource allocation (RA).

## I. INTRODUCTION

The fifth-generation (5G) systems are under commercialization and deployment; however, complete integration of Machine Learning (ML), decentralization, and security remain unaddressed. On the contrary, the sixth-generation (6G) aims to support the complete integration of ML, decentralized, and highly secure network infrastructure. Moreover, 6G aims to support tremendously high data rates, ubiquitous and seamless communication, improving Quality of Service and Experience (QoSE), high network capacity, spectrum efficiency, energy efficiency (EE), increased user and connectivity density, ultra-low latency, high mobility, and enhanced system throughput and dependability [1], [2]. However, the necessity of large data volumes and massive connectivity imposes the challenges of privacy, security, and

The associate editor coordinating the review of this manuscript and approving it for publication was Pavlos I. Lazaridis.

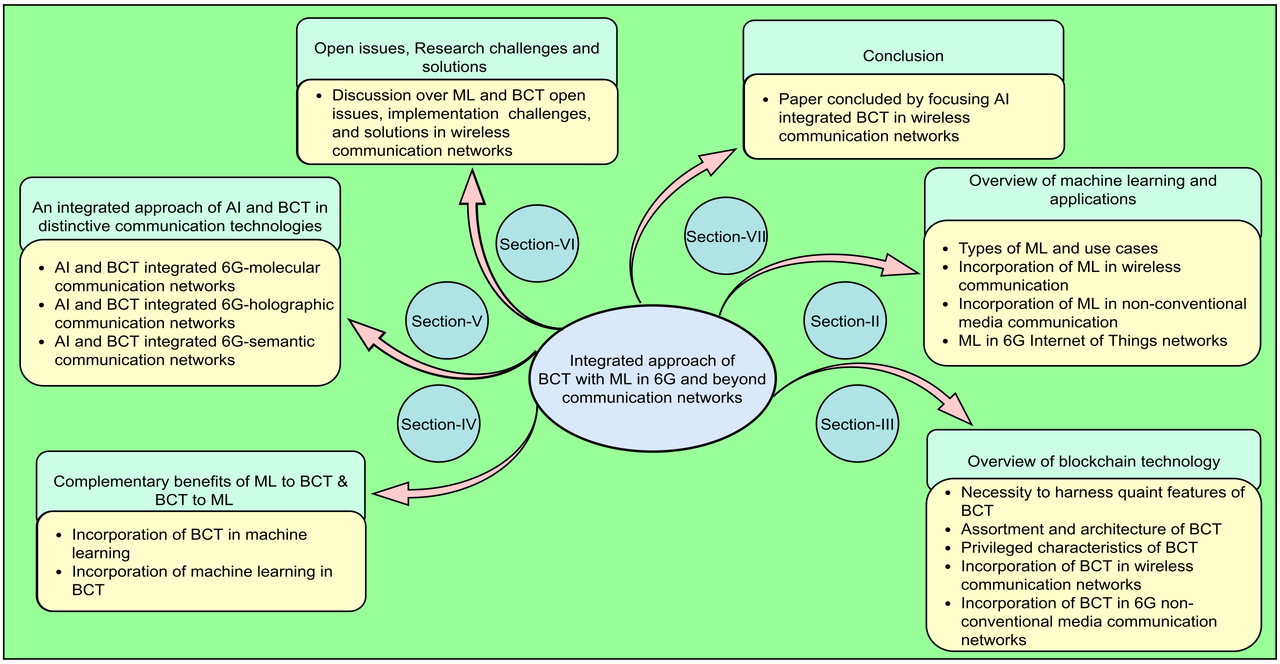

Open issues, Research challenges and solutions
Discussion over ML and BCT open issues, implementation challenges, and solutions in wireless communication networks
Conclusion
Paper concluded by focusing AI integrated BCT in wireless communication networks
An integrated approach of AI and BCT in distinctive communication technologies
AI and BCT integrated 6G-molecular communication networks
AI and BCT integrated 6G-holographic communication networks
AI and BCT integrated 6G-semantic communication networks
Overview of machine learning and applications
Types of ML and use cases
Incorporation of ML in wireless communication
Incorporation of ML in non-conventional media communication
ML in 6G Internet of Things networks
Section-VI
Section-VII
Section-V
Section-II
Integrated approach of BCT with ML in 6G and beyond communication networks
Section-IV
Section-III
Complementary benefits of ML to BCT & BCT to ML
Incorporation of BCT in machine learning
Incorporation of machine learning in BCT
Overview of blockchain technology
Necessity to harness quaint features of BCT
Assortment and architecture of BCT
Privileged characteristics of BCT
Incorporation of BCT in wireless communication networks
Incorporation of BCT in 6G non-conventional media communication networks

**FIGURE 1.** Outline to explore ML-integrated BCT in next-generation communication networks.

resource management in 6G wireless networks. Therefore, intelligent, automated, and decentralized resource allocation is an immediate necessity in 6G wireless networks.

Moreover, in 6G, the generation of big data mainly originates from three primary sources: social media, machine data, and transaction data. It can also be collected through edge devices, trading, internet, sensing, mobile data, and similar massive data-generating sources that are not competently handled and exhaust existing network resources [3], [4]. Consequently, this calls for intelligent, reconfigurable, and independent systems at the server and edge level, which leads to the involvement of ML. Indeed, ML allows extracting knowledge from these real-time data based on past data or experiences without being indubitably programmed. However, 6G wireless network infrastructure triggers security concerns that must be solved using intelligent technologies, such as blockchain (BC). To this end, conceiving these peculiar requirements, we are impending to the integrated approach where ML and BC work jointly. As a result, communication networks are equipped with unusual characteristics such as decentralization, transparency, audibility, security, immutability, tamperproof, integrity, pseudonymity, autonomy, and trustability by the exclusive pittance of BCT incorporated over ML [5]. Moreover, ML is a communal virtue of optimized energy, resource efficiency, optimized scalability, improved privacy and security, intelligent smart contracts, and an ML-based mining algorithm to handle tasks rather than opting for the brute force approach [6]. Subsequently, this shows that the integrated approach is an inevitable technology with a significant potential holding to make systems more stable and robust and promotes the development of an intelligent and secure communication network.

ML-based techniques and algorithms are exploited adequately to optimize and enhance the network performance even in complicated scenarios such as an unmanned aerial vehicle (UAV), virtual reality (VR), image recognition, traffic prediction, self-driving car, online fraud detection, and some other intelligent applications [7]. Moreover, the ML-based technique is segregated, including supervised learning, unsupervised learning, and reinforcement learning (RL), where the model gets trained and learns from massive data generated and deployed in a real-time application without human intervention. In the communication network, the intelligent end devices are reassured to collect browsed or sensed data from the network, fed to the ML model for learning and training purposes, and stored on BC in a distributed manner. BCT-enabled ML solution exemplifies distributed data processing, control, and sharing, enhancing resource allocation (RA), security, and trustworthiness of communication networks [8].

In addition, BCT is a widely fascinating technique in the digital cryptocurrency era, captivating both industry and academic interest. It is a distributed ledger connecting participants in a peer-to-peer (P2P) network. This decentralized approach enables independent and equal involvement without needing a central controller [9]. BCT is a versatile block structure that allows for efficient P2P networks, enhancing information sharing, governance, and resource utilization. Consequently, it ensures data validity, integrity, and dynamic access control, benefiting various domains such as security services, the Internet of Things (IoT), healthcare systems,

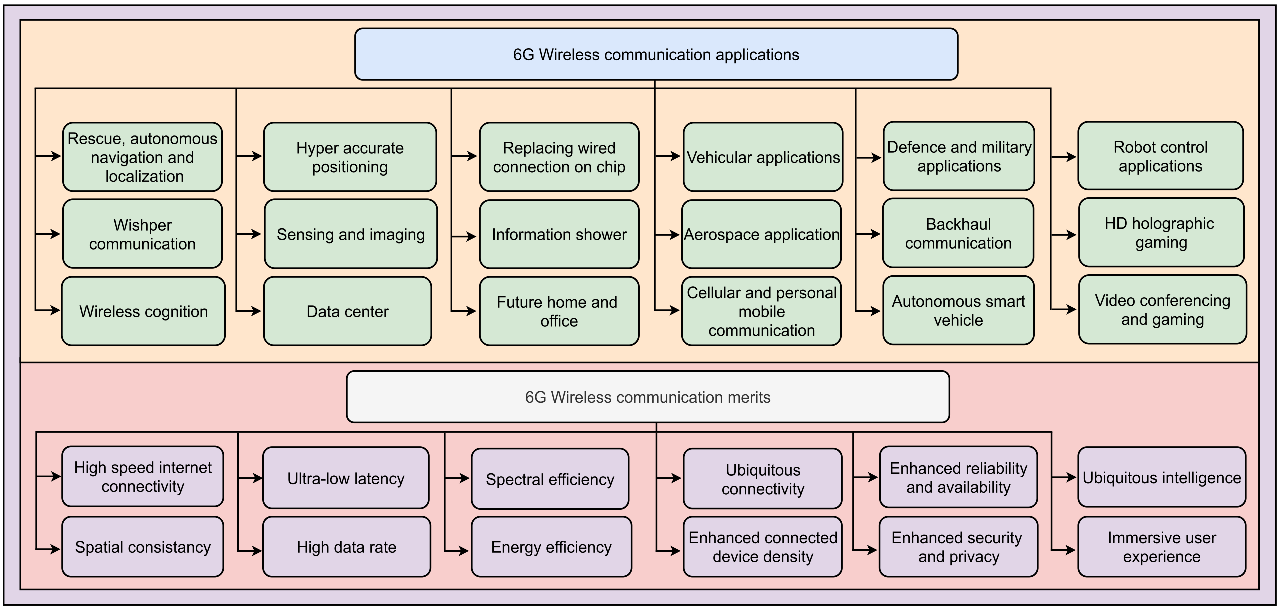

6G Wireless communication applications
Rescue, autonomous navigation and localization
Wishper communication
Wireless cognition
Hyper accurate positioning
Sensing and imaging
Data center
Replacing wired connection on chip
Information shower
Future home and office
Vehicular applications
Aerospace application
Cellular and personal mobile communication
Defence and military applications
Backhaul communication
Autonomous smart vehicle
Robot control applications
HD holographic gaming
Video conferencing and gaming
6G Wireless communication merits
High speed internet connectivity
Spatial consistancy
Ultra-low latency
High data rate
Spectral efficiency
Energy efficiency
Ubiquitous connectivity
Enhanced connected device density
Enhanced reliability and availability
Enhanced security and privacy
Ubiquitous intelligence
Immersive user experience

**FIGURE 2.** **Next-generation wireless communication applications and merits.**

and more. Further, the BCT's applicability extends even to non-conventional media communication networks [9].

Consequently, such integrated networks possess distinctive traits such as agility, autonomy, cooperation, learning, adaptability, and fault tolerance [10]. These attributes contribute to making networks more prudent. Researchers strive to enhance system efficiency at a lower cost to meet increasing demands for positioning accuracy (PA), EE, high throughput, network densification (ND), and low latency. Intelligent solutions, including machine-level and perceptron-level learning methods, are crucial in achieving fast and efficient decision-making, saving energy, and improving efficiency in wireless communication applications. Deploying these intelligent learning methods in 6G and beyond networks enhances overall system efficiency [11].

The primary contributions of this survey encompass the following:

- A detailed review of an integrated approach of BCT and artificial intelligence (AI)/ML in 6G and beyond communication networks.
- A comprehensive analysis of standalone ML and BCT applications and their mutually beneficial integration in the 6G wireless communication networks.
- Discussion on various BCT-integrated distinctive topics for next-generation wireless networks, including:
  1) BCT-enabled spectrum refarming
  2) BCT-enabled spectrum allocation, sharing, and management
  3) BCT-enabled energy-efficient wireless networks
  4) BCT-enabled rate splitting multiple access
  5) BCT-enabled 6G radar-based communication
  6) BCT-enabled reconfigurable intelligent surfaces
  7) BCT-enabled visible light communication
  8) BCT-enabled integrated sensing and communication networks
- Discussion on the integrated approach of AI and BCT in novel 6G communication technologies such as:
  1) Molecular communication (MC)
  2) Holographic communication (HC)
  3) Semantic communication (SC)
- A compendium of open issues, research challenges, and solutions from a broader perspective.

To this end, as per the best of the authors' knowledge, such an innovative pervasive survey on an integrated approach of BCT and ML applications in wireless communication has yet to be presented, considering a vast research landscape.

The rest of the paper is organized as follows. Section II furnishes an overview of existing ML techniques and their applications. Section III presents an overview of BCT in detail, including the taxonomy, architecture of BCT, privileged characteristics of BCT, and incorporation of BCT in communication systems and networking. Section IV details the complementary benefits of ML to BC and vice-versa. Section V discusses an integrated approach of AI and BC in novel distinctive 6G communication technologies, which include MC, HC, and SC, in detail. Section VI summarises the open issues, research challenges, and solutions. Lastly, section VII concludes the paper. The complete flow diagram of the survey paper is depicted in Fig. 1. However, the ML-assisted wireless communication applications are shown in Fig. 2.

## II. OVERVIEW OF ML AND ITS APPLICATIONS

ML is a subset of AI, where computer machines can learn from massive data. ML can be classified mainly into

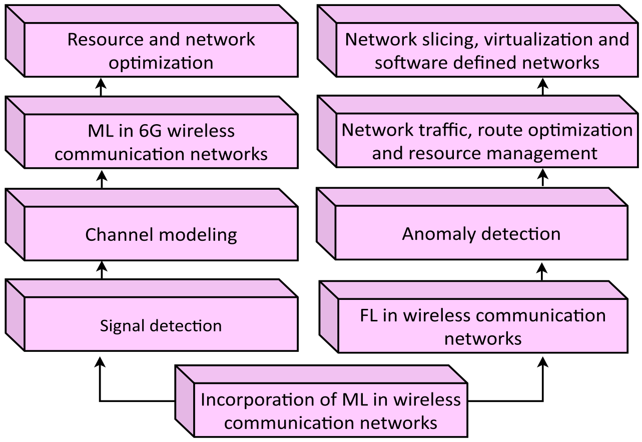

Resource and network optimization
Network slicing, virtualization and software defined networks
ML in 6G wireless communication networks
Network traffic, route optimization and resource management
Channel modeling
Anomaly detection
Signal detection
FL in wireless communication networks
Incorporation of ML in wireless communication networks

**FIGURE 3.** ML integration in wireless communication networks.

supervised, unsupervised, and RL. ML algorithms build a model during its learning phase using past sample data called training data in these methods. Further, it anticipates the outcome of unfamiliar tasks based on previous learning. Further, the argument is why ML is required to support the illustrated context. Indeed, networks are diverse and heterogeneous in characteristics and requirements, thus constituting a complex stochastic environment. As a result, it is tough to fulfill the communication network demands such as ND, PA, energy and spectrum efficiency, high throughput, high data rate, reliability, self-organization, and independency [12]. This calls for the systems to be equipped with intelligent techniques to manage the systems autonomously.

## A. TYPE OF ML AND ITS USE CASES

### 1) SUPERVISED LEARNING

Labeled data is used to train an ML model for predictions or to classify new objects. The model can map inputs to outputs through the training set's labeled examples. The primary objective is to learn a mapping function that can accurately predict the desired result when presented with new input. This type of learning is extensively applied in wireless networks, particularly in tasks such as RA, mobility prediction, load balancing, path selection, and fading detection [13]. These wireless network applications heavily rely on supervised learning techniques, including linear and logistic regression (LR), support vector machine (SVM), Naive Bayes (NB), k-nearest neighbor (KNN) algorithm, and neural network (NN) [7].

### 2) UNSUPERVISED LEARNING

Unsupervised ML involves training models on unlabeled data to discover patterns or structures without knowing the desired outputs. It aims to uncover hidden relationships in the data without guidance on expected outcomes. Examples include clustering, dimensionality reduction, anomaly detection (AD), and NN. These methods can be applied in wireless networks for fault detection, network configuration, handover management, spectrum sharing, and energy/power management [13], [14]. Unsupervised learning enhances efficiency, independence, and intelligence in wireless systems by leveraging hidden patterns and structures in the data. [15].

### 3) REINFORCEMENT LEARNING

It is an ML approach where an agent interacts with its environment and learns to make decisions by maximizing cumulative reward. The agent takes actions in an environment and receives feedback in the form of rewards or penalties, based on which it learns what actions to take in the future. Consequently, it has broad applicability in wireless networks, which include resource and channel allocation, hand-off decision-making, power control, spectrum management, congestion control, network optimization, and beamforming and antenna control [16]. However, the goal is to find a policy that maximizes the expected cumulative reward over time [17].

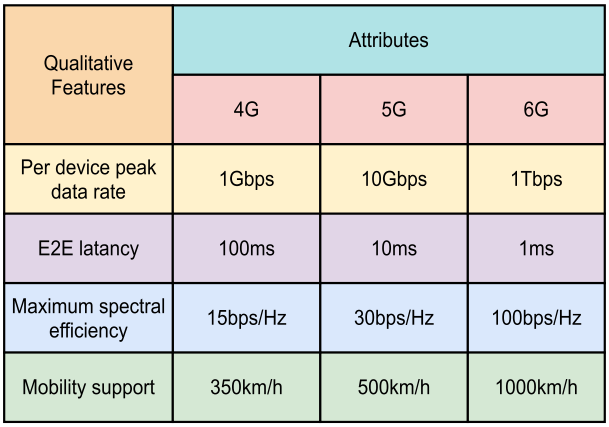
*Summary:* Supervised learning is expected to refine predictive analytics and optimize network management. Unsupervised learning will aid in anomaly detection and pattern recognition for enhanced security. Lastly, reinforcement learning will facilitate autonomous network optimization and adaptive resource allocation, boosting efficiency and performance in next-generation wireless communication networks.

## B. INCORPORATION OF ML IN WIRELESS COMMUNICATION

ML techniques have triggered a revolution in wireless communication. This revolution is particularly evident in the context of 5G and B5G networks, characterized by many end-users and the ever-increasing heterogeneity and complexity of the wireless communication system. These complexities arise from the need to support a wide range of novel and anticipated services, each with contrasting requirements. Consequently, there is a growing recognition of the importance of integrating ML into the design and operation of the upcoming 6G wireless communication system and network [5]. In this context, Fig. 3 illustrates the various aspects of ML utilization within a 6G wireless communication network, highlighting its crucial role in addressing the challenges posed by such advanced networks.

### 1) ML IN SIGNAL DETECTION

ML techniques are crucial in signal processing for wireless communication networks. They are used to estimate and predict system efficiency, including parameters such as bit error rate (BER), EE, power efficiency (PE), and signal-to-noise ratio (SNR). In signal detection, the objective is to identify the characteristics of received signals once they reach a predefined threshold, as described in [IEEE std.802.11.a]. Consequently, DL has gained popularity in signal processing due to its applications in various domains, such as voice assistance, digital health, and radar. DL models can be



| Qualitative Features | Attributes | | |
|---|---|---|---|
| | 4G | 5G | 6G |
| Per device peak data rate | 1Gbps | 10Gbps | 1Tbps |
| E2E latancy | 100ms | 10ms | 1ms |
| Maximum spectral efficiency | 15bps/Hz | 30bps/Hz | 100bps/Hz |
| Mobility support | 350km/h | 500km/h | 1000km/h |

**FIGURE 4.** **Key performance indicators of wireless networks.**

built using simulation tools, enabling the development of real-world intelligent signal processing systems [18]. The process involves accessing and managing data, which can be acquired from hardware devices, generated synthetically through simulation, or augmented using techniques such as data augmentation. Two primary approaches are commonly employed when data is ready for training DL models. The first approach involves converting the signal into a time-frequency representation and training a custom convolutional neural network (CNN) to extract patterns directly from these representations. This representation enhances patterns that may not be visible in the original signal. Techniques such as spectrograms, continuous wavelet transform, and constant Q-transform can be used. On the other hand, the second approach is to feed the signal directly into a deep neural network (DNN), such as a long short-term memory (LSTM) network. To facilitate rapid pattern learning, reducing signal dimensionality and variability is essential. This can be achieved by manually extracting features from the signal or using techniques like invariant scattering convolutional networks, which automatically extract low variant representations without losing critical information [19], [20].

### 2) ML IN CHANNEL MODELING

The increased end-users and diverse service demands in wireless communication networks have led to complex and heterogeneous network configurations. This complexity necessitates frequent handling of channel parameters and efficient utilization of available resources. Moreover, in the upcoming 6G wireless communication era, a wide range of new frequency bands is expected, which can be effectively utilized by deploying numerous beamforming antennas. These antennas help overcome significant path loss at THz frequencies. Another critical aspect of the 6G wireless communication era is generating a large amount of data containing valuable channel knowledge and information-bearing features. Hence, it encourages the integration of big data analytics, extensive antenna usage, and exploiting the unoccupied THz frequency range. Therefore, investigating the implications of these advancements in the 6G communication landscape becomes essential. This analysis includes examining the channel modeling effects in terms of significant data channel impulse response, introducing new characteristic features such as 3D double directional angle and non-stationarity in the spatial-temporal frequency domain, as well as employing techniques like spherical wavelet, high path loss, high delay resolution, and geometry-based stochastic model [3]. Moreover, applying ML techniques in wireless channel modeling has gained significant attention. ML methods such as classification, SVM, relevance vector machines (RVM), clustering algorithms like NB, k-means clustering, KNN, and regression techniques such as least absolute shrinkage and selection operator have been deployed for various purposes. These include model performance management, Gaussian process regression, path loss prediction, multipath component estimation, power delay profile determination, noise filtering, received power estimation, channel impulse response estimation, and channel feature extraction [21], [22], [23]. These comprehensive analyses make the network more competent, self-reliant, and robust, enabling autonomous decision-making capabilities. Overall, the combination of advanced technologies, extensive data analysis, and the integration of ML techniques paves the way for a more efficient, adaptive, and intelligent wireless communication system in the 6G era.

### 3) ML IN 6G WIRELESS COMMUNICATION

In the current wireless communication landscape, deploying ultra-dense small cells and heterogeneous and diversified networks has become commonplace. This can be attributed to the widespread usage of smartphones, the emergence of intricate communication scenarios, the adoption of massive antenna elements, and the availability of new frequency bands. As a result, there is a growing need to study and analyze the big data generated by these communication networks. According to a white paper by Cisco in February 2017, global mobile data has increased 18-fold recently, highlighting the unprecedented data growth in 5G and future communication technologies [24]. This exponential data generation reinforces the use of intelligent mobile and self-reliant devices within advanced cellular networks.

ML's involvement in the 6G network context enhances network efficiency in managing the enormous volume of mobile data traffic. These ML-driven technologies improved data rates, energy, and power efficiency and reduced latency in the 6G network. Furthermore, the proliferation of massive antenna elements, smartphones, and the utilization of extensive frequency bands generates a significant amount of mobile traffic data. Such big wireless data exhibit distinct characteristics, such as unique dimensions, personalized and multisensory features, and real-time attributes [25]. User trajectory information is captured in real-time scenarios through multidimensional spatiotemporal data from multiple sensors. These real-time mobile traffic data exhibit strong correlations and patterns, incorporating exclusive statistical features in diverse dimensions, including location and time [26]. Moreover, the received signal in wireless communication comprises highly correlated multipath signals that undergo direct transmission, scattering, reflection, and diffraction. The faded or multipath components exhibit correlations related to scatterer distribution, transmitter (Tx) and receiver (Rx) locations, carrier frequency, and more. Notably, statistical properties such as root mean square (RMS), received power, delay spread, RMS angle spread, and angular momentum align closely with the channel. However, the channel state and conditions in wireless communication systems exhibit frequent variations, making it time-consuming to run existing models repeatedly. In contrast, recent approaches utilize artificial neural networks (ANNs), such as feed-forward neural networks (FNNs) and radial basis function neural networks, to learn directly from real-time generated data [3]. These ANN-based channel model frameworks offer improved accuracy compared to traditional stochastic channel modeling approaches. ML applications in wireless communication encompass various tasks, including clustering, classification, and regression. Learning, training, and validating these data improve the network's efficiency, accuracy, and intelligence. ML techniques have been widely employed in indoor and outdoor localization/positioning tasks, with SVM and RVM serving as practical algorithms for non-probabilistic binary and probabilistic classification, respectively [27], [28], [29], [30]. Additionally, SVM has been utilized for spectrum sensing and antenna selection [31], while SVM and NB algorithms have been applied to antenna selection in different scenarios [32]. Other notable ML applications include caching, resource allocation, interference management, channel estimation, modulation classification, scenario classification, user clustering, communication protocol-based route selection, optimal node deployment, geographical area-based cluster size selection, and optimized cluster size classification.

#### 4) FEDERATED LEARNING IN COMMUNICATION NETWORKS

Traditional ML techniques used in 5G rely on centralized data collection and processing, which can lead to privacy concerns and scalability issues in large-scale implementations. The evolution towards 6G communication emphasizes decentralized and intelligent learning, connecting intelligence across various devices and objects to address these limitations [33]. The goal is to establish a human-centric approach, shifting away from solely data-centric, machine-centric, or application-centric. Consequently, federated learning (FL) emerges as a promising technique in 6G to support privacy over open channels. FL is crucial in novel applications such as holographic communication, remote area connectivity, autonomous vehicle mobility, smart railway mobility, industrial automation, and extended reality.

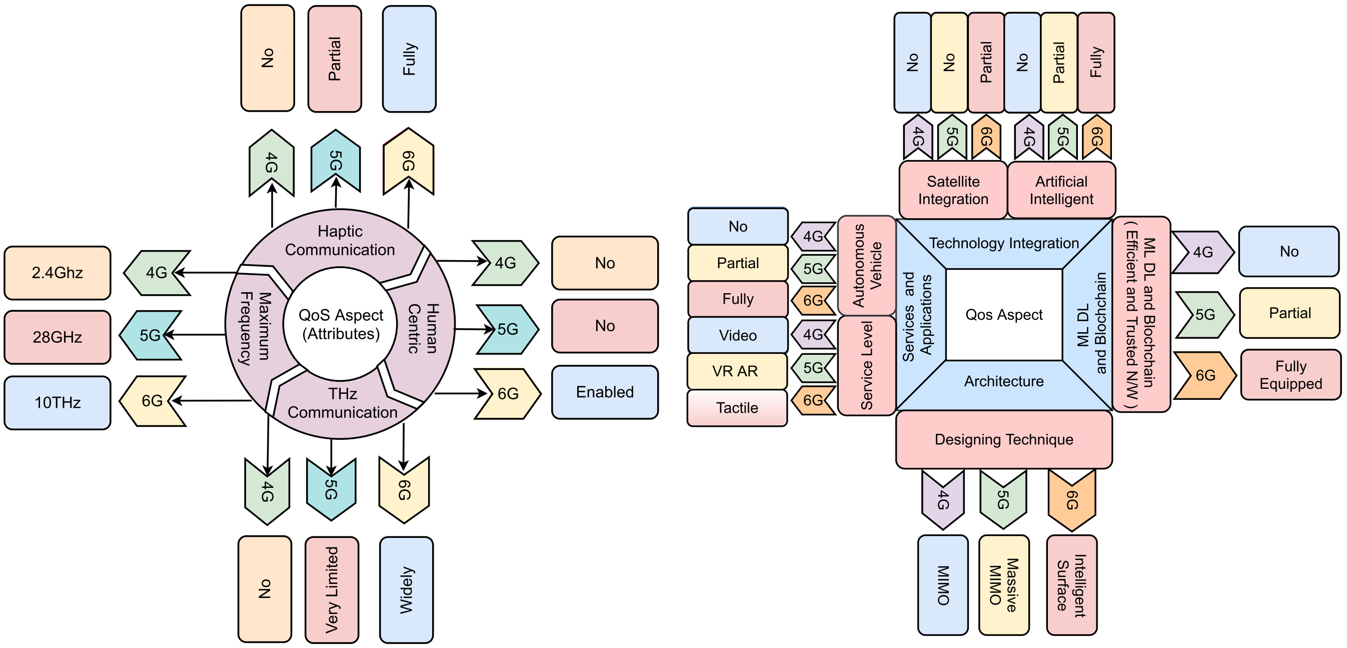
The integration of AI in 6G enables rapid and efficient data collection, learning, and transmission, supporting a wide range of innovative applications and services [34]. Compared to 5G, 6G communication is expected to provide enhanced security measures. The integrated FL approach in 6G eliminates single-point failures, ensuring robust data-driven ML in large-scale heterogeneous and diversified networks. FL in 6G communication empowers distributed learning at the edge, where private data is kept locally on training devices. Training is conducted at the edge level, preserving network security rather than relying on a central server through the wireless channel. This federated understanding of 6G communication attracts attention from academia and industries [35], [36].

In FL, edge devices collaborate to train a shared model using their locally generated data, uploading only model updates rather than raw data to centralized parametric servers. However, challenges are associated with long-range communication costs and security issues arising from the involvement of numerous participating entities and heterogeneous components [37], [38]. In a vast 6G network, edge-level model training and inference efficiency pose significant challenges due to the immense number of intelligent edge mobile devices. Despite the aforementioned challenges, the desirable features of seamless intelligence, high-performance connectivity, and secure networking drive the development of ubiquitously distributed learning-enabled 6G communication. This approach aims to enhance network robustness and intelligence through high-performance networking, energy efficiency, security, privacy protection, increased device density, and green communication.

#### 5) ML IN RESOURCE AND NETWORK OPTIMIZATION

Deploying densely populated small cells in areas with high user density and resource demands has led to optimizing diversified networks to meet the requirements of multimedia traffic, end-to-end (E2E) QoS, and overall efficiency. Notably, ML is pivotal in resource and network optimization in 6G communication. ML techniques enable intelligent resource allocation, scheduling, and optimization in ultra-dense and highly dynamic networks. ML algorithms can adaptively allocate resources, optimize network performance, and enhance QoS parameters based on analyzing large volumes of data and learning from network behavior. ML-based approaches facilitate efficient utilization of limited resources, improve network capacity, mitigate interference, and ensure seamless connectivity in 6G wireless communication systems [39]. For example, RL can be utilized for resource allocation and scheduling, genetic algorithms, SVM, particle swarm optimization, and Bayesian optimization for resource allocation as well as optimization.

Furthermore, ML can be leveraged for intelligent beamforming in 6G wireless communication networks by maintaining consistency in the allocated workload. In the context of receive beamforming, the objective is to maximize the SNR by finding an optimal beamformer while considering constraints such as keeping the signal gain constant and



(a) Summary of QoS in recent communication technology

(b) Summary of QoS in technology integration

**FIGURE 5.** Distinctive potential QoS in progressive generations of wireless communication networks.

minimizing noise power while maximizing the signal gain. This beamforming optimization adds to the overall efficiency and performance of the 6G wireless communication network. For illustration, consider receiving beamforming conditions in the single input multiple output case where any of the above-illustrated optimization techniques can be exploited. In the following consideration, the single transmit antenna and $i$ receive antennas, $x$ transmitted symbol, $y_i$ received symbol on $i^{th}$ place, $h_i$ fading channel coefficient corresponding to antenna $i$. Moreover, the system is given as [19]

$$\bar{y} = \bar{h}x + \bar{n} \tag{1}$$

and the corresponding received signal is

$$r = w_1y_1 + w_2y_2 + w_3y_3 + \ldots.. + w_iy_i \tag{2}$$

here performing the weighted combination of received signals; however, the received signal $r$ can be seen as follows

$$r = \bar{w}^T\bar{y} = \begin{bmatrix} w_1 & w_2 & w_3 \ldots . w_i \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_i \end{bmatrix} \tag{3}$$

Here in this network optimization problem, it is necessary to find the optimal vector $\bar{w}$ to maximize SNR. By choosing these optimal weights, the beam can be formed in a particular direction to achieve beamforming subject to constraint $\bar{w}^T\bar{y} = 1$, which is a convex function, considering the first condition of optimization, minimize $\sigma^2\|\bar{w}\|^2$ with signal constraint $\bar{w}^T\bar{h} = 1$. Consequently, based on the above analysis, one can define a convex optimization problem as a summation of the convex objective function + convex constraint. Furthermore, by using the Lagrangian multiplier λ deduce $\bar{w}$ in $\bar{w}^\star$ form, which is an optimal beamformer vector for which $\bar{w}^\star = \frac{\bar{h}}{\|\bar{h}\|^2}$ and $SNR = \|\bar{H}\|^2\frac{P}{\sigma^2}$ where $\frac{P}{\sigma^2}$ is transmit $SNR$ and $\|\bar{h}\|^2$ is norm of fading channel vector [40].

### 6) ML FOR AD IN WIRELESS COMMUNICATION NETWORKS

Wireless communication networks, including personal area networks, local area networks, metropolitan area networks, wide area networks, and virtual private networks, rely on wireless data connections between mobile network nodes [41]. However, the shared wireless channel raises privacy concerns and necessitates robust network security [42]. Moreover, intruder attacks such as wardriving, RF jamming, bluesnarfing, and encryption attacks are common in wireless networks. Consequently, intrusion detection systems (IDS) and network monitoring are crucial to combat these threats. Thusly, AD plays a significant role in identifying network abnormalities using statistical methods, streaming algorithms, and ML approaches. ML enables the classification of normal and abnormal network behavior, providing efficient AD and improved network security. ML algorithms can adaptively detect intrusions and classify network behavior in real-time by analyzing network data [43], [44]. ML in AD offers a scalable and effective solution to protect wireless communication networks from malicious activities. Further, the author in [45] proposed an ensemble learning (EL) algorithm based AD in wireless communication networks.

**TABLE 1.** ML applicability for AD in wireless communication networks.

| Method | Anomaly type | Type of ML used | Useful facts |
|---|---|---|---|
| Supervised learning | Known anomalies | Decision Trees, Random Forests, SVMs | Required labeled training data with labeled anomalies for training the model. Features extracted from network traffic can be used for classification. Supervised learning is effective when specific types of anomalies are well-defined and labeled in the training data. |
| Unsupervised learning | Unknown anomalies | Clustering such as k-means, Gaussian Mixture Models | It does not require labeled data, as it aims to discover anomalies based on deviations from normal behavior. Cluster-based techniques group similar data points, while density estimation methods identify outliers. Unsupervised learning is suitable when the types of anomalies are not well-known or labeled. |
| Semi-supervised learning | Known and unknown anomalies | Combination of labeled and unlabeled data | It initially uses a small set of labeled data to train a model and then applies the model to a more extensive set of unlabeled data. Combining both labeled and unlabeled data helps improve the detection of known and unknown anomalies. It balances the availability of labeled data and the need for broader anomaly detection. |
| Deep learning | Known and unknown anomalies | DNNs, Recurrent Neural Networks (RNNs), Autoencoders | Deep learning techniques like DNNs and RNNs can capture complex patterns in network traffic data and sequential dependencies. Autoencoders can reconstruct normal behavior and identify deviations. Deep learning is effective when the network data exhibits intricate patterns or when sequential analysis is necessary. |
| Ensemble methods | Known and unknown anomalies | Combination of multiple ML models | Ensemble methods combine predictions from multiple models to enhance accuracy and robustness. Bagging, boosting, and stacking techniques can be used to create an ensemble of models. Ensemble methods are useful for improving overall performance and reducing false positives or false negatives. |

Here, the IDS model consists of four stages combined for a robust and secure network. However, random forests and SVMs have been extensively exploited for EL, resulting in improved network accuracy and false alarms. Furthermore, the author in [46] discussed the complexity of AD by a traditional method while inferring the enhanced capability of the ML-enabled IDS. Here, the author presented an extensive survey of ML applicability for AD in communication networks. As a result, we present a crisp summary of it in a tabulated form, as shown in Table 1.

### 7) ML IN THE CLASSIFICATION OF NETWORK TRAFFIC, ROUTING OPTIMIZATION, RESOURCE MANAGEMENT, AND NETWORK SECURITY

The present subsection covers ML applications in network traffic classification, routing optimization, resource management, and network security.

#### *a: NETWORK TRAFFIC CLASSIFICATION*

Understanding network traffic, load, and demand is crucial for service providers. Network traffic is typically categorized into two parts, payload and host-based approaches, but these have limitations, such as being deceptive, computationally exhaustive, and vulnerable to routing asymmetry. Consequently, ML offers a comprehensive solution for traffic analysis, including traffic prediction, connection analysis, load balancing, volume estimation, and intensity monitoring. Supervised learning techniques like SVM, kernel methods, and NN are commonly used. ML enables data collection, feature extraction, algorithm selection, and model design, leading to more accurate network traffic analysis. Thusly, service providers can enhance network robustness, intelligence, self-reliance, and connectivity by acknowledging the limitations and leveraging the appropriate ML techniques [47], [48].

#### *b: OPTIMIZATION IN NETWORK ROUTING*

Route optimization is crucial for improving communication and networking performance. The adaptive and shortest-path algorithms are the prominent methods used for this purpose. However, the adaptive algorithm's high computational complexity imposes constraints and limits its operation in the current network, which relies on data-driven algorithms. In contrast, the widely adopted shortest path algorithm offers a more efficient solution with minimal resource utilization in the network. Moreover, the ML technique has emerged as a powerful tool for addressing optimization challenges in network routing. It enables networks to become independent, intelligent, and self-configurable. In [49], bio-inspired algorithms like ant colony optimization (ACO) and particle swarm optimization were employed to find optimal paths and avoid link failures. The authors in [50] utilized a field-based routing (FBR) algorithm for wireless mesh networks, optimizing speed, time, and network resources. However, incorporating the crank back routing extension in ACO, as described in [51], made the network vulnerable to authenticated nodes exhibiting anomalous or defective behavior, leading to network failures. In the context of heterogeneous and diversified networks, as discussed in [52], the sudden increase of IoT devices and applications resulted in traffic bursts, which were effectively handled using software-defined networking (SDN). Similarly, enhanced optimized FBR [53] incorporated neighbor node position, velocity, and cognition in a micro-mobility scenario, sustaining least-cost routing in wireless mesh networks. Furthermore, in a study involving wireless sensor networks in [54], ACO was utilized with protocols like ad-hoc on-demand distance vector, destination-sequenced distance vector, and dynamic source routing, resulting in improved packet delivery ratio, E2E delay, and optimal packet arrival time. These optimization techniques significantly enhance network performance and ensure a better QoS [5].

### c: NETWORK RESOURCE MANAGEMENT

ML enables networks to become self-configurable, convergent, self-reliant, intelligent, and robust by optimizing resource utilization through innovative resource-sharing and scheduling algorithms. In [55], the underutilization of available network resources due to limited computational capacity in cloud radio access networks (C-RANs) was addressed by integrating C-RAN with SDN and network function virtualization (NFV), resulting in a self-optimized network. The study compared SVM, time-delay neural network, and LSTM for predicting performance Another in [56] emphasized the importance of efficient resource management (RM) in cloud computing, as over-provisioning and provisioning can increase costs for service providers and cause violations of service level agreements. Consequently, optimal RM schemes such as container placement, job scheduling, and multi-resource scheduling were proposed to address these challenges. Similarly, in the context of edge computing, where small applications and edge devices provide computational resources, optimizing resource utilization becomes crucial to avoid waste of energy and resources [57]. Task distribution and resource allocation were addressed in heterogeneous networks using unsupervised ML techniques such as k-means. In 5G C-RAN environments, computational RM faced challenges related to latency, throughput, and optimization trade-offs [58]. Dynamic RM and ML algorithms were employed to improve resource utilization, and the DRMAC-PF framework was shown to provide significant enhancements. Cloud resource management, characterized by combinatorial problems, was addressed using RL-based solutions like Deep RM plus, which demonstrated improved performance [59]. Finally, in resource-intensive IoT applications and ultra-dense 5G networks, techniques such as multi-access edge computing (MEC) and ultra-dense edge computing were explored. Incorporating BCT and applying two-time scale deep reinforcement learning helped minimize offloading time and enhance network resource utilization [60]. These studies collectively highlight the significance of ML in optimizing RM and improving network performance in diverse application scenarios.

### d: NETWORK SECURITY

Network security is a constant concern in network operation and management. ML has emerged as an efficient technique for enhancing network security through classification, analysis, and improvement in recent years. Maintaining network security has become increasingly challenging with the proliferation of devices, applications, and network data [61]. Notably, ML offers powerful capabilities in handling massive network data, enabling automatic learning, detection, identification, and the evolution of innovative ideas.

Ensuring security is crucial in IoT networks where numerous interconnected devices communicate. In [62], the authors propose a biometric authentication system that enhances data access security. Whereas in [63], the authors introduce an adaptive online intrusion detection model based on incremental rule learning, allowing the model to self-learn and adapt to unforeseen conditions. Network security evaluation is addressed in [64] using SVM and a binary tree, minimizing risk through structural risk minimization. In [65], large-scale data analysis from the internet infrastructure is leveraged to enhance the ML-based IDS. The authors propose an extensive data-based hierarchical DL system to better understand behavior and content features. Unsupervised ML methods are explored in [66] for detecting known, unknown, and zero-day attacks, utilizing subspace clustering and one-class SVMs. In wireless sensor networks (WSNs), ML and DL solutions for IDS are extensively analyzed in [67], where a restricted Boltzmann machine-based clustered IDS is proposed and compared with existing approaches. The adoption of ML in WSNs is motivated by the difficulty of detecting intruder data patterns. In [68], a framework called AB-TRAP is introduced to detect transmission control protocol port scanning attacks in both local area networks and global internet environments. A comprehensive review of DL methods for IDS in WSNs is presented in [69] to provide a clear understanding of ML adoption. These studies collectively demonstrate the significance of ML in enhancing network security by addressing various aspects of intrusion detection and prevention.

### 8) ML IN NETWORK SLICING, NETWORK VIRTUALIZATION, AND SDN

The future 6G and beyond networks aim to provide ubiquitous connectivity for various devices in wireless networks. These networks will offer ultra-high data rates, ultra-low latency, and support for high mobility. They will handle dense and opaque wireless environments, enabling massive machine-type communications (mMTC) and reducing energy consumption by 90%. Low-power devices will connect seamlessly with significantly more devices and available bandwidth per unit area. Advanced technologies such as NFV, SDN, cloud edge computing, device-to-device (D2D) communication, millimeter-wave and TeraHertz (THz) communication, and network slicing will support these capabilities [70], [71].

### a: NETWORK SLICING

Network slicing is a crucial technology in 6G and beyond communication networks. It involves dividing a physical network into multiple logical networks with distinct attributes. In this scenario, various bandwidth-intensive applications can be served with a vast frequency range available. Different service classes, such as enhanced mobile broadband (eMBB), mMTC, and ultra-reliable low-latency communication (URLLC) in 5G, and super eMBB, super URLLC, and machine-type communication in 6G, cater to specific network demands, as shown in Fig. 4 and Fig. 5. Heterogeneous networks accommodate diverse consumer requirements, including IoT-enabled and factory automation applications [72]. Network slicing enables the creation of E2E slices to fulfill specific service needs, with LR, ANN, random forest, NB, and KNN models providing accurate solutions [71]. In another approach, where the authors in [73], discussed the involvement of DL in classifying packets for different applications across RAN slices, considering application-specific spectrum sharing and evolved packet core (EPC) slicing. The involvement of network slicing, EPC, and MEC slice significantly improves overall network QoS. Fog computing is employed in another study to bring cloud capabilities to the IoT edge network, using a multi-objective optimization algorithm based on ML for priority classification and enhancing QoS and delay performance [74]. In vehicle-to-everything (V2X) services, network slicing is explored as a solution to support stringent and dynamic requirements. ML techniques are leveraged to automate the network and allocate network resources to different slices, ensuring the virtualization of network functions and multi-dimensional network efficiency [75].

#### *b: NFV*

NFV is an approach to executing network functions using software applications on commodity hardware devices. It allows tasks like routing, load balancing, and firewall to be performed on ordinary hardware, maximizing flexibility and cost-effectiveness [76]. In the context of 6G and beyond communication networks, NFV aims to simplify the provisioning a wide range of network services, maximizing QoS and efficiency. This opens up new opportunities for revenue generation through innovative services [76]. The authors in [77] combine NFV with ML techniques to enable intelligent estimation, forecasting, and adaptive model reshaping in the face of temporal network fluctuations. NFV facilitates the deployment of logically sliced networks tailored to specific applications and user demands within a diverse and heterogeneous network environment [77]. Furthermore, the authors in [78] address the RA problem in dense, heterogeneous IoT networks where low-cost devices with limited computational power are prevalent. The proposed approach integrates NFV and RL to solve the RA problem efficiently. By leveraging RL techniques and accessing network resources through NFV, data transmission in IoT networks can be optimized. The substrate network, enabled by NFV, supports data transmission and service function chaining to fulfill users' requests [78]. Additionally, NFV is recognized as an enabling technology for cost-effective and efficient operations in telecommunication service provider infrastructures. It contributes to developing a zero-touch network and service management system, integrating ML approaches [79].

#### *c: SDN*

SDN is a widely recognized and essential technique in the architecture of 6G and beyond communication networks [71]. Leveraging software applications, enables centralized and intelligent control of network functions. In heterogeneous networks, SDN technology is crucial in making network architecture more intelligent, dynamic, and customized. Consequently, an integrated approach combining AI and ML significantly enhances the network's controllability, security, economic efficiency, efficient network resource management, route planning, traffic classification, scheduling, fault detection, diagnosis, and network security [80].

In [81], the authors explore the estimation of application-specific ML models based on the extensive and diverse data collected from SDN. Proper classification of the collected information and data types is performed to cater to the varying demands of an intelligent communication network in a dynamic network environment.

The softwarization of the network through techniques such as NFV and SDN proves beneficial in accommodating new user demands [82]. The exponential growth in internet usage has led to a massive influx of data generated per second [83]. Consequently, innovative techniques such as cloud computing have emerged to meet these increasing demands. SDN addresses the need for energy-efficient networks, offering improved QoS, centralized control, reduced latency, efficient routing, and effective handling of heterogeneous communication networks. When combined with MEC and ML, SDN enhances network efficiency in QoS and self-organized WLANs [84]. As user demands increase rapidly, networks become more prominent, complex, and heavily loaded. As an intelligent and proactive approach, SDN enables centralized control, traffic prediction, and autonomous network management [85]. QoS becomes a critical requirement in networks with multiple flows. In [86], a QoS-aware routing protocol and an efficient rule placement algorithm based on Deep Reinforcement Learning (DRL) are proposed to determine optimal paths and predict future traffic loads dynamically. Furthermore, in [87], the IoT in vehicular networks is replaced by the Internet of Vehicles (IoV), demanding substantial computational capabilities. SDN improves RM in IoV networks, while Road Side Units placement is optimized to ensure security and reduce communication delays. Furthermore, the intrusion attack in communication networks is addressed in [88] using an ML-based IDS in SDN. SDN facilitates data access across the network, and the paper proposes an anomaly-based network IDS called Neptune, which utilizes multiple ML classifiers and traffic flow features. Additionally, SDN proves valuable in combating Distributed Denial of Service (DDoS) attacks, with techniques such as DDoS degree and improved KNN helping to identify and mitigate such attacks [88]. Overall, SDN plays a significant role in enhancing network intelligence, security, and performance, while its integration with ML techniques enables proactive management and adaptation to dynamic network conditions.

### *C. ML IN NON-CONVENTIONAL MEDIA COMMUNICATION*

In the current wireless communication landscape, the scope extends beyond terrestrial networks to include non-conventional media communication, such as Underground Wireless Sensor Networks (UGWSNs) and Underwater Wireless Sensor Networks (UWWSNs). These networks facilitate the deployment of the Internet of Underwater Things ($IoT_W$) and Internet of Underground Things ($IoT_G$) ecosystems, connecting objects in underground living, and underwater environments. ML techniques are leveraged to infuse intelligence into these network ecosystems, making the networks more sophisticated, autonomous, and self-reliant. The applications include intelligent ships, automated marine transportation systems, underwater and underground research, disaster prediction and management, the classification, processing, and monitoring of underwater habitats and marine life, along with the global oceanic and mainland trade [89]. Non-conventional media communication networks, including UWWSNs and UGWSNs, face inherent challenges due to their incongruity and the need to operate in harsh environmental conditions. These challenges include limited resources, channel constraints, energy constraints, physical requirements, marine blockage, and Big Marine Data management generated by specialized sensors, hydrophones, and waterproof cameras. ML and DL techniques are adopted in these networks to handle this vast amount of data efficiently. However, the wireless communication network for non-conventional media communication still needs to be developed, with limited resources and knowledge in this domain [90]. Furthermore, the extensive operational areas of sea, ocean, and coastal monitoring often need more sensor node deployment. To overcome this challenge, low-energy sensors are widely employed in non-conventional media communication networks characterized by immense, inhospitable, and erratic channel conditions.

Exploring and analyzing data collected from these networks has significant implications for human and marine life. For instance, sensor data can be used to assess the impact of human activities on resources in marine and mainland ecosystems, as well as monitor pollution levels in land and sea environments [90]. In UWWSNs and UGWSNs, the sparsely deployed sensor nodes pose challenges in achieving adequate coverage. Consequently, these nodes are connected to the internet, transforming the network into an IoT ecosystem comprised of sensing and communication units. ML and DNNs, such as fully connected networks, dense networks, deep belief networks, CNNs, autoencoders, recursive neural tensor networks, and RNNs, are employed for tasks such as data classification, input data reconstruction, hierarchy extraction, data sequence prediction, and time-series analysis. Multiple hidden layers in NNs enable complex learning and inference [91]. Localization and synchronization of nodes pose significant challenges in non-conventional media communication networks due to the unpredictable nature of underwater and underground channels, influenced by factors like temperature fluctuations, salinity variations, pressure changes, marine life interactions, and internal waves. Additionally, these networks often lack global positioning system coverage. ML techniques are employed to address these challenges. For example, a framework for synchronization and localization utilizing ray-tracing for channel modeling and ML estimation techniques, such as the maximum likelihood estimator, has been proposed [92]. Non-convex ML problems are solved using Gaussian network algorithms, resulting in more accurate and energy-efficient solutions compared to previous approaches [92]. Similarly, models utilizing received signal strength and NN responses are employed to estimate distances between nodes and predict node locations in underwater and underground environments. Various network architectures, including feed-forward, recurrent, time delay, and distributed delay networks, are incorporated for position estimation with low prediction error. However, due to the varying channel conditions, it remains challenging for next-generation non-conventional media communication networks to locate and recognize targets accurately. Moreover, using traditional ML algorithms for extensive data analysis poses limitations and can be computationally expensive. A dense CNN model has been proposed to address the issue of variable underwater acoustic channels and the need for efficient target identification. This model utilizes the fluctuating nature of non-conventional media communication channels and leverages natural resource utilization in maritime areas, military surveillance, and oceanographic research. The model classifies Modulation and Coding Scheme (MCS) levels using a boosted regression tree, achieving high accuracy levels of up to 99.97% [93].

In non-conventional media communication networks, such as Underwater Acoustic (UAC) networks, channel conditions are spatially and temporally varying, making it challenging to establish reliable links and optimize network efficiency. Adaptive modulation and coding techniques have been developed to match transmission parameters with the current channel conditions, improving network performance. Rule-based strategies have been employed to measure sea trial datasets and select appropriate links based on channel attributes. However, the limitations of rule-based approaches, such as subjectivity and expert knowledge dependence, limited adaptability, difficulty in capturing complex relationships, limited generalization, scalability issues, and lack of learning and adaptation, have led to the adoption of ML techniques. For instance, an ML-based concept is utilized to enhance network efficiency and stability in the UAC network, using the ML algorithm for classifying MCS levels. The results demonstrate high accuracy and efficient system performance [90]. In UWWSNs and UGWSNs, accurately predicting and measuring physical parameters, such as oxygen levels, pressure, temperature, water stream direction, velocity, water pollution, salinity, and volcanic activity, pose challenges due to the dynamic nature of sensor node movement within the vast water environment. This physical motion leads to rapid changes in network topology. Additionally, no well-established routing protocols exist for non-conventional media communication networks. A balanced routing protocol based on ML approaches has been developed to address these challenges and consider abnormalities in such networks. The proposed RL-based (Q-learning) approach enhances energy efficiency and reduces latency, improving overall network performance [94]. Furthermore, ML techniques have been applied in underwater wireless optical communication, where simulations of visual irradiance profiles and diffraction patterns are performed using the Monte Carlo method. Convolutional and fully connected layers are employed to analyze the data. The proposed transfer learning (TL) based ML framework exploits image features and channel information, and fine-tuning is utilized to improve network performance [95].

In summary, the current state of non-conventional media communication networks, including UWWSNs and UGWSNs, presents unique challenges related to harsh environmental conditions, limited resources, channel constraints, and managing vast amounts of data. ML and DL techniques are crucial in addressing these challenges and making the networks more intelligent and efficient. Localization, synchronization, target identification, routing, and optimization are vital areas where ML techniques are applied. By leveraging ML algorithms and adaptive approaches, these networks can overcome the limitations of traditional methodologies and pave the way for advancements in non-conventional media communication.

### D. ML IN 6G-IOT

Many IoT devices have sensors, processing capability, software, and advanced ML technology. These devices exchange data with one another, enabling ubiquitous connectivity and enhanced embedded systems. The applications of IoT devices span various sectors, including organizational, infrastructure, industrial, consumer, and military domains. Furthermore, the scope of IoT extends beyond terrestrial networks to underwater and underground sensor networks.

The IoT network generates vast amounts of big data due to numerous sensors, intelligent devices, and user demands. Effectively managing and interpreting such extensive data from WSNs poses significant challenges. Researchers have explored ML techniques for online learning and vision applications in 6G-enabled IoT networks to address this [96]. By leveraging massive, diverse smart devices, ML-based online learning aims to make the system intelligent and adaptable, thereby improving efficiency. This ML-enabled online learning includes RL, online gradient descent, SVM, clustering, and Q-learning for network sites, device side, and edge networks [97].

One of the proposed ML models is gradient-boosting decision tree-based NN, which enhances the learning ability of the system through hidden layers of neural networks. Experiments demonstrate improved performance in prediction and explanation using this model. Additionally, ML techniques have been employed in various applications such as augmented reality, gaming, education, healthcare monitoring, and agriculture systems in [98]. An ML-guided image compression framework has been proposed to facilitate efficient transmission to compress image data while maintaining essential features for pattern recognition [98]. Another notable area where ML is utilized is analyzing big data generated by IoT networks [99], [100]. ML models can achieve high accuracy in human movement direction detection by capturing data from analog pyroelectric infrared sensors. These intelligent approaches extend to diverse IoT applications like the Industrial Internet of Things (IIoT) and smart meter operations. Recognizing the challenges posed by IoT devices' limited compatibility with heavy data sets, researchers have divided massive data sets into centralized and distributed scenarios, employing TL techniques tailored to each scenario's characteristics. Utilizing the VGG-16 model reduces training time and improves accuracy. Furthermore, ML plays a crucial role in decision support systems for IoT networks, specifically in predicting costs for intelligent meter operations and recommending actions.

Considering the vast amount of heterogeneous data generated in cloud-based IoT networks, ML techniques offer an opportunity to manage and process data efficiently [101]. Learning at the edge, closer to the devices, is desirable, but resource limitations make deploying trained ML models in the cloud a more feasible solution. Cognitive radio and machine-to-machine communication in IoT networks also benefit from ML techniques. Cognitive radio mitigates spectrum crowding by maximizing utility, throughput, and packet transmission efficiency through Q-learning-based transmission scheduling. Additionally, ML-based reinforcement learning techniques are employed for resource allocation in NFV-enabled IoT networks. ML's potential to enhance cybersecurity, indoor localization, and distributed learning RM is also evident in the IoT domain. By utilizing ML algorithms such as SVM, KNN, and random forest, significant improvements are achieved in localization accuracy, market mood analysis and prediction, deep eigenspace learning, and malware detection. In the realm of IoT, adopting ML techniques is crucial for addressing challenges and harnessing the full potential of interconnected devices [102]. Consequently, integrating ML into IoT networks flourishes smooth and efficient network functioning.

However, unfortunately, deploying ML models in resource-constrained IoT devices remains a significant obstacle. To overcome this limitation, cloud-based solutions offer a promising approach by offloading the computational burden to more powerful servers. By leveraging parallelism in computation, ML empowers IoT networks to process and analyze the massive amounts of data generated by diverse applications and devices. This is particularly relevant in intelligent healthcare, agriculture, environment monitoring, intrusion detection, and education systems [103]. The cognitive radio network, which combines IoT and ML, effectively addresses the issue of limited spectrum

**TABLE 2. Comparative summary of public BC, private BC, and consortium BC.**

| Feature | Public BC | Private BC | Consortium BC |
|---|---|---|---|
| Definition | A BC that is open to anyone to participate in and validate transactions. | A BC that is permissioned and only allows a selected number of participants to validate transactions. | A BC that is permissioned and allows a group of organizations to validate transactions. |
| Accessibility | Open to anyone. | It is restricted to a selected group of participants. | It is restricted to a consortium of organizations. |
| Transparency | High, as transactions and their validation are visible to anyone on the network. | Low, as transactions and their validation may not be visible to everyone on the network. | Medium, as transactions and their validation are visible to consortium members. |
| Security | High, as public BCs are secured by a decentralized network of nodes. | High, as private BCs can implement additional security measures such as encryption. | High, as consortium BCs are secured by a limited number of trusted participants. |
| Speed of Transactions | Slow, as the network, relies on consensus from numerous nodes. | Faster than public BCs, as the network has fewer nodes. | Faster than public BCs, as the network has fewer nodes. |
| Cost of Transactions | Typically low, as no central authority needs compensation. | Higher than public BCs, as the cost of maintaining a private network is higher. | Higher than public BCs, as the cost of maintaining a consortium network is higher. |
| Control over Data and Transactions | It is decentralized, with no single entity having control. | It is centralized, with a single entity or a select few having control. | It has centralized, with control split among members of the consortium. |

availability and maximizes system utility through intelligent transmission scheduling. In terms of security, ML plays a vital role in safeguarding IoT networks from cyber threats and intrusions. ML-based learning for cybersecurity in IoT and cyber-physical systems offers insights into different use cases, including sound, harmful, and malicious scenarios. ML algorithms help detect anomalies and identify patterns that signify potential attacks, contributing to the resilience and protection of IoT ecosystems [78]. Furthermore, ML techniques enhance localization accuracy in indoor environments, where traditional methods face challenges due to signal irregularities. ML-based outlier detection and localization models, utilizing supervised and unsupervised learning approaches, demonstrate significant improvements in accurately locating network nodes and constituents. Distributed learning RM in IoT networks also benefits from ML, enabling efficient analysis of market moods, prediction models, and malware detection. ML algorithms such as deep eigenspace learning and ensemble classifiers provide valuable insights and enhance decision-making in complex IoT environments.

In conclusion, integrating ML techniques into IoT networks has transformative potential. ML empowers IoT ecosystems to unlock their full capabilities, from intelligent resource allocation and efficient data management to enhanced security and accurate localization. As IoT continues to evolve and expand, further advancements in ML will undoubtedly play a crucial role in shaping the future of interconnected devices and applications.

## III. THE ESSENCE OF BCT

BCT, initially conceived for cryptocurrencies, has gained significant attention in wireless networks as it facilitates secure and traceable connections between anonymous individuals. BCT is a decentralized database that ensures secure and tamper-proof record-keeping through cryptography. It consists of interconnected blocks, forming a continuously growing list of records. Indeed, wireless networks can leverage BCT to ensure secure and reliable data sharing. This section provides a comprehensive overview of the fundamental concepts of BCT, its necessity, importance, characteristics, variety, and architecture. We also explore the application of BCT in wireless communication systems and non-conventional media communication.

### A. NECESSITY TO HARNESS QUAINT FEATURES OF BCT

With the rapid growth of the IoT, wireless networks have become more complex and widespread, leading to heightened security risks and challenges. This necessitates harnessing the extensive exploitation of BCT owing to the intense use of the internet and the generation of vast amounts of data; there is a need to regulate digital commerce, protect personal data, and ensure network security and privacy. Furthermore, BCT finds application in terrestrial and non-terrestrial wireless networks, including air, underwater, and underground networks, as well as secured IoT, network logistics, supply chain management, medical information sharing, and government benefits. This has motivated the investigation of BCT for wireless networks driven by its breakthrough applications in cryptocurrencies.

BCT operates as a collection of interconnected blocks that follow specific rules. Each block in the BC contains the previous block's generated hash, creating an immutable and tamper-proof ledger for digital transactions and events. Adding new blocks is achieved through a consensus mechanism executed by all participants, ensuring the integrity of the stored information. BCT's decentralized nature allows it to effectively manage the digital ecosystem without centralized control or human intervention, leveraging attributes such as decentralization, anonymity, immutability, transparency, pseudonymity, autonomy, and audibility.

In the realm of 6G wireless communication networks, BCT integrated with ML plays a significant role. BCT can also provide valuable information in wireless networks, such as the best routing protocols, node identity details, battery and power status of nodes, available spectrum details, network optimization parameters, and characteristics of malicious nodes. Additionally, in dense and diverse communication networks, evaluating network performance metrics can be challenging due to dynamic channel conditions. As a result, smart contracts offer an intelligent solution as computer programs that automatically execute the terms of specific agreements, contributing to efficient network management. The combination of BCT and ML and smart contract utilization pave the way for secure, reliable, and optimized wireless communication networks.

### *B. ASSORTMENT AND ARCHITECTURE OF BCT*

In the BCT architecture, multiple nodes in a decentralized network hold copies of the entire database, eliminating the need for a centralized authority. This approach offers enhanced security and reliability. The versatility of BCT is reflected in its applications, including cryptocurrencies, smart contracts, supply chain management, and digital identity management [104]. By securely storing and managing data, BCT has the potential to revolutionize various industries and transform transactional processes. The architecture of BCT is detailed in Fig. 6, showcasing its components and their interconnections. Within the BCT ecosystem, the assortment is done across three main categories, which will be discussed in the subsequent subsection. The governance aspect is vital to ensure appropriate access to sensitive data and establish an effective administrative model for BCT implementation. This involves addressing the complexities associated with different participants, such as governors, administrators, consumers, providers, developers, and validators, along with the associated levels of jurisdiction, liability, and responsibility. A set of predefined rules governs these interactions. Additionally, the access and control layer of BCT utilizes ledger construction in a decentralized manner aligned with the requirements of the network. It involves adhering to predefined governance rules that authenticate and regulate operation and management functions. These rules grant users access to BC services and resources, considering security, activity, permission management, and system and node-level permissions. BC networks may have varying permission levels, determining who can read or write data. The system's design must address these considerations to ensure smooth functioning, whether in a public or private internet setting or within a general-purpose network such as Ethereum [105].

BC is broadly categorized into public BC (permissionless), private BC (permissioned), and consortium BC. Each category has distinct characteristics, advantages, and disadvantages, which Table 2 discusses in detail. Further insights into public, private, and consortium BCs are provided in Fig. 9 [106], [107].

#### 1) ARCHITECTURE OF BCT

BCT is an immutable network that facilitates secure digital transactions and maintains a record of online activities through a series of interconnected blocks. These blocks cannot be altered and provide indefinite verification. The authentication of ledger records is typically managed by a P2P network of users who must reach a consensus on any changes made to the blocks. Majorly the BCT architecture comprises distributed networks, blocks, cryptography, consensus mechanism, smart contracts, decentralization, privacy and security, network protocol, and tokenization. Which we discuss in this section in detail. Herein, we explore the design, implementation, and ongoing research of critical components within BC, including the architecture, blocks, networks, and consensus mechanisms. A block comprises a block header, and the body stores the transaction information, while the block header contains fields such as the block validation rule, merkle tree root, timestamp, nonce, and a hash of the parent block, as shown in Fig. 7. The block's size and transaction volume determine its capacity. Within the BC network, there are two types of nodes: complete and light nodes, each with its capabilities [108]. Fig. 8 and Table 3 provide a detailed illustration of these BC nodes.

Beyond diverse applicability, BCT is being adopted in various industries to develop decentralized applications, including gaming, client resource networks, IoT, complex supply chains, provenance traceability, and currency distribution credits. These applications leverage the features of BCT to achieve reduced latency, streamlined authentication and authorization, offline transaction capabilities, and robust reliability for system upgrades and error recovery [109]. Numerous innovative uses of BC have been explored, such as coupling it with existing cloud solutions to enhance productivity, performance, security, and safety within cloud data centers [110]. BC finds applications in various domains, such as validating credentials, tracking the provenance of items through a chain of custody, and more. The authors in [110] present a hierarchical architecture for decentralized application development in this paper.

Next, we delve into smart contracts as an intelligent approach to problem-solving within the BC ecosystem. Smart contracts are automated transaction methods that execute predefined agreements without relying on a central authority. They have been extensively studied in literature and are implemented as computer programs in BC applications such as Ethereum and Hyperledger. Stakeholders can enforce specific agreements related to activities or transactions in a BC P2P network, and the records of these activities are stored within the BC. The sequencing of transactions on the BC determines the status of the agreement and the stakeholders' wealth [109].

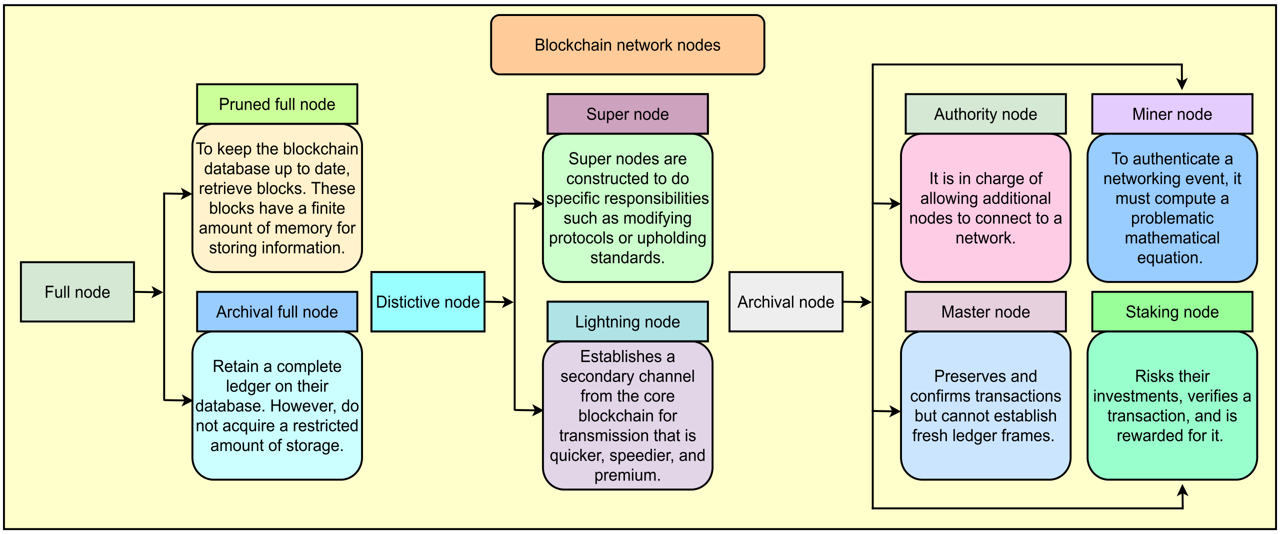

Blockchain network nodes
Full node
Pruned full node
To keep the blockchain database up to date, retrieve blocks. These blocks have a finite amount of memory for storing information.
Archival full node
Retain a complete ledger on their database. However, do not acquire a restricted amount of storage.
Distictive node
Super node
Super nodes are constructed to do specific responsibilities such as modifying protocols or upholding standards.
Lightning node
Establishes a secondary channel from the core blockchain for transmission that is quicker, speedier, and premium.
Archival node
Authority node
It is in charge of allowing additional nodes to connect to a network.
Miner node
To authenticate a networking event, it must compute a problematic mathematical equation.
Master node
Preserves and confirms transactions but cannot establish fresh ledger frames.
Staking node
Risks their investments, verifies a transaction, and is rewarded for it.

**FIGURE 6.** Description of distinctive BC nodes in a decentralized ecosystem.

### 2) SMART CONTRACT PECULIARITIES

- BCT architecture utilizes multiple languages, scripts, protocols, and smart contracts to enable extensive programmable transactions. The agreement layer provides automation and programmability to the BC.
- Smart contracts are private state regulations maintained on the BC that enable the management of virtual currencies, articulate business logic, and define the rights and responsibilities of stakeholders.
- When entities agree on a smart contract, it is executed cryptographically and shared on the BC for confirmation. The contract operates autonomously, following established rules when conditions are met [115].
- A smart contract is a self-executing mechanism on the BC network. It is verified by network entities, similar to cryptocurrency transactions, confirming input-output credentials and contract status.
- Ethereum is the first BC ecosystem that supports Turing-complete smart contract languages, making it highly accessible.
- Ethereum's Turing-complete programming allows flexible rule creation transaction formats and decentralized application deployment through smart contracts.
- Solidity is widely utilized in Ethereum for developing smart contracts, making it one of the most commonly used programming languages [116].
- Furthermore, intelligent contracts, such as those for citizens, healthcare, grid, transportation, and education, extend the application of BCT to intelligent cities [117].

### 3) CONSENSUS MECHANISM

A BC is a decentralized public distributed ledger managed collectively by the network. It relies on consensus techniques to ensure an accurate and transparent history of events. While consensus based on PoW can handle thousands of untrustworthy entities, it has drawbacks such as network latency, lower transaction frequency, and high energy consumption [118]. The consensus process choice depends on the BC platform's specific requirements and applications. Experts have developed novel algorithms like proof of stake (PoS) and proof of elapsed time (PoET) to address EE, reducing the need for costly computational mining [119], [120]. Additionally, researchers have explored block finalization algorithms based on Byzantine Fault Tolerance (BFT) unanimity. Various consensus mechanisms are depicted in Fig. 10, and detailed comparisons are presented in Tables 4 and 5 for better understanding.

## C. PRIVILEGED CHARACTERISTICS OF BCT

### 1) IMMUTABILITY

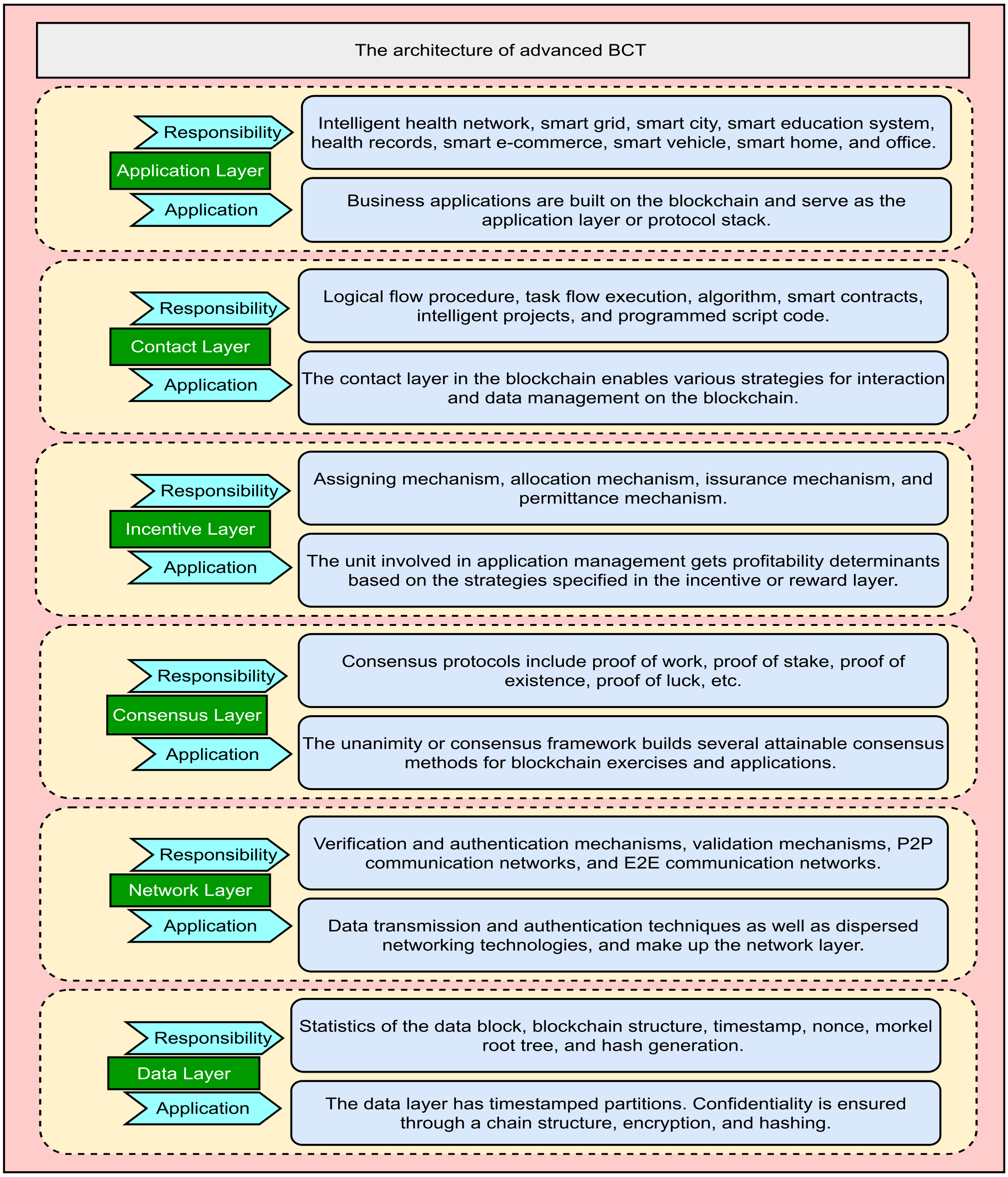
In the BC, an immutable ledger refers to a document that cannot be modified once created. Immutability signifies that modifying without collaboration is exceptionally arduous. The BC ledger's primary concept is data protection and verification that data has not been updated or manipulated once recorded in a BC.

### 2) SECURITY

BC security encompasses a robust threat management system, including affirmation services, cybersecurity standards, and diligent practices to mitigate fraud and breaches. Its decentralized and anonymized nature ensures reliable and tamper-resistant data. With a dense network of nodes, simultaneous hacking becomes highly improbable. Data immutability, a fundamental characteristic of decentralized ledger technology (DLT), ensures data protection.

### 3) AUDITABILITY

In the BC, the evidence of transactions is represented by their hashes. Unlike relying on a limited number of random


The architecture of advanced BCT

Application Layer

- Responsibility: Intelligent health network, smart grid, smart city, smart education system, health records, smart e-commerce, smart vehicle, smart home, and office.
- Application: Business applications are built on the blockchain and serve as the application layer or protocol stack.

Contact Layer

- Responsibility: Logical flow procedure, task flow execution, algorithm, smart contracts, intelligent projects, and programmed script code.
- Application: The contact layer in the blockchain enables various strategies for interaction and data management on the blockchain.

Incentive Layer

- Responsibility: Assigning mechanism, allocation mechanism, issurance mechanism, and permittance mechanism.
- Application: The unit involved in application management gets profitability determinants based on the strategies specified in the incentive or reward layer.

Consensus Layer

- Responsibility: Consensus protocols include proof of work, proof of stake, proof of existence, proof of luck, etc.
- Application: The unanimity or consensus framework builds several attainable consensus methods for blockchain exercises and applications.

Network Layer

- Responsibility: Verification and authentication mechanisms, validation mechanisms, P2P communication networks, and E2E communication networks.
- Application: Data transmission and authentication techniques as well as dispersed networking technologies, and make up the network layer.

Data Layer

- Responsibility: Statistics of the data block, blockchain structure, timestamp, nonce, morkel root tree, and hash generation.
- Application: The data layer has timestamped partitions. Confidentiality is ensured through a chain structure, encryption, and hashing.

**FIGURE 7. Illustration of advanced BCT architecture in communication layer.**

samples, BCT allows users to make decisions based on the entire history of transactions. This greatly enhances the confidence and assurance auditors can provide the public regarding their audit findings.

### 4) AUTONOMY

In the BC, each node autonomously transmits and gathers transactions using consensus protocols. Through the use of public or private cryptographic keys, transactions are guided and processed without the need for human intervention or a trusted third party. This ensures the prevention of conflicting or duplicate entries in the BC.

### 5) PSEUDONYMITY

In BCs like Bitcoin and Ethereum, instead of being anonymous, they utilize pseudonyms. An address is an alias for the individual who owns the corresponding private key. However, the actual identity of this person remains unknown. Nevertheless, all actions associated with this address can be traced back to them.

**TABLE 3. Illustration of distinctive nodes in BCT [111], [112], [113], [114].**

| Types of node | Attribute | Explanation |
|---|---|---|
| Full node | Server role performer | In a BC network, a full node acts as a domain controller and stores data and records of all nodes. It ensures consensus, verifies transactions and plays a role in decision-making and planning processes. |
| Lightweight node | A simple payment verification node that consumes fewer resources | A low-resource, simple payment authentication node is becoming popular in BC deployments. However, an issue arises: lightweight nodes get paid, while full nodes as light clients do not. To fix this, intelligent contracts can create fairness with a "smart light payment mechanism," encouraging full nodes to help lightweight clients on the BC network. |
| Listening node | Such nodes are openly visible and accessible | Supernodes, also referred to as listening nodes, are a sub-category of nodes in the BC network. A listening node, which is a full node, actively connects to any node that chooses to establish a connection with it. On the other hand, a reliable supernode operates continuously, distributing BC and accounting records to multiple nodes. |
| Pruned full node | It updates the newer block and eliminates the older one after the validation process | The trimmed node variant fetches block chunks, discarding older ones after a set limit, keeping headers and chain order. Recent blocks stay within memory limits, while older block access needs authentication. Unlike archival nodes, trimmed nodes offer an overview of the BC network, maintaining block metadata but retaining only headers and chain order upon size limit. |
| Light node | Local activity monitoring system, which enables faster transactions | In a search engine setup, the local server stores critical data for quick retrieval, fetching new information from the central server as required. Light nodes, or simplified payment verification nodes, aid in this process. They hold vital data like block addresses without complete block verification. These nodes are ideal for fast daily tasks. Besides lightweight nodes, exploring other node types within the BC network is essential. |
| Archival full node | Full archival nodes store the entire ledger data without memory limitations. They preserve the complete BC history. | When discussing full nodes, they usually refer to full archival nodes that store the entire BC. These nodes are responsible for achieving consensus, validating blocks, and maintaining the BC's integrity. The main difference between archival and pruned nodes is the amount of storage they occupy on the server's hard drive. |
| Lightning node | Create a network alongside the BC network for fast, speedy, and cost-effective transactions. | Lightning nodes alleviate congestion in the BC network by relaying transactions to the primary BC through a secondary network. This enables faster and more cost-effective transactions, reducing strain and improving efficiency. |
| Master node | Only validate the transactions | Master nodes are full nodes that maintain the BC database and verify transactions but do not contribute new blocks to the BC. |
| Super node | Purposefully established to alter protocols and conserve the rule | Supernodes are specialized nodes in specific BCs that perform specific tasks, such as implementing protocol revisions and enforcing BC standards. |
| Mining node | Solve complex mathematical problems to authenticate a transaction in a network | Miner nodes validate transactions on a BC and earn rewards. They prove their work, store transactions, and solve complex problems. These dedicated nodes focus on mining operations and consume significant resources. |
| Stacking node | Bids their investment, confirms the transaction, and is appreciated for the effort | Like minor nodes, nodes validate and maintain transactions for consensus in the network. They participate in algorithms like PoS, where nodes stake their wealth, verify transactions, and receive rewards. Selection criteria determine the node's chance to authenticate transactions. Minor nodes do not require extensive processing power. |
| Authority node | Accountable for authenticating the other node to join the network | In public BCs, anyone can join and access content. However, for controlled data access, authorized institutions use governance nodes. These nodes oversee network entry and data pathways. Authority nodes manage node identities like a valet service provider in specific networks like Hyperledger Fabric. |

### 6) FASTER SETTLEMENT

Traditional banking systems often need shorter settlement times, sometimes taking several days to complete transactions. This inefficiency highlights the need for modernization within these financial institutions. BC, on the other hand, offers a solution by enabling rapid money transfers and settlements. This saves organizations time and money and benefits the users by providing faster and more efficient transactions.

### 7) ENHANCED CAPACITY

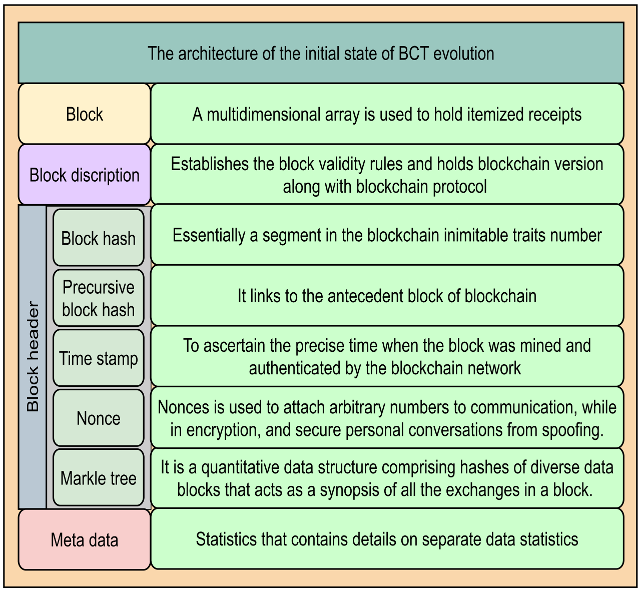
BC's primary and fundamental characteristic is its ability to enhance network capacity. Unlike centralized systems with a limited number of machines, BC harnesses the collective power of numerous computers, significantly increasing its overall capacity. This decentralized approach allows for a more robust and efficient network infrastructure.

### 8) ENHANCED SECURITY

BC provides enhanced security by eliminating the risk of system termination. Indeed, traditional monetary systems are susceptible to cyber-attacks. However, unlike conventional monetary systems, BC, such as Bitcoin, has never been hacked. This is because the network relies on a group of computer nodes, which validate transactions and ensure the network's security. The distributed nature of BC and the consensus mechanism employed by nodes contribute to its robust security infrastructure.

### 9) IRREVERSIBILITY

Each new block in a BC network includes a record that incorporates previously confirmed transactions. The intermittent process validations and the design of the BC architecture ensure the irreversible nature of transactions. This guarantees the integrity and permanence of the transactions within the network.



| The architecture of the initial state of BCT evolution | | |
|---|---|---|
| Block | | A multidimensional array is used to hold itemized receipts |
| Block discription | | Establishes the block validity rules and holds blockchain version along with blockchain protocol |
| Block header | Block hash | Essentially a segment in the blockchain inimitable traits number |
| | Precursive block hash | It links to the antecedent block of blockchain |
| | Time stamp | To ascertain the precise time when the block was mined and authenticated by the blockchain network |
| | Nonce | Nonces is used to attach arbitrary numbers to communication, while in encryption, and secure personal conversations from spoofing. |
| | Markle tree | It is a quantitative data structure comprising hashes of diverse data blocks that acts as a synopsis of all the exchanges in a block. |
| Meta data | | Statistics that contains details on separate data statistics |

**FIGURE 8. Illustration of the evolutionary architecture of BCT.**

### 10) TRANSPARENCY

A BC is a distributed ledger of transactions shared across interconnected computers, ensuring accessibility and transparency. It maintains a permanent record of data, preventing unauthorized modifications. This is achieved through robust cryptography and security measures implemented in the BC network. The transparency provided by BC fosters trusts and accountability in the system.

### 11) DECENTRALIZED P2P COMMUNICATION

A P2P network is a decentralized platform where individuals can freely interact without intermediaries. It allows direct communication and transactions between buyers and sellers using the P2P service. This eliminates the need for third-party intervention and promotes direct P2P interactions.

### 12) CONSENSUS ENABLED AWARENESS

Consensus methods are employed in networks with potentially unreliable nodes to establish trust and reliability. In the context of a BC, consensus serves as a mechanism that brings decentralized record-keeping closer to a centralized database. It is an automated process that ensures all nodes agree on a single valid version of a document, enhancing the integrity of the network.

### 13) TIMESTAMPING

Timestamps are commonly used to track information on the web or a machine. They record when data is published, transmitted, edited, or removed. For example, a machine file may have a timestamp indicating the most recent modification, demonstrating the practical application of timestamps in tracking changes and actions related to data.

### 14) INTEGRITY

In a decentralized database like BC, if someone attempts to update data, the platform verifies the integrity of the entire chain and compares it to the updated data. Any modifications not aligning with the existing chain are rejected, preventing unauthorized alterations. This mechanism ensures the security and immutability of the data stored in the BC.

### 15) SMART CONTRACTS

Smart contracts aim to facilitate the seamless fulfillment of agreements, ensuring that all involved parties can instantly verify the outcome without intermediaries or time-consuming processes. This automated approach eliminates the need for additional costs and delays, providing a more efficient and transparent way to execute commitments.

### 16) ACCESS CONTROL MANAGEMENT

BC offers transparent and decentralized protection, reducing human errors and defending against cybersecurity threats. It is crucial for access control systems to store data across the network in a distributed ledger. Each node keeps copies of transactions and their hash, enhancing cryptographic security over centralized repositories.

### 17) NON-REPUDIATION

Non-repudiation ensures that participants in an e-commerce transaction on a BC cannot deny or dispute the transaction. The purpose of a non-repudiation system is to securely store, transmit, and validate indisputable evidence of information exchanged between the sender and the recipient.

### 18) SCALABILITY

The scalability issue in BC arises when the network expands in size and transaction volume. This challenge is especially prominent in public BC networks, where every node must process and validate each transaction, resulting in an increased computational workload.

### 19) CONFIDENTIALITY

Security and anonymity are intertwined concepts in BC, as they protect transaction and node information. BC has emerged as a cutting-edge solution for decentralized data distribution and storage. The data stored in each block is immutable, meaning it cannot be altered or tampered with easily. Any attempt to modify the stored data is complex and robust, ensuring confidentiality and data integrity.

### 20) EFFICIENCY

Private BCs ensure effectiveness by limiting access and permissions to authorized nodes, enabling efficient operations. On the other hand, public BC networks face scalability challenges due to many users accessing the ledger concurrently. Private BC technologies offer superior solutions for scalability concerns and tailored use cases.

#### 21) DATA HANDLING

In a private BC, a single entity has exclusive read and write privileges for a specific ledger, with limited access to authorized participants. They can remove a block from the ledger as specified in the rules. Once finalized, the ledger becomes immutable, setting it apart from public BCs. This level of control and permanence guarantees the integrity and reliability of the private BC.

#### 22) TRANSACTION SPEED

Private BCs restrict access to authenticated participants, maintaining a consistent transaction rate. In public BCs, anyone can view and request transactions, leading to longer processing times and reduced network efficiency. Public BCs prioritize openness but sacrifice transaction speed.

#### 23) TRANSACTION COST

Private BC platforms provide cost-effective solutions with stable pricing unaffected by request volume. Expenses remain consistent, accurate, and affordable. Conversely, public BC platforms incur higher transaction costs due to compromised efficiency caused by numerous nodes. Slower response times result in increased processing costs for public BC platforms.

#### 24) TRACEABILITY

BC-based traceability brings the advantage of uncovering counterfeit products and fraudulent transactions while providing comprehensive tracking and tracing capabilities for commodity origins and logistic activities. This enhanced traceability simplifies documentation processing and ensures greater transparency in supply chains.

### D. INCORPORATION OF BCT IN WIRELESS COMMUNICATION NETWORKS

BCT disrupts wireless communication with decentralized security, smart contracts for seamless device integration, and improved privacy. Proof of stake or directed acyclic graph consensus ensures trust, eradicating centralized vulnerabilities. This fusion revolutionizes connectivity paradigms, boosting efficiency and resilience in the wireless ecosystem [124].

#### 1) BC-ENABLED SPECTRUM ALLOCATION, SHARING, AND MANAGEMENT IN 6G WIRELESS COMMUNICATION NETWORKS

Spectrum resources are limited in 6G, leading to challenges in meeting increased throughput requirements while minimizing latency and congestion. The shared spectrum is susceptible to interference from multiple communication technologies, making practical spectrum-sharing algorithms and innovative approaches essential for 6G networks [125].

As the 6G wireless networks aim to connect trillions of devices rapidly and efficiently, they must provide an extensive spectrum, precise time and phase synchronization, and reliable geographical coverage. However, with growing connectivity and emerging applications, ensuring privacy and security becomes more complex [126]. Moreover, the communication networks require fully decentralized, independent, and secure communication, leading to BCT integration. BCT is a promising technology that can enhance efficiency, reduce costs, mitigate security and privacy risks, and establish a secure data-sharing ecosystem. Thus, BC can be utilized for spectrum allocation, sharing, and regulation. However, utilization of BC for spectrum management, evaluates different spectrum-sharing schemes and proposes a consortium BC-based spectrum-sharing service that ensures confidentiality and security [127]. Additionally, a BC authentication system can facilitate secure spectrum sharing in mobile cognitive radio networks. A BC-based spectrum-sharing architecture incentivizes primary users to share excess spectrum and achieve optimal spectrum allocation with minimal complications [128]. In the context of 5G communication systems, heterogeneous networks that incorporate small cells within the footprint of microcells have been proposed to maximize terrestrial resource reuse and enhance user service quality compared to homogeneous networks. However, mutual interference and scarcity of spectrum resources in heterogeneous networks require effective radio access techniques (RAT) to address interference issues and enable spectrum cooperation and sharing. Consequently, BCT can facilitate efficient processing of RAT and enable spectrum cooperation and sharing [129].

Integrating MEC and RAN facilities and the liberalization of 5G and beyond communication presents new challenges and opportunities. Incentives and orchestration of various 5G domains are necessary to meet performance expectations. A novel BC-based paradigm for cellular data accessibility is proposed in [130], allowing major 5G stakeholders to sell, distribute, and utilize mobile edge networking assets in a decentralized, untraceable, and resilient manner.

Looking ahead to spectrum management, the convergence of dynamic spectrum access and BC is envisioned as a solution to existing challenges in centralized spectrum management systems, including security threats and low assignment efficiency. BC's inherent qualities, such as digitalization and tamper-proof nature, make it suitable for addressing the spectrum management difficulties posed by the increasing number of IoT devices in future wireless communication networks [131], [132]. The authors in [131] proposed DAG-based BC approach enhances user autonomy in spectrum sharing, addressing the operational challenges of large-scale IoT networks with heterogeneous devices, and further highlights the potential of BC-assisted networks regarding decentralization, independence, and efficiency.

#### 2) BC-ENABLED RELIANCE-BASED DATA INTERFACE, INTEGRITY PLAUSIBILITY, AND DATA LEGITIMACY IN 6G WIRELESS COMMUNICATION NETWORKS

BCT has emerged as a potential solution to address various challenges and security concerns in communication

**TABLE 4.** Illustration of consensus mechanisms in BCT [121], [122], [123].

| Consensus mechanism | | **(A)** A DDoS attack by obtaining control of more than 51% of the network is financially impractical due to the high computational power required. The cost incurred by the intruder outweighs any potential profit they may gain. Thus, the consensus mechanism of PoW enhances the robustness and security of BC networks by acting as a deterrent against such attacks. |
|---|---|---|
| Proof of Work (PoW) | | **(B)** PoW is a widely recognized and utilized consensus protocol. Nodes engage in mining to solve complex computational puzzles and create new blocks. The Bitcoin network adjusts the difficulty of these puzzles to ensure regular block creation. Although the puzzles are challenging, network validation is efficient. Occasionally, multiple nodes solve puzzles simultaneously, leading to temporary forks. However, all nodes eventually adopt the longest chain, discarding the others. |
| | | **(C)** PoW has the iconic problem of harnessing a considerable amount of power or energy when collated with other consensus protocols. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissionless BC |
| Directed Acyclic Graph (DAG) | | **(A)** DAG-based systems offer high transaction speeds as they are not dependent on block creation or miners. This eliminates transaction fees and consumes minimal energy, making it more environmentally friendly than traditional mining-based BC systems. |
| | | **(B)** A DAG is a data modeling tool used in cryptocurrency that differs from traditional BC structures. Transactions are represented as vertices in a directed cyclic network, allowing for simultaneous authentication. Unlike BC, there are no blocks in a DAG. Transactions are stacked and confirmed using PoW. In contrast to a BC, the main difference is that a DAG can handle multiple transactions concurrently. |
| | | **(C)** Due to its low transaction volume, the network is vulnerable to attacks. Additionally, as it is still in its early stages, it needs a significant level of decentralization. |
| | | **(D)** IOTA, Nano, and Obyte cryptocurrencies. |
| | | **(E)** Permissionless BC |
| Proof of Stake (PoS) | **(A)** Attribute | **(A)** The primary motivation for PoS is to avoid the extensive energy consumption of PoW while maintaining sustainability and enhancing privacy. An intelligently designed incentive system could achieve these goals effectively. |
| | **(B)** Description | **(B)** PoS is a category of BC consensus mechanisms that select validators based on their cryptocurrency stakes, holdings, or assets in the network. This approach aims to avoid the computational expenses associated with PoW algorithms. |
| | **(C)** Disadvantage | **(C)** Critics argue that the PoS model is considered less reliable than PoW. They further contend that PoS could lead to increased centralization in the cryptocurrency BC system, as it prioritizes clients with a significant amount of digital currency. This concentration of crypto holdings may significantly impact the management and governance of BC. |
| | **(D)** Currency types | **(D)** Bitcoin and Ethereum Network |
| | **(E)** BC network types | **(E)** Industry-leading PoS BC such as Polkadot, EOSIO, Cardano, and Ethereum 2.0, it's a public or permissionless BC |
| Proof of Existence (PoE) | | **(A)** The platform ensures privacy by safeguarding crucial data integrity, authenticity, and timestamps while providing robust authentication and resistance to malware. It eliminates the need for in-person document submission, offering a tamper-proof solution. The platform securely captures and stores the hash of digital items, ensuring their integrity. |
| | | **(B)** PoE acts as a BC-based database for authenticated user data and commodity details. It provides a secure and transparent way to timestamp copyright notices for contract transactions. Once stored in the BC, artifacts can be verified for existence and content at specific times. PoE utilizes cryptographic hashes, timestamps, and metadata to ensure tamper-proof records. |
| | | **(C)** In PoE, digital documents are assigned unique identifiers or timestamps when uploaded to the BC network. This proves their existence and can be applied to various records such as educational certificates, MoUs, driving licenses, health records, employment records, tax returns, property registrations, and birth/death certificates. |
| | | **(D)** Bitcoin and Ethereum Network |
| | | **(E)** Permissionless BC |
| Proof of Exercise (PoX) | | **(A)** In a PoX-based mechanism, this technique effectively addresses challenges associated with PoW, including riddle hardness, tunable hardness, parallelization, verification ease, block sensitivity, and energy efficiency. |
| | | **(B)** PoX tackles scientific problems by solving matrix operations, enabling tasks such as DNA/RNA scheduling, statistics compression, image analysis, and mathematical modeling. It offers an efficient approach for handling computationally intensive tasks in various scientific domains. |
| | | **(C)** A prerequisite for implementing this consensus mechanism in the BC is a deep understanding of mathematically intensive scientific problems. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissionless BC |
| Byzantine Fault Tolerant (BFT) | | **(A)** BFT consensus mechanism is an energy-efficient, low record variance, and facilitates transaction finality. |
| | | **(B)** Liskov and Castro pioneered the Byzantine fault consensus algorithm. BFT empowers distributed networks to agree despite malicious elements. It tackles various fault types. A byzantine breakdown is when a service fails due to a defect, testing fault tolerance and detection. A byzantine fault is random and unpredictable in decentralized systems unless built with BFT. |
| | | **(C)** In a distributed BC network with fewer nodes, BFT performs efficiently. However, as the number of nodes increases, the communication overhead escalates, making BFT vulnerable to the scaling effects of Sybil attacks. |
| | | **(D)** Bitcoin, Digital cash, E-gold, Internet money, etc. |
| | | **(E)** Permissioned BC or Private BC |
| Consensus mechanism | | **(A)** Consensus mechanism provides low latency validation of transactions, minimizes energy consumption, and ensures predictable confirmation times. |
| Proof of Luck (PoL) | | **(B)** PoL is employed to select a consensus leader in the BC network, utilizing trusted execution environment platforms. It incorporates a random number generator for efficient transaction verification, predictable confirmation times, low energy consumption, and evenly distributed mining. |
| | | **(C)** Due to the multiple verifications involved, PoL experiences a power drawback in determining access to rewards. Additionally, a time delay between the node and the network can diminish the node's chances of being selected for rewards. |

**TABLE 4.** ***(Continued.)*** **Illustration of consensus mechanisms in BCT [121], [122], [123].**

| | | |
|---|---|---|
| | | **(D)** Bitcoin |
| | | **(E)** Permissioned or Private BC |
| Proof of Importance (PoI) | | **(A)** PoI tracks the duration and quantity of cryptocurrencies in a virtual wallet, encouraging investors to store their coins and engage in transactions. It provides a reliable measure of significance by promoting coin mobility and rewarding different transaction categories. More significant and frequent transactions are given a higher weight, enhancing the system's overall reliability. |
| | | **(B)** PoI is a consensus algorithm used in the new economy movement (NEM) cryptocurrency network to determine node power for block publication. It introduces harvesting, similar to mining, and ranks accounts based on vested and unvested coins using a networking approach. |
| | | **(C)** PoI ensures that wealth accumulation is not favored, treating cryptocurrency more as a circulating commodity than something to hoard in virtual wallets. While PoI may not be widely adopted, it promotes cryptocurrency circulation among individuals. |
| | | **(D)** NEM |
| | | **(E)** Permissionless BC |
| Proof of Elapsed Time (PoET) | **(A)** Attribute | **(A)** PoET consensus is a simplified version of PoW that focuses solely on the time-based mining process. Each participant in the network is assigned a random countdown object, and the participant whose countdown expires first becomes the block leader and creates the next block. This randomized timing scheme ensures fairness and efficiency in block generation. |
| | **(B)** Description | **(B)** PoET is a consensus algorithm introduced by Intel Corporation to determine the block producer in a permissioned BC network. It employs a lottery method that evenly distributes the chance of winning among network participants, ensuring fair participation. Compared to Bitcoin's PoW, PoET consumes less energy by allowing nodes to sleep and engage in other tasks for a specified duration, making the network more energy-efficient. |
| | **(C)** Disadvantage | **(C)** The software guard extension technology in PoET consensus raises concerns due to a severe flaw that requires specialized hardware security. The randomness of BC and sleep time limitations can make the network vulnerable to harm from compromised nodes. |
| | **(D)** Currency types | **(D)** Bitcoin |
| | **(E)** BC network types | **(E)** Permissioned BC |
| Proof of Capacity (PoC) | | **(A)** PoC is a verification system in cryptocurrency that solves hashing challenges using extra space on a hard drive. It is more efficient than PoW and PoS. Storj, Burst, Chia, and Spacemint are examples of BC networks that use PoC. |
| | | **(B)** PoC is a consensus method in BC that allows mining devices to establish mining power and validate transactions based on their available hard drive space. |
| | | **(C)** PoC eliminates unnecessary developers and ensures that the data stored on the hard disk is exclusively relevant to coin mining. This reduces wasted space. Unlike PoW mining, PoC minimizes PC slowdown. Additionally, it makes it more challenging to detect illicit use of extra hardware space. |
| | | **(D)** Burst coin cryptocurrency |
| | | **(E)** Permissionless BC |
| Proof of Identity (PoID) | | **(A)** Accenture's biometrics and BC-based PoID solution offer users enhanced mobility, flexibility, privacy, control, and advanced authentication capabilities. This innovative technology ensures secure and efficient identification and authentication processes. |
| | | **(B)** BC enables the decentralized public critical infrastructure (DPKI), providing a tamper-proof and trustworthy approach for distributing authentication and cryptographic keys. Decentralized DPKI allows users to establish and store keys on the BC securely and organized. |
| | | **(C)** In the realm of unstructured data, accountability is vital for ownership and monetization. The data we generate on the internet is intangible, invisible, and intricate, making data monetization essential. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissionless BC |
| Proof of Authority (PoA) | | **(A)** PoA network operates without mining due to its permissioned nature, allowing network participants to benefit from surplus by running multiple nodes under the same identity. |
| | | **(B)** PoA is a BC consensus mechanism that employs ethnicity as a stake for faster transactions. Vechain is a prominent platform utilizing PoA. It relies on trusted validators to generate blocks and enhance network efficiency through a BFT algorithm and authenticity as a stake. |
| | | **(C)** PoA is not designed for trustless environments, unlike public BC, as it relies on clients trusting verifiers and authorizers. This makes it less suitable for non-enterprise services that aim to achieve trustlessness. |
| | | **(D)** Bitcoin, it's likely to outperform bitcoin and ethereum |
| | | **(E)** Permissioned BC |
| Proof of Activity (PoA) | | **(A)** PoA combines elements of both PoW and PoS consensus algorithms. It starts with a PoW mining process, but once a new block is successfully mined, it transitions into a PoS system, incorporating the best features of both approaches. |
| | | **(B)** PoA is a consensus method used in BC and cryptocurrencies to ensure the validity of all actions and reach a consensus among miners. |
| | | **(C)** Due to the unpredictable signing peer and the competition between signatories, PoA can also be susceptible to a 51% attack, similar to PoW and PoS, as computational power cannot be accumulated within a single group. |
| | | **(D)** Bitcoin cryptocurrency and Decred cryptocurrency |
| | | **(E)** Permissionless BC |
| Consensus mechanism | | **(A)** A consensus method is a fault-tolerant mechanism used in computer and BC networks to obtain consent across distributed processes. It ensures data value or network state agreement in multi-agent systems, such as digital currencies. |
| Consensus as a Service (CaaS) | | **(B)** The introduction of consensus as a service offers a decentralized alternative to centralized systems or applications built on private ledgers. Companies often prioritize the privacy of a private ledger, where data is not shared publicly. |
| | | **(C)** CaaS has drawbacks such as high energy consumption, costliness, and the potential for a 51% attack, where a majority of hostile miners could take control of the network. This poses a threat to decentralization. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissionless BC |

**TABLE 4.** *(Continued.)* Illustration of consensus mechanisms in BCT [121], [122], [123].

| | | |
|---|---|---|
| Daura | | **(A)** Daura technology enables Swiss companies with restricted shares to electronically register and issue digital share certificates, facilitating capital gain and expanding investor opportunities through the Daura platform. This streamlines capital processing and provides non-listed enterprises access to a broader investor pool. |
| | | **(B)** Daura, a BC platform, utilizes swisscom's consensus as a service mechanism. Collaborators post finance, and swisscom have the authority to verify transactions on the Daura platform. |
| | | **(C)** The platform allows for the automatic assignment of tasks but does not support currency trading and settlement of BC-based share tokens. |
| | | **(D)** Bitcoin and Token cryptocurrency |
| | | **(E)** Permissionless BC |
| Ripple | **(A)** Attribute | **(A)** Ripple is a BC-based digital payment network that utilizes its currency, XRP. Unlike traditional BC mining, Ripple verifies transactions through a consensus process involving a consortium of bank-owned computers. |
| | **(B)** Description | **(B)** All terminal nodes regularly employ the ripple protocol consensus algorithm (RPCA) to maintain the network's accuracy and unanimity. Once consensus is achieved, the current ledger is considered closed and becomes the final secure ledger. |
| | **(C)** Disadvantage | **(C)** Ripple exhibits some notable drawbacks, such as increased centralization. It relies on trusted validators to authenticate transactions and maintain BC integrity. Since there are no financial incentives for mining, fewer individuals participate in securing the BC, leading to potential security risks. |
| | **(D)** Currency types | **(D)** XRP cryptocurrency |
| | **(E)** BC network types | **(E)** Permissionless BC |
| Proof of Deposit (PoD) | | **(A)** To acquire block production rights, validating nodes must submit a security deposit. Verifier nodes face penalties for generating inaccurate or invalid blocks. |
| | | **(B)** PoD is an enhanced version of the traditional proof-of-stake consensus algorithm implemented in the Ethereum network. In PoD, authenticator nodes are required to provide a security deposit to gain block production authority. Unlike mining nodes in PoW, there is no stake or deposit at risk. |
| | | **(C)** Nodes in PoD have a higher risk of being malicious than nodes in PoS, as they have a stake to lose and the privilege to participate in block creation. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissionless BC |
| Proof of Concept (PoC) | | **(A)** POC has multiple benefits, including validating BC projects, identifying flaws, and saving time and resources. |
| | | **(B)** BC PoC is essential to assess the feasibility of implementing a project concept in the real world. It serves as a typical consensus algorithm in BC, ensuring the idea can function as intended. |
| | | **(C)** BC PoC finds application in various domains, including finance, supply chain, healthcare, identity verification, payments, insurance, government, IoT, and asset management. However, managing network data and documents can be challenging. |
| | | **(D)** Bitcoin |
| | | **(E)** Permissioned BC |

networks. It facilitates effective resource sharing, enhances data integrity, enables secure permissions, and preserves privacy. Moreover, BC offers valuable traceability, certification, and supervisory features in 6G wireless communication systems. Recent studies have focused on adapting BC technologies to these networks [133]. In 6G wireless communication networks, wireless congestion and connectivity density increase significantly due to network heterogeneity and diverse user demands. Efficient communication and collaboration among multiple data sources are crucial for delivering better services. However, establishing secure interactions and validating authenticity and integrity become nearly impossible due to the lack of trust relationships among data owners in the cellular network [134].

Researchers have recently utilized BC to establish mutual trust between devices and create a reliable pathway for highly secure data transactions [135]. The use of BC in promoting reliable data exchanges in wireless networks primarily revolves around ensuring the trustworthiness of network identities and improving the validity of transmitted data. In BC-enabled 6G wireless communication networks, various BC nodes are present and must operate faithfully. If the BC nodes fail to serve faithfully, it can lead to a significant drastic decline in the QoS of the network. To mitigate this issue, each node can be assigned a trust value to participate in the BC as a participant. Each unit may acquire a believability rating based on specific criteria such as historical actions and authorization, which is used to determine identification and reputation. Only nodes meeting specific trustworthiness criteria can communicate with other nodes, while malicious nodes are identified and expelled through a trust management technique [136].

In the context of a BC-based V2X network, in [137], the authors proposed an agreement algorithm that validates data communication using the reputation grades of vehicles. Privacy rights and management of digital certificates are enhanced by combining centralized personas with an underlying layer of BC. Furthermore, the authors developed a trustless system paradigm for intelligent vehicles in vehicular ad-hoc networks, leveraging BC and a certificate authority [137].

The 6G wireless communication network introduces an edge computing mechanism to ensure a secure, independent, self-reliant, and decentralized network. However, cluster-based intellectual assessment and consensus procedures can guarantee data correctness and validity. A BC-based trustworthiness strategy for edge computing data governance utilizes suitable affirmation methods and user-defined dedicated data encryption. Additionally, a decentralized trust-based management system is proposed in [138] and [139], where BC is employed for green communication and network establishment, accessing the trustworthiness of traffic communication through a Bayesian interference framework [138], [139]. Moreover, a concrete evidence (PoE) agreement paradigm is introduced for vehicular communication, which relies on passing motorists and vehicles to authenticate the validity of congestion information recorded by roadside devices [140].

### 3) BC-ENABLED SPECTRUM REFARMING IN 6G WIRELESS COMMUNICATION NETWORKS

In modern wireless communication technology, repurposing the existing band, such as the lower band spectrum, can be expected to fulfill the services of the higher band spectrum. For example, a global system for mobile communications association (GSMA)-based band spectrum refarming technique that can be used to transform the lower band technology, such as GSM in 2G, to a higher band technology which is universal mobile telecommunications system for 3G, long-term evolution in 4G, massive multiple inputs multiple outputs (mMIMO), beamforming, mm-wave in 5G and visible light communication (VLC), THz spectrum, reconfigurable intelligent surface (RIS), AI, data-centric automated processing in 6G.

Consequently, such frequency refarming (SR) technique can enhance the network capacity and efficiency within the available resources in densely deployed users and various services in a 6G wireless network. As we know, the SR is a radio RM technique to support different generations of the cellular network within the same band spectrum. Notably, the authors in [141] proposed an underlay orthogonal frequency division multiplexing (OFDM)-based SR model for sharing the code division multiple access systems spectra. However, the method is static and limits the network's growth. Further, the authors of [142] proposed a dynamic broadband SR for OFDMA systems, as a result, enhancing the network efficacy. Notice that the concept also can be applied to the 6G wireless network to exploit the available resources within the unplumbed band spectrum to fulfill the diverse need of the enormous number of end users. However, security concerns remain due to the diverse demand of enormous end users and wireless network infrastructure, which tempt the involvement of some guarded technology such as BC.

Additionally, SR suffers due to severe concerns, including centralized network resource allocation, security breaches, high network administrative costs, intermediates to purchase spectrum, cyber-attacks, and sluggish response for spectrum sharing contracts and agreements. Further, in cognitive radio communication networks, if a primary user is coexisting with a private network; designing a fair dedicated access system is critical. As a result, BC plays a vital role, which includes efficient resource allocation and management, resource lease and fair accessing mechanism, intelligent contracts, fair resource auction mechanism, faster payments settlement, immutable and confidential ledger records, decentralized, secured data records, and efficient transaction management and executions. The network is flourished by aforementioned peculiarities, which are leveraged by the BC characteristics in 6G spectrum refarming due to its vast capability to improve the spectrum usage visibility and audibility of the end users to make network transparency. In summary, for effective utilization of available resources in the SR technique, BC avails a trustless, decentralized, and accessible resource trading platform to ensure a security-proof efficient network.

### 4) BC-ENABLED RATE SPLITTING MULTIPLE ACCESS TECHNIQUE IN 6G WIRELESS COMMUNICATION NETWORKS

Rate splitting multiple access (RSMA) is a promising technique for 6G networks due to its ability to efficiently utilize the available resources, reduce interference, and improve overall system performance [143]. RSMA can be in 6G wireless communication networks to enhance the system capacity and improve the network's performance. In RSMA, the users divide their transmission rate into common and private parts. They simultaneously transmit a common message, decoded by all users, and private messages, decoded individually. Advanced signal processing techniques are used to separate the messages at the receiver side. RSMA improves spectral efficiency and network capacity by exploiting interference and enabling simultaneous access to the wireless channel. Further, combining these two parts results in an increased data rate for the user, allowing the network to handle more users with the same resources. However, the network suffers from security concerns; consequently, BC-enabled RSMA techniques can be illuminated. Further, incorporating the BC into RSMA ensures the security and transparency of the network. Hence leveraging the specialty of the BC, the system turns into a robust network against safety vulnerabilities.

Consequently, BC can be used in the RSMA technique in the 6G wireless communication network to enhance the security and reliability of data transmission. The decentralized nature of BC allows for the secure and transparent distribution of resources among multiple users in a wireless network. With RSMA, the available bandwidth is divided among multiple users, and each user is assigned a specific rate. BC can be used to monitor and verify the allocation of these rates among users, ensuring that each user only uses the bandwidth assigned to them. Additionally, the immutability of BC can provide an auditable record of the bandwidth allocation and usage, allowing for effective network management and troubleshooting. However, due to the diverse demand and immense versatile infrastructure of the wireless network, the system shows the delicacy of manipulating the transacted data.

Consequently, BC ensures tamper-proof RSMA techniques in 6G wireless communication networks by using cryptographic algorithms and consensus mechanisms to ensure the integrity of the data stored on the network. Once data is recorded on the BC, it is difficult to modify or alter, as each block in the chain is linked to the previous block through cryptographic hashes. In the case of RSMA, the data transactions between wireless devices can be recorded on the BC network, ensuring that the data remains tamper-proof. The consensus mechanism in the BC network ensures that all nodes have the same version of the data, and the network will detect and reject any attempt to modify or alter the data.

Additionally, the decentralized nature of the BC network ensures no single point of control or failure, making it more difficult for malicious actors to tamper with the data stored on the network. This provides a high level of security for the data transmitted in RSMA in 6G wireless communication networks, as it reduces the risk of data breaches, tampering, or other security threats. Furthermore, scalability issues exist due to the vast and diversified network demand at the user end, which is a significant problem in wireless networks. Consequently, BC ensures scalability in RSMA techniques in the 6G wireless communication network by providing a decentralized network architecture that allows for the dynamic allocation of resources among multiple users. With BC, the network does not rely on a central authority to manage resource allocation and distribution. Instead, each node in the network participates in the resource allocation process, enabling the network to accommodate various users and devices.

In RSMA, the available bandwidth is divided among multiple users, and each user is assigned a specific rate. With BC, the allocation of bandwidth can be automated and distributed among the nodes in the network, enabling the network to scale and accommodate a growing number of users and devices. Additionally, the decentralized nature of BC allows for the efficient distribution of resources and reduces the likelihood of bottlenecks, which can improve the overall scalability and performance of the network. However, this diverse demand contains many challenges, which we have studied in the tabulated form as shown in Table 7, where we vastly covered the illustration of various use cases, challenges, and how to mitigate the implementation challenges and explained associated ML/BC contributions.

#### 5) BC-ENABLED 6G ENERGY-EFFICIENT WIRELESS COMMUNICATION NETWORKS

Deploying 6G networks will require significant energy, which could lead to increased carbon emissions and other environmental impacts. A BC-enabled 6G network could use a distributed energy system that utilizes renewable energy sources such as solar or wind power to address this issue. This would reduce not only the environmental impact of the network but also lower the overall cost of energy consumption. Moreover, a BC-enabled 6G network could provide a secure and decentralized platform for communication, which could enhance privacy and security while reducing the potential for network downtime due to cyber-attacks [144].

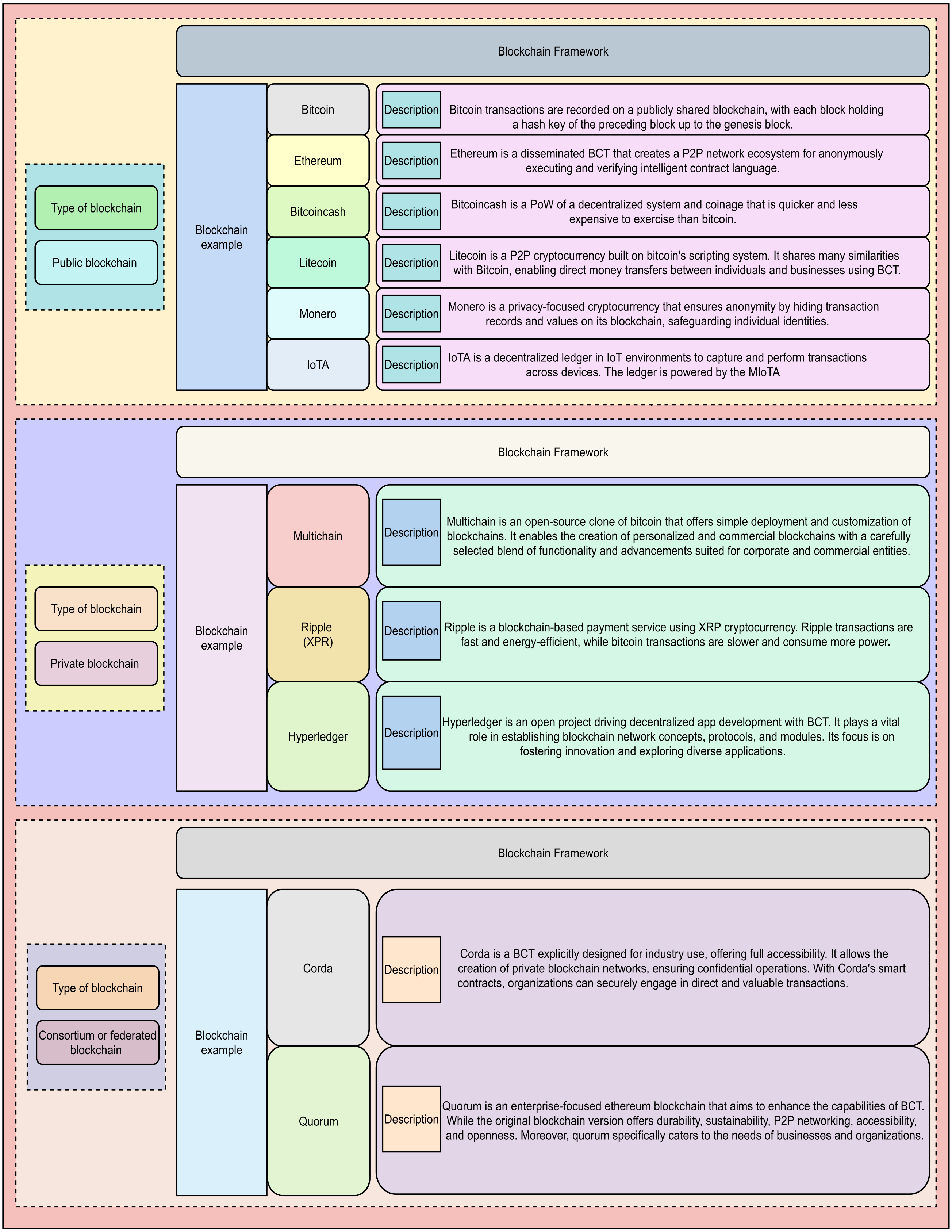
In essence, a BC-enabled energy-efficient 6G-wireless communication network has the potential to transform the telecommunications industry by providing a secure, decentralized, and sustainable platform for communication. However, the successful deployment of such a network will require collaboration among industry players, policymakers, and other stakeholders to ensure that it meets the needs of all parties involved. We illustrate the applicability of the BCT in a 6G-diversified network to make it more energy efficient by implementing the following approaches [145]:

- Decentralized Energy Management: BC can be used to create a decentralized energy management system that optimizes the energy usage of devices and nodes in the 6G network. Nodes can negotiate and agree on the energy needed for their operations via intelligent contracts, preventing them from using excessive energy.
- Energy Trading: BC can enable energy trading between nodes and devices in the 6G network. This will allow nodes to trade energy with each other in real-time, which will help to balance the energy demand and supply in the network [146].
- Incentivization: BC can incentivize users and nodes in the 6G network to consume less energy by offering rewards for energy-efficient behavior. For example, nodes that consume less energy than their agreed limit can be rewarded with tokens or other incentives.
- Network Optimization: BC can be used to optimize the network by monitoring the energy usage of each node and device. This will allow network operators to identify and rectify any network inefficiencies causing energy wastage.
- Data Integrity: BC can help to ensure the integrity of the data generated by the 6G network. Using a distributed ledger, BC can prevent any malicious tampering with the energy statistical-related data, which will help to ensure that the network operates efficiently.

The application of BCT in 6G wireless communication will make the network more energy-efficient by optimizing energy usage, promoting energy trading, incentivizing energy-efficient behavior, optimizing the network, and ensuring data integrity [147].

#### 6) BC-ENABLED 6G RADAR-BASED COMMUNICATION NETWORKS

Radar and wireless communication are vital to radio frequency technologies. Radar is used for target detection, while communication enables information transmission between devices. Traditionally, it is developed independently, serving different purposes and operating in separate frequency bands [148]. However, the increasing spectrum scarcity due to the growing number of wireless devices, data traffic, and the need for enhanced radar capabilities in complex electromagnetic



Bitcoin transactions are recorded on a publicly shared blockchain, with each block holding a hash key of the preceding block up to the genesis block.

Ethereum is a disseminated BCT that creates a P2P network ecosystem for anonymously executing and verifying intelligent contract language.

Bitcoincash is a PoW of a decentralized system and coinage that is quicker and less expensive to exercise than bitcoin.

Litecoin is a P2P cryptocurrency built on bitcoin's scripting system. It shares many similarities with Bitcoin, enabling direct money transfers between individuals and businesses using BCT.

Monero is a privacy-focused cryptocurrency that ensures anonymity by hiding transaction records and values on its blockchain, safeguarding individual identities.

IoTA is a decentralized ledger in IoT environments to capture and perform transactions across devices. The ledger is powered by the MIoTA

Multichain is an open-source clone of bitcoin that offers simple deployment and customization of blockchains. It enables the creation of personalized and commercial blockchains with a carefully selected blend of functionality and advancements suited for corporate and commercial entities.

Ripple is a blockchain-based payment service using XRP cryptocurrency. Ripple transactions are fast and energy-efficient, while bitcoin transactions are slower and consume more power.

Hyperledger is an open project driving decentralized app development with BCT. It plays a vital role in establishing blockchain network concepts, protocols, and modules. Its focus is on fostering innovation and exploring diverse applications.

Corda is a BCT explicitly designed for industry use, offering full accessibility. It allows the creation of private blockchain networks, ensuring confidential operations. With Corda's smart contracts, organizations can securely engage in direct and valuable transactions.

Quorum is an enterprise-focused ethereum blockchain that aims to enhance the capabilities of BCT. While the original blockchain version offers durability, sustainability, P2P networking, accessibility, and openness. Moreover, quorum specifically caters to the needs of businesses and organizations.

**FIGURE 9.** Description of BC framework consisting of cryptocurrency examples with its usage and responsibilities.

environments necessitate the joint design of it. By integrating these technologies, improved efficiency and effectiveness can be achieved, allowing for rapid data fusion and optimizing resource utilization.

On the other hand, it calls the security concerns alongside such as unauthorized access, data integrity, interference, spoofing and jamming, cyber-attacks, and network infrastructure vulnerabilities, consequently entailing the integration of BCT. As a result, a hypothetical BC-enabled 6G radar-based wireless communication network (RADCOM-WSN) is developed to create a secure, reliable, and high-speed network. The authors in [149] proposed an OFDM-based RADCOM, discussing a classical direct matching filtering approach and an efficient RADAR processing system. However, the authors presented its security concerns, such as its vulnerability in multi-user access systems for interference. Consequently, BCT-integrated RADCOM intelligent spectrum management is needed for canceling interference. The authors in [150] discussed efficient RADCOM processing. Here a signal handling and processing approach is discussed, which includes techniques such as time-sharting to reuse the antenna, transmitter, and receiver, a sub-beam for phased array radar when it undergoes a regional breakdown, and a signal sharing technique where communication signal and radar signal are mixed. Consequently, BCT integration is needed for data integrity. Moreover, the authors in [151] and [152] discussed the RADCOM in frequency-modulated ultra-wideband and bio-medical sensing, respectively, and exploited it in intelligent healthcare for critical medical data sharing, resulting in a need for BCT-integrated RADCOM for medical application.

Furthermore, it enables advanced network analytics, QoS monitoring, and network optimization [153]. Combining 6G and RADCOM technologies with BC could enable various innovative applications, including smart city infrastructure, autonomous vehicles, remote healthcare, and other advanced use cases requiring secure and reliable communication. Moreover, there are several technical and practical challenges to overcome before a BC-enabled 6G RADCOM-WSN can become a reality. Nonetheless, it is an exciting area of research and development that could lead to significant advancements in wireless communication and network security. By using BCT-RADCOM, networks could potentially store network activity logs and other essential data in a transparent, traceable, and secure way from unauthorized access or manipulation. For example, BC-based distributed ledger technology could create a secure and decentralized record of network events, which could be used to monitor and analyze network performance, identify security threats, and provide valuable insights for network optimization and improvement.

### 7) BC-ENABLED 6G RECONFIGURABLE INTELLIGENT SURFACE COMMUNICATION NETWORKS

BC-enabled 6G-RIS communication technology has the potential to revolutionize the way we communicate and exchange information. RIS is a promising technology expected to be a vital component of the 6G wireless network. It is a planar surface with many passive elements that reflect, refract, and modify the properties of electromagnetic waves (EMW), improving the SNR of the signal. This technology can enhance wireless communication by shaping the signal and improving quality [154]. However, it calls for several security concerns, such as unauthorized access, privacy and data leakage, secure RIS configuration and management, malware and software vulnerabilities, covert channel attacks, the trustworthiness of RIS configuration, physical security of RIS, side-channel attacks, scalability and management complexity and interference with legacy systems. Consequently, it necessitates integrating BCT.

Furthermore, the authors in [155] proposed a 6G-RIS for EE in a D2D communication network. Here the authors presented a passive beamforming and power control for the EE network. However, for the efficient functioning of the network, a decentralized and frequent RIS configuration and parameter updates are required, which motivates the integration of BCT with 6G-RIS. BCT's integrated approach can provide a secure and decentralized platform for RIS communication. It can enable safe and transparent transactions between the RIS and other devices, manage the lucid network functioning and ensure communication integrity. One potential use case for BC-enabled 6G-RIS communication technology is in the IoT. The BC-enabled RIS can improve the signal quality and coverage of IoT devices while maintaining translucent transactions and ensuring the security and privacy of the data exchanged between the devices. Another potential use case is in the development of smart cities. BC-enabled RIS technology can create a WSN that covers a large area while sustaining acceptable network functioning standards and ensuring the security of the data exchanged. In summary, combining BCT and RIS can bring about noble and innovative ways to enhance wireless communication and create a more secure and decentralized network [156]. Furthermore, we have illustrated the BCT applicability along with RIS as mentioned below:

- Security and privacy: RIS-enabled communication requires a secure and private platform to oversee communication between RIS and other devices. BCT can fulfill this role by guaranteeing secure and transparent transactions on the network.
- Decentralization: BCT enables a decentralized RIS network management platform. This means there is no central point of control, and all nodes on the network have equal access to information.
- Smart contracts: A smart contract can automatically update the RIS configuration based on changes in the wireless environment.
- Network management: BCT can be used to manage the RIS network by ensuring that all nodes on the network have equal access to information.

Consequently, the application of BCT in RIS can provide a more secure, decentralized, and efficient platform for managing the communication between RIS and other devices.

### 8) BC-ENABLED 6G VISIBLE LIGHT COMMUNICATION NETWORKS

VLC is a wireless communication technology that uses visible light to transmit data. It is a promising technology for indoor environments because it does not interfere with other wireless technologies and can provide high data rates [157]. However, it is vulnerable to several security attacks, such as eavesdropping, jamming, spoofing, replay attacks, denial of service, physical attacks, side-channel attacks, optical channel capturing, optical covert channels, optical phishing, optical injection attacks, and optical malware. Consequently, a BC-enabled 6G-VLC network can be developed and viewed as a secure potential future communication technology that combines BCT, 6G wireless technology, and VLC to create a secure and efficient communication network. Moreover, the authors in [158] discussed VLC for UAVs. The VLC links of a UAV network inevitably suffer due to the jittering effect, which is a consequence of network congestion, transmission delay, clock synchronization, and timing information. The authors in [159] discussed the visible light positioning system. The research proposed a position estimation DNN model that shares learned feature parameters from pilot carriers. However, it is susceptible to network attacks.

Further, the authors in [160] discussed physical layer security concerns of multi-user MIMO systems in VLC, which suffer due to the eavesdropper. Consequently, a BCT-integrated VLC is required to mitigate the drawback mentioned above. Furthermore, such an integrated approach is not limited to the conventional VLC but extended to non-conventional media communication, such as underwater and underground [161]. In this research article, underwater source and sink node communication can be protected through BCT integration. Additionally, one of the potential applications of this technology could be in the healthcare industry. A BC-enabled VLC network can transmit patient data between medical devices in a hospital environment while ensuring privacy and secrecy. Consequently, this integrated approach could have various applications in healthcare, manufacturing, and transportation industries [162]. Further, we have illustrated the applicability of the BCT integrated with VLC as mentioned below:

- Secure Data Transmission: In VLC, BCT can be used to ensure the security of data transmission. With BCT, data transmitted over the VLC network can be encrypted and authenticated, ensuring that it is not tampered with or altered.
- Decentralized Network: In VLC, a decentralized network can ensure that communication is not disrupted due to a single point of failure. Additionally, a decentralized network can improve network performance and efficiency.
- Smart Contracts: BCT enables smart contracts, which automate verifying, executing, and enforcing contract terms. In VLC, intelligent contracts automate medical data transfer and model update, improving network efficiency.
- Data Privacy: By encrypting data using BCT, users can ensure that their data is not visible to others on the network. Additionally, using BCT can ensure that data is not collected and sold by third-party entities without the user's consent.

Consequently, the applicability of BC in the VLC network includes secure data transmission, a decentralized network, smart contracts, data privacy, and traceability. These benefits can improve the security, efficiency, and reliability of VLC communication networks, making them a promising technology for the future.

### 9) BC-ENABLED 6G INTEGRATED SENSING AND COMMUNICATION NETWORKS

The network relies on a combination of BCT and 6G to facilitate seamless communication and data exchange between devices and users. Additionally, integrated sensing technology (IST) is an essential component of the integrated sensing and communication (ISAC) network, as it allows devices to sense and gather data from the environment and transmit it to other devices and the BC for processing and analysis. Moreover, the authors in [163] presented a radio resource allocation scheme for the ISAC network. However, a notable drawback of the system was identified: it needed to handle multiple simultaneous requests adequately, ensuring the integrity of the information. In [164], the authors designed a joint communication and sensing (JCAS) framework. The authors emphasized the prominent concern of security. The sensing function necessitated signals interacting extensively with the environment to capture surrounding information in the waveform. Consequently, it increased the risk of eavesdropping. In another research paper [165], the authors proposed a beam squint-aware ISAC technique specifically tailored for hybrid analog/digital massive MIMO LEO satellite systems. The authors intended to leverage statistical channel state information; however, faced challenges due to the dynamic nature of the channel conditions, which caused variations in the information.

Further, in [166], federated learning was discussed as a collaborative approach wherein distributed edge devices transmit wireless signals to sense targeted objects. These devices would then exchange intermediate computed vectors to collectively recognize the perceived objects, all while ensuring stringent security measures. Furthermore, the utilization of ISAC in vehicular and vehicular-to-infrastructure communication was explored in [167] and [168]. The authors emphasized the necessity of decentralized parameter updates in BCT-assisted roadside units to avoid unwanted accidents and ensure smooth network operations [169]. These networks need to be mentioned above, necessitated to integrate the

BCT. Consequently, a BC-enabled 6G ISAC network is developed, a next-generation network architecture combining the capabilities of BCT, 6G, and IST to enable a more efficient, secure, and reliable communication system. The ISAC networks are equipped with IST and are designed to support various applications, including smart cities, smart homes, healthcare, transportation, and more [170]. This enables real-time monitoring and control of various processes and systems, which can help improve efficiency, reduce costs, and enhance safety [171]. The BC component of the ISAC network provides a decentralized and secure platform for storing, processing and verifying data. This ensures the integrity and privacy of the data exchanged between devices and users and prevents unauthorized access or tampering. Moreover, the BC provides decentralized management as the ISAC network is distributed, with no central authority controlling the network. This means that all nodes in the network have equal access to data and can participate in network management. This ensures the network is transparent and free from bias, making it ideal for applications requiring transparency and fairness. For example, the network can monitor patient health remotely, manage real-time traffic flow, or control energy usage in smart homes. Consequently, a BC-enabled 6G ISAC network is expected to offer significant benefits over existing network architectures.

### E. INCORPORATION OF BCT IN 6G NON-CONVENTIONAL MEDIA COMMUNICATION NETWORKS

The proliferation of intelligent cities has accelerated in recent years, driven by the growing impact of the IoT on various aspects of human life, including underwater environments. The current research suggests that water covers a significant portion of the earth's surface, with much of the underwater realm remaining unexplored. In this context, the Internet of Underwater Things $(\text{IoUT})_W$ has emerged as a network of interconnected intelligent aquatic devices for environmental monitoring, underwater expedition, disaster risk reduction, and defense. However, concerns about security and rogue nodes necessitate the verification and reliable coupling of entities in autonomous underwater equipment exchanges. Typically, centralized identification and security measures require a trusted third party, leading to increased computing costs and energy dissipation, especially in underwater communications. Consequently, BCT has been proven to be a promising and efficient solution for enhancing the 6G wireless communication network to accomplish the aforementioned advantages. Additionally, the authors in [172] focused on understanding the operation of innovative underwater vehicles under variable channel conditions. Multiple autonomous underwater vehicles (AUVs) were deployed for diverse underwater tasks like surveillance and exploration. However, the presence of various AUVs in close proximity raised security concerns. To address this, the authors proposed a reliable and energy-efficient collaborative processing strategy enabled by BCT, ensuring confidentiality by exploiting BC cryptography [172]. Furthermore, in [173], the authors discussed integrating off-shore wireless communication, satellite links, and non-conventional media in the 6G network. This integration is expected to establish ubiquitous connectivity in aquatic systems, with AI playing a crucial role in facilitating efficient network service evolution. In variable channel conditions with sparsely deployed floating nodes in deep water, applications such as environmental observance, underwater expedition, adversity avoidance, and defense generate substantial amounts of data that require processing [173]. As a result, the increasing demand for innovative services necessitates effective management of large volumes of data, encompassing preservation, computation, and assessment while ensuring protection against unauthorized alterations. The authors propose a recent BC-based vulnerability management method for AI applications in 6G technology to address it. From these findings, it can be inferred that expanded operations in deep-sea environments can significantly benefit from the communication capabilities offered by an underwater network, enabling the establishment of an ocean surveillance system. Moreover, an underwater network has the potential to integrate various underwater communication methods, including submarines, unmanned surface vehicles, and sensors, creating a collaborative network and achieving interconnectedness with other network layers [173].

## IV. COMPLEMENTARY BENEFITS OF ML TO BC AND BC TO ML

BC offers a groundbreaking opportunity for applying ML algorithms in various sectors, including signal processing, communications, and networking systems. Its distinct features of decentralization, immutability, and transparency make it conducive for ML applications. This section explains how BC can assist ML in enhancing performance.

### A. INCORPORATION OF BCT IN ML

#### 1) IMMUNE TO DATA COMMERCIALIZATION

Organizations utilize BC for global data trade in the corporate world, leveraging ML models to enhance operational speed, monitor network trading channels, verify data, and strengthen cryptography. ML methodologies, such as training on large datasets and high-throughput streaming analytics, enable more precise and trustworthy machine predictions. Traditional data trade techniques, such as hosting and consolidation, often make data owners hesitant to share their data due to data protection and disclosure concerns. The authors in [197] propose a data trading paradigm with smart contracts, BC, and ML to address these challenges. This approach aims to create a secure and commercialized data trading ecosystem. Specifically, scalable and safe BC-enabled data exchanging methods are suggested in vehicular communications and the IoV [198]. Further, the authors propose a broad BC-enabled data trade paradigm for IoV, utilizing consortium-BC solutions for trustworthy

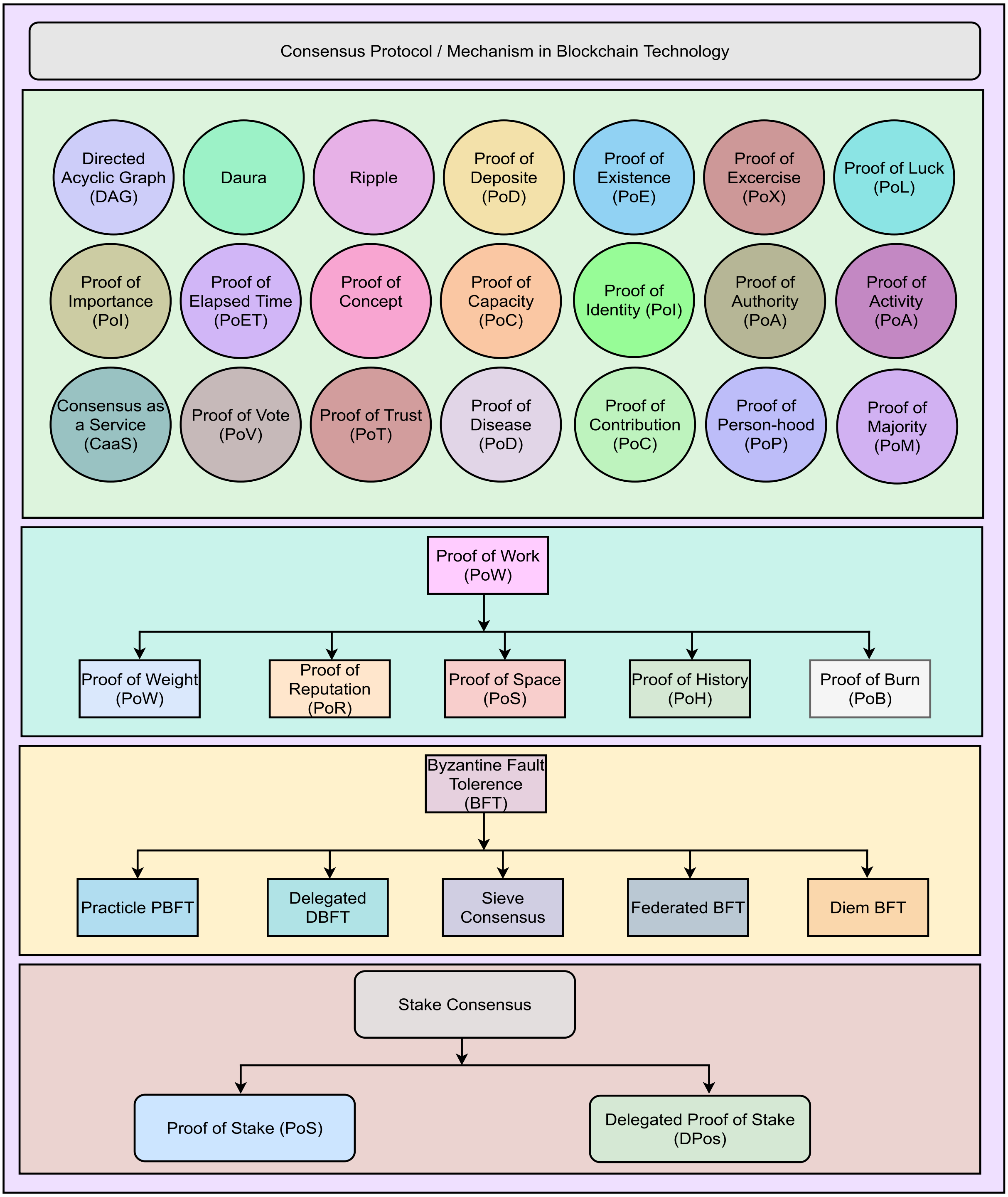


**FIGURE 10.** Summary of consensus mechanisms involved in BC processing methodology.

and reliable data exchange. Scalability issues in BC-enabled data markets are addressed by leveraging BC innovation and developing a decentralized IoV data-trading system [199]. Furthermore, the authors in [200] discussed the internet of electric vehicle (IoEV) ecosystem, encompassing fuel vehicles and EVs, trading conflicts, and illicit activities managed through consortium BC and intelligent contracts. Data cloning validation and real-time data authentication enhance data integrity and reduce preservation costs [201].

The application of BC and ML expands beyond IoV and IoEV to the broader IoT, where decentralized approaches based on distributed ledger technology enable secure data

**TABLE 5.** Distinctive trait comparison of consensus mechanisms in BCT.

| CM | PT | PC | EE | P/S | SP | SC | TC | DH | I | AC | C | AR | AU |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PoW | PL | H | L | SR | S | L | H | MH | H | A | RA | UF | D |
| PoS | PL | L | H | SR | H | H | L | MH | H | A | RA | UF | D |
| DAG | PL | M | H | SR | H | H | L | MH | H | A | RA | UF | D |
| BFT | P | L | H | M | H | M | L | SH | P | SO | NC | F | C |
| PoL | P | L | H | SS | H | H | L | SH | P | SO | NC | F | C |
| PoE | PL | H | M | SS | H | H | H | MH | H | A | RA | UF | D |
| PoET | P | L | H | SR | M | H | L | SH | P | SO | NC | F | C |
| PoI | Both | L | H | SS | H | M | M | Both | P | Both | RA | UF | D |
| PoA | P | L | H | SS | H | H | L | SH | P | SO | NC | F | C |
| PoA | PL | M | M | SR | S | M | H | MH | H | A | RA | UF | D |
| Ripple | PL | L | H | SR | H | H | H | MH | H | A | RA | UF | D |
| PoC | P | L | H | SR | H | H | L | SH | P | SO | NC | F | C |
| PoR | P | L | H | SR | H | H | L | SH | P | SO | NC | F | C |
| PoB | PL | L | H | SR | M | H | H | MH | H | A | RA | UF | D |
| FBFT | PL | M | M | SS | H | H | H | MH | H | A | RA | UF | D |
| DPoS | PL | M | M | SR | H | H | H | MH | H | A | RA | UF | D |
| PBFT | P | L | H | LS | H | L | L | SH | P | SO | NC | F | C |
| Raft | P | L | H | SS | H | L | L | SH | P | SO | NC | F | C |
| IBFT | P | L | H | SS | H | L | L | SH | P | SO | NC | F | C |
| DBFT | Both | L | H | M | H | H | M | Both | P | A | RA | UF | D |

**Acronyms:** Consensus mechanism (CM), Permission type (PT), Power consumption (PC), Energy efficiency (EE), Privacy and Security (P/S), Speed (SP), Scalability (SC), Transaction cost (TC), Data handling (DH), Immutability (I), Access (AC), Collision (C), Actors (AR), Authority (AU), Permissioned (P), Permission less (PL), High (H), Low (L), Moderate (M), Secure (SR), Semi-secure (SS), Least secure (LS), Slow (S), Multi-handed (MH), Single-handed (SH), Partially (P), Anyone (A), Specific one (SO), Risk available (RA), No chance (NC), Unfamiliar (UF), Familiar (F), Decentralized (D), Centralized (C)

exchange while ensuring trustworthiness, confidentiality, and anonymity, eliminating the need for centralized third-party entities. This shift in data trading methodology has the potential to facilitate compliance assessment with domestic and international regulations, leveraging data gathered from mobile devices equipped with sensors for monitoring various metrics [197], [202].

### 2) ANATOMIC IOT OPERATING SYSTEM

The IoT enables connectivity, data exchange, and value creation through integrated physical products such as sophisticated electronics, sensors, and actuators communicating with the IoT network infrastructure. However, concerns over confidentiality and security vulnerabilities have hindered the widespread adoption of IoT. Consequently, IoT devices are often susceptible to security flaws, making them targets for DDoS attacks [203]. These attacks disrupt businesses and individuals by overwhelming the intended systems with data requests. To address these issues, integrating IoT with BCT can enhance security and sustainability. Moreover, BC enables devices to securely transmit data to commercial BC networks, ensuring tamper-proof records of transactions. By eliminating the need for centralized coordination, BC facilitates direct data exchange and authentication among IoT devices and participants, mitigating conflicts and building trust within the network [204]. Furthermore, BC can also address privacy and sustainability challenges in the IoT ecosystem by exploiting accompanying ways:

- The distributed ledger in a BC system is tamper-resistant, eliminating the need for trust between parties. The vast amount of data generated by IoT devices exceeds the capacity of any single organization.
- Storing IoT data on BC enhances security against cybercriminals attempting unauthorized access. BCT provides robust encryption that makes deleting metadata entries nearly impossible.
- BC enables transparency, allowing authorized individuals to track previous transactions and quickly address privacy breaches.
- BCT enables seamless transaction execution and synchronization among interconnected devices. As pervasive computing grows, DLT provides a practical solution for various activities.
- BC eliminates computational costs for IoT hubs, enabling cost savings and establishing stakeholder trust.

However, BC offers an open, trustworthy ecosystem for the IoT, although its implementation in lower computing spectrums is still infancy [205]. With the IoT's expansion across industries, challenges arise regarding confidentiality, legitimacy, dependability, and sustainability. Consequently, BC's security, openness, stability, and predictability make it an ideal solution for enhancing IoT systems and supporting future growth. For example, the authors in [206] explain how IoT devices can provide real-time patient data in a hospital setting, but centralized data processing poses risks. BC addresses these concerns by offering decentralized

**TABLE 6.** A comparative study of bilateral enlightenment of ML/BCT in the view of existing research.

| | | |
|---|---|---|
| **authors and Publication year** | **Perceptive description** | BC-enabled IoT, resource optimization for delay tolerant data |
| Meng Li [174], 2020 | **Consequential holding** | The IoT network connects machine-type communication devices (MTCDs) for efficient machine-to-machine (M2M) communication. A joint optimization framework is utilized to meet network demands like edge computing, caching, and security. This framework incorporates a dynamic decision process using deep Q-network (DQN) and BCT as a solution. |
| | **Consequential flaw and criticism** | The focus should be reducing average service latency and accommodating different cache storage capacities at the edge computing server. The system should also reward assorted block sizes within acceptable time limits. Additionally, employing various optimization strategies for MTCDs will further enhance performance. |
| | **Conclusive comment** | To enhance system performance and minimize unnecessary latency, this research proposes a novel approach incorporating caching storage, computational servers, and BC systems for reliable data in M2M communication networks. |
| **authors and Publication year** | **Perceptive description** | BC-based event identification and trust validation by exploiting ML |
| Zeinab Shahbazi [175], 2021 | **Consequential holding** | This research work focuses on developing a solution for managing disasters and emergencies. It utilizes ML, DL, and natural language processing techniques in supervised and unsupervised learning methods for text analysis. |
| | **Consequential flaw and criticism** | The nature of microblogging, with its acronyms, internal language, and character limits, poses challenges for generalization. |
| | **Conclusive comment** | The proposed work employed a seamless BC and ML pipeline to connect emergencies and disasters with patient care organizations, facilitating efficient relief operations. |
| **authors and Publication year** | **Perceptive description** | By utilizing supervised learning, node characters are exposed to a BC. |
| Radoslaw Michalski [176], 2020 | **Consequential holding** | The authors explored alternative methods, such as analyzing extensive behavioral datasets, to detect the identity of members in a BC-based system without explicitly revealing it. |
| | **Consequential flaw and criticism** | The presented findings of the paper emphasize that not all BC implementations follow the same principles and protocols as the Bitcoin network, indicating a lack of generalization. |
| | **Conclusive comment** | The primary objective of this study was to determine whether a specific set of features could be utilized to reveal the characteristics of nodes within a BC-based network. |
| **authors and Publication year** | **Perceptive description** | BC-enabled ML in medical imaging for privacy preservation and trustworthiness. |
| Fadila Zerka [177], 2020 | **Consequential holding** | The research introduced chained distributed ML, combining sequential distributed learning with BC. It demonstrated its feasibility and comparable results to centralized systems while ensuring privacy and security. |
| | **Consequential flaw and criticism** | Accurate and trustworthy AI models in healthcare depend on high-quality data, which can be challenging to obtain in sufficient quantities. |
| | **Conclusive comment** | This study confirms the viability of the proposed hypothesis combining chained distributed ML and a BC-based platform. It yields comparable results to the conventional centralized approach. |
| **authors and Publication year** | **Perceptive description** | Adaptivity enabled, BC network by exploiting DRL. |
| Chao Qiu [178], 2020 | **Consequential holding** | The study explores the application of DRL to improve scalability and adaptivity in future BC networks, dynamically allocating computing and bandwidth resources to meet diverse user needs. |
| | **Consequential flaw and criticism** | The proposed work is in its early stages and still lacks maturity compared to other aspects, such as storage, hardware, cryptography, and topology. |
| | **Conclusive comment** | This article explores the use of adaptivity to address scalability challenges in the BC-enabled IoT network. |
| **authors and Publication year** | **Perceptive description** | BC-enabled congestion control mechanism using ML for next-generation vehicular networks. |
| Saida Maaroufi [179], 2021 | **Consequential holding** | The study introduces BCOOL, a novel BC congestion control system for vehicular networks. BCOOL addresses the gap in reliable BC congestion prediction and incorporates a dynamic and hybrid BC fog-based distributed trust contract strategy to manage message and vehicle trustworthiness. |
| | **Consequential flaw and criticism** | The method has several constraints that need to be relaxed in future designs of BCOOL to improve performance for real-world scenarios. |
| | **Conclusive comment** | Simulation results indicate that BCOOL surpasses other comparable techniques by 85% and 100% in terms of reliability and efficiency advantages during severe data congestion conditions. |
| **authors and Publication year** | **Perceptive description** | BC-enabled FL for heavy haul railway. |
| Gaofeng Hua [180], 2020 | **Consequential holding** | Implementing intelligent control in heavy-load rail systems is an important goal to pursue. The authors introduce a BC-based FL method to enable asynchronous cooperative ML among distributed agents with their data. |
| | **Consequential flaw and criticism** | The work has drawbacks, including slower convergence speed, suboptimal local solutions, and potential overfitting in the ML algorithm model. Additionally, training time is significantly increased due to the need to train multiple models in the DAG. |
| | **Conclusive comment** | The authors suggests a BC-based FL system to ensure user data privacy and security. They also employ an SVM classification model for intelligent control of large haul trains, specific traction, or electric brake control. |
| **authors and Publication year** | **Perceptive description** | BC-enabled FL for autonomous vehicles. |
| Shiva Raj Pokhrel [181], 2020 | **Consequential holding** | The authors introduce an autonomous BC-based FL system for privacy-aware and efficient vehicular communication networking. It utilizes a distributed approach to communicate and verify local on-vehicle ML (OVML) model updates. |
| | **Consequential flaw and criticism** | The proposed BC FL system has two drawbacks: centralization and loyalty. |
| | **Conclusive comment** | The BC FL system model facilitates decentralized sharing and validation of updates among local OMVL learning modules, enhancing autonomous vehicle communication. |

**TABLE 6.** ***(Continued.)*** **A comparative study of bilateral enlightenment of ML/BCT in the view of existing research.**

| | | |
|---|---|---|
| **authors and Publication year** | **Perceptive description** | Network coverage of trusted UAVs by exploiting ML, BC, and auction mechanism. |
| Amjad Saeed Khan [182], 2020 | **Consequential holding** | The authors examined the utilization of BC and auction mechanisms to enable autonomous decision-making and outsourced network coverage for meeting QoS requirements. |
| | **Consequential flaw and criticism** | The research utilizes a private BC system, which faces challenges related to centralization and reduced security due to potential data breaches. |
| | **Conclusive comment** | The authors devised an auction method that addresses economic aspects and service provider adverse selection in UAV-based network coverage. Through theoretical analysis, it was shown that truthful bidding is the most profitable strategy in the auction. |
| **authors and Publication year** | **Perceptive description** | BC-enabled SVM training for IoT data in smart cities. |
| Meng Shen [183], 2019 | **Consequential holding** | The authors propose a privacy-preserving SVM training scheme called fast and secure SVM, designed explicitly for encrypted IoT data in a BC-based environment. The authors establish a secure and dependable platform for exchanging data from multiple sources by leveraging BCT. |
| | **Consequential flaw and criticism** | The SVM algorithms adopted in this study could be better for handling large datasets and may exhibit subpar performance when confronted with noisy data. |
| | **Conclusive comment** | The authors introduced a novel and secure SVM training scheme that leverages BC to address privacy and impurity concerns in multipart scenarios with diverse data providers. This approach ensures the confidentiality and integrity of IoT data during SVM training. |
| **authors and Publication year** | **Perceptive description** | A BC-based incentive for auditable and privacy-preserving DL. |
| Jaisi Weng [184], 2021 | **Consequential holding** | The authors proposes a secure and fair DL framework to address security issues in popular FL methods. This framework ensures the integrity and reliability of the training process, particularly in preventing participant misbehavior during gradient collection. |
| | **Consequential flaw and criticism** | The current incentive mechanisms have limitations, such as being adequate only for repetitive tasks and potentially causing resentment. |
| | **Conclusive comment** | The authors present a distributed and secure DL approach that guarantees confidentiality, auditability, and fairness. |
| **authors and Publication year** | **Perceptive description** | Bayesian RL for MEC by utilizing BC |
| Alia Asheralieva [185], 2021 | **Consequential holding** | The authors introduce a game-theoretic framework combining Bayesian RL and DL in MEC to analyze the behavior of miners in both public and consortium-BC settings. |
| | **Consequential flaw and criticism** | In the game-theoretic approach, firms are assumed to have knowledge of each other's strategies and can create a payoff matrix to analyze potential solutions. |
| | **Conclusive comment** | The authors have proposed a novel RL and DL framework to model the interactions among miners in a BC with MEC. The framework accounts for stochastic games with incomplete information. |
| **authors and Publication year** | **Perceptive description** | A decentralized electricity trading for the connected vehicle by exploiting ML and BC |
| Dhaou Said [187], 2021 | **Consequential holding** | The authors designed a distributed intelligent contract system for connected electric vehicles (CEVs) to improve road safety and reduce traffic congestion. Through a stochastic bidding process, it enables CEVs to sell and buy electricity at the highest profit. |
| | **Consequential flaw and criticism** | The work focused on electricity trading, where participants with more cryptocurrency are given preference. However, the network exhibits a slight bias. |
| | **Conclusive comment** | The authors conducted simulations in MATLAB and solidity, comparing the proposed profit method with PETCON. The results showed the effectiveness of the proposed approach. |
| **authors and Publication year** | **Perceptive description** | BC-enabled FL for intelligent edge computing by utilizing unintended property leakage |
| Meng Shen [188], 2021 | **Consequential holding** | The authors propose a novel property inference attack in BC-assisted FL for intelligent edge computing. The research explores unintentional property leaking and develops an active method to learn and identify participants with specific properties from model updates. |
| | **Consequential flaw and criticism** | The limitations of the property inference attack are highlighted, including the attack model's time cost and reduced accuracy. These limitations arise from the large number of iterations required in the attack model and the increased selection of participants. |
| | **Conclusive comment** | The authors proposed a novel approach in BC-assisted FL for intelligent edge computing to leverage the unintentional leakage of characteristics from model updates. |
| **authors and Publication year** | **Perceptive description** | BC-enabled FL for knowledge sharing in IoV. |
| Haoye Chai [189], 2021 | **Consequential holding** | This study introduces a hierarchical BC architecture and FL algorithm for knowledge sharing. Vehicles utilize ML methods to learn environmental data and exchange their acquired knowledge with others. |
| | **Consequential flaw and criticism** | In an IoV scenario, it is essential to analyze the overhead and transaction throughput of the proposed hierarchical BCT. This investigation provides insights into the practical implementation of the system. |
| | **Conclusive comment** | The simulation findings indicate that the proposed hierarchical approach enhances sharing efficiency and improves learning quality. Additionally, the BC-enabled infrastructure demonstrates effective resilience against various hostile threats. |
| **authors and Publication year** | **Perceptive description** | Energy exchange for smartgrid by utilizing DL and BC. |
| Mohamed Amine Ferrag [190], 2020 | **Consequential holding** | The authors propose a DL and BC-based energy architecture for smart grids, incorporating a reliable P2P energy system and employing the BFT algorithm for high throughput. The architecture also focuses on security using short signatures and hash functions for block generation. |
| | **Consequential flaw and criticism** | Efficient operation is a limitation due to the need to minimize the number of nodes to reduce communication overhead. |
| | **Conclusive comment** | The authors introduced DeepCoin, an innovative energy architecture combining deep learning and blockchain for intelligent grid operations. |
| **authors and Publication year** | **Perceptive description** | BC and FL for privacy-preserved data sharing in IIoT. |

**TABLE 6.** ***(Continued.)*** **A comparative study of bilateral enlightenment of ML/BCT in the view of existing research.**

| | | |
|---|---|---|
| Yunlong Lu [191], 2020 | **Consequential holding** | The authors developed a secure data-sharing architecture leveraging blockchain for multiple distributed parties. Additionally, they introduced privacy-preserving FL to address the data-sharing challenge in an IIoT network. |
| | **Consequential flaw and criticism** | Centralization and security are significant concerns in a permissioned or private blockchain network. |
| | **Conclusive comment** | The proposed data-sharing methodology demonstrates high precision, reliability, and confidentiality, supported by numerical results from real-world statistics. |
| **authors and Publication year** | **Perceptive description** | BC-based FL for device failure in IIoT. |
| Weishan Zhang [192], 2021 | **Consequential holding** | The study applies BC-based FL for IIoT device failure detection and incorporates a merkle tree for data integrity. A centroid distance-weighted federated averaging algorithm is employed to handle data heterogeneity and account for different class distances. |
| | **Consequential flaw and criticism** | The study is limited to the client-server model and does not address the exploration of shifting the client-server to the client device, which presents an unexplored area for further research. |
| | **Conclusive comment** | The study proposed a BC-enabled FL approach for detecting equipment failures in IIoT. The control server coordinates client servers to train a global model using locally recorded raw data, facilitating accurate identification. |
| **authors and Publication year** | **Perceptive description** | ML and BC in communication systems and networking |
| Yiming Liu [5], 2021 | **Consequential holding** | The survey papers exclusively concentrate on integrating ML and BC in wireless communication. |
| | **Consequential flaw and criticism** | The survey paper lacks specific information about the types of nodes in BC and the consensus algorithm used. |
| | **Conclusive comment** | The survey paper highlights the reciprocal advantages of ML and BC, providing detailed coverage of their respective applications and synergies. |
| **authors and Publication year** | **Perceptive description** | Hybrid BC for resources trading in edge computing |
| Sizheng Fan [193], 2021 | **Consequential holding** | The authors suggest a hybrid BC resource trading system incorporating public and consortium BC. An intelligent contract enables automated reverse auctions among edge nodes. |
| | **Consequential flaw and criticism** | The proposed work can also be extended to explore trading markets with multiple requesters, requiring further investigation and attention. |
| | **Conclusive comment** | The authors introduce a hybrid BC-based resource trading system for FL in edge computing. They propose a data quality-driven reverse auction (DQDRA) using a consortium-BC's smart contract for automated and auditable auctions among edge nodes. Simulation results show the superiority of DQDRA over existing reverse auction mechanisms. |
| **authors and Publication year** | **Perceptive description** | Intrusion detection in vehicular edge computing by exploiting BC and FL |
| Hong Liu [194], 2021 | **Consequential holding** | The study introduces a distributed cooperative intrusion detection mechanism that offloads the training model to edge devices. This approach reduces the resource usage of the central server while maintaining security and privacy. |
| | **Consequential flaw and criticism** | BC in vehicular communication networks may face storage limitations due to model training, offloading aggregation, and heavy storage requirements. |
| | **Conclusive comment** | The paper investigates known attacks and shows that the proposed strategy achieves cooperative privacy preservation with reduced communication overhead and computation costs. |
| **authors and Publication year** | **Perceptive description** | BC for private and secure FL |
| Muhammad Shayan [195], 2021 | **Consequential holding** | The study employs a decentralized P2P multiparty ML approach that ensures confidentiality-protected ML operations among collaborating clients using blockchain and cryptographic techniques. |
| | **Consequential flaw and criticism** | The study highlights the limitations of the proposed approach, such as the challenge of utilizing a large number of samples in a distributed system network, difficulty in scaling to large DL models with millions of parameters due to communication overhead, and concerns regarding model leakage and stake limitations. |
| | **Conclusive comment** | The analysis indicates that the proposed work is highly scalable, resilient to faults, and robust against known threats. |
| **authors and Publication year** | **Perceptive description** | DL oriented BC on the internet of drones environment. |
| Maninderpal Singh [196], 2021 | **Consequential holding** | The article proposes a blockchain-based security mechanism for cyber-physical systems, ensuring secure data flow among drones. |
| | **Consequential flaw and criticism** | The study does not adequately address the reduction in the blockchain size of individual drones, which presents an area for further exploration. |
| | **Conclusive comment** | The study proposes a secure D2D and device-to-everything communication model, incorporating blockchain technology to ensure secure data dissemination. The solution utilizes zero-knowledge proof (ZKP) in an interoperability device (IoD) environment. Validation of various components, such as computing cost, communication cost, and real-time performance, has been conducted. The IoD environment ensures data integrity and privacy. |

**TABLE 7.** Diverse use cases of integrated approach of ML, BCT together with 6G.

| Use cases | Explanation | Challenges | ML/BC Contribution |
|---|---|---|---|
| Applications in industry 5.0 | Industry 5.0 utilizes intelligent robots for complex tasks while humans focus on routine jobs. It integrates AI/ML, VR/AR/XR, digital twins, and advanced robots. However, 6G communication technologies enable efficient URLLC, mMTC, and more operations. | Challenges are scalability, security, AI/ML utilization, network centralization drawbacks, and resource optimization in dynamic industry applications. | BC integrated with edge computing enables enhanced scalability, security, and privacy while decentralizing decision-making. |
| Smart healthcare | 6G communication networks will transform the medical industry, providing ultra-high reliability, low latency, and excellent mobility for advanced medical applications. | The essential requirements include privacy protection, high reliability, decentralized operations, and intelligent device management. | BC is widely used in medical applications for secure and decentralized medical data management in IoT environments. It enables robust and reliable intelligent medical systems with efficient records management and protection against attacks. |
| UAV applications | UAVs have evolved from military to civilian applications and are expected to play a vital role in the 6G mobile network. Moreover, UAVs are also utilized in intelligent cities for traffic control, video surveillance, remote sensing, agriculture, and construction. | UAV applications require reliable network availability, enhanced fault tolerance, security resilience, and minimal latency. | BC envisions incorporating UAVs into 6G technology, enabling decentralized decision-making, secure data exchange, privacy preservation, and intelligent contract-based access control. |
| Connected autonomous vehicles | Future networks will witness the emergence of connected and autonomous vehicles (CAVs) that rely on advanced technologies for real-time sensing, secure networking, and automated driving decisions. | Real-time reliability, AI/ML processing, optimized sharing, and trusted transactions are vital for CAVs. | BC seamlessly integrates with 6G networks, enabling innovative CAV applications with smart contracts, decentralized management, P2P trading, and privacy preservation. |
| Extended reality | 6G enables XR applications to leverage high-speed data, large capacity, and ultra-low latency for immersive experiences. | XR applications face challenges such as file format compatibility, security vulnerabilities, processing delays, and scalability concerns. | 6G networks with BC integration support XR applications, live experiences in music and sports, virtual community building, and resolve file format challenges in VR/AR. |
| 3D Networking | In the 6G era, mobile networks aim to extend horizontal and vertical coverage, integrating terrestrial and non-terrestrial systems for broad and comprehensive network reach. | Needs are interoperability, privacy protection, decentralized data exchange, and intelligent decision-making in 6G. | Researchers have incorporated a multi-chain solution in BC-enabled 3D networking, enabling a decentralized heterogeneous network with enhanced cross-chain security. |
| Resource management | Efficient RM in 6G leads to increased utilization, cost reduction, improved QoS, and wealth generation. However, managing resources across industries, IoE devices, and subscriber growth poses complexity. | Managing resources in 6G is challenging due to the diverse connectivity requirements and dynamic nature of needs. | BC enables secure RM and transparent operation of decentralized mobile networks, ensuring visibility and immutability. |
| Ubiquitous intelligence | Integrating AI in 6G networks brings community intelligence, efficiency, and sustainability. Network management-level automation enables diverse environments to reap the benefits of AI-based technologies. | Critical concerns are AI integration, actor reliability, distributed systems, security, and scalable ubiquitous intelligence in 6G. | BC enables the secure sharing of training data and uploading locally trained ML models in FL-based systems. In 6G, mobile users can safely exchange data for AI model training using BC, similar to FL. |
| Mobility management | Tiny cells and a 3D system in 6G will result in high mobility and frequent handoffs in horizontal and vertical directions. | 6G requires reliable and mobility management for high-speed, low-latency communications. Mobile networks must address traceability, immutability, security, and decentralization. | BC enables decentralized operation, secure authentication, roaming fraud protection, anonymity, equitable economic incentives, and resilience against network attacks. |
| Interference management | Interference management optimize spectrum usage by reducing interference. | The critical challenges are to mitigate different types of interference, such as co-channel, adjacent, out-of-the-band, and remote interferences, to enhance the SINR. | BC prevents interference through currency exchange among nodes, minimizing interference and enhancing financial assets. |
| Quantum communication | Quantum communication encodes information in quantum states and enables secure transfer between sites using quantum components. | Quantum mechanics principles, such as entanglement and superposition, guarantee secure information transfer, as any access or copying would disrupt the quantum state. | BC's decentralized storage and stringent access control features enable support for quantum communication applications in the 6G network. |

computation and data preservation. Consequently, integrating IoT with BCT enables a decentralized intelligent E-healthcare system. [206]

### 3) INDIVIDUAL INTEGRITY PROTECTION

BCT's impact on user identification and experience in BC services is an essential discussion for further investigation. The digital explosion has highlighted the hazards of centralized digital interactions, necessitating alternative solutions that provide security, convenience, and user control. Combining unique identifiers and authenticated qualities, self-sovereign identification allows users to assert sovereignty over their data and gain insights from its exploitation [207]. Consequently, decentralized identity management on BC, such as Hyperledger, offers irreversible and robust verification [207]. Decentralized ledgers, hashing mechanisms, and smart contracts provide potential solutions for identity verification in local community networks. Moreover, utilizing BCT, private information can be scrambled, and identities can be managed using public-private keys [208]. An expanded framework utilizing DLT improves confidence in online transactions and marketing networks while maintaining privacy features [209]. Furthermore, BC-enabled assurance platforms offer insurance service options for private online identification, endpoint security, and data confidentiality. The network's security and tamper-resistant capability are ensured through smart contracts and, consequently, the individual's integrity [210].

#### 4) DISTRIBUTED, LEGITIMIZED SECURITY AND PRIVACY

The emergence of new ML algorithms has traditionally relied on a consolidated or centralized framework, where a single entity possesses the necessary resources and expertise to handle complex data and solve diverse objectives. However, such consolidated ML systems may face limitations in dealing with highly intricate attributes, leading to communication and networking restrictions. Consequently, it can be non-scalable, commercially inefficient, and prone to inefficiency. A Decentralized Machine Learning (DML) has emerged as a viable framework to address these concerns by leveraging dispersed heterogeneous resources [209]. DML improves training efficiency, reduces throughput and power usage, and eliminates the need for a central authority. However, privacy concerns arise in existing decentralized ML platforms, necessitating the integration of BCT into the communication system. BCT's decentralized nature provides the necessary regulations for decentralized ML algorithms prioritizing safety and confidentiality. ML can be performed on individual computers in decentralized and distributed systems using BCT, enhancing training and decision-making process. Safeguarding and preserving data confidentiality is crucial in applying ML to communications and networking. Centralized ML frameworks are susceptible to manipulation, and data theft can lead to privacy breaches. As a result, BC offers secure data storage with encryption technology, protecting sensitive and confidential information and allowing for anonymized storage on a distributed ledger. BC's consensus mechanisms prevent fraudulent data registration, and its characteristics, such as openness and verifiability, support monitoring information updates. BC-enabled approaches have gained recognition in various domains, including medical, IoT, cloud storage, intelligent driving, transportation systems, and authentication systems [211], [212], [213], [214], [215].

BC-based solutions have been proposed for verification, anonymity, transparency, information integrity, and data planning and management [216]. Privacy-preserving techniques utilizing BCT have been developed, such as personal SVM training and privacy-preserving DL architectures [183], [217]. These advancements aim to overcome reliability, scalability, and resilience issues while ensuring privacy and confidentiality.

### B. INCORPORATION OF ML IN BCT

Despite BC being a viable technology, it has its problems and constraints. This section focuses on the core challenges of BC and proposes ML-based solutions to enhance various aspects of BCT, including energy and resource efficiency, scalability, confidentiality, and intelligent contract implementation.

#### 1) OPTIMIZED RESOURCE AND ENERGY EFFICIENCY

This section delves into the challenges related to energy consumption and resource efficiency in BC, mainly due to the PoW consensus algorithm, which is still utilized in several BC approaches [218].

The computational intensity of cryptographic hashing and the competition among miners to solve complex puzzles result in significant energy consumption [218]. To address this, researchers are exploring sustainable consensus procedures that incorporate ML, such as proof of learning [218], proof of DL [219], proof of training excellence, and proof of valuable work [191]. Moreover, energy efficiency remains a persistent challenge in BC systems. Consequently, integrating ML into BCT can lead to more intelligent mining strategies that prioritize critical transactions and process them faster [220]. Consequently, the authors in [221], investigate the integration of BC, ML, and SDN in IoT networks to create a secure and energy-efficient framework [221]. The proposed framework utilizes public and private BCs, decentralized credibility, and a novel routing algorithm to facilitate P2P communication among IoT devices and SDN controllers. This approach aims to make BC suitable for resource-constrained IoT devices. Furthermore, the authors in [222] explore the application of RL and BCT in intelligent electric vehicle (EV) charging networks to reduce energy usage and enhance network security. BCT is utilized in charging infrastructure payment gateways to ensure the validity and confidentiality of charging database communication [222]. To overcome BC's computational and energy-related challenges, the authors propose a billing data transfer method that combines BC, ML, and MEC [223]. This method improves nodes' processing capability and reduces the consensus mechanism's energy consumption [223]. The study also emphasizes the potential of SDN and BC in establishing secure and trustworthy network architectures [223]. An optimized and energy-efficient BC-enabled software-defined IoT architecture is presented in [223], leveraging ML, SDN, and BC to control resource utilization and enable reliable network communication effectively.

In the context of UAV-enabled IoT applications, safety and energy optimization are crucial [224]. Integrating ML-oriented BC into UAV networks enables data gathering with a focus on safety and energy sustainability [224]. The ML-oriented UAV network acts as a peripheral data-gathering node, updating and sharing information on the BC using ML techniques [224]. The authors also propose an energy-conserving consensus mechanism called Proof of AI (PoAI) and an intelligent node selection process to ensure efficiency, decentralization, and security in BC networks [224]. An ideal bidding based on DL methodology is also suggested for edge computing resource allocation, aiming to reduce energy consumption and enhance network efficiency in mobile BC applications [225].

All in all, integrating ML with BC presents opportunities to address energy efficiency, scalability, and confidentiality challenges [218]. By leveraging ML algorithms, BC systems can become more intelligent, secure, and resource-efficient, enabling advancements in various domains such as IoT [221], EV charging networks [222], and edge computing [223].

### 2) RL ENABLED OPTIMIZATION IN MINING STRATEGIES

Mining involves using computational resources to estimate values for executing tasks on a BC. Successful miners add legitimate queued transactions to the BC, ensuring it remains updated. Incentives like Bitcoin and transaction fees are given to miners. Moreover, this section explores ML approaches to optimize mining operations and prevent resource theft.

In January 2021, Taotao Wang et al. presented a research paper on using RL to optimize BC mining techniques for cryptocurrency [226]. The study found that RL approaches can forecast more efficient and accurate mining algorithms, even without prior knowledge of the BC methodology or relevant factors like computing resources and processing fees. The unpredictable nature of cryptocurrency mining makes it challenging to create reliable models. The research introduced a multivariate RL algorithm using Q-Learning, demonstrating its effectiveness in enhancing cryptocurrency mining. Mining cryptocurrencies like Bitcoin is profitable, with companies such as Argo BC, Riot BC, and Hive BC mining bitcoins worth millions. Further, the authors in [226], leverage RL-enabled AI-ML techniques to determine the optimized BC mining technique without requiring specific BC network knowledge. While formulating a Markov decision process model could be an option, accurately determining the parameter values defining the BC network model is complicated and subject to change. To overcome this, the authors dynamically develop a mining strategy using RL that achieves performance comparable to the ideal strategy. A new multi-dimensional RL technique is proposed to address this challenge. Furthermore, in [227], the authors present a unique decentralized approach using DRL and a multi-agent profound predictable policy gradient technique. They employ a game-theoretic approach to describe competition and cooperation in unloading and mining.

In summary, these research efforts demonstrate the utility of ML approaches, such as RL and DRL, in optimizing mining operations and preventing resource larceny. RL enables the development of effective mining strategies without detailed knowledge of the BC network, while a multi-dimensional RL technique addresses the challenges of parameter value uncertainty. The decentralized DRL approach offers insights into competition and cooperation in mining and results in an efficient network.

### 3) DL/GRAPH CONVOLUTIONAL NEURAL NETWORKS (GCN) ENABLED TACKLING CRYPTOJACKING

Science labs and government institutions, which possess substantial computing resources and capital, have become prime targets for cryptojackers. These malicious actors hijack computers and exploit them for cryptocurrency mining, resulting in widespread incidents that frequently make headlines. To combat this threat, researchers from the United States have collaborated to develop a solution for identifying fraudulent applications that aim to commandeer computing resources. The technology devised by these experts is called SiCaGCN, which combines graph convolutional neural networks and capsule networks. SiCaGCN operates by analyzing the correlation between two programs or pieces of code, utilizing observations on a structured graph representation of the algorithms. This innovative system integrates DL, ML methodologies, and NN topologies. By leveraging these advanced techniques, SiCaGCN aims to effectively detect and mitigate cryptojacking attacks. Furthermore, it is crucial to monitor specific execution statistics to enhance the effectiveness of SiCaGCN. These statistics include computational resource utilization, network traffic patterns, anomalous behaviors, and code execution patterns. By closely monitoring and analyzing these metrics, the SiCaGCN system can identify and prevent unauthorized exploitation of computing resources by cryptojackers. Moreover, DL applicability is also found in several areas, such as fraud detection, AD, consensus optimization, and privacy-preserving smart contracts. In summary, the collaboration among researchers from academic and government institutions has resulted in the development of SiCaGCN [228].

### 4) OPTIMIZED SCALABILITY AND IMPROVED PRIVACY AND SECURITY

In the current BC landscape, scalability poses a significant bottleneck as transaction frequency increases, impeding the overall growth of BC systems. The need arises to reduce the time, cost, and complexity associated with transaction approval and authentication processes, particularly in communication and networking systems that cater to numerous users and require rapid scaling. BC systems such as Bitcoin need help to handle high transaction volumes efficiently, leading to challenges in node startup and transaction authentication [5]. To address scalability limitations, various consensus mechanisms have been proposed. First-layer scalability solutions such as sharding, segregated witness, and hard forks aim to enhance scalability. Second-layer scalability solutions include state channels, sidechains, plasma, and lightning networks. Other consensus mechanisms, such as DPoS, PoA, and BFT, have been discussed in previous research [5], [229] These scalable mechanisms are particularly beneficial in scenarios with a high volume of transactions, such as wireless communication and networks. Rather than processing or storing the entire transactional data of the BC, the network is scaled up into sub-networks (shards), where each shard independently processes a substantial amount of transactional data. Consequently, ML and RL techniques can be effectively employed to optimize the execution of these scalable techniques by making intelligent decisions [229].

It is evident that wireless networks often require concurrent ML processing due to diverse applications and datasets. However, concurrent ML training challenges resource consumption, scalability, and performance consistency. Addressing these challenges, the research emphasizes the importance of considering unique data types and characteristics when dealing with large-scale ML frameworks. Statistical features of the dataset, such as sample variance, sparseness, heterogeneity, and sampling pattern matching, can be used to measure example disparities and transform the network into an efficient and scalable communication system [230]. A DRL-based parallelization methodology has been proposed for BC-based IIoT networks, aiming to overcome scalability issues and boost productivity in the IIoT. This methodology enables selecting and modifying block creators, consensus mechanisms, block size, and block periods to improve efficiency and support various applications [230]. While BC itself may be difficult to trace, subsequent layers and applications raise concerns about confidentiality, especially as the volume of private information stored in BC-enabled communication systems grows. A probability-enabled factor model (PFM) combined with unsupervised ML techniques has been applied to BC to identify vulnerabilities and predict potential harm intelligently. The PFM utilizes factor analysis and probabilistic modeling to issue injunctive relief based on historical data [231]. Supervised ML models have been employed to tackle cybercrime behaviors in the context of cybersecurity in the Bitcoin network. The process involves data stream processing, classifier construction and evaluation, and generating final outputs. ML methods use pre-processing approaches to collect and aggregate addresses and classify unsorted information. Multiple classifiers are examined, and the classifier trained on categorized events predicts the class of unsorted events, generating visualizations to aid analysis and investigations [231]. A DML framework has been proposed to tackle safety, reliability, and potency challenges in private BC systems, focusing on differential confidentiality. This framework incorporates a differentially permissible stochastic gradient descent method and an error-based consolidation strategy to enhance the system's resistance, potency, and safety against attacks by adversary nodes [184]. Furthermore, integrating sophisticated DL techniques into BCT can improve reliability compared to conventional ML methods across various applications. Moreover, a comprehensive representation of comparative study in terms of bilateral enlightenment of ML/BCT in the view of existing research work has been shown in Table 6.

## V. INTEGRATED APPROACH OF AI AND BCT IN DISTINCTIVE COMMUNICATION TECHNOLOGIES

### A. AI AND BCT INTEGRATED 6G-MC NETWORK

A viable communication technology can be a molecular mode of communication in the next-generation wireless network. Nevertheless, the approach is still infancy. The underlying concept of MC technology is to use of biological signals for information transport. The authors in [232] suggested a method of mobile-MC that permitted the Tx, recipients, and access points to work together during movement. Owing to communication and authentication procedures in MC, numerous privacy and security issues have been noted. Nonetheless, these security concerns include data leakage and tempering data between Tx and the recipient. In addition, these security attacks are broadly classified into four categories: signaling attacks in the physical layer, transport layer attacks, link layer attacks, and network layer attacks.

Further, in [233], the authors tried to link it with the nano-things, a future diagnostic system is proposed that uses MC and ML methods to assess and explore illness biomarkers online. It is one of the applications of the Internet of BioNano Things (IoBNT). For illustration, consider intra-body sensing and actuation, where bio nano-objects dispersed within the human body work together and cooperatively gather health-related data. Hereafter, the data is transmitted through the internet to a third-party healthcare provider [234], [235]. Moreover, a gateway between the MC and the cyber realm is required to enable information sharing between the nano network. The gateway must reliably receive the molecular data and convert it to EM attributes and vice versa. However, one of the primary obstacles to the practical implementation of IoBNT is the creation of such gateways and confidentiality of data transmission. Mitigating the security concern necessitates considering a decentralized and guarded technology [236]. The authors in [237] investigate a multi-hop MC network and propose distinct relaying strategies to enhance the range of diffusion-based MC. Consequently, an undisclosed decision threshold was discussed to mitigate self-interference while security concerns remain unaddressed. In [238], the authors explore the potential of MC via diffusion (MCvD) for constructing nano-networks. However, the inherent diffusion characteristics of information molecules in MCvD result in slow data rates, significant inter-symbol interference effects, and security flaws. In [239], shared communication medium accommodating multiple Tx-Rx pairs within nano-bio networks lead to Rx saturation due to intersymbol and multi-user interference, resulting in potential outages and security inadequacy. In the context of MC systems discussed in [240], multiple Rx nanomachines coexist within a communication channel, which can result in Rx interference.

**TABLE 8.** 6G open issues, research challenges and solutions.

| Challenges | Solutions |
|---|---|
| Scalability | Implement dynamic scaling techniques to handle varying network demand and workload fluctuations. Utilize advanced DLT, such as DAG or Tangle, for improved performance. Explore advanced consensus algorithms such as PoW with sharding or hierarchical consensus to enhance wireless network efficiency. |
| Privacy and Security | A wireless network is susceptible to security breaches, enhancing privacy by integrating zero-knowledge proofs and secure multi-party computation. Safeguard sensitive data using FL approaches. Ensure secure and decentralized user authentication through BC-based identity management solutions. |
| Resource Constraints | In a wireless network, address resource limitations of devices by developing specialized ML algorithms with low power and memory requirements. Offload computation and enable local model training and inference using edge AI techniques. Optimize resource consumption through adaptive compression and model pruning techniques. |
| Latency | Minimize latency by leveraging edge computing infrastructure and deploying ML models at the wireless network edge. Reduce data retrieval delays through effective caching mechanisms for frequently accessed data. Enhance block validation speed by implementing advanced consensus mechanisms such as DPoS. |
| Interoperability | Enable seamless integration of heterogeneous systems through standardized data formats and protocols such as InterPlanetary File System and GraphQL. Achieve cross-chain interoperability for data exchange and transactions between BC networks. Enhance BC interoperability with external systems using oracles and smart contracts. |
| Energy Efficiency | Reduce energy consumption by exploring energy-efficient consensus mechanisms such as PoS or PoA. Enhance EE in IoT devices by employing energy harvesting techniques and low-power communication protocols. Optimize energy usage in wireless network operations by utilizing AI-powered optimization algorithms. |
| Data Quality and Integrity | Ensure data integrity by implementing cryptographic techniques such as digital signatures and hashes for data validation. Identify and filter unreliable or malicious data sources using reputation systems and consensus-based verification mechanisms. Improve data quality by employing fusion techniques to integrate data from multiple sources. |
| Model Fairness and Bias | Mitigate bias, and promote equitable outcomes by integrating fairness-aware algorithms during ML model training and deployment. Ensure fairness through regular audits using metrics like disparate impact and equal opportunity. Address biases with transparent and explainable AI methods to enhance model fairness. |
| Regulatory Compliance | Comply with data privacy and financial regulations by developing general data protection regulation-aligned BC frameworks. Use technologies like zero-knowledge proofs for data protection. Collaborate for seamless BC integration in wireless networks. |
| Governance and Consensus | Promotes transparency and accountability by establishing decentralized governance models that involve network participants in decision-making. Explore efficient consensus mechanisms such as DPoS or Liquid Democracy for democratic decision-making, specifically for resource allocation in wireless networks. |
| Network Bandwidth | Reduce data transmission volume through data compression and intelligent filtering. Improve scalability with off-chain or sidechain solutions to alleviate the leading BC network. Enhance bandwidth capacity and explore advanced communication technologies like 6G for faster and more efficient data transmission in collaboration with network providers. |
| Long-Term Sustainability | Minimize energy consumption through energy-efficient consensus mechanisms and low-power hardware designs. Promote sustainability by integrating carbon offsetting and green energy usage in BC operations. Drive research and innovation in scalability, energy efficiency, and resource optimization for the long-term sustainability of BC networks. |

Consequently, the network needs a decentralized spectrum management system to address the above-stated drawbacks and ensure security. Further, the authors in [241] focus on molecular-based nano-networks, examining two types of attacks. The blackhole attack involves malicious bio-nano entities emitting chemoattractants to disrupt localization tasks, while the sentry attack employs chemo-repellents to prevent legitimate bio-nano entities from reaching their intended destinations. The author also considers the disruptive role of eavesdroppers. In [242], the authors have discussed MC, and nano-electromagnetic communication has attracted substantial attention. However, challenges persist regarding data rate, reliability, and security levels. Furthermore, the authors in [243] highlight the extensive research on abnormality detection and localization in WSNs that employ electromagnetic waves. The security and privacy requirements vary across applications, and intrusion into the body poses a risk of bio-cyber attacks. Protecting against various attack types, such as spoofing, sentry, blackhole, and eavesdropping, is crucial for minimizing network intrusion in intra-sensor and sensor-to-fusion center links. Consequently, integrating BCT with MC is imperative to address the privacy and security challenges highlighted in the above-discussed papers. Incorporating BCT into MC networks makes it possible to enhance data privacy, establish trust among network participants, and provide a secure framework for managing communication and transactional data. BCT integration can strengthen these networks' overall privacy and security, making them more robust against attacks and ensuring the integrity of transmitted information. Moreover, extending the concept to the wireless scenarios, it is evident that wireless systems are generally considered stochastic environments and do not pretend to scale the wireless services. However, only some wireless scenarios are compatible with sound information-carrying wave propagation. Although, MC exploits some noble modulation techniques, such as chemical encoding and multi-scale propagation. Furthermore, the authors in [244] find some applications closely related to defense and security concerns due to the non-scalability of the wireless environment. Consequently generates to think over an alternative to ensure security anxiety in a random environment along with scalability, which needs to be handled by any intelligent and guarded technology, as mentioned above, that includes underwater and underground communication too. Furthermore, the authors in [236] also explore the possibility of incorporating MC systems into upcoming next-generation communication networks. The authors begin by outlining the benefits of MC over traditional wireless communication using EM waves at various scales, specifically at the micro and macro scales.

Consequently, listed some of the principal difficulties in incorporating MC into subsequent-generation of wireless networks and pointed out that attaining communication security and bridging the gap between the chemical and internet domains are two types of the biggest concerns. As a solution to the above-stated concerns, modern communication technology tempts us to integrate AI/ML to make the network self-reliant, salable, and adaptive under its peculiar characteristics, which is illustrated in detail in Section- II.

### B. AI AND BCT INTEGRATED 6G-HC NETWORK

HC is a communication technique that utilizes holography principles to transmit and display information over a wireless communication network. It involves encoding, transmitting, and reconstructing holographic data to enable the realistic visualization of 3D objects or scenes at the receiver's end. HC in 6G wireless networks revolutionizes interaction and collaboration, offering immersive 3D experiences and realistic telepresence. However, it poses security concerns such as hologram spoofing, replay attacks, injection, DoS attacks, phishing, data leakage, and eavesdropping. Consequently, an intelligent and adaptive safeguard technology is needed to address these challenges to secure the futuristic communication network. In [245], the authors discuss reconfigurable holographic surfaces, where holographic beamforming is achieved by constructing holographic patterns. However, the fading effect can impact transactional pattern integrity. In [246], a new space-division multiple access technique called holographic-pattern division multiple access (HDMA) is proposed. While HDMA offers advantages, it is also susceptible to security flaws, including collision, interference, unauthorized access, and eavesdropping.

Further, a MIMO-enabled HC is explored in [247], raising open issues for 6G networks such as holographic channel estimation, robust beamforming, communication blockage, security and privacy of transactional information, and distributed RA. In [248], a multi-user holographic MIMO surface (MU-HMIMOS) concept is introduced as an EE solution for wireless networks. However, addressing the tractable and decentralized channel modeling parameter update of MU-HMIMOS signal propagation still needs to be addressed. Furthermore, in [249], the authors try to combine augmented reality and virtual reality; HC enables real-time communication and interaction through realistic 3D avatars. However, latency and motion sickness pose adoption challenges, emphasizing the need for a decentralized safeguard technology to update the network and ensure decentralized motion awareness. Subsequently, in [250], security flaws in reality and HC are discussed, particularly in human and metaverse communication and machine and metaverse communication. Real-time interactions between machines and the dynamic world are vulnerable to security risks. Besides, the authors in [251] highlight radio localization's significance and speculate on holographic localization, where EM wave characteristics are controlled for improved wireless localization. Decentralized storage of reflected EM wave properties enhances network awareness and statistics.

Consequently, the integrated approach of BCT and HC is crucial for tackling the privacy and security concerns mentioned in the above-discussed papers. This integrated approach enhances data privacy, establishes trust among network participants, and implements a secure framework for effectively managing communication and transactional data. Furthermore, extending it to 6G is critical as the futuristic wireless communication network demands massive connectivity, efficient network and spectrum management, EE, and security and privacy. Moreover, in a wireless network, metrics such as spectrum management, beamforming, and lucid network operations cannot be defined in a single instance due to the dynamic nature of a stochastic environment. Consequently, integrating AI with BCT enables intelligent learning and storage of such metrics updates in a decentralized network. Any changes in the dynamics of the communication medium can be updated in the BC network through smart contracts and consensus mechanisms. This approach ensures that the network continuously adapts to evolving conditions and optimizes its operations based on real-time data, fostering efficient and adaptive wireless communication. Consequently, AI integration with HC and BCT enables the network with intelligent resource management, real-time network optimization, autonomous network operation, a self-adaptive and reliant network, and intelligent user experience, parallelly ensuring enhanced security and privacy.

### C. AI AND BCT INTEGRATED 6G-SC NETWORKS

In the context of 6G wireless communication networks, achieving unprecedented metrics such as ultra-high data rates and ultra-low latency is a primary objective. However, these networks face limitations imposed by Claude Shannon's information theory. To overcome these limitations, SC systems have emerged as a potential solution, leveraging Knowledge Graph-oriented analysis to reduce semantic ambiguity and error rates. In [252], the authors developed a SC system for optimized bandwidth usage during image transmission. However, challenges arise from the noisy channel, necessitating error mitigation techniques to ensure security. A comprehensive survey in [253] highlights security concerns in wireless environments, including fading channels and limited network resources. These resources and heterogeneous network devices limit network efficiency. Consequently, efficient and secure RA and management are crucial for minimizing unnecessary resource consumption and ensuring acceptable BER. Further, to enhance resource utilizability, the authors in [254] presented a one-to-many SC system focusing on broadcasting scenarios. However, interference challenges between users call for decentralized dedicated user identities to mitigate interference. Moreover, the idea is extended to multimedia transmission; here, the authors in [255] propose high-efficiency coding methods for video transmission over noisy wireless channels. However, further security considerations need to be addressed. Conclusively, the wireless RA and semantic information extraction for energy-efficient communication are investigated in [256]. However, security concerns such as semantic information leakage and data integrity remain open. In addition, the spectral efficiency and semantic-aware RA are discussed in [257], suggesting a unique identity-based approach to enhance network robustness and security; however, the data integrity and tamper-proof are still challenging due to the massive network.

Further, highlighting the IoV in [258] emphasizes the challenge of spectrum scarcity due to the massively connected devices and ever-increasing data traffic tempts the need for an intelligent and decentralized resource management system. As evident, the 6G technology is constrained by the count of base station installation to enhance the communication range. Consequently, it is necessary to facilitate the network with virtual flexibility to overcome physical hindrances posed by the network. Furthermore, [259] focuses on delivering virtual reality over wireless networks, underscoring security challenges raised by data volume, low latency requirements, and limited bandwidth resources. Additionally, scalability, congestion, power consumption, and interference assert critical challenges in massive wireless networks. The research papers discussed above in the context of 6G or large-scale wireless networks lack comprehensive security measures, leaving vulnerabilities unresolved, which include semantic spoofing, eavesdropping, semantic data leakage, and interference. To address these security flaws, the integration of AI and BCT is crucial. AI enables intelligent threat detection and adaptive security mechanisms, while BCT ensures secure transactions and decentralized trust. This integration forms a robust security framework, enhancing the protection of wireless networks and sensitive data.

## VI. OPEN ISSUES AND RESEARCH CHALLENGES

There exist many unresolved problems and issues that future initiatives must address adequately by integrating BCT and ML in the 6G wireless communications networks. These issues mainly include the consequences of the BCT integration in a wireless network, such as bandwidth constraints, network connectivity and coverage, network latency and delay, QoS, dynamic network topology, signal interference and spectrum management, network scalability, privacy and security. However, BCT and ML integration in the 6G wireless network is crucial. Moreover, several other issues also impact the continuous advancements of BCT and ML. To increase the functionality of BCT and ML, this section first covers some of the most significant open problems and research concerns. However, rather than implementing the BCT in wireless communication, there also exist some significant challenges which need to be considered in the next generation of wireless communication. In this context, we illustrate critical challenges and their solutions and study them in a tabulated form, as shown in Table 8. Furthermore, some challenges continue, including current industrial applications, intelligent and competent healthcare, UAV applications, connected autonomous vehicles, extended reality, 3D networking, efficient resource allocation and management, ubiquitous intelligence, mobility management, interference management, and quantum communication. However, these diverse demand contains many challenges, which we have presented in Table 7, where we vastly covered the illustration of various use cases, challenges, and how to mitigate the implementation challenges and explained associated ML/BCT contributions.

## VII. CONCLUSION

This survey primarily focused on integrating AI and BCT in 6G. We highlighted that the diverse nature of networks and distinctive user demands necessitate intelligent network management. Consequently, we explored the utilization of ML in 6G, including use cases and its incorporation in conventional, non-conventional media communication and in the 6G-IoT network. Moreover, due to the infrastructure of wireless communication networks, privacy and security are crucial concerns, leading to the study of BCT in detail. As a result, this review paper examined BCT's features, architecture, and applications in various communication scenarios, such as spectrum refarming, rate splitting multiple access, 6G radar-based communication, reconfigurable intelligent surfaces, visible light communication, integrated sensing, and communication networks. Further, in the subsequent section, we delved into the detailed examination of AI and BCT, their integration, and impact on wireless communication networks. This integrated approach brings unique characteristics to the network, such as intelligence, secure and decentralized data, and model sharing, which are vital for wireless communication and networks. Moreover, we discussed the integrated approach of AI and BCT in novel distinctive 6G communication technologies, which include molecular, holographic, and semantic communication. In the end, we discussed some open issues, research challenges, and their solutions while implementing them in the 6G wireless networks. To summarize, this survey offers researchers a comprehensive understanding of the integrated approach of AI and BCT in a wireless network, resulting in a self-sufficient, reliant, intelligent, decentralized, and secured network.

## REFERENCES

[1] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[2] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[3] J. Huang, C.-X. Wang, L. Bai, J. Sun, Y. Yang, J. Li, O. Tirkkonen, and M.-T. Zhou, "A big data enabled channel model for 5G wireless communication systems," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 211–222, Jun. 2020.

[4] J. Zhu, C. Gong, S. Zhang, M. Zhao, and W. Zhou, ''Foundation study on wireless big data: Concept, mining, learning and practices,'' *China Commun.*, vol. 15, no. 12, pp. 1–15, Dec. 2018.

[5] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, ''Blockchain and machine learning for communications and networking systems,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1392–1431, 2nd Quart., 2020.

[6] J. Jiao, X. Sun, L. Fang, and J. Lyu, ''An overview of wireless communication technology using deep learning,'' *China Commun.*, vol. 18, no. 12, pp. 1–36, Dec. 2021.

[7] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, ''Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions,'' *IEEE Access*, vol. 7, pp. 137184–137206, 2019.

[8] S. Velliangiri, R. Manoharan, S. Ramachandran, and V. Rajasekar, ''Blockchain based privacy preserving framework for emerging 6G wireless communications,'' *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4868–4874, Jul. 2022.

[9] X. Li, P. Russell, C. Mladin, and C. Wang, ''Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities,'' *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 86–95, Apr. 2021.

[10] P. Zhang, L. Li, K. Niu, Y. Li, G. Lu, and Z. Wang, ''An intelligent wireless transmission toward 6G,'' *Intell. Converged Netw.*, vol. 2, no. 3, pp. 244–257, Sep. 2021.

[11] S. J. Pan and Q. Yang, ''A survey on transfer learning,'' *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

[12] B. Mao, F. Tang, Y. Kawamoto, and N. Kato, ''AI models for green communications towards 6G,'' *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 210–247, 1st Quart., 2022.

[13] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, ''Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks,'' *IEEE Access*, vol. 6, pp. 32328–32338, 2018.

[14] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, ''Artificial neural networks-based machine learning for wireless networks: A tutorial,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3039–3071, 4th Quart., 2019.

[15] H. Hojatian, J. Nadal, J.-F. Frigon, and F. Leduc-Primeau, ''Unsupervised deep learning for massive MIMO hybrid beamforming,'' *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7086–7099, Nov. 2021.

[16] S. Gong, D. T. Hoang, D. Niyato, A. El Shafie, A. De Domenico, E. C. Strinati, and J. Hoydis, ''Introduction to the special section on deep reinforcement learning for future wireless communication networks,'' *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 4, pp. 1019–1023, Dec. 2019.

[17] Y. Xiao, J. Liu, J. Wu, and N. Ansari, ''Leveraging deep reinforcement learning for traffic engineering: A survey,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2064–2097, 4th Quart., 2021.

[18] J. Kaur, M. A. Khan, M. Iftikhar, M. Imran, and Q. E. Ul Haq, ''Machine learning techniques for 5G and beyond,'' *IEEE Access*, vol. 9, pp. 23472–23488, 2021.

[19] H. Dahrouj, R. Alghamdi, H. Alwazani, S. Bahanshal, A. A. Ahmad, A. Faisal, R. Shalabi, R. Alhadrami, A. Subasi, M. T. Al-Nory, O. Kittaneh, and J. S. Shamma, ''An overview of machine learning-based techniques for solving optimization problems in communications and signal processing,'' *IEEE Access*, vol. 9, pp. 74908–74938, 2021.

[20] J. Zhu, Q. Li, L. Hu, H. Chen, and N. Ansari, ''Machine learning-based signal detection for PMH signals in load-modulated MIMO systems,'' *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4452–4464, Jul. 2021.

[21] Z.-M. Liu, Z.-T. Huang, and Y.-Y. Zhou, ''An efficient maximum likelihood method for direction-of-arrival estimation via sparse Bayesian learning,'' *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 1–11, Oct. 2012.

[22] X. Ma, J. Zhang, Y. Zhang, and Z. Ma, ''Data scheme-based wireless channel modeling method: Motivation, principle and performance,'' *J. Commun. Inf. Netw.*, vol. 2, no. 3, pp. 41–51, Sep. 2017.

[23] L. Azpilicueta, M. Rawat, K. Rawat, F. M. Ghannouchi, and F. Falcone, ''A ray launching-neural network approach for radio wave propagation analysis in complex indoor environments,'' *IEEE Trans. Antennas Propag.*, vol. 62, no. 5, pp. 2777–2786, May 2014.

[24] Z. Lv, R. Lou, J. Li, A. K. Singh, and H. Song, ''Big data analytics for 6G-enabled massive Internet of Things,'' *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5350–5359, Apr. 2021.

[25] A. Gandomi and M. Haider, ''Beyond the hype: Big data concepts, methods, and analytics,'' *Int. J. Inf. Manage.*, vol. 35, no. 2, pp. 137–144, Apr. 2015.

[26] X. Cheng, L. Fang, X. Hong, and L. Yang, ''Exploiting mobile big data: Sources, features, and applications,'' *IEEE Netw.*, vol. 31, no. 1, pp. 72–79, Jan. 2017.

[27] S. Maranò, W. M. Gifford, H. Wymeersch, and M. Z. Win, ''NLOS identification and mitigation for localization based on UWB experimental data,'' *IEEE J. Sel. Areas Commun.*, vol. 28, no. 7, pp. 1026–1035, Sep. 2010.

[28] T. Van Nguyen, Y. Jeong, H. Shin, and M. Z. Win, ''Machine learning for wideband localization,'' *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1357–1380, Jul. 2015.

[29] H. Zou, B. Huang, X. Lu, H. Jiang, and L. Xie, ''A robust indoor positioning system based on the Procrustes analysis and weighted extreme learning machine,'' *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1252–1266, Feb. 2016.

[30] X. Liang, H. Zhang, T. Lu, and T. A. Gulliver, ''Extreme learning machine for 60 GHz millimetre wave positioning,'' *IET Commun.*, vol. 11, no. 4, pp. 483–489, Mar. 2017.

[31] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, ''Machine learning techniques for cooperative spectrum sensing in cognitive radio networks,'' *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2209–2221, Nov. 2013.

[32] D. He, C. Liu, T. Q. S. Quek, and H. Wang, ''Transmit antenna selection in MIMO wiretap channels: A machine learning approach,'' *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 634–637, Aug. 2018.

[33] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, ''The roadmap to 6G: AI empowered wireless networks,'' *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[34] K. David and H. Berndt, ''6G vision and requirements: Is there any need for beyond 5G?'' *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018.

[35] Y. Xiao, G. Shi, and M. Krunz, ''Towards ubiquitous AI in 6G with federated learning,'' 2020, *arXiv:2004.13563*.

[36] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, ''Federated learning: Strategies for improving communication efficiency,'' 2016, *arXiv:1610.05492*.

[37] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, ''Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory,'' *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[38] Y. Shi, K. Yang, T. Jiang, J. Zhang, and K. B. Letaief, ''Communication-efficient edge AI: Algorithms and systems,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2167–2191, 4th Quart., 2020.

[39] Y. Shen, Y. Shi, J. Zhang, and K. B. Letaief, ''LORM: Learning to optimize for resource management in wireless networks with few training samples,'' *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 665–679, Jan. 2020.

[40] X. Zhang, H. Qi, X. Zhang, and L. Han, ''Spectral efficiency improvement and power control optimization of massive MIMO networks,'' *IEEE Access*, vol. 9, pp. 11523–11532, 2021.

[41] Y. Lu, J. Wang, M. Liu, K. Zhang, G. Gui, T. Ohtsuki, and F. Adachi, ''Semi-supervised machine learning aided anomaly detection method in cellular networks,'' *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8459–8467, Aug. 2020.

[42] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, ''Machine learning for anomaly detection: A systematic review,'' *IEEE Access*, vol. 9, pp. 78658–78700, 2021.

[43] M. F. Kucuk and I. Uysal, ''Anomaly detection in self-organizing networks: Conventional versus contemporary machine learning,'' *IEEE Access*, vol. 10, pp. 61744–61752, 2022.

[44] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, ''Enhanced network anomaly detection based on deep neural networks,'' *IEEE Access*, vol. 6, pp. 48231–48246, 2018.

[45] H. W. Oleiwi, D. N. Mhawi, and H. Al-Raweshidy, ''MLTs-ADCNs: Machine learning techniques for anomaly detection in communication networks,'' *IEEE Access*, vol. 10, pp. 91006–91017, 2022.

[46] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, ''Machine learning in network anomaly detection: A survey,'' *IEEE Access*, vol. 9, pp. 152379–152396, 2021.

[47] J. Kwon, D. Jung, and H. Park, ''Traffic data classification using machine learning algorithms in SDN networks,'' in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 1031–1033.

[48] S. M. Rachmawati, D.-S. Kim, and J.-M. Lee, ''Machine learning algorithm in network traffic classification,'' in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2021, pp. 1010–1013.

[49] A. R. Deshmukh and S. S. Dorle, ''Bio-inspired optimization algorithms for improvement of vehicle routing problems,'' in *Proc. 7th Int. Conf. Emerg. Trends Eng. Technol. (ICETET)*, Nov. 2015, pp. 14–18.

[50] S. Shakya and S. R. Pokhrel, ''Global optimization of field based routing in wireless mesh network (GOFBR-WMN),'' in *Proc. 3rd Asian Himalayas Int. Conf. Internet*, Nov. 2012, pp. 1–5.

[51] A. V. da Silva and G. S. Pavani, ''Tackling multiple Byzantine failures in optical networks routed by means of ant colony optimization,'' in *Proc. 21st Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2019, pp. 1–4.

[52] S. Xu, X. Wang, G. Yang, J. Ren, and S. Wang, ''Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint,'' *J. Commun. Netw.*, vol. 22, no. 2, pp. 145–158, Apr. 2020.

[53] S. R. Pokhrel and S. Shakya, ''Enhanced optimization of field based routing for macro mobility in IEEE 802.11s mesh,'' in *Proc. 10th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, Jul. 2013, pp. 1–5.

[54] T. L. Lin, Y. S. Chen, and H. Y. Chang, ''Performance evaluations of an ant colony optimization routing algorithm for wireless sensor networks,'' in *Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2014, pp. 690–693.

[55] R. Guerra-Gómez, S. R. Boqué, M. García-Lozano, and J. O. Bonafé, ''Machine-learning based traffic forecasting for resource management in C-RAN,'' in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 200–204.

[56] S. Goodarzy, M. Nazari, R. Han, E. Keller, and E. Rozner, ''Resource management in cloud computing using machine learning: A survey,'' in *Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2020, pp. 811–816.

[57] A. Alnoman, ''Machine learning-based task clustering for enhanced virtual machine utilization in edge computing,'' in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Aug. 2020, pp. 1–4.

[58] R. Guerra-Gómez, S. Ruiz-Boqué, M. García-Lozano, and J. O. Bonafe, ''Machine learning adaptive computational capacity prediction for dynamic resource management in C-RAN,'' *IEEE Access*, vol. 8, pp. 89130–89142, 2020.

[59] W. Guo, W. Tian, Y. Ye, L. Xu, and K. Wu, ''Cloud resource scheduling with deep reinforcement learning and imitation learning,'' *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3576–3586, Mar. 2021.

[60] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, ''When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network,'' *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2238–2251, Feb. 2021.

[61] Y. He, ''Research on the key technology of network security based on machine learning,'' in *Proc. 6th Int. Conf. Intell. Comput. Signal Process. (ICSP)*, Apr. 2021, pp. 972–975.

[62] T. P. Anithaashri and G. Ravichandran, ''Security enhancement for the network amalgamation using machine learning algorithm,'' in *Proc. Int. Conf. Smart Electron. Commun. (ICOSEC)*, Sep. 2020, pp. 411–416.

[63] W. Yang, X. C. Yun, and L. J. Zhang, ''Using incremental learning method for adaptive network intrusion detection,'' in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 7, Nov. 2005, pp. 3932–3936.

[64] C.-C. Li, A.-L. Guo, and D. Li, ''Application research of support vector machine in network security risk evaluation,'' in *Proc. Int. Symp. Intell. Inf. Technol. Appl. Workshops*, Dec. 2008, pp. 40–43.

[65] W. Zhong, N. Yu, and C. Ai, ''Applying big data based deep learning system to intrusion detection,'' *Big Data Mining Anal.*, vol. 3, no. 3, pp. 181–195, Sep. 2020.

[66] G. Pu, L. Wang, J. Shen, and F. Dong, ''A hybrid unsupervised clustering-based anomaly detection method,'' *Tsinghua Sci. Technol.*, vol. 26, no. 2, pp. 146–153, Apr. 2021.

[67] S. Otoum, B. Kantarci, and H. T. Mouftah, ''On the feasibility of deep learning in sensor network intrusion detection,'' *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 68–71, Jun. 2019.

[68] G. De Carvalho Bertoli, L. A. P. Júnior, O. Saotome, A. L. Dos Santos, F. A. N. Verri, C. A. C. Marcondes, S. Barbieri, M. S. Rodrigues, and J. M. P. De Oliveira, ''An end-to-end framework for machine learning-based network intrusion detection system,'' *IEEE Access*, vol. 9, pp. 106790–106805, 2021.

[69] J. Lansky, S. Ali, M. Mohammadi, M. K. Majeed, S. H. T. Karim, S. Rashidi, M. Hosseinzadeh, and A. M. Rahmani, ''Deep learning-based intrusion detection systems: A systematic review,'' *IEEE Access*, vol. 9, pp. 101574–101599, 2021.

[70] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, ''Blockchain for 5G and beyond networks: A state of the art survey,'' *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[71] S. Wijethilaka and M. Liyanage, ''Survey on network slicing for Internet of Things realization in 5G networks,'' *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[72] V. A. Cunha et al., ''5Growth: Secure and reliable network slicing for verticals,'' in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jul. 2021, pp. 347–352.

[73] P. Du, A. Nakao, L. Zhong, and R. Onishi, ''Intelligent network slicing with edge computing for Internet of Vehicles,'' *IEEE Access*, vol. 9, pp. 128106–128116, 2021.

[74] A. Ksentini, M. Jebalia, and S. Tabbane, ''Fog-enabled industrial IoT network slicing model based on ML-enabled multi-objective optimization,'' in *Proc. IEEE 29th Int. Conf. Enabling Technol., Infrastruct. Collaborative Enterprises (WETICE)*, Sep. 2020, pp. 177–180.

[75] J. Mei, X. Wang, and K. Zheng, ''Intelligent network slicing for V2X services toward 5G,'' *IEEE Netw.*, vol. 33, no. 6, pp. 196–204, Nov. 2019.

[76] Y. Li and M. Chen, ''Software-defined network function virtualization: A survey,'' *IEEE Access*, vol. 3, pp. 2542–2553, 2015.

[77] G. Kibalya, J. Serrat, J.-L. Gorricho, R. Pasquini, H. Yao, and P. Zhang, ''A reinforcement learning based approach for 5G network slicing across multiple domains,'' in *Proc. 15th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2019, pp. 1–5.

[78] H. A. Shah and L. Zhao, ''Multiagent deep-reinforcement-learning-based virtual resource allocation through network function virtualization in Internet of Things,'' *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3410–3421, Mar. 2021.

[79] S. Moazzeni, P. Jaisudthi, A. Bravalheri, N. Uniyal, X. Vasilakos, R. Nejabati, and D. Simeonidou, ''A novel autonomous profiling method for the next-generation NFV orchestrators,'' *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 1, pp. 642–655, Mar. 2021.

[80] Y. Zhao, Y. Li, X. Zhang, G. Geng, W. Zhang, and Y. Sun, ''A survey of networking applications applying the software defined networking concept based on machine learning,'' *IEEE Access*, vol. 7, pp. 95397–95417, 2019.

[81] P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares, and H. S. Mamede, ''Machine learning in software defined networks: Data collection and traffic classification,'' in *Proc. IEEE 24th Int. Conf. Netw. Protocols (ICNP)*, Nov. 2016, pp. 1–5.

[82] W. Kellerer, P. Kalmbach, A. Blenk, A. Basta, M. Reisslein, and S. Schmid, ''Adaptable and data-driven softwarized networks: Review, opportunities, and challenges,'' *Proc. IEEE*, vol. 107, no. 4, pp. 711–731, Apr. 2019.

[83] R. Etengu, S. C. Tan, L. C. Kwang, F. M. Abbou, and T. C. Chuah, ''AI-assisted framework for green-routing and load balancing in hybrid software-defined networking: Proposal, challenges and future perspective,'' *IEEE Access*, vol. 8, pp. 166384–166441, 2020.

[84] M. Abderrahim, A. Ben Letaifa, A. Haji, and S. Tabbane, ''How to use MEC and ML to improve resources allocation in SDN networks ?'' in *Proc. 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, May 2018, pp. 442–447.

[85] A. R. Mohammed, S. A. Mohammed, and S. Shirmohammadi, ''Machine learning and deep learning based traffic classification and prediction in software defined networking,'' in *Proc. IEEE Int. Symp. Meas. Netw. (M&N)*, Jul. 2019, pp. 1–6.

[86] E. H. Bouzidi, A. Outtagarts, and R. Langar, ''Deep reinforcement learning application for network latency management in software defined networks,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[87] S. Anbalagan, A. K. Bashir, G. Raja, P. Dhanasekaran, G. Vijayaraghavan, U. Tariq, and M. Guizani, ''Machine-learning-based efficient and secure RSU placement mechanism for software-defined-IoV,'' *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13950–13957, Sep. 2021.

[88] J. Aiken and S. Scott-Hayward, ''Investigating adversarial attacks against network intrusion detection systems in SDNs,'' in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2019, pp. 1–7.

[89] A. Lee-Leon, C. Yuen, and D. Herremans, "Underwater acoustic communication receiver using deep belief network," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3698–3708, Jun. 2021.

[90] M. S. M. Alamgir, M. N. Sultana, and K. Chang, "Link adaptation on an underwater communications network using machine learning algorithms: Boosted regression tree approach," *IEEE Access*, vol. 8, pp. 73957–73971, 2020.

[91] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of Underwater Things and big marine data analytics—A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 904–956, 2nd Quart., 2021.

[92] B. Zhang, H. Wang, L. Zheng, J. Wu, and Z. Zhuang, "Joint synchronization and localization for underwater sensor networks considering stratification effect," *IEEE Access*, vol. 5, pp. 26932–26943, 2017.

[93] V.-S. Doan, T. Huynh-The, and D.-S. Kim, "Underwater acoustic target classification based on dense convolutional neural network," *IEEE Geosci. Remote Sens. Lett.*, vol. 19, pp. 1–5, 2022.

[94] L. Alsalman and E. Alotaibi, "A balanced routing protocol based on machine learning for underwater sensor networks," *IEEE Access*, vol. 9, pp. 152082–152097, 2021.

[95] W. Wang, P. Wang, Y. Song, W. Pang, S. Li, and Y. Nie, "Machine learning framework combining radial phase grating and channel information-assisted underwater wireless optical OAM communications," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3614–3618, Nov. 2021.

[96] J. Huang, G. Li, J. Tian, and S. Li, "Accurate interpretation of the online learning model for 6G-enabled Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15228–15239, Oct. 2021.

[97] O. A. López, O. M. Rosabal, D. Ruiz-Guirola, P. Raghuwanshi, K. Mikhaylov, L. Lovén, and S. Iyer, "Energy-sustainable IoT connectivity: Vision, technological enablers, challenges, and future directions," 2023, *arXiv:2306.02444*.

[98] P. Chakraborty, J. Cruz, and S. Bhunia, "MAGIC: Machine-learning-guided image compression for vision applications in Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7303–7315, May 2021.

[99] J. Yun and J. Woo, "A comparative analysis of deep learning and machine learning on detecting movement directions using PIR sensors," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2855–2868, Apr. 2020.

[100] X. Liu, W. Yu, F. Liang, D. Griffith, and N. Golmie, "Toward deep transfer learning in industrial Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12163–12175, Aug. 2021.

[101] F. Samie, L. Bauer, and J. Henkel, "From cloud down to things: An overview of machine learning in Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4921–4934, Jun. 2019.

[102] H. Qin, S. Zawad, Y. Zhou, S. Padhi, L. Yang, and F. Yan, "Reinforcement-learning-empowered MLaaS scheduling for serving intelligent Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6325–6337, Jul. 2020.

[103] C. Di, B. Zhang, Q. Liang, S. Li, and Y. Guo, "Learning automata-based access class barring scheme for massive random access in machine-to-machine communications," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6007–6017, Aug. 2019.

[104] F. E. Alzhrani, K. A. Saeedi, and L. Zhao, "A taxonomy for characterizing blockchain systems," *IEEE Access*, vol. 10, pp. 110568–110589, 2022.

[105] S. Cao, L. W. Cong, M. Han, Q. Hou, and B. Yang, "Blockchain architecture for auditing automation and trust building in public markets," *Computer*, vol. 53, no. 7, pp. 20–28, Jul. 2020.

[106] *Public vs Consortium vs Federated vs Private Blockchain*. Accessed: Sep. 2022. [Online]. Available: https://originstamp.com/blog/public-consortium-private-blockchain/

[107] P. Paul, P. S. Aithal, and S. Ricardo, "Blockchain technology and its types—A short review," *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, pp. 189–200, Dec. 2021.

[108] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[109] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018.

[110] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020.

[111] D. Geroni. *Blockchain Nodes Details*. Accessed: Jul. 2022. [Online]. Available: https://101blockchains.com/blockchain-nodes/

[112] D. Gruber, W. Li, and G. Karame, "Unifying lightweight blockchain client implementations," in *Proc. Workshop Decentralized IoT Secur. Standards (DISS)*, Feb. 2018, pp. 1–7, doi: 10.14722/diss.2018.23010.

[113] *What is a Blockchain Node and How is it Used in Cryptocurrency*. Accessed: Jul. 2022. [Online]. Available: https://shorturl.at/hlDE1

[114] *Blockchain Architecture*. Accessed: Jul. 2022. [Online]. Available: https://www.pluralsight.com/guides/Blockchain-architecture

[115] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[116] *Solidity*. Accessed: Jul. 2022. [Online]. Available: https://solidity.readthedocs.io/en/develop/

[117] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[118] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 4, no. 1, pp. 1–14, Apr. 2017.

[119] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[120] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, Jul. 2017, pp. 357–388.

[121] P. Zhang, D. C. Schmidt, J. White, and A. Dubey, "Consensus mechanisms and information security technologies," *Adv. Comput.*, vol. 115, pp. 181–209, Jun. 2019.

[122] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[123] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[124] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 353–385, 1st Quart., 2023.

[125] P. Yang, L. Kong, and G. Chen, "Spectrum sharing for 5G/6G URLLC: Research frontiers and standards," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 120–125, Jun. 2021.

[126] S. Shao, W. Gong, H. Yang, S. Guo, L. Chen, and A. Xiong, "Data trusted sharing delivery: A blockchain-assisted software-defined content delivery network," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 11949–11959, Jul. 2021.

[127] S. T. Muntaha, P. I. Lazaridis, M. Hafeez, Q. Z. Ahmed, F. A. Khan, and Z. D. Zaharis, "Blockchain for dynamic spectrum access and network slicing: A review," *IEEE Access*, vol. 11, pp. 17922–17944, 2023, doi: 10.1109/ACCESS.2023.3243985.

[128] A. H. Khan, N. Ul Hassan, C. Yuen, J. Zhao, D. Niyato, Y. Zhang, and H. V. Poor, "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.

[129] Y. Xu, G. Gui, H. Gacanin, and F. Adachi, "A survey on resource allocation for 5G heterogeneous networks: Current research, future trends, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 668–695, 2nd Quart., 2021.

[130] D. Xenakis, A. Tsiota, C.-T. Koulis, C. Xenakis, and N. Passas, "Contract-less mobile data access beyond 5G: Fully-decentralized, high-throughput and anonymous asset trading over the blockchain," *IEEE Access*, vol. 9, pp. 73963–74016, 2021.

[131] Y. Liang, C. Lu, Y. Zhao, and C. Sun, "Interference-based consensus and transaction validation mechanisms for blockchain-based spectrum management," *IEEE Access*, vol. 9, pp. 90757–90766, 2021.

[132] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8012–8023, Jun. 2022.

[133] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 1180–1184.

[134] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," *Softw., Pract. Exper.*, vol. 51, no. 10, pp. 2051–2064, Oct. 2021.

[135] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[136] M. Cinque, C. Esposito, and S. Russo, "Trust management in fog/edge computing by means of blockchain technologies," in *Proc. IEEE Green Comput. Commun. (GreenCom)*, Jul. 2018, pp. 1433–1439.

[137] H. Chai, S. Leng, K. Zhang, and S. Mao, "Proof-of-reputation based-consortium blockchain for trust resource sharing in Internet of Vehicles," *IEEE Access*, vol. 7, pp. 175744–175757, 2019.

[138] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2013–2021, Mar. 2020.

[139] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[140] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[141] S. Han, Y.-C. Liang, and B.-H. Soong, "Spectrum refarming: A new paradigm of spectrum sharing for cellular networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1895–1906, May 2015.

[142] S. Han, Y.-C. Liang, B.-H. Soong, and S. Li, "Dynamic broadband spectrum refarming for OFDMA cellular systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6203–6214, Sep. 2016.

[143] Y. Mao, O. Dizdar, B. Clerckx, R. Schober, P. Popovski, and H. V. Poor, "Rate-splitting multiple access: Fundamentals, survey, and future research trends," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2073–2126, 4th Quart., 2022.

[144] N. S. Alghamdi and M. A. Khan. *Energy-Efficient and Blockchain-Enabled Model for IoT*. Accessed: Feb. 2023. [Online]. Available: https://www.techscience.com/cmc/v66n3/41089

[145] G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi, and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustain. Comput., Informat. Syst.*, vol. 28, Dec. 2020, Art. no. 100464.

[146] O. L. A. López, H. Alves, R. D. Souza, S. Montejo-Sánchez, E. M. G. Fernández, and M. Latva-Aho, "Massive wireless energy transfer: Enabling sustainable IoT toward 6G era," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8816–8835, Jun. 2021.

[147] S. Rani, H. Babbar, S. H. A. Shah, and A. Singh, "Improvement of energy conservation using blockchain-enabled cognitive wireless networks for smart cities," *Sci. Rep.*, vol. 12, no. 1, pp. 13013–13023, Jul. 2022.

[148] Z. Feng, Z. Fang, Z. Wei, X. Chen, Z. Quan, and D. Ji, "Joint radar and communication: A survey," *China Commun.*, vol. 17, no. 1, pp. 1–27, Jan. 2020.

[149] A. Gameiro, D. Castanheira, J. Sanson, and P. P. Monteiro, "Research challenges, trends and applications for future joint radar communications systems," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 81–96, Mar. 2018.

[150] S. Quan, W. Qian, J. Guq, and V. Zhang, "Radar-communication integration: An overview," in *Proc. 7th IEEE/Int. Conf. Adv. Infocomm Technol.*, Nov. 2014, pp. 98–103.

[151] B. Gupta, D. Valente, E. Cianca, and R. Prasad, "FM-UWB for radar and communications in medical applications," in *Proc. 1st Int. Symp. Appl. Sci. Biomed. Commun. Technol.*, Oct. 2008, pp. 1–5.

[152] C. G. Bilich, "Bio-medical sensing using ultra wideband communications and radar technology: A feasibility study," in *Proc. Pervasive Health Conf. Workshops*, Nov. 2006, pp. 1–9.

[153] J. A. Zhang, F. Liu, C. Masouros, R. W. Heath, Z. Feng, L. Zheng, and A. Petropulu, "An overview of signal processing techniques for joint communication and radar sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 15, no. 6, pp. 1295–1315, Nov. 2021.

[154] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[155] S. Jia, X. Yuan, and Y.-C. Liang, "Reconfigurable intelligent surfaces for energy efficiency in D2D communication network," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 683–687, Mar. 2021.

[156] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021.

[157] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, 3rd Quart., 2020.

[158] S. Wang, K. Zhang, B. Zhu, W. Wang, and Z. Zhang, "Visible light communications for unmanned aerial vehicle: Channel modeling and experimental validation," *IEEE Commun. Lett.*, vol. 27, no. 6, pp. 1530–1534, Jun. 2023.

[159] X. Lin and L. Zhang, "Intelligent and practical deep learning aided positioning design for visible light communication receivers," *IEEE Commun. Lett.*, vol. 24, no. 3, pp. 577–580, Mar. 2020.

[160] N. Su, E. Panayirci, M. Koca, A. Yesilkaya, H. V. Poor, and H. Haas, "Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2585–2598, Apr. 2021.

[161] M. Jain, N. Sharma, A. Gupta, D. Rawal, and P. Garg, "Performance analysis of NOMA assisted underwater visible light communication system," *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1291–1294, Aug. 2020.

[162] M. Katz and I. Ahmed, "Opportunities and challenges for visible light communications in 6G," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[163] L. Zhao, D. Wu, L. Zhou, and Y. Qian, "Radio resource allocation for integrated sensing, communication, and computation networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 10, pp. 8675–8687, Oct. 2022.

[164] X. Fang, W. Feng, Y. Chen, N. Ge, and Y. Zhang, "Joint communication and sensing toward 6G: Models and potential of using MIMO," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4093–4116, Mar. 2023.

[165] L. You, X. Qiang, C. G. Tsinos, F. Liu, W. Wang, X. Gao, and B. Ottersten, "Beam squint-aware integrated sensing and communications for hybrid massive MIMO LEO satellite systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 10, pp. 2994–3009, Oct. 2022.

[166] P. Liu, G. Zhu, W. Jiang, W. Luo, J. Xu, and S. Cui, "Vertical federated edge learning with distributed integrated sensing and communication," *IEEE Commun. Lett.*, vol. 26, no. 9, pp. 2091–2095, Sep. 2022.

[167] X. Cheng, D. Duan, S. Gao, and L. Yang, "Integrated sensing and communications (ISAC) for vehicular communication networks (VCN)," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23441–23451, Dec. 2022.

[168] Z. Du, F. Liu, W. Yuan, C. Masouros, Z. Zhang, S. Xia, and G. Caire, "Integrated sensing and communications for V2I networks: Dynamic predictive beamforming for extended vehicle targets," *IEEE Trans. Wireless Commun.*, vol. 22, no. 6, pp. 3612–3627, Jun. 2022.

[169] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1212–1239, 2nd Quart., 2022.

[170] W. Zhou, R. Zhang, G. Chen, and W. Wu, "Integrated sensing and communication waveform design: A survey," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 1930–1949, 2022.

[171] T. Wild, V. Braun, and H. Viswanathan, "Joint design of communication and sensing for beyond 5G and 6G systems," *IEEE Access*, vol. 9, pp. 30845–30857, 2021.

[172] X. Li, Y. Guo, L. Yan, and X. Xu, "Energy-aware blockchain for multiple autonomous underwater vehicles cooperative operation," in *Proc. 40th Chin. Control Conf. (CCC)*, Jul. 2021, pp. 3005–3010.

[173] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31–37, Nov. 2020.

[174] M. Li, F. R. Yu, P. Si, W. Wu, and Y. Zhang, "Resource optimization for delay-tolerant data in blockchain-enabled IoT with edge computing: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9399–9412, Oct. 2020.

[175] Z. Shahbazi and Y.-C. Byun, "Blockchain-based event detection and trust verification using natural language processing and machine learning," *IEEE Access*, vol. 10, pp. 5790–5800, 2022.

[176] R. Michalski, D. Dziubałtowska, and P. Macek, "Revealing the character of nodes in a blockchain with supervised learning," *IEEE Access*, vol. 8, pp. 109639–109647, 2020.

[177] F. Zerka, V. Urovi, A. Vaidyanathan, S. Barakat, R. T. H. Leijenaar, S. Walsh, H. Gabrani-Juma, B. Miraglio, H. C. Woodruff, M. Dumontier, and P. Lambin, "Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM)," *IEEE Access*, vol. 8, pp. 183939–183951, 2020.

[178] C. Qiu, X. Ren, Y. Cao, and T. Mai, "Deep reinforcement learning empowered adaptivity for future blockchain networks," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 99–105, 2021.

[179] S. Maaroufi and S. Pierre, "BCOOL: A novel blockchain congestion control architecture using dynamic service function chaining and machine learning for next generation vehicular networks," *IEEE Access*, vol. 9, pp. 53096–53122, 2021.

[180] G. Hua, L. Zhu, J. Wu, C. Shen, L. Zhou, and Q. Lin, "Blockchain-based federated learning for intelligent control in heavy haul railway," *IEEE Access*, vol. 8, pp. 176830–176839, 2020.

[181] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[182] A. S. Khan, G. Chen, Y. Rahulamathavan, G. Zheng, B. Assadhan, and S. Lambotharan, "Trusted UAV network coverage using blockchain, machine learning, and auction mechanisms," *IEEE Access*, vol. 8, pp. 118219–118234, 2020.

[183] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[184] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 5, pp. 2438–2455, Sep./Oct. 2021.

[185] A. Asheralieva and D. Niyato, "Bayesian reinforcement learning and Bayesian deep learning for blockchains with mobile edge computing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 1, pp. 319–335, Mar. 2021.

[186] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021.

[187] D. Said, "A decentralized electricity trading framework (DETF) for connected EVs: A blockchain and machine learning for profit margin optimization," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6594–6602, Oct. 2021.

[188] M. Shen, H. Wang, B. Zhang, L. Zhu, K. Xu, Q. Li, and X. Du, "Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2265–2275, Feb. 2021.

[189] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, Jul. 2021.

[190] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.

[191] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.

[192] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in Industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5926–5937, Apr. 2021.

[193] S. Fan, H. Zhang, Y. Zeng, and W. Cai, "Hybrid blockchain-based resource trading system for federated learning in edge computing," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2252–2264, Feb. 2021.

[194] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021.

[195] M. Shayan, C. Fung, C. J. M. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1513–1525, Jul. 2021.

[196] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure Internet of Drones environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4404–4413, Jul. 2021.

[197] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102331–102344, 2019.

[198] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[199] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9098–9111, Oct. 2019.

[200] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in Internet of Electric Vehicles," *IEEE Access*, vol. 9, pp. 7000–7020, 2021.

[201] W. Xiong and L. Xiong, "Data trading certification based on consortium blockchain and smart contracts," *IEEE Access*, vol. 9, pp. 3482–3496, 2021.

[202] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in IoT networks," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6487–6497, Apr. 2021.

[203] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, pp. 36868–36878, 2021.

[204] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent advances in smart contracts: A technical overview and state of the art," *IEEE Access*, vol. 8, pp. 117782–117801, 2020.

[205] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of IoT and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021.

[206] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Syst. J.*, vol. 15, no. 1, pp. 85–94, Mar. 2021.

[207] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 97–101.

[208] P. Gururaj, "Identity management using permissioned blockchain," in *Proc. Int. Conf. Mainstreaming Block Chain Implement. (ICOMBI)*, Feb. 2020, pp. 1–3.

[209] R. T. Moreno, J. García-Rodríguez, J. B. Bernabé, and A. Skarmeta, "A trusted approach for decentralised and privacy-preserving identity management," *IEEE Access*, vol. 9, pp. 105788–105804, 2021.

[210] Y. Guo, Z. Qi, X. Xian, H. Wu, Z. Yang, J. Zhang, and L. Wenyin, "WISChain: An online insurance system based on blockchain and DengLu1 for web identity security," in *Proc. 1st IEEE Int. Conf. Hot Information-Centric Netw. (HotICN)*, Aug. 2018, pp. 242–243.

[211] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[212] N. Fabiano, "Internet of Things and blockchain: Legal issues and privacy. The challenge for a privacy standard," in *Proc. IEEE Green Comput. Commun. (GreenCom)*, Jun. 2017, pp. 727–734.

[213] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.

[214] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[215] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 20–29, Jul. 2018.

[216] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[217] L. Lyu, J. Yu, K. Nandakumar, Y. Li, X. Ma, J. Jin, H. Yu, and K. Siong Ng, "Towards fair and privacy-preserving federated deep models," 2019, *arXiv:1906.01167*.

[218] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Apr. 2019, pp. 119–124.

[219] C. Chenli, B. Li, Y. Shi, and T. Jung, "Energy-recycling blockchain with proof-of-deep-learning," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 19–23.

[220] Y. Zhang, H.-M. Wang, T.-X. Zheng, and Q. Yang, "Energy-efficient transmission design in non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2852–2857, Mar. 2017.

[221] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 625–638, Jul. 2020.

[222] H. M. Abdullah, A. Gastli, and L. Ben-Brahim, "Reinforcement learning based EV charging management systems—A review," *IEEE Access*, vol. 9, pp. 41506–41531, 2021.

[223] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "SmartBlock-SDN: An optimized blockchain-SDN framework for resource management in IoT," *IEEE Access*, vol. 9, pp. 28361–28376, 2021.

[224] J. Chen, K. Duan, R. Zhang, L. Zeng, and W. Wang, "An AI based super nodes selection algorithm in blockchain networks," 2018, *arXiv:1808.00216*.

[225] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[226] T. Wang, S. C. Liew, and S. Zhang, "When blockchain meets AI: Optimal mining strategy achieved by machine learning," 2019, *arXiv:1911.12942*.

[227] T. Wang, X. Bai, H. Wang, S. C. Liew, and S. Zhang, "Game-theoretical analysis of mining strategy for Bitcoin-NG blockchain protocol," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2708–2719, Jun. 2021.

[228] P. Haridas, G. Chennupati, N. Santhi, P. Romero, and S. Eidenbenz, "Code characterization with graph convolutions and capsule networks," *IEEE Access*, vol. 8, pp. 136307–136315, 2020.

[229] *What are the Various Blockchain Scalability Solutions*. Accessed: Sep. 2022. [Online]. Available: https://www.leewayhertz.com/blockchain-scalability-solutions/

[230] D. Cheng, S. Li, H. Zhang, F. Xia, and Y. Zhang, "Why dataset properties bound the scalability of parallel machine learning training algorithms," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 7, pp. 1702–1712, Jul. 2021.

[231] H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, pp. 136481–136495, 2019.

[232] T. Nakano, Y. Okaie, S. Kobayashi, T. Hara, Y. Hiraoka, and T. Haraguchi, "Methods and applications of mobile molecular communication," *Proc. IEEE*, vol. 107, no. 7, pp. 1442–1456, Jul. 2019.

[233] F. H. Juwono, R. Reine, W. K. Wong, Z. A. Sim, and L. Gopal, "Envisioning 6G molecular communication for IoBNT diagnostic systems," in *Proc. Int. Conf. Green Energy, Comput. Sustain. Technol. (GECOST)*, Jul. 2021, pp. 1–5.

[234] N. Varshney, A. Patel, Y. Deng, W. Haselmayr, P. K. Varshney, and A. Nallanathan, "Abnormality detection inside blood vessels with mobile nanomachines," *IEEE Trans. Mol., Biol. Multi-Scale Commun.*, vol. 4, no. 3, pp. 189–194, Sep. 2018.

[235] R. Mosayebi, A. Ahmadzadeh, W. Wicke, V. Jamali, R. Schober, and M. Nasiri-Kenari, "Early cancer detection in blood vessels using mobile nanosensors," *IEEE Trans. Nanobiosci.*, vol. 18, no. 2, pp. 103–116, Apr. 2019.

[236] H. Werner, S. Andreas, F. Georg, A. Christoph, B. Holger, H. A. Peter, D. Falko, and S. Robert, "Integration of molecular communications into future generation wireless networks," in *Proc. 1st IEEE 6G Wireless Summit*, Levi, Finland, Jul. 2019, pp. 1–2.

[237] A. Ahmadzadeh, A. Noel, and R. Schober, "Analysis and design of multi-hop diffusion-based molecular communication networks," *IEEE Trans. Mol., Biol. Multi-Scale Commun.*, vol. 1, no. 2, pp. 144–157, Jun. 2015.

[238] Z. Ma, M. Liu, H. Yan, and L. Lin, "Electric field assisted molecular communication for high data rate transmission," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1571–1574, Dec. 2019.

[239] E. Dinc and O. B. Akan, "Theoretical limits on multiuser molecular communication in Internet of Nano-Bio Things," *IEEE Trans. Nanobiosci.*, vol. 16, no. 4, pp. 266–270, Jun. 2017.

[240] N. V. Sabu, A. K. Gupta, N. Varshney, and A. Jindal, "Channel characterization and performance of a 3-D molecular communication system with multiple fully-absorbing receivers," *IEEE Trans. Commun.*, vol. 71, no. 2, pp. 714–727, Feb. 2023.

[241] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. U. Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication in context of molecular communication and terahertz communication for body-centric nanonetworks," *IEEE Trans. Mol., Biol. Multi-Scale Commun.*, vol. 6, no. 2, pp. 107–133, Nov. 2020.

[242] Y. Lu, R. Ni, and Q. Zhu, "Wireless communication in nanonetworks: Current status, prospect and challenges," *IEEE Trans. Mol., Biol. Multi-Scale Commun.*, vol. 6, no. 2, pp. 71–80, Nov. 2020.

[243] A. Etemadi, M. Farahnak-Ghazani, H. Arjmandi, M. Mirmohseni, and M. Nasiri-Kenari, "Abnormality detection and localization schemes using molecular communication systems: A survey," *IEEE Access*, vol. 11, pp. 1761–1792, 2023.

[244] W. Guo, M. Abbaszadeh, L. Lin, J. Charmet, P. Thomas, Z. Wei, B. Li, and C. Zhao, "Molecular physical layer for 6G in wave-denied environments," *IEEE Commun. Mag.*, vol. 59, no. 5, pp. 33–39, May 2021.

[245] R. Deng, B. Di, H. Zhang, D. Niyato, Z. Han, H. V. Poor, and L. Song, "Reconfigurable holographic surfaces for future wireless communications," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 126–131, Dec. 2021.

[246] R. Deng, B. Di, H. Zhang, and L. Song, "HDMA: Holographic-pattern division multiple access," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1317–1332, Apr. 2022.

[247] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. D. Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, Oct. 2020.

[248] L. Wei, C. Huang, G. C. Alexandropoulos, W. E. I. Sha, Z. Zhang, M. Debbah, and C. Yuen, "Multi-user wireless communications with holographic MIMO surfaces: A convenient channel model and spectral efficiency analysis," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2022, pp. 488–493.

[249] N. Petkov, N. Christoff, A. Manolova, K. Tonchev, and V. Poulkov, "Comparative study of latent-sensitive processing of heterogeneous data in an experimental platform for 3D video holographic communication," in *Proc. Global Conf. Wireless Opt. Technol. (GCWOT)*, Feb. 2022, pp. 1–6.

[250] I. F. Akyildiz, "Metaverse: Challenges for extended reality and holographic-type communication in the next decade," in *Proc. ITU Kaleidoscope-Extended Reality Boost Quality Exp. Interoperability*, Dec. 2022, pp. 1–2.

[251] A. Elzanaty, A. Guerra, F. Guidi, D. Dardari, and M.-S. Alouini, "Toward 6G holographic localization: Enabling technologies and perspectives," *IEEE Internet Things Mag.*, vol. 6, no. 3, pp. 138–143, Sep. 2023.

[252] M. U. Lokumarambage, V. S. S. Gowrisetty, H. Rezaei, T. Sivalingam, N. Rajatheva, and A. Fernando, "Wireless end-to-end image transmission system using semantic communications," *IEEE Access*, vol. 11, pp. 37149–37163, 2023.

[253] W. Yang, H. Du, Z. Q. Liew, W. Y. B. Lim, Z. Xiong, D. Niyato, X. Chi, X. Shen, and C. Miao, "Semantic communications for future Internet: Fundamentals, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 213–250, 1st Quart., 2023.

[254] H. Hu, X. Zhu, F. Zhou, W. Wu, R. Q. Hu, and H. Zhu, "One-to-many semantic communication systems: Design, implementation, performance evaluation," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2959–2963, Dec. 2022.

[255] S. Wang, J. Dai, Z. Liang, K. Niu, Z. Si, C. Dong, X. Qin, and P. Zhang, "Wireless deep video semantic transmission," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 1, pp. 214–229, Jan. 2023.

[256] Z. Yang, M. Chen, Z. Zhang, and C. Huang, "Energy efficient semantic communication over wireless networks with rate splitting," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 5, pp. 1484–1495, May 2023.

[257] L. Yan, Z. Qin, R. Zhang, Y. Li, and G. Y. Li, "Resource allocation for text semantic communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1394–1398, Jul. 2022.

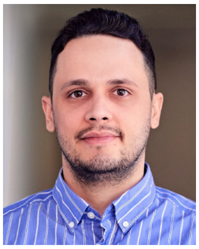
[258] W. Xu, Y. Zhang, F. Wang, Z. Qin, C. Liu, and P. Zhang, "Semantic communication for the Internet of Vehicles: A multiuser cooperative approach," *IEEE Veh. Technol. Mag.*, vol. 18, no. 1, pp. 100–109, Mar. 2023.

[259] L. Xia, Y. Sun, C. Liang, D. Feng, R. Cheng, Y. Yang, and M. A. Imran, "WiserVR: Semantic communication enabled wireless virtual reality delivery," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 32–39, Apr. 2023.

**VIVEK PATHAK** received the B.Tech. degree from Uttar Pradesh Technical University, Lucknow, India, and the M.Tech. degree from the Department of Electronics and Communication Engineering, Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India. He is currently pursuing the Ph.D. degree with the Electrical, Electronics, and Communication Engineering (EECE) Department, Indian Institute of Technology Dharwad, India. His research interests include 6G wireless communication networks, optimization theory and algorithms in wireless communication, machine learning, deep learning, and game theory applications in wireless communication.

**RAHUL JASHVANTBHAI PANDYA** (Senior Member, IEEE) received the M.Tech. degree from the Electrical Engineering Department, Indian Institute of Technology (IIT) Delhi, New Delhi, in 2010, and the Ph.D. degree from the Bharti School of Telecommunication, IIT Delhi, in 2014. He was a Senior Network Design Engineer in optical networking industry with Infinera Pvt. Ltd., Bengaluru, from 2014 to 2018. Later, from 2018 to 2020, he was an Assistant Professor with the ECE Department, National Institute of Technology, Warangal. Currently, he is with the Electrical, Electronics, and Communication Engineering (EECE) Department, IIT Dharwad. His research interests include wireless communication, optical communication, optical networks, computer networks, machine learning, and artificial intelligence. He is also working on multiple projects, such as SERB, SPARC, SGNF, and RSM.

**VIMAL BHATIA** (Senior Member, IEEE) received the Ph.D. degree from the Institute for Digital Communications, The University of Edinburgh, Edinburgh, U.K., in 2005. He is currently a Professor with the Indian Institute of Technology (IIT) Indore, India, and an Adjunct Faculty Member of IIT Delhi and IIIT Delhi, India. During the Ph.D. degree, he also received the IEE Fellowship for collaborative research with the Department of Systems and Computer Engineering, Carleton University, Canada. He is also a Young Faculty Research Fellow from MeitY, Government of India. He was a recipient of the Prof SVC Aiya Memorial Award, in 2019. He has worked with various IT companies for over 11 years, both in India and the U.K. He is also a PI/Co-PI/Coordinator for external projects with funding of over USD 20 million from MeitY, DST, UKIERI, MoE, AKA, IUSSTF, and KPMG. He has more than 350 peer-reviewed publications and has filed 13 patents (with five granted). He has supervised 18 awarded Ph.D. thesis and two Ph.D. thesis submitted. His research interests include communications, non-Gaussian non-parametric signal processing, and machine/deep learning with applications to communications and photonics. He is an IEEE, Elsevier, Wiley, Springer, and IET reviewer. He is a fellow of IETE and OSI and a certified SCRUM Master. He was also the General Co-Chair of IEEE ANTS 2018 and the General Vice-Chair of IEEE ANTS 2017. He has served as the Founder and the Head for the Center for Innovation and Entrepreneurship, the Associate Dean of Research and Development, and the Dean of Academic Affairs. He has delivered many talks and tutorials, conducted faculty development programs for the World Bank's NPIU TEQIP-III, and was invited to talk at WWRF46-Paris. He is also an Associate Editor of *IETE Technical Review*, *Frontiers in Communications and Networks*, *Frontiers in Signal Processing*, and IEEE Wireless Communications Letters. He is also a DRISHTI CPS Chair Professor with IIT Indore. He is a current member of Steering Committee of IEEE ANTS. He has been mentioned among the world's top 2% scientists by Stanford University.



**ONEL ALCARAZ LOPEZ** (Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering from the Central University of Las Villas, Cuba, in 2013, the M.Sc. degree in electrical engineering from the Federal University of Paraná, Brazil, in 2017, and the D.Sc. degree (Hons.) in electrical engineering from the University of Oulu, Finland, in 2020. He is the coauthor of the book titled "Wireless RF Energy Transfer in the Massive IoT Era: Toward Sustainable Zero-Energy Networks" (Wiley, December 2021). He is currently a Collaborator to the 2016 Research Award given by the Cuban Academy of Sciences, a co-recipient of the 2019 and 2023 IEEE EuCNC Best Student Paper Award, and the recipient of the 2020 Best Doctoral Thesis Award granted by Finland TEK and TFiF, in 2021. He also holds an Assistant Professorship (tenure track) in sustainable wireless communications engineering with the Centre for Wireless Communications (CWC), Oulu, Finland. His research interests include wireless communications, signal processing, the sustainable IoT, and wireless RF energy transfer.